

Privatnost podataka i upotreba veštačke inteligencije u osnovnom obrazovanju u Srbiji: svest učenika i podrška odraslih

Milena Škobo¹ 

Filološki fakultet, Univerzitet Sinergija, Bijeljina, Bosna i Hercegovina

Milena Šović 

Fakultet za ekonomiju i inženjerski menadžment,
Univerzitet Privredna akademija u Novom Sadu, Novi Sad, Srbija

Apstrakt

Sve učestalija primena alata zasnovanih na veštačkoj inteligenciji (VI) u obrazovanju otvara važna pitanja u vezi sa zaštitom privatnosti podataka učenika, naročito najmlađih korisnika. Ova studija ispituje u kojoj meri učenici osnovnih škola u Srbiji razumeju principe zaštite podataka u kontekstu obrazovnih platformi koje koriste VI. Posebna pažnja posvećena je odnosu između svesti učenika o rizicima po privatnost, posredovanju odraslih – nastavnika i roditelja – kao i tome da li češća upotreba VI korelira sa smanjenim nadzorom odraslih. Strukturirani upitnik primenjen je na uzorku od 240 učenika od petog do osmog razreda. Na osnovu Likertove skale su formirane kompozitne varijable, a podaci su analizirani primenom neparametarskih statističkih metoda, uključujući Spirmanov koeficijent korelacije i Vilkoksonov test znakova. Rezultati ukazuju na to da komunikacija sa odraslima ima ograničen uticaj na razumevanje privatnosti kod učenika, pri čemu se roditeljska podrška pokazala uticajnijom od nastavničke. Rezultati ukazuju na hitnu potrebu za programima digitalne pismenosti koji su prilagođeni uzrastu, institucionalnom odgovornosti i ciljanim vidovima podrške, kako za nastavnike tako i za roditelje, budući da učenici često ne poseduju konkretno razumevanje apstraktnih pojmova privatnosti, te da zahtevaju strukturisanu podršku prilagođenu njihovom razvoju, a koja bi omogućila bezbedno korišćenje tehnologija zasnovanih na VI.

Ključne reči:

veštačka inteligencija u obrazovanju; privatnost podataka učenika; učenici osnovne škole; posredovanje odraslih; digitalna pismenost.

¹ mskobo@sinergija.edu.ba

Uvod

Prisustvo veštačke inteligencije (VI) u obrazovanju ne menja samo način na koji učenici uče, već i način na koji se oni prate i njihovo znanje procenjuje. Određeni alati, kao što su platforme za adaptivno učenje i sistemi za automatsko davanje povratnih informacija, danas rutinski prikupljaju i analiziraju detaljne podatke o ponašanju i postignućima učenika. Ova promena otvorila je ozbiljna pitanja o obimu prikupljanja podataka, nedostatku transparentnosti u vezi sa načinom njihove upotrebe, kao i o izostanku informisanog pristanka (Lupton & Williamson, 2017; Williamson, 2017). U mnogim slučajevima učenici nisu svesni da se njihove digitalne aktivnosti – kliktanje, davanje odgovora i vreme provedeno na zadacima – beleže i dele, ponekad i sa eksternim pružaocima usluga koji deluju van nadzora škole (Williamson, 2019).

Regulatorna tela i međunarodne organizacije počele su da donose konkretne smernice usmerene na zaštitu ljudskog dostojanstva i prava dece u kontekstu razvoja veštačke inteligencije. Na primer, kineska „Etička pravila za veštačku inteligenciju nove generacije“ (2021) naglašavaju da razvoj VI mora doprinositi dobrobiti čoveka (Huang, 2023, str. 2578). Slično tome, Uneskova *Preporuka o etici veštačke inteligencije* (2022) poziva na zaštitu ljudskih prava, slobode, dostojanstva i autonomije. Oba dokumenta ističu da se lični podaci nikada ne smeju prikupljati bez informisanog pristanka, te zagaravaju jasna pravila o tome kako se podaci o deci prikupljaju, čuvaju i koriste – naročito u školskom okruženju.

Kako škole počinju da koriste sve veći broj tehnologija zasnovanih na algoritmiima, učenici se često predstavljaju kroz svojevrsne podatkovne profile, koji utiču na način na koji se podučavaju i ocenjuju (Williamson, 2019). Ovi sistemi su retko transparentni, a njihov uticaj na proces učenja otvara važna pitanja o tome ko kontroliše podatke o učenicima i kako se donose odluke. Kao odgovor na to, istraživači ističu da digitalna pismenost mora prevazići osnovne računarske veštine. Ona bi takođe trebalo da pomogne učenicima da razumeju koji se lični podaci prikupljaju, kako se koriste i kakve to posledice ima po njihovo učenje i privatnost (Hillman et al., 2024; Yeşilyurt & Vezne, 2023).

Problem je posebno izražen u osnovnom i srednjem obrazovanju, gde učenici često nemaju razvijene kognitivne i jezičke kapacitete za razumevanje složenih koncepata digitalne privatnosti. Empirijska istraživanja pokazuju da deca imaju poteškoće da razumeju pojmove kao što su „deljenje podataka“, „lični podaci“ ili „praćenje“, osim ako se oni ne objasne na konkretan način, koji je primeren njihovom uzrastu. Iako je upotreba digitalnih platformi među decom u porastu, što potvrđuju i podaci zasnovani na algoritamskim analizama, učenici se retko podučavaju tome kako ovi sistemi funkcionišu, na koji način mogu biti pristrasni i koja prava imaju prilikom njihove upotrebe. Institucionalni mehanizmi zaštite su neujednačeni: istraživanja ukazuju na nedostatak obuke nastavnika u oblasti etike VI i zaštite podataka (CoSN, 2025; Kelly et al., 2023), dok je posredovanje roditelja često nedosledno i uslovljeno nedovoljnom informisanošću (Livingstone & Blum-Ross, 2020).

Ovo istraživanje u svom fokusu ima osnovno obrazovanje u Srbiji, gde su istraživanja o veštačkoj inteligenciji, zaštiti podataka i autonomiji učenika i dalje ograničena. U radu

se ispituje kako deca percipiraju rizike po privatnost, na koji način posredovanje odraslih (nastavnika i roditelja) utiče na to razumevanje i da li učestala upotreba VI smanjuje nivo nadzora. Takođe, rad pruža empirijske dokaze, koji doprinose međunarodnim debatama o digitalnim pravima dece, kao i ulozi škola u stvaranju bezbednih i podsticajnih obrazovnih okruženja posredovanih veštačkom inteligencijom.

Pregled literature

Međunarodna istraživanja dosledno ukazuju na povrede privatnosti, na ograničenu autonomiju učenika i na nedovoljnu regulisanost algoritamskih sistema kao ključne etičke izazove u primeni veštačke inteligencije u obrazovanju (Guo, 2021; Zhao et al., 2021). Ovi sistemi često prikupljaju podatke na netransparentan način i stvaraju neravnotežan odnos moći između korisnika i pružalaca tehnoloških usluga. Kao odgovor na to, istraživači predlažu etičke okvire usmerene na učenika (Hao et al., 2019; Liu et al., 2021), fleksibilnije i proaktivnije regulatorne pristupe (Xue & Zhao, 2019), kao i stroža pravila za upravljanje podacima u školama (Jia & Jiang, 2017). Ono što je zajedničko svim ovim pristupima jeste zahtev da sistemi veštačke inteligencije u obrazovanju funkcionišu transparentno i uz jasnu odgovornost kada je reč o načinu njihovog rada i posledicama njihove primene.

Savremeni razvoj tehnologija za obradu podataka dodatno je otežao jasno razgraničenje između korisnih obrazovnih alata i različitih oblika digitalnog nadzora. Pojedini sistemi veštačke inteligencije danas mogu donositi zaključke o ponašanju, emocionalnim stanjima ili obrascima mišljenja učenika na osnovu njihovih aktivnosti na internetu, čime granica između podrške učenju i nadzora postaje sve manje jasna (Huang, 2023, str. 2582). Regulatornim mehanizmima, poput Opšte uredbe o zaštiti podataka (GDPR) i tzv. „prava na zaborav“ (Hoofnagle et al., 2019; Shi & Zhou, 2022), jeste cilj da pojedincima obezbede veću kontrolu nad načinom korišćenja njihovih ličnih podataka. Druge strategije, kao što je ugrađivanje zaštite privatnosti već u fazi dizajna digitalnih alata (engl. *privacy by design*) (Zhao et al., 2016), nastoje da osiguraju da se o zaštiti podataka vodi računa od samog početka razvoja tehnologije. Institucionalni predlozi, poput Vangovog (Wang, 2016) modela upravljanja podacima na nivou škole, dodatno naglašavaju potrebu usklađivanja tehničkih rešenja sa pravnim i etičkim obavezama.

Empirijska istraživanja pokazuju da mnoga mlađa deca i dalje nemaju dovoljno razvijeno razumevanje digitalne privatnosti. Vang i saradnici (Wang et al., 2019) utvrdili su da deca uzrasta od 6 do 10 godina mogu prepoznati osnovne rizike, kao što je prekomerno deljenje ličnih informacija, ali imaju poteškoća da razumeju apstraktnije probleme, poput načina na koji platforme prate njihovo ponašanje ili predlažu sadržaje. Slično tome, Andriz i Robertson (Andries & Robertson, 2023) pokazali su da učenici osnovnih škola u Škotskoj ne razumeju način na koji funkcionišu sistemi veštačke inteligencije, što ukazuje na potrebu za uvođenjem sadržaja o digitalnim tehnologijama koji su prilagođeni uzrastu već u ranim fazama obrazovanja.

Klasične teorije dečjeg razvoja mogu dodatno objasniti zašto deca imaju poteškoća u razumevanju digitalne privatnosti, kao i koncepta povezanih sa veštačkom intelligen-

cijom. Prema Pijažeu, većina dece u osnovnoj školi nalazi se u fazi konkretnih operacija (najčešće između sedme i jedanaeste godine), tokom koje mogu logički da razmišljaju o konkretnim situacijama, ali i dalje imaju poteškoća sa razumevanjem apstraktnih pojmova. Iako mogu prepoznati očigledne rizike, kao što je deljenje ličnih podataka na internetu, teže razumeju manje vidljive opasnosti, poput praćenja putem aplikacija ili ciljanog prikazivanja sadržaja.

Teorija Zone narednog razvoja (ZNR) Vigotskog dodatno objašnjava kako deca mogu usvajati apstraktne pojmove uz adekvatnu podršku odraslih ili vršnjaka. Vigotski je isticao da je učenje najefikasnije kada dete ima podršku kompetentnijih osoba – nastavnika, roditelja ili vršnjaka – koji kroz zajedničku interakciju, postavljanje pitanja i podsticanje refleksije pomažu u razumevanju složenijih koncepata. U kontekstu veštačke inteligencije i digitalne privatnosti, to znači da deca verovatno neće usvojiti etičke principe niti prepoznati rizike digitalnog nadzora ukoliko im se ti fenomeni jasno ne objasne kroz proces podučavanja koji je u skladu sa njihovim uzrastom i nivoom razumevanja. I Pijaže i Vigotski ukazuju na to da su deci potrebni strukturisana podrška i njima bliski, konkretni primeri kako bi mogla da razumeju digitalne alate i potencijalne rizike koje oni nose.

Gao i saradnici (Gao et al., 2025) sarađivali su sa nastavnicima na zajedničkom osmišljavanju kratkih nastavnih jedinica za decu od vrtićkog uzrasta do učenika osmog razreda. Njihovi rezultati pokazuju da čak i kratke, ali dobro integrisane aktivnosti mogu unaprediti sposobnost dece da prepoznaju pretnje po privatnost i da adekvatno reaguju na njih. Do sličnih zaključaka došli su i Vartiainen i saradnici (Vartiainen et al., 2025), kroz nastavne intervencije zasnovane na upotrebi posebno razvijenih aplikacija, koje su dovele do merljivog napretka u razvoju tzv. podatkovne agencnosti (engl. data agency), odnosno sposobnosti učenika da kritički razumeju podatke. Njihovo istraživanje pokazalo je da su učenici postali svesniji načina na koji algoritmi društvenih mreža utiču na sadržaje koje vide na internetu i, pritom, uzrokuju da takvi sadržaji oblikuju njihovo ponašanje.

Jim i Su (Yim & Su, 2025) ukazuju na to da većina postojećih programa za razvoj pismenosti u oblasti VI previše naglašava tehničke veštine, dok zanemaruje kritičko promišljanje pitanja poput informisanog pristanka, digitalnog nadzora i algoritamske pristranosti. Oni predlažu višedimenzionalni model koji objedinjuje pravne, etičke i tehničke kompetencije. U sistematskom pregledu istraživanja o digitalnom građanstvu kod dece uzrasta od 0 do 8 godina, Li i saradnici (Lee et al., 2025) zaključuju da je ovakav vid obrazovanja i dalje nedovoljno zastupljen, ali da daje pozitivne rezultate kada se integriše u osnovne nastavne predmete kroz strategije učenja zasnovane na igri i saradnji. Njihova studija posebno naglašava značaj ranih i strukturisanih obrazovnih intervencija, koje decu ne posmatraju samo kao pasivne subjekte zaštite, već kao buduće digitalne građane sposobne da razumeju privatnost, pristanak i etičko učešće u digitalnom okruženju.

Mnogi obrazovni programi ne ostvaruju očekivane rezultate, što nije prouzrokovano loše osmišljenim nastavnim planovima, već time što nastavnici nisu u dovoljnoj meri osposobljeni za njihovu primenu. Koristeći validirani okvir *DigCompEdu*, Muamar i saradnici (Muammar et al., 2023) procenjivali su digitalne kompetencije nastavnika u više ključnih oblasti. Njihovi nalazi pokazuju da čak i univerzitetski profesori pokazuju neujednačen

nivo kompetencija u oblastima kao što su zaštita podataka i pedagoška integracija digitalne etike, što ukazuje na hitnu potrebu za sistematskom obukom nastavnika na svim nivoima obrazovanja. Bez adekvatne pripreme, nastavnici mogu da izbegavaju upotrebu digitalnih alata ili da se oslanjaju na restriktivne mere koje ograničavaju aktivno učešće učenika.

Istraživanja takođe pokazuju da se digitalna etika ne može uspešno razvijati kroz izdvojene činjenice ili apstraktna pravila. Umesto toga, potrebno ju je integrisati u svakodnevnu nastavu kroz diskusije koje su prilagođene uzrastu i smislenu interakciju. Kako ističe Ngugen (Nguyen, 2023), kritičko razumevanje zaštite podataka kod dece najefikasnije se razvija kroz razgovor, vršnjačku interakciju i simulacije situacija iz stvarnog života, a ne kroz izolovane nastavne jedinice. Oslanjajući se na konstruktivističke pristupe učenju, Solberg (Solberg, 2023) zagovara model digitalne pismenosti, u kojem učenici i nastavnici zajednički promišljaju realne digitalne situacije – kao što su korišćenje aplikacija, deljenje fotografija ili komunikacija sa četbotovima. Ovakvi pristupi izbegavaju jednosmerno prenošenje znanja i polaze od pretpostavke da su deca sposobna da razumeju etičke dileme. Na taj način deca razvijaju sopstveno razumevanje kroz iskustvo u stvarnom digitalnom okruženju.

Rezultati projekta KOALA (Wang et al. 2019) pokazuju da deca često mogu prepoznati očigledne rizike, kao što je deljenje pravog imena, ali imaju poteškoća sa uočavanjem skrivenijih ili apstraktnijih pretnji, poput praćenja njihovih aktivnosti na internetu ili prikazivanja sadržaja zasnovanih na njihovom ponašanju. Upravo iz tih razloga je važno da obrazovanje o privatnosti u školama prevaziđe pukio nabranje pravila. Učenicima je potrebno pomoći da razumeju kako digitalni alati funkcionišu, kao i kako utiču na njihove izbore i iskustva koja stiču. Šuli i saradnici (Shouli, 2025) iznose sličan stav, naglašavajući da decu treba posmatrati kao aktivne učesnike digitalnog okruženja, a ne samo kao pasivne korisnike. Njihov model predlaže da škole u redovnu nastavu uključe sadržaje o pravima u vezi sa podacima, načinu donošenja odluka putem algoritama i značenju informisanog pristanka.

U Srbiji i dalje postoji veoma malo istraživanja i javnih politika koje se bave načinom na koji deca koriste veštačku inteligenciju, kao i pitanjem kako se njihovi podaci upotrebljavaju u obrazovnom kontekstu. Postojeći zakonski okvir – poput Zakona o zaštiti podataka o ličnosti (2019), Zakona o socijalnoj zaštiti (2011) i Zakona o maloletnim učiniocima krivičnih dela i krivičnopravnoj zaštiti maloletnih lica (2005) – ne prepoznaje specifične rizike koje sistemi veštačke inteligencije donose u školskom okruženju. Ni Nacrt zakona o pravima deteta, koji je u pripremi, ne sadrži odredbe koje se odnose na digitalna prava, etiku podataka ili uticaj algoritamskih sistema na obrazovni proces.

Strateški dokumenti, poput Strategije razvoja veštačke inteligencije Republike Srbije (2020–2025) i Etičkih smernica za razvoj, primenu i upotrebu pouzdane i odgovorne veštačke inteligencije (2022), prepoznaju opšte rizike, poput zloupotrebe podataka, ali ne predviđaju posebne mehanizme zaštite dece. Osnivanje Instituta za veštačku inteligenciju Srbije predstavlja pozitivan institucionalni korak, ali se ova institucija do sada nije sistematski bavila etičkim pitanjima primene veštačke inteligencije u nastavi, niti njenim uticajem na decu (Danaj et al., 2024).

Ignjatovićeva (Ignjatović, 2024) ukazuje da primena zakona o zaštiti podataka o ličnosti u školskom kontekstu ostaje neujednačena i u velikoj meri nedovoljno regulisana uprkos njenoj formalnoj usklađenosti sa GDPR regulativom, što je naročito slučaj kada se alati VI koriste za svrhe kao što su biometrijska identifikacija ili praćenje ponašanja. Etičke smernice imaju savetodavni karakter i ne sadrže konkretne odredbe koje bi se odnosile na prava deteta. Takođe, ne postoji jasno određeno regulatorno telo nadležno za nadzor nad primenom sistema VI u obrazovanju, što školama ostavlja nedovoljno definisane mehanizme kontrole i odgovornosti. Takvo stanje povećava rizik od zloupotrebe podataka o deci, kao i mogućnost da budu izložena digitalnom nadzoru bez svog znanja. Danajeva i saradnice (Danaj et al., 2024) dodatno upozoravaju da nedostatak empirijskih istraživanja u ovoj oblasti otežava razvoj konkretnih i kontekstualno utemeljenih rešenja. Nastavnicima i donosiocima odluka je otežano da osmisle efikasne mehanizme zaštite ukoliko im takvi podaci nisu na raspolaganju.

Iako roditeljsko posredovanje ima ključnu ulogu u oblikovanju digitalnog ponašanja dece, ono se suočava i sa jasnim strukturnim ograničenjima. Najnoviji nalazi istraživanja koje su sprovedli Matovićeva i Žunić-Pavlovićeva (Matović i Žunić-Pavlović, 2020) pokazuju da se mnogi roditelji pretežno oslanjaju na restriktivne pristupe – poput ograničavanja vremena provedenog pred ekranom ili zahteva za pristup lozinkama svoje dece – umesto na razvoj otvorene komunikacije i dugoročne digitalne pismenosti. Iako ovakve strategije proizlaze iz namere da se deca zaštite, one su uglavnom reaktivnog karaktera umesto preventivnog i ne doprinose dovoljno razvoju dugoročne digitalne otpornosti. U medijskom intervjuu, Kuzmanovićeva naglašava da digitalna prava dece – kao što su pravo na privatnost, učešće i pristup sadržajima primerenim uzrastu – moraju biti u potpunosti priznata u digitalnom okruženju, a ne samo uređena kroz zabrane i ograničenja. Ona ističe da bi institucionalna odgovornost, a ne prekomerna roditeljska kontrola, trebalo da bude osnova za oblikovanje bezbednog digitalnog prostora (Andrić, 2025).

Nešićeva (Nešić, 2023) u svojoj analizi obrazovnih politika ukazuje da, iako je roditeljski dijalog važan mehanizam zaštite, mnoga deca izbegavaju da prijave rizična ili osetljiva iskustva sa interneta. Autorka ističe da otvorena komunikacija ostaje neophodna, ali da je treba dopuniti konkretnim merama, koje uključuju povremenu proveru istorije pretrage, upotrebu filtera na uređajima i alate za roditeljski nadzor. Međutim, efikasna primena ovih mera zahteva viši nivo digitalne pismenosti roditelja, kao i sistemsku podršku institucija. Iako restriktivni oblici roditeljskog nadzora i dalje dominiraju, oni mogu dovesti i do narušavanja digitalnih prava dece. Kuzmanovićeva upozorava da čak i postupci sa dobrim namerama, kao što je objavljivanje fotografija dece na internetu (engl. *sharenting*), mogu predstavljati povredu dečje privatnosti, te zagovara sveobuhvatno digitalno opismenjavanje i dece i odraslih (Andrić, 2025). Osim navedenog, institucionalna saradnja između roditelja i škola, kakvu predlažu Li i saradnici (Li et al., 2025) i Gao i saradnici (Gao et al., 2025), može ponuditi alternativni pristup, zasnovan na partnerstvu i podeljenoj odgovornosti, umesto prebacivanja celokupnog tereta na roditelje.

Ovo istraživanje nastoji da odgovori na nedostatak empirijskih podataka u Srbiji analizom načina na koji učenici osnovnih škola razumeju zaštitu podataka o ličnosti, kao i uticaja podrške odraslih na interakciju učenika sa obrazovnim alatima zasnovanim na veštačkoj inteligenciji.

Metodologija istraživanja

U cilju prevazilaženja nedostatka empirijskih istraživanja u ovoj oblasti, u radu je primenjeno kvantitativno istraživanje poprečnog tipa, da bi se ispitali načini na koje učenici osnovnih škola u Srbiji percipiraju i upravljaju zaštitom podataka o ličnosti, u kontekstu obrazovnih tehnologija zasnovanih na veštačkoj inteligenciji. Istraživanje se posebno usredsređuje na odnose između upoznatosti učenika sa sistemima VI, njihovog nivoa svesti o zaštiti podataka, kao i posredničke uloge podrške odraslih – pre svega, nastavnika i roditelja. Studija je vođena sledećim istraživačkim pitanjima:

1. U kojoj meri su učenici osnovnih škola upoznati sa pitanjima privatnosti i zaštite podataka u kontekstu korišćenja alata VI i aplikacija?
2. Na koji način komunikacija sa nastavnicima i roditeljima utiče na razumevanje zaštite podataka kod učenika u okruženju posredovanom veštačkom inteligencijom?
3. Da li postoji razlika u nivou podrške i nadzora koji pružaju roditelji u odnosu na nastavnike kada je reč o korišćenju aplikacija VI od strane učenika?
4. Da li je učestalost korišćenja aplikacija VI povezana sa nivoom roditeljskog nadzora u kućnom okruženju?

Uzorak

Istraživanje je sprovedeno na uzorku od 240 učenika osnovnih škola u Srbiji, od petog do osmog razreda. Raspodela po razredima bila je gotovo ujednačena: 25,0% učenika pohađalo je peti razred, 25,0% šesti, 25,4% sedmi, a 24,6% osmi razred. Prema polnoj strukturi, 53,3% ispitanika činili su dečaci, dok su 46,7% činile devojčice. Učenici su uključeni u istraživanje iz škola u urbanim i prigradskim sredinama, primenom prigodnog uzorka.

Prikupljanje podataka

Link ka upitniku distribuiran je putem profesionalnih nastavničkih mreža i grupa na društvenim mrežama. Aktivnost su sa svojim odeljenjima realizovali isključivo nastavnici koji su dobrovoljno iskazali interesovanje za učešće u istraživanju. Prema informacijama koje su dostavili nastavnici, roditelji su usmeno obavешteni na roditeljskim sastancima da će učenici učestvovati u probnoj upotrebi obrazovnog četbota, nakon čega će imati mogućnost da popune dobrovoljan i anoniman upitnik, uz mogućnost da odbiju učešće. Nije bilo prijavljenih primedbi. Svi upitnici popunjeni su u školskom okruženju, uz nadzor nastavnika.

Izjava o etičkom postupanju

Učešće u istraživanju bilo je u potpunosti dobrovoljno, a sadržaj upitnika bio je neutralan i procenjen kao istraživanje minimalnog rizika. Nisu prikupljeni lični podaci (kao

što su imena, podaci o školama ili IP adrese), niti su istraživači imali mogućnost naknadne identifikacije učesnika. Svi učesnici popunjavali su upitnik u školskom okruženju, uz nadzor nastavnika. U skladu sa uvodnom odredbom 26 Opšte uredbe EU o zaštiti podataka (GDPR) i Zakonom o zaštiti podataka o ličnosti Republike Srbije, potpuno anonimizovani podaci se ne smatraju ličnim podacima, te stoga formalna saglasnost roditelja i odobrenje etičkog odbora nisu bili obavezni. Istraživanje je sprovedeno u skladu sa principima Helsinške deklaracije i relevantnim nacionalnim propisima koji se odnose na zaštitu podataka i istraživanja u oblasti obrazovanja.

Hipoteze

Formulisane su sledeće hipoteze:

H1. Učenici koji češće koriste aplikacije VI ređe su pod roditeljskim nadzorom u kućnom okruženju.

H2. Komunikacija sa odraslima doprinosi boljem razumevanju zaštite podataka kod učenika. Učenici koji razgovaraju sa nastavnicima o veštačkoj inteligenciji i digitalnoj bezbednosti pokazaće viši nivo svesti o pitanjima privatnosti (H2.1). Učenici koji o digitalnoj privatnosti razgovaraju sa roditeljima pokazaće viši nivo svesti o zaštiti podataka (H2.2). Učenici koji dobijaju smernice i od roditelja i od nastavnika pokazaće najviši nivo razumevanja zaštite podataka (H2.3).

H3. Institucionalna podrška manje je razvijena u odnosu na porodičnu podršku. Veća je verovatnoća da će učenici dobiti dozvolu roditelja nego dozvolu nastavnika za korišćenje alata VI (H3.1). Učenici češće koriste aplikacije VI pod nadzorom roditelja nego pod nadzorom nastavnika (H3.2). Učenici doživljavaju roditelje kao informisanije od nastavnika kada je reč o bezbednosti alata VI (H3.3).

Istraživački instrument

Primarni instrument za prikupljanje podataka bio je upitnik samoprocene, posebno konstruisan za potrebe ovog istraživanja. Upitnik nije preuzet niti prilagođen iz postojećih validiranih skala, već je razvijen na osnovu pregleda relevantne literature i konsultacija sa stručnjacima iz oblasti obrazovne psihologije i informacionih tehnologija. Upitnik je sadržao 22 zatvorena pitanja merena petostepenom Likertovom skalom (1 uopšte se ne slažem, 5 u potpunosti se slažem) i bio je organizovan u pet tematskih celina: upoznatost i korišćenje aplikacija VI (pitanja 1 – 2), svest o zaštiti podataka (pitanja 3 – 10), iskustvo sa deljenjem podataka i nadzorom (pitanja 11 – 13), uključenost nastavnika i roditelja (pitanja 12 – 19) i motivacija i obrazovne potrebe (pitanja 20 – 22).

Pre glavnog prikupljanja podataka, sprovedena je pilot-studija na uzorku od 38 učenika osnovne škole (od petog do osmog razreda) iz jedne urbane sredine. Cilj pilot-studije bio je da se procene jasnoća pitanja, dužina upitnika i tehnička izvodljivost. Na osnovu povratnih informacija iz pilot faze, izvršene su manje jezičke korekcije u pitanjima 4, 13 i 20 kako bi se poboljšala razumljivost i smanjila mogućnost različitog tumačenja.

Za potrebe testiranja hipoteza i provere konstruktne validnosti formirano je pet kompozitnih (latentnih) varijabli, agregiranjem tematski povezanih pitanja. To su: (1) nivo samostalnosti u korišćenju alata VI, izveden iz pitanja 2 i 17 (uz obrnutu skalu kodiranja); (2) indeks svesti o privatnosti, zasnovan na pitanjima 3, 4 i 7; (3) komunikacija sa odraslima, formirana na osnovu pitanja 15 i 19; (4) indeks podrške nastavnika, formiran na osnovu pitanja 12, 13 i 14; i (5) indeks roditeljske podrške, zasnovan na pitanjima 16, 17 i 18.

Svaka kompozitna varijabla izračunata je kao prosečna vrednost pripadajućih pitanja. Ovi konstrukti korišćeni su za ispitivanje odnosa između varijabli i proveru postavljenih hipoteza. Grupisanje pitanja zasnovano je na teorijskim modelima digitalne pismenosti i posredovanja u oblasti privatnosti kod dece (Stoilova i sar., 2019) i odražava konceptualnu koherentnost posmatranih dimenzija.

Validnost razvijenog instrumenta potvrđena je na tri ključna osnova: (1) teorijskoj utemeljenosti konstrukata, zasnovanoj na relevantnim modelima digitalne pismenosti i posredovanja privatnosti kod dece; (2) zadovoljavajućoj internoj konzistentnosti, potvrđenoj koeficijentima pouzdanosti (Kronbahov $\alpha > .70$) za sve indekse; (3) empirijskoj potvrdi kroz međusobne korelacije kompozitnih varijabli u skladu sa postavljenim hipotezama.

Radi procene interne konzistentnosti ovih konstrukata, Kronbahov alfa koeficijent izračunat je na osnovu podataka celokupnog uzorka ($n = 240$). Rezultati su pokazali zadovoljavajući nivo pouzdanosti za svih pet indeksa: indeks samostalnosti u korišćenju alata VI imao je vrednost $\alpha = .72$; indeks svesti o privatnosti $\alpha = .81$; komunikacija sa odraslima $\alpha = .76$; indeks podrške nastavnika $\alpha = .79$; dok je indeks roditeljske podrške pokazao najvišu pouzdanost ($\alpha = .83$). Sve vrednosti premašuju uobičajeni prag od .70, što ukazuje na prihvatljivu internu konzistentnost svih konstrukata. Potrebno je napomenuti da procene pouzdanosti za skale sa samo dva pitanja, kao što su „Komunikacija sa odraslima“ i „Nivo samostalnosti u korišćenju alata VI“, treba tumačiti sa oprezom, jer je Kronbahov alfa u takvim slučajevima manje stabilan; ipak, obe skale su imale vrednosti iznad .70 i odražavale su konceptualno koherentne dimenzije (Eisinga i sar., 2013).

Ove kompozitne varijable su potom korišćene za ispitivanje odnosa između ključnih dimenzija istraživanja, kao i za proveru postavljenih hipoteza. Preliminarni dokazi konstruktne validnosti dobijeni su korelacionom analizom između kompozitnih varijabli, koja je pokazala statistički značajne veze u očekivanim smerovima.

Konstruktna validnost kompozitnih varijabli potvrđena je kako teorijskim utemeljenjem tako i empirijskim nalazima zasnovanim na njihovim međusobnim korelacijama. Indeks samostalnosti u korišćenju aplikacija VI bio je statistički značajno negativno povezan sa roditeljskim nadzorom ($\rho = -.189, p < .01$), dok je indeks roditeljske podrške takođe pokazao značajnu negativnu korelaciju sa nivoom svesti učenika o privatnosti ($\rho = -.163, p < .05$). Nasuprot tome, indeks komunikacije sa odraslima nije pokazao statistički značajnu povezanost sa razumevanjem privatnosti kod učenika ($\rho = .052, n.s.$), što ukazuje na tematsku diferenciranost ovih konstrukata. Dodatno, Vilkoksonov test potvrdio je statistički značajne razlike u percepciji podrške roditelja i nastavnika od strane učenika ($Z = -3.397, p < .01$), čime je dodatno potvrđena interna validnost definisanih indeksa.

Iako instrument nije zasnovan na postojećim validiranim skalama, njegova koherentna tematska struktura, jasno definisani indikatori i konzistentni empirijski obrasci pružaju

snažnu osnovu za procenu njegove adekvatnosti u ispitivanju stavova i iskustava učenika u vezi sa korišćenjem alata VI, razumevanjem zaštite podataka i ulogom podrške odraslih.

Analiza podataka

Svi odgovori iz upitnika su numerički kodirani (1 – 5) i agregirani radi formiranja kompozitnih skorova za svaku latentnu varijablu. Distribucija varijabli testirana je na normalnost primenom Kolmogorov–Smirnovljevog i Šapiro–Vilkovog testa. Kako nijedna od varijabli nije pratila normalnu distribuciju, primenjene su neparametrijske statističke metode, uključujući Spirmanov koeficijent rang-korelacije (za ispitivanje povezanosti između varijabli) i Vilkoksonov test rangova za zavisne uzorke (za poređenje povezanih odgovora, posebno u vezi sa indikatorima podrške nastavnika i roditelja).

Rezultati

Spirmanova rho korelacija (Tabela 1) pokazuje statistički značajnu negativnu povezanost između učestalosti korišćenja alata VI i nivoa roditeljskog nadzora u kućnom okruženju ($\rho = -.189, p < .01$), čime je potvrđena hipoteza (H1) da su učenici koji češće koriste alate VI ređe pod roditeljskim nadzorom. Takođe, roditeljski nadzor pokazuje negativnu povezanost sa nivoom svesti o privatnosti ($\rho = -.163, p < .05$), što ukazuje na to da učenici koji su pod većim roditeljskim nadzorom pokazuju niži nivo razumevanja pitanja privatnosti u kontekstu alata VI. Jedno od mogućih objašnjenja jeste da učenici pod strožim roditeljskim nadzorom imaju manje prilika za samostalno istraživanje alata VI i sticanje iskustva u razumevanju pitanja privatnosti. S druge strane, učestalost korišćenja alata VI nije pokazala statistički značajnu povezanost sa nivoom svesti o privatnosti ($\rho = .106$), niti sa nivoom komunikacije sa odraslima ($\rho = .013$), što ukazuje na to da samostalnost u digitalnom okruženju nije direktno povezana sa razumevanjem privatnosti, niti sa učestalošću razgovora sa odraslima o ovim temama. Rezultat da je veća učestalost korišćenja alata VI statistički značajno povezana sa nižim nivoom roditeljskog nadzora potvrđuje postavljenu hipotezu. Na osnovu toga može se zaključiti da je hipoteza H1 u potpunosti potvrđena.

Tabela 1

Povezanost učestalosti korišćenja alata VI, roditeljskog nadzora, svesti o zaštiti podataka i komunikacije sa odraslima (N 240)

Varijabla	Učestalost korišćenja VI	Roditeljski nadzor	Nivo svesti o privatnosti	Nivo komunikacije sa odraslima
Učestalost korišćenja VI	1.000	-.189**	.106	.013
Roditeljski nadzor		1.000	-.163*	.052
Nivo svesti o privatnosti			1.000	.052
Nivo komunikacije sa odraslima				1.000

Napomena. **Korelacija je statistički značajna na nivou .01 (2-tailed). *Korelacija je statistički značajna na nivou .05 (2-tailed).

Uticaj komunikacije učenika sa odraslima na njihovo razumevanje pitanja privatnosti u kontekstu alata VI (H2) ispitano je primenom Spirmanovog koeficijenta rang-korelacije. Kao što je prikazano u Tabeli 2, povezanost između komunikacije sa nastavnicima i svesti o privatnosti bila je slaba i statistički neznačajna ($p = .096$, p n.s.). Komunikacija sa roditeljima pokazala je još slabiju, blago negativnu povezanost ($p = -.010$, p n.s.). Nasuprot tome, ukupna komunikacija sa odraslima bila je snažno povezana i sa komunikacijom sa nastavnicima ($p = .739$, $p < .01$) i sa komunikacijom sa roditeljima ($p = .735$, $p < .01$), što ukazuje na to da učenici koji češće razgovaraju sa jednom grupom odraslih uglavnom češće komuniciraju i sa drugom. Međutim, ova ukupna komunikacija nije bila povezana sa značajnim porastom svesti o privatnosti, što sugerise da takve interakcije, čak i kada su učestale, verovatno ne obuhvataju pitanja zaštite podataka na dovoljno smislen ili strukturisan način.

U vezi sa hipotezom H2.1, utvrđena je slaba i statistički neznačajna povezanost između komunikacije sa nastavnicima i svesti o privatnosti ($p = .096$, p n.s.). Ovaj rezultat pokazuje da razgovori između nastavnika i učenika imaju ograničen uticaj na razumevanje digitalne privatnosti. Neka od mogućih objašnjenja jesu da teme vezane za privatnost nisu dovoljno zastupljene u nastavnim programima ili da nastavnici nemaju dovoljno obuke za njihovu efikasnu obradu.

U vezi sa hipotezom H2.2, povezanost između komunikacije sa roditeljima i svesti o privatnosti bila je izuzetno slaba i blago negativna ($p = -.010$, p n.s.), što ukazuje na odsustvo značajne veze. Ovaj rezultat može ukazivati na to da učenici ili ne dobijaju relevantne informacije od roditelja ili takve razgovore ne doživljavaju kao primenljive na sopstveno korišćenje alata VI. Jedno od mogućih objašnjenja jeste i nedovoljna informisanost roditelja o pitanjima privatnosti u kontekstu veštačke inteligencije, što može ograničiti kvalitet i obuhvat informacija koje prenose deci.

Hipoteza H2.3 ispitivala je da li je ukupna komunikacija sa odraslima (kombinovana komunikacija sa roditeljima i nastavnicima) snažniji prediktor razumevanja privatnosti. Iako su utvrđene snažne povezanosti između opšte komunikacije sa odraslima i komunikacije sa nastavnicima ($p = .739$) i roditeljima ($p = .735$, $p < .01$), direktna povezanost između ukupne komunikacije i svesti o privatnosti ostala je slaba i statistički neznačajna ($p = .052$, p n.s.). Ovaj rezultat sugerise da, iako učenici razgovaraju i sa roditeljima i sa nastavnicima, ti razgovori verovatno češće obuhvataju opšta pitanja korišćenja tehnologije, a ređe konkretne teme koje se odnose na zaštitu podataka i privatnost.

Rezultati ukazuju da komunikacija sa nastavnicima i roditeljima nema značajan uticaj na nivo svesti učenika o zaštiti podataka. Iako postoji snažna i statistički značajna povezanost između komunikacije sa nastavnicima i roditeljima ($p = .739$ i $p = .735$, $p < .01$), takve interakcije se ne odražavaju na viši nivo razumevanja privatnosti kod učenika.

Hipoteze H2.1 i H2.2 nisu potvrđene, jer ni komunikacija sa nastavnicima ni komunikacija sa roditeljima ne pokazuju statistički značajan uticaj na svest o privatnosti. Hipoteza H2.3 je samo delimično potvrđena: iako je ukupna komunikacija sa odraslima snažno povezana sa njenim pojedinačnim komponentama, ona ne predstavlja značajan prediktor razumevanja privatnosti kod učenika. Ovi rezultati ukazuju na mogućnost da učenici najveći deo znanja o zaštiti podataka stiču kroz lično iskustvo, a ne kroz razgovore sa odraslima. U skladu s tim, opšta hipoteza H2 nije potvrđena. Ovakvi rezultati ukazuju na potrebu za jasnijim i sistematičnijim obrazovanjem o zaštiti podataka, kako u školskom, tako i u porodičnom okruženju.

Tabela 2

Povezanost nivoa svesti o privatnosti, komunikacije sa nastavnicima, roditeljima i ukupnog nivoa komunikacije sa odraslima (N 240)

Varijabla	Nivo svesti o privatnosti	Komunikacija sa nastavnicima	Komunikacija sa roditeljima	Nivo komunikacije sa odraslima
Nivo svesti o privatnosti	1.000	.096	-.010	.052
Komunikacija sa nastavnicima		1.000	.106	.739**
Komunikacija sa roditeljima			1.000	.735**
Nivo komunikacije sa odraslima				1.000

Napomena. **Korelacija je statistički značajna na nivou 0,01 (2-tailed).

Rezultati Vilkoksonovog testa rangova za zavisne uzorke (Tabela 3) podržavaju hipotezu H3 i ukazuju na to da učenici percipiraju roditeljsku podršku u korišćenju alata VI kao razvijeniju u odnosu na podršku nastavnika. Hipoteza H3.1 je potvrđena: učenici navode da roditelji češće daju dozvolu za korišćenje alata VI nego nastavnici ($Z = -2,579, p < .05$). Hipoteza H3.2 nije potvrđena: nije utvrđena statistički značajna razlika u nivou nadzora nad korišćenjem alata VI između roditelja i nastavnika ($Z = -1,072, p = .284$), što ukazuje na uporediv nivo nadzora u školskom i porodičnom okruženju. Hipoteza H3.3 je potvrđena: učenici percipiraju roditelje kao informisanije o bezbednosti podataka u odnosu na nastavnike ($Z = -1,901, p < .05$). Takođe, utvrđena je snažna i statistički značajna razlika u ukupnom nivou podrške u korist roditelja ($Z = -3,397, p < .01$). Ovi rezultati potvrđuju da je roditeljska podrška generalno razvijenija od školske podrške u usmeravanju učenika u korišćenju alata VI, čime je hipoteza H3 u celini potvrđena.

Rezultati ukazuju da roditelji imaju ključnu ulogu u pružanju podrške učenicima u korišćenju alata VI, dok je uticaj nastavnika ograničen, što se može dovesti u vezu sa nedovoljnom prilagođenošću nastavnih programa i pristupa ovoj temi.

Tabela 3

Rezultati Vilkoksonovog testa rangova za zavisne uzorke za podršku nastavnika i roditelja u korišćenju alata VI i aplikacija (N 240)

Podrška nastavnika i roditelja	Dozvola nastavnika u školi – roditelja kod kuće za korišćenje alata VI i aplikacija	Korišćenje alata VI samo uz nadzor nastavnika u školi – roditeljski nadzor kod kuće	Informisanost nastavnika – roditelja o bezbednosti podataka u alatima VI i aplikacijama	Nivo podrške nastavnika – nivo podrške roditelja
Z	-2.579	-1.072	-1.901	-3.397
Asymp. Sig. (2-tailed)	.010	.284	.039	.001

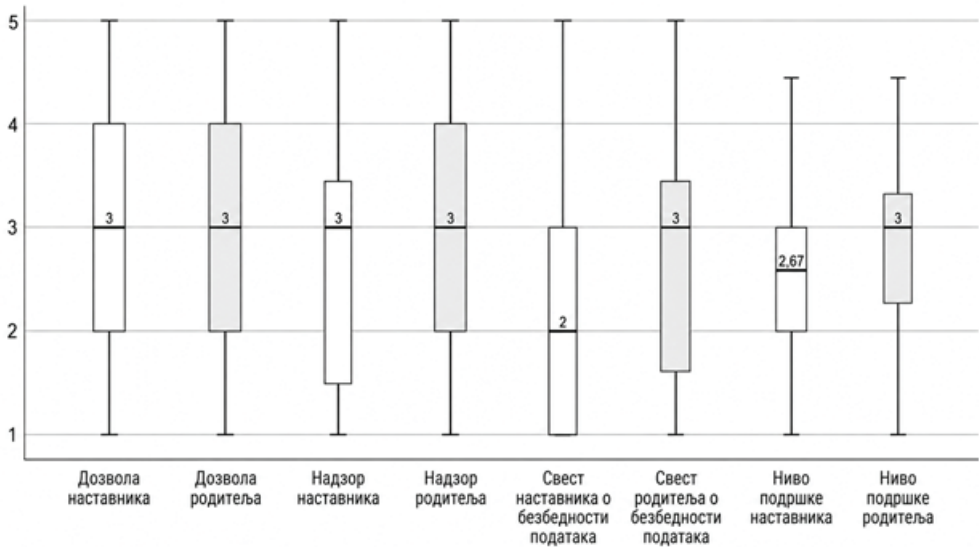
Napomena: Negativna Z-vrednost ukazuje na to da su sve vrednosti koje se odnose na roditelje više u odnosu na odgovarajuće vrednosti koje se odnose na nastavnike.

Grafikon 1 vizuelno potvrđuje prethodne nalaze, koji ukazuju da roditelji pružaju viši nivo podrške učenicima u gotovo svim aspektima korišćenja alata VI, uključujući davanje dozvole za njihovu upotrebu, nadzor nad korišćenjem alata VI, kao i nivo informisanosti o bezbednosti podataka. Prikazani rezultati pokazuju da su medijalne vrednosti podrške nastavnika niže u svim kategorijama, osim u segmentu nadzora, gde razlika nije statistički značajna. Posebno se izdvaja razlika u proceni informisanosti o bezbednosti podataka, gde učenici smatraju da su roditelji bolje upoznati sa pitanjima zaštite privatnosti od nastavnika. Najveća razlika uočava se u ukupnom nivou podrške, gde je roditeljska podrška izraženija u odnosu na podršku nastavnika (medijana 3 naspram 2,67).

Ovi rezultati potvrđuju da se učenici u većoj meri oslanjaju na podršku roditelja nego na podršku nastavnika prilikom korišćenja alata VI i aplikacija, što ukazuje na potrebu za snažnijim obrazovnim inicijativama i sistemskom podrškom u okviru školskog sistema.

Grafikon 1

Poređenje podrške nastavnika i roditelja u korišćenju alata VI



Diskusija

Rezultati ovog istraživanja pokazuju da posredovanje odraslih – bilo da je reč o roditeljima ili nastavnicima – ima samo ograničenu povezanost sa razumevanjem zaštite podataka kod učenika osnovnih škola. Uključenost roditelja pokazala je nešto jaču povezanost u odnosu na angažovanje nastavnika, ali su oba efekta bila slaba (npr. povezanost između roditeljskog nadzora i svesti o privatnosti ($p = -.163$, $p < .05$). Ovaj rezultat dovodi u pitanje uvreženo mišljenje da je samo prisustvo odraslih, bez odgovarajuće obuke ili institucionalne podrške, dovoljno da osigura bezbedne digitalne prakse.

Podrška odraslih u ovom kontekstu deluje ograničeno i po svom obliku i po sadržaju. Kako ističu Matovićeva i Žunić-Pavlovićeva (Matović i Žunić-Pavlović, 2020), mnogi roditelji u Srbiji oslanjaju se na restriktivne mere umesto na podsticanje otvorenog dijaloga. Takve strategije mogu razviti zavisnost umesto samostalnosti, što čini učenike nedovoljno pripremljenim za suočavanje sa rizicima po privatnost u radu sa alatima zasnovanim na veštačkoj inteligenciji. Naši rezultati takođe potvrđuju zapažanje Nešićeve (Nešić, 2023) da verbalna komunikacija, ukoliko nije praćena konkretnim alatima ili jasnim primerima, retko pomaže deci da prepoznaju i procene digitalne rizike. Čak i kada odrasli pokušavaju da intervenišu, objašnjenja su često apstraktna, primeri isuviše opšti, a efekti ograničeni.

Istovremeno, statistički značajna povezanost između roditeljskog nadzora i svesti o privatnosti mora se tumačiti sa oprezom. Podaci ukazuju na postojanje veze, ali ne i na njen smer. Jedno moguće objašnjenje jeste da restriktivne roditeljske strategije mogu ograničiti razvoj kritičkog promišljanja privatnosti kod dece, podstičući zavisnost umesto autonomije. Međutim, podjednako je moguće i da učenici koji već poseduju viši nivo svesti o zaštiti podataka teže većoj samostalnosti, pa su stoga manje izloženi roditeljskom nadzoru. Treći mogući faktor – kao što su digitalna pismenost roditelja ili njihov socioekonomski status – može istovremeno uticati i na roditeljski pristup i na razumevanje kod deteta. Za razjašnjenje ovih odnosa potrebna su longitudinalna istraživanja ili istraživanja zasnovana na kombinovanju kvantitativnih i kvalitativnih metoda.

Uprkos svojoj formalnoj obrazovnoj ulozi, nastavnici su pokazali ograničen uticaj na razvoj svesti učenika o zaštiti privatnosti. Ovaj rezultat je u skladu sa činjenicom da u Srbiji nedostaje obuka i alata koji bi nastavnicima omogućili da se sistematski bave pitanjima privatnosti i etike veštačke inteligencije u nastavi (Danaj et al., 2024; Ignjatović, 2024). Kako ističu Škobo i Šovićeva (Škobo i Šović, 2025), spremnost nastavnika da primene alate VI uslovljena je ne samo nedostatkom resursa već i kašnjenjem u razvoju obrazovnih politika, infrastrukturnim ograničenjima i slabom institucionalnom podrškom. Učenici koji su izloženi alatima VI u škola retko mogu da objasne na koji način se njihovi podaci mogu koristiti, što pokazuje da je njihova integracija u nastavu i dalje površna i nedovoljno razvijena sa etičkog stanovišta.

Ovi rezultati se delimično mogu objasniti i razvojnim karakteristikama učenika. Prema Pijaževom modelu kognitivnog razvoja, učenici uzrasta od 11 do 14 godina tek počinju da razvijaju sposobnost apstraktnog mišljenja (McLeod, 2009). Naši rezultati potvrđuju da učenici često daju formalno tačne odgovore, ali bez dubljeg razumevanja sadržaja. Ukoliko podrška odraslih nije usklađena sa razvojnim nivoom dece – bilo kroz upotrebu jednostavnog jezika, vizualnih prikaza ili primera iz svakodnevnog života, kako sugerise teorija Zona narednog razvoja Vigotskog – učenje verovatno neće imati stvarni obrazovni efekat. Učenici mogu popunjavati upitnike koji sadrže tehničke ili pravne termine, a da pritom ne razumeju u potpunosti njihovo značenje, što dodatno ukazuje na potrebu za obrazovnim materijalima koji su prilagođeni uzrastu i jasno strukturirani.

Rešavanje ovog problema zahteva promene kako na nivou porodice tako i na nivou škole. Povremeni časovi ili opšti razgovori o ovim temama nisu dovoljni za razvoj trajne podatkovne i digitalne pismenosti. Škole bi trebalo da pitanja privatnosti i digitalne etike integrišu u svakodnevnu nastavu. Na primer, apstraktne teme poput pristanka ili deljenja podataka mogu se približiti učenicima kroz aktivnosti kao što su simulacije digitalnih dilema (igre uloga), razgovori o svakodnevnim situacijama korišćenja alata VI ili praktični pri-

kazi podešavanja privatnosti u alatima koje učenici već koriste. Nastavnicima je potrebna obuka za osmišljavanje nastavnih aktivnosti koje ove teme čine razumljivim, relevantnim i prilagođenim uzrastu učenika. Takođe, potrebna im je podrška u vidu gotovih nastavnih materijala, primera scenarija i mogućnosti razmene materijala kroz školske mreže ili profesionalne onlajn zajednice.

Roditelji takođe imaju ključnu ulogu, ali često nemaju dovoljno sigurnosti ili znanja da pruže konstruktivnu podršku. Potrebna im je sistemska podrška škola, donosilaca obrazovnih politika i digitalnih platformi. Škole mogu ponuditi ilustrovane vodiče, kratke edukativne video-materijale, kao i predloge tema za razgovor koje bi pomogle porodicama da sa decom razgovaraju o pitanjima poput dozvola aplikacija, digitalnog pristanka ili rizika prekomernog deljenja ličnih informacija. Aktivnosti u porodičnom okruženju mogu uključivati zajedničko pregledanje podešavanja aplikacija, kreiranje porodičnih pravila o korišćenju digitalnih uređaja ili gledanje i razgovor o kratkim edukativnim sadržajima o bezbednosti na internetu. Takođe, škole bi mogle da deo roditeljskih sastanaka posvete praktičnim primerima kako voditi ovakve razgovore sa decom na konstruktivan način.

Ovo istraživanje ima nekoliko ograničenja. Prvo, uzorak je obuhvatio učenike iz ograničenog broja škola u urbanim i prigradskim sredinama u Srbiji, te se rezultati ne mogu u potpunosti generalizovati na ruralna ili etnički raznovrsnija okruženja, gde se pristup tehnologiji i podrška odraslih u vezi sa korišćenjem alata VI mogu razlikovati. Drugo, rezultati se zasnivaju na samoproceni učenika; iako su odgovori bili anonimni, moglo je doći do toga da mlađi ispitanici pogrešno razumeju pojedina pitanja, daju društveno poželjne odgovore ili imaju poteškoće da adekvatno izraze svoja iskustva. Treće, s obzirom na to da podaci nisu prikupljeni tokom dužeg vremenskog perioda, oni ne omogućuju uvid u to kako se razumevanje privatnosti kod dece menja tokom vremena ili sa učestalijom upotrebom alata VI. Na kraju, iako je upitnik pažljivo konstruisan i pokazao zadovoljavajuću internu konzistentnost, nije zasnovan na postojećim međunarodno validiranim skalama. Ovakav pristup bio je uslovljen potrebom za prilagođavanjem lokalnom kontekstu i jeziku, ali istovremeno ograničava mogućnost poređenja rezultata sa istraživanjima iz drugih zemalja.

Buduća istraživanja bi trebalo da koriste longitudinalne ili kombinovane (kvantitativno-kvalitativne) istraživačke pristupe kako bi se pratio razvoj stavova dece o privatnosti tokom vremena i ispitalo kako kontinuirana podrška odraslih utiče na taj proces. Kvalitativne metode, poput intervju a ili fokus grupa sa decom, mogle bi pružiti dublji uvid u to kako učenici razumeju savete odraslih i koje vrste smernica smatraju smislenim i primenljivim. Takođe bi bilo korisno ispitati efikasnost novih nastavnih materijala posebno osmišljenih za ovaj uzrast – poput kratkih animiranih video-materijala, jednostavnih interaktivnih igara ili ilustrovanih vodiča koji pojmove kao što su pristanak ili deljenje podataka objašnjavaju kroz svakodnevne situacije. Na primer, nastavnici bi mogli da koriste priče ili igre uloga za uvođenje pojmova kao što su digitalni tragovi ili bezbednost na internetu. Ove teme se mogu povezati sa svakodnevним nastavnim sadržajima kroz poznate likove ili situacije bliske učenicima – na primer kroz priču o animiranom liku koji nenamerno podeli previše informacija na internetu – umesto kroz apstraktne pravne formulacije. S tim u vezi, trebalo bi posebno podsticati saradnju između škole i porodice, koja se zasniva na prevođenju apstraktnih pojmova na primere koji su deci razumljivi i koji se svakodnevno koriste u govoru. Ukoliko se ovakav pristup dosledno razvija, on može doprineti poveziva-

nju digitalne pismenosti sa razvojem kritičkog mišljenja, odgovornog ponašanja u digitalnom okruženju i ranih oblika građanske svesti.

Zaključak

Rezultati ovog istraživanja potvrđuju da se bezbedna i smisleno osmišljena primena veštačke inteligencije u osnovnom obrazovanju ne može zasnivati na povremenim nastavnim aktivnostima i kratkoročnim inicijativama. Neophodan je dugoročniji i sistemski pristup, koji podrazumeva promišljene izmene nastavnih programa, konkretnu podršku nastavnicima i stvarnu saradnju sa porodicama. Iako mnogi učenici razgovaraju sa odraslima o digitalnim alatima i rizicima, takvi razgovori su često površni ili nedovoljno dosledni da bi kod njih razvili sigurnost u snalaženju u složenim pitanjima, posebno kada je reč o zaštiti podataka. Digitalna pismenost mora biti integrisana u redovni nastavni proces, a ne da se tretira kao izdvojena tema ili ograniči isključivo na nastavu informatike. Nastavni materijali moraju biti prilagođeni njihovom uzrastu učenika, njihovom jezičkom nivou i kognitivnom razvoju, naročito u slučaju mlađih učenika.

Na institucionalnom nivou, školama je potrebno više od tehničkih smernica. Nastavnici treba da imaju jasna i primenljiva uputstva za odgovoran izbor alata VI i bezbedno upravljanje podacima učenika. Istovremeno, škole bi trebalo da razvijaju zajedničko razumevanje odgovornog digitalnog ponašanja, kao i da takve vrednosti učine vidljivim u svakodnevnoj nastavnoj praksi, a ne samo na nivou formalnih dokumenata.

Uspešna integracija VI u obrazovanje podrazumeva i posmatranje dece kao aktivnih učesnika procesa učenja. Učenike treba podsticati da postavljaju pitanja, iznose svoje nedoumice i kritički promišljaju sopstveno digitalno ponašanje. Takvo digitalno osnaživanje, posebno kada je podržano i u porodici i u školi, predstavlja važan preduslov za razvoj dugoročne otpornosti – ne samo u tehničkom već i u kritičkom i odgovornom smislu.

Istovremeno, obrazovni sistem u Srbiji i dalje se suočava sa strukturnim ograničenjima. Zastareli nastavni programi, infrastrukturni nedostaci i nedovoljna obuka nastavnika u oblasti digitalne etike otežavaju pretvaranje dobrih ideja u svakodnevnu praksu. Nastavnici ne bi trebalo da snose ovu odgovornost sami – potrebno je da im se obezbedi sistem-ska podrška kroz kvalitetnu obuku, dostupne nastavne resurse i institucionalno poverenje koje će im omogućiti da preuzmu aktivnu ulogu u ovom procesu.

Literatura

- Andrić, V. (2025, June 29). Digitalna prava dece: Šta podrazumevaju i ko ih najčešće krši? *Danas*. <https://www.danas.rs/vesti/drustvo/digitalna-prava-dece-sta-podrazumevaju-i-ko-ih-najcesce-krsi/>
- Andries, V. & Robertson, J. (2023). Alexa doesn't have that many feelings: Children's understanding of AI through interactions with smart speakers in their homes. *Computers and Education: Artificial Intelligence*, 5, 1-17. <https://doi.org/10.1016/j.caeai.2023.100176>
- CoSN (2025). *2025 National Student Data Privacy Report*. Consortium for School Networking. <https://www.cosn.org/wp-content/uploads/2025/03/2025-CoSN-National-Student-Data-Privacy-Report-Part-1-Final-031825.pdf>

- Danaj, A., Škorić, J. & Galetin, M. (2024). Comparative analysis of the legal frameworks of the Republic of Serbia and Republic of Albania: The application of Artificial Intelligence and child protection. In M. Počuča (Ed.), *XXI međunarodni naučni skup „Pravnički dani-Prof. dr Slavko Carić“, Odgovori pravne nauke na izazove savremenog društva*, (Radovi) (pp. 413-425). Faculty of Law for Commerce and Judiciary, University of Novi Sad. <https://doi.org/10.5937/PDSC24413D>
- Eisinga, R., Grotenhuis, M.t. & Pelzer, B. (2013). The reliability of a two-item scale: Pearson, Cronbach, or Spearman-Brown?. *International Journal of Public Health*, 58, 637–642. <https://doi.org/10.1007/s00038-012-0416-3>
- Gao, L., Blinder, E. B., Barnes, A., Song, K., Clegg, T., Vitak, J. & Chetty, M. (2025). Creating and Evaluating Privacy and Security Micro-Lessons for Elementary School Children. *arXiv preprint arXiv:2503.07427*. <https://doi.org/10.48550/arXiv.2503.07427>
- Guo, Y. (2021). The Cultural Implications and Ethical Risks of Algorithm Society. *Chinese Book Review*, 9, 45-53. <https://doi.org/10.3969/j.issn.1002-235X.2021.09.006>
- Hao, X., Wang, F. & Qi, C. (2019). The current status and developmental trends of educational artificial intelligence. *Modern Educational Technology*, 2, 12-18.
- Hillman, V., Manolev, J., Johnston, S.K., Kumar, P.C., Martin, F., Zeide, E., Vladova, G. & Lai, R. (2024). Children, Education, and Technologies: Current Debates, Key Concerns, and Future Directions Around Data Privacy, Surveillance, and Datafication. In D. A. Christakis & L. Hale (Eds.), *Handbook of Children and Screens* (pp. 557-567). Springer. https://doi.org/10.1007/978-3-031-69362-5_76
- Hoofnagle, C. J., Van Der Sloot, B. & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1), 65-98. <https://doi.org/10.1080/13600834.2019.1573501>
- Huang, L. (2023). Ethics of artificial intelligence in education: Student privacy and data protection. *Science Insights Education Frontiers*, 16(2), 2577-2587. <https://doi.org/10.15354/sief.23.re202>
- Ignjatović, G. (2024). AI TECHNOLOGIES IN EDUCATION: Regulatory frameworks at the international, regional and national level. *Zbornik radova Pravnog fakulteta u Nišu*, 63(103), 235-260. <https://doi.org/10.5937/zrpf1-55374>
- Jia, K. & Jiang, Y. (2017). Three basic issues of artificial intelligence governance: Technical logic, challenges, and public policy making. *Chinese Public Administration*, 10, 40-45. <https://doi.org/10.3782/j.issn.1006-0863.2017.10.07>
- Li, L., Valdez, J.P.M. & Du, Y. (2025). Digital citizenship education at the early childhood level: how is it implemented? A systematic review. *International Journal of Child Care and Education Policy*, 19, 13. <https://doi.org/10.1186/s40723-025-00153-2>
- Liu, S., Liu, S., Sun, J., Shen, X., & Liu, Z. (2021). Key issues in the development of intelligent education. *Distance Education in China*, 4, 69-76. <https://doi.org/10.13541/j.cnki.chinade.2021.04.001>
- Livingstone, S. M. & Blum-Ross, A. (2020). *Parenting for a digital future: How hopes and fears about technology shape children's lives*. Oxford University Press.
- Lupton, D. & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*, 19(5), 780-794. <https://doi.org/10.1177/1461444816686328>
- Matović, M. & Žunić-Pavlović, V. (2020). Povezanost restriktivnih strategija roditeljskog nadzora i digitalnog nasilja u adolescenciji. *CM: Communication and Media*, 15(47), 35-56. <https://doi.org/10.5937/cm15-27100>
- McLeod, S. (2009). Piaget's Theory and Stages of Cognitive Development. *Simply Psychology*. <https://doi.org/10.5281/zenodo.15241970>

- Muammar, S., Hashim, K. F. B. & Panthakkan, A. (2023). Evaluation of digital competence level among educators in UAE Higher Education Institutions using Digital Competence of Educators (DigComEdu) framework. *Education and Information Technologies*, 28, 2485–2508. <https://doi.org/10.1007/s10639-022-11296-x>
- Nešić, A. (2023). Zaštita podataka o deci na internetu. *Savremene studije bezbednosti*, 16(1), 29-48. <https://doi.org/10.5937/ssb202301029N>
- Nguyen, A., Ngo, H. N., Hong, Y., Dang, B. & Nguyen, B. P. T. (2023). Ethical principles for artificial intelligence in education. *Education and Information Technologies*, 28(4), 4221-4241. <https://doi.org/10.1007/s10639-022-11316-w>
- Shi, Y. & Zhou, X. (2022). The debate on the “right to be forgotten” in the era of big data: To be remembered or forgotten? *Editorial Friends*, 12, 88-99. <https://doi.org/10.13786/j.cnki.cn14-1066/g2.2022.12.012>
- Shouli, A., Barthwal, A., Campbell, M. & Shrestha, A. K. (2025). Ethical AI for Young Digital Citizens: A Call to Action on Privacy Governance. *arXiv preprint arXiv:2503.11947*. <https://doi.org/10.48550/arXiv.2503.11947>
- Solberg, J. (2023). Privacy in Early Childhood Education and Care: The Management of Family Information in Parent–Teacher Conferences. *Human Studies* 47, 367–388. <https://doi.org/10.1007/s10746-023-09683-5>
- Stoilova, M., Livingstone, S. & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age*. Research findings. London School of Economics and Political Science.
- Škobo, M. & Šović, M. (2025). Teachers' perspectives on Chatbots and AI agents in primary and secondary education. *International Journal on Studies in Education*, 7(2), 410-442. <https://doi.org/10.46328/ijonse.352>
- UNESCO. (2022). *Recommendation on the Ethics of Artificial Intelligence*. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
- Vartiainen, H., Pope, N., Kahila, J., López-Pernas, S. & Tedre, M. (2025). Classroom Activities and New Classroom Apps for Enhancing Children's Understanding of Social Media Mechanisms. *arXiv preprint arXiv:2501.16494*. <https://doi.org/10.48550/arXiv.2501.16494>
- Wang, Z. (2016). American student data privacy protection legislation and governance frameworks in the era of big data. *International and Comparative Education*, 11, 28-33. <https://doi.org/10.20013/j.cnki.ice.2016.11.005>
- Wang, G., Zhao, J. & Shadbolt, N. (2019). Are children fully aware of online privacy risks and how can we improve their coping ability? *arXiv preprint arXiv:1902.02635*. <https://doi.org/10.48550/arXiv.1902.02635>
- Williamson, B. (2017). *Big data in education: The digital future of learning, policy and practice*. SAGE.
- Williamson, B. (2019). Datafication of education: a critical approach to emerging analytics technologies and practices. In H. Beetham & R. Sharpe (Eds.), *Rethinking pedagogy for a digital age* (pp. 212-226). Routledge.
- Xue, L. & Zhao, J. (2019). Paths to agile governance: The development of emerging industries and regulatory models. *Chinese Public Administration*, 8, 28-34. <https://doi.org/10.19735/j.issn.1006-0863.2019.08.02>
- Yeşilyurt, E. & Vezne, R. (2023). Digital literacy, technological literacy, and internet literacy as predictors of attitude toward applying computer-supported education. *Education and Information Technologies*, 28(8), 9885-9911. <https://doi.org/10.1007/s10639-022-11311-1>

- Yim, I. H. Y. & Su, J. (2025). Artificial intelligence literacy education in primary schools: a review. *International Journal of Technology and Design Education*, 35, 2175-2204. <https://doi.org/10.1007/s10798-025-09979-w>
- Zhao, H., Jiang, Q. & Zhao, W. (2016). The security of big data-based learning analytics and privacy protection. *Modern Educational Technology*, 26(3), 5-11. <https://doi.org/10.3969/j.issn.1009-8097.2016.03.001>
- Zhao, Z., Xu, F., Gao, F., Li, F., Hou, H. & Li, M. (2021). An evaluation of ethical risks in artificial intelligence. *China Soft Science*, 6, 1-12.

Primljeno: 22.07.2025.

Korigovana verzija primljena: 07.10.2025.

Prihvaćeno za štampu: 08.10.2025.

Milena Škobo

Filološki fakultet, Univerzitet Sinergija, Bijeljina, Bosna i Hercegovina
<https://orcid.org/0000-0001-8427-2051>

Milena Šović

Fakultet za ekonomiju i inženjerski menadžment,
Univerzitet Privredna akademija u Novom Sadu, Novi Sad, Srbija
<https://orcid.org/0009-0009-5774-5672>



Ovaj rad je objavljen pod licencom Creative Commons Attribution 4.0 International (CC BY 4.0). Dopušteno je da se delo kopira i distribuira u svim medijima i formatima, da se prerađuje, menja i nadograđuje u bilo koje svrhe, uključujući i komercijalne, pod uslovom da se na pravilan način citiraju njegovi prvobitni autori, postavi link ka originalnoj licenci i naznači da li je delo izmenjeno. Korisnici su pri tome dužni da navedu pun bibliografski opis članka objavljenog u ovom časopisu (autori, naslov rada, naslov časopisa, volumen, sveska, paginacija), kao i njegovu DOI oznaku, a u slučaju objavljivanja u elektronskoj formi takođe su dužni da postave i HTML link.

Data Privacy and AI Use in Primary Education in Serbia: Student Awareness and Adult Support

Milena Škobo¹ 

Faculty of Philology, Sinergija University, Bijeljina, Bosnia and Herzegovina

Milena Šović 

Faculty of Economics and Engineering Management,
University Business Academy in Novi Sad, Novi Sad, Serbia

Abstract

Student data privacy, especially among younger users, raises critical concerns since the growing use of AI tools in education. This study examines how primary school students in Serbia understand data protection in the context of AI-enhanced educational platforms. It specifically investigates the relationship between student awareness of privacy risks and adult mediation—by teachers and parents—as well as whether increased AI use corresponds with reduced adult supervision. A structured questionnaire was administered to 240 students in grades 5 through 8. Composite variables were generated from Likert-scale items and results were analyzed using nonparametric methods, including Spearman's rank correlation and the Wilcoxon Signed-Rank test. The findings indicate that adult communication has a limited effect on students' data privacy understanding, although parental support appears to be more influential than teacher involvement. These results point to the urgent need for age-appropriate digital literacy initiatives, institutional accountability and targeted support for teachers and parents, since students often lack a concrete understanding of abstract privacy concepts and require structured, developmentally adapted guidance to safely engage with AI technologies.

Keywords: *AI in education; student data privacy; primary school students; adult mediation; digital literacy.*

Introduction

The presence of artificial intelligence (AI) in education is changing not only how students learn but also how they are monitored and evaluated. Tools such as adaptive

¹ mskobo@sinergija.edu.ba

learning platforms and automated feedback systems now routinely collect and analyze detailed information about students' behavior and performance. This shift has raised serious concerns about the scope of data collection, the lack of transparency in how information is used, as well as of the absence of meaningful consent (Lupton & Williamson, 2017; Williamson, 2017). In many cases, students remain unaware that their digital activities — clicks, answers, time spent on tasks — are being recorded and shared, sometimes with third-party providers operating beyond the school's oversight (Williamson, 2019).

Regulatory bodies and international organizations have begun to issue specific guidelines aimed at protecting human dignity and children's rights in the context of AI development. China's "Ethical Rules for New-generation Artificial Intelligence" (2021), for example, emphasize that "AI development must promote human well-being" (Huang, 2023, p. 2578). Similarly, UNESCO's *Recommendation on the Ethics of Artificial Intelligence* (2022) calls for the protection of human rights, freedom, dignity and autonomy. Both documents stress that personal data should never be collected without informed consent and they advocate for clear rules about how children's data are gathered, stored and used — especially in school settings.

As schools begin to use more algorithm-based technologies, students are often represented by data profiles that shape how they are taught and assessed (Williamson, 2019). These systems are rarely transparent and their influence on learning raises important questions about who controls student data and how decisions are made. Scholars have responded by arguing that digital literacy must go beyond basic computer skills. It should also help students understand what personal data are being collected, how they are used and what this means for their learning and privacy (Hillman et al., 2024; Yeşilyurt & Vezne, 2023).

The problem is especially visible in primary and secondary education, where students often lack the cognitive and linguistic tools to interpret complex ideas about digital privacy. Empirical studies show that children struggle to grasp terms such as "data sharing", "personal information" or "tracking" unless explained in clear, age-appropriate ways. Even though children's use of digital platforms is rising, as shown by algorithms, they are rarely taught what these systems do, how they might be biased, or what rights they have when using them. Institutional safeguards are uneven: research highlights a lack of teacher training in AI ethics and data protection (CoSN, 2025; Kelly et al., 2023), while parental mediation tends to be inconsistent and often uninformed (Livingstone & Blum-Ross, 2020).

This study focuses on primary education in Serbia, where research on AI, data privacy and student agency remains limited. It investigates how children perceive privacy risks, how adult mediation (from teachers and parents) affects that understanding and whether frequent AI use reduces supervision. It also offers empirical evidence to international debates on children's digital rights as well as to the role of schools in creating safe and supportive AI-mediated learning environments.

Literature review

International research has constantly pointed to privacy infringement, limited autonomy and the lack of algorithmic systems as key ethical concerns in using AI in education

(Guo, 2021; Zhao et al., 2021). These systems often collect data covertly and create asymmetrical power relations between users and technology providers. In response, scholars have proposed student-centered ethical frameworks (Hao et al., 2019; Liu et al., 2021), more flexible and responsive forms of regulation (Xue & Zhao, 2019) and stronger rules for data management in schools (Jia & Jiang, 2017). These contributions share a common focus: ensuring that AI systems used in education operate transparently and are accountable.

New developments in data technologies have made it even harder to separate helpful educational tools from forms of digital monitoring. “Some AI systems can now make assumptions about a student’s behavior, emotions, or thinking patterns based on their online activity, making it harder to tell where support ends and surveillance begins” (Huang, 2023, p. 2582). Regulatory responses such as the General Data Protection Regulation (GDPR) and the so-called “right to be forgotten” (Hoofnagle et al., 2019; Shi & Zhou, 2022) aim to give people more control over how their personal data are used. Other strategies, such as privacy built into the design of digital tools (Zhao et al., 2016), try to ensure that data protection is considered from the beginning. Institutional proposals such as Wang’s (2016) model for school-based data governance stress the need to align technical solutions with legal and ethical responsibilities.

Empirical studies show that many young children are still unable to understand digital privacy. Wang and others (Wang et al., 2019) found that children aged 6 to 10 could recognize basic risks such as oversharing, but had difficulty comprehending more abstract issues, such as how platforms track behavior or suggest content. Similarly, Andries and Robertson (Andries & Robertson, 2023) demonstrated that primary students in Scotland did not understand how AI works, indicating a need for introducing age-appropriate lessons about digital technologies early in education.

Classic theories of child development can explain children’s difficulty in a better way with digital privacy and AI-related concepts. According to Piaget, most children in primary school are in the concrete operational stage (typically ages 7–11), during which they can reason logically about concrete events, but often struggle with abstract ideas. While they may recognize obvious risks like sharing personal details online, they find it more difficult to comprehend less tangible dangers, such as being tracked by apps or targeted by online content.

Vygotsky’s theory of the zone of proximal development (ZPD) helps explain how children can learn abstract ideas when guided by adults or peers. He emphasized that learning is most effective when children are guided by more knowledgeable others — teachers, parents, or peers — who can scaffold abstract concepts through collaborative interaction, questions and reflection. In the context of AI and digital privacy, this implies that children are unlikely to internalize ethical principles or identify surveillance threats unless these are made visible through clear guidance and adapted to children’s level of understanding. Piaget and Vygotsky remind us that children need structured support and relatable examples to make sense of digital tools and the risks they carry.

Gao and others (Gao et al., 2025) worked with teachers to co-design micro-lessons for K–8 students. They showed that even short, well-integrated activities can enhance

children's capacity to identify and respond to privacy threats. Vartiainen and others (Vartiainen et al., 2025) reached similar conclusions through classroom interventions using custom-built apps, which led to measurable improvements in data agency — students' ability to understand data critically. Their study found that students became more aware of how social media algorithms affect what they see online and how this shapes their behavior.

Yim and Su (Yim & Su, 2025) argue that most existing AI literacy programs overemphasize technical skills while neglecting critical engagement with issues such as consent, surveillance and algorithmic bias. They propose a multidimensional model that integrates legal, ethical and technical competencies. In their systematic review of digital citizenship education for children aged 0 to 8, Li and others (Li et al., 2025) found that such instruction is rare but effective when integrated into core subjects, using gamified and collaborative learning strategies. Their review emphasizes the importance of early, structured interventions that do not treat children as passive recipients of protection, but as emerging digital citizens capable of understanding privacy, consent and ethical digital participation.

Many educational efforts fall short not because of poor curriculum design, but because teachers are not fully prepared to implement them. Using the validated Dig-CompEdu framework, Muammar and others (Muammar et al., 2023) assessed educators' digital competence across several key areas. Their findings show that even higher education faculty demonstrate inconsistent proficiency in areas like data protection and pedagogical integration of digital ethics, stressing the urgent need for teacher training at all educational levels. Without adequate preparation, teachers may avoid digital tools altogether or rely on restrictive measures which limit student engagement.

Research shows that digital ethics should not be introduced through isolated facts or abstract rules. Instead, they need to be integrated into everyday teaching through discussions suitable for children of a particular age and meaningful interaction. As Nguyen (Nguyen, 2023) emphasizes, children's critical engagement with data privacy emerges most effectively through discussion, peer interaction and real-life simulations, rather than isolated lessons. Solberg (Solberg, 2023), building on constructivist ideas, calls for a digital literacy approach, where students and teachers reflect together on real-life digital situations — such as using apps, sharing photos or talking to chat-bots. Such approaches avoid one-way teaching and treat children as capable of making sense of ethical issues. In this way, children build their own understanding through real-world digital experience.

Findings from the KOALA Project (Wang et al., 2019) show that children, despite often being able to spot obvious risks such as sharing their real names, tend to struggle with more hidden or abstract threats, such as being tracked online or shown content based on their behavior. This is why it is important to integrate privacy education in schools that goes beyond simply listing rules. Instead, students need help understanding how digital tools work and how they affect their choices and experiences. Shouli and others (Shouli et al., 2025) make a similar point, arguing that children should be treated as active participants in digital life, not just passive users. Their model encourages schools to include lessons on data rights, how algorithms make decisions, and what it means to give informed consent, as a part of regular classroom teaching.

In Serbia, there is still very little research or policy frameworks regarding how children interact with AI and how their data is used in educational settings. Existing legislation — such as the *Law on Personal Data Protection* (2019), the *Law on Social Protection* (2011) and the *Law on Juvenile Offenders and Criminal Protection of Juveniles* (2005) — does not address the specific risks posed by AI systems in schools. The forthcoming *Draft Law on Children's Rights* similarly lacks provisions concerning digital rights, data ethics or algorithmic educational influence.

Strategic documents like the *Artificial Intelligence Development Strategy of the Republic of Serbia (2020–2025)* and the *Ethical Guidelines for the Development, Implementation and Use of Reliable and Responsible AI* (2022) acknowledge general risks, such as data misuse, but do not include child-specific protections. The establishment of the Research and Development Institute for AI in Serbia is a positive step, yet it has not addressed the ethical concerns related to the use of AI in classrooms or its impact on children (Danaj et al., 2024).

Ignjatović (Ignjatović, 2024) notes that while Serbia's data protection law is formally harmonized with the GDPR, its application within schools is inconsistent and largely unregulated, particularly when AI tools are used for purposes like biometric recognition or behavioral monitoring. Ethical guidelines remain non-binding and contain no specific provisions for children's rights. Furthermore, no regulatory body has been designated to oversee AI applications in educational settings, leaving schools without clear oversight or accountability. This situation increases the risk that children's data will be misused or that they will be exposed to digital surveillance without knowing it. Danaj and others (Danaj et al., 2024) further warn that the absence of empirical research on this issue prevents the development of practical, context-specific responses. Without such data, it is difficult for educators and policymakers to design meaningful safeguards.

Parental mediation, although essential in shaping children's digital behavior, also faces clear structural limitations. Recent findings by Matović and Žunić-Pavlović (Matović i Žunić-Pavlović, 2020) indicate that many parents tend to rely on restrictive methods — such as limiting screen time or requiring access to their children's passwords — rather than fostering open dialogue or long-term digital literacy. Although these strategies may reflect a desire to protect, they are reactive rather than proactive and fall short in promoting long-term digital resilience. In a media interview, Kuzmanović notes that children's digital rights — such as privacy, participation and access to age-appropriate content — must be fully recognized in digital environments, not only regulated through restrictions or bans. She argues that institutional responsibility, rather than excessive parental control, should guide the design of safe digital spaces (Andrić, 2025).

Nešić (Nešić, 2023), in her policy analysis, notes that while parental dialogue remains an important mechanism, many children avoid disclosing risky or sensitive online experiences. She argues that while open communication remains vital, it should be supported by practical strategies such as browsing history checks, device-based filters and parental control tools. However, implementing such measures effectively requires higher levels of digital literacy among parents, as well as institutional support. While restrictive parental mediation remains dominant, it may infringe on children's digital rights. Kuzmanović warned that even well-intentioned actions, such as posting children's photos online ("sharing"), may violate children's privacy, advocating instead for comprehensive digital

literacy for both children and adults (Andrić, 2025). In addition, institutional partnerships with parents and schools, as proposed in Li and others (Li et al., 2025) and Gao and others (Gao et al., 2025), could offer a non-restrictive path forward — one that promotes shared responsibility instead of placing the burden solely on parents.

This study responds to the absence of empirical evidence in Serbia by examining how primary school students understand data privacy and how the support from adults influences their interaction with AI-enhanced educational tools.

Research Methodology

In order to address the identified research gap, this study employed a quantitative, cross-sectional research design to investigate how primary school students in Serbia perceive and manage data privacy in the context of AI-enhanced educational technologies. Specifically, it explores the relationships between students' familiarity with AI systems, their awareness of data protection practices and the mediating role of adult support — particularly from teachers and parents. The following research questions guided the study:

1. To what extent are primary school students aware of data privacy and protection in the context of using AI tools and applications?
2. How does communication with teachers and parents influence students' understanding of data privacy in AI environments?
3. Is there a difference in the level of support and supervision provided by parents compared to teachers regarding students' use of AI applications?
4. Does the frequency of AI application use relate to the level of parental supervision at home?

Sample

The study was conducted with a sample of 240 primary school students from grades 5 through 8 in Serbia. The grade-level distribution was nearly even: 25.0% were in 5th grade, 25.0% in 6th grade, 25.4% in 7th grade and 24.6% in 8th grade. Regarding gender, 53.3% of participants identified as male and 46.7% as female. Students were recruited from both urban and semi-urban schools using convenience sampling.

Data Collection

The survey link was distributed through professional teacher networks and social-media groups. Only teachers who voluntarily expressed interest conducted the activity with their own classes. According to information provided by these teachers, parents were verbally informed during parent-teacher meetings that students would engage in a trial of the educational chatbot followed by a voluntary, anonymous survey, and were given the opportunity to refuse participation; no objections were reported. All questionnaires were completed in school settings under teacher supervision.

Ethical statement

Participation was entirely voluntary and the survey content was neutral, as well as classified as minimal risk. No personal data (such as names, school identifiers, or IP addresses) were collected and the researchers have no means of subsequent participant identification. All participants completed the questionnaire in school settings under teacher supervision. According to EU GDPR Recital 26 and the Serbian Law on Personal Data Protection, fully anonymous data are not considered personal data; therefore, formal parental consent and institutional ethics approval were not required. The research was conducted in accordance with the principles of the Declaration of Helsinki and relevant national regulations on data protection and educational research.

Hypotheses

The following hypotheses were formulated:

H1. Students who use AI applications more frequently are less likely to be supervised by parents at home.

H2. Communication with adults improves students' understanding of data privacy. Students who communicate with teachers about AI and digital safety will demonstrate greater awareness of privacy issues (H2.1). Students who discuss digital privacy with their parents will show higher levels of privacy awareness (H2.2). Students who receive guidance from both parents and teachers will exhibit the highest levels of data privacy awareness (H2.3).

H3. Institutional support is less developed than familial support. Students are more likely to receive parental permission than teacher permission to use AI tools (H3.1). Students use AI applications more frequently under parental supervision than under teacher supervision (H3.2). Students perceive parents as being more informed than teachers about the safety of AI tools (H3.3).

Research Instrument

The primary instrument for data collection was a self-report questionnaire, originally constructed for the purpose of this study. It was not adapted from any existing validated scale, but developed based on a review of relevant literature and expert consultations in the fields of educational psychology and information technology. The questionnaire consisted of 22 closed-ended items measured on a five-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree) and was grouped into five thematic sections: Familiarity and Use of AI Applications (items 1 – 2), Awareness of Data Privacy (items 3 – 10), Experience with Data Sharing and Supervision (items 11 – 13), Teacher and Parental Engagement (items 12 – 19) and Motivation and Educational Needs (items 20 – 22).

Prior to the main data collection, a pilot test was conducted with a sample of 38 primary school students (grades 5 – 8) from an urban school. The aim of the pilot was to assess item clarity, questionnaire length and technical feasibility. Based on pilot test

feedback, minor linguistic adjustments were made to items 4, 13 and 20 to improve comprehension and reduce ambiguity.

For the purpose of hypothesis testing and construct validation, five composite (latent) variables were developed by aggregating thematically related items. These included: (1) Level of Independence in AI Use, derived from items 2 and 17 (reverse-coded); (2) Privacy Awareness Index, based on items 3, 4 and 7; (3) Communication with Adults, composed of items 15 and 19; (4) Teacher Support Index, formed from items 12, 13 and 14 and (5) Parental Support Index, based on items 16, 17 and 18.

Each composite variable was computed as the mean score of its constituent items. Constructs were used to test the relationships among variables and evaluate the proposed hypotheses. These groupings were theoretically informed by existing models of digital literacy and privacy mediation in children (Stoilova et al., 2019) and reflect conceptual coherence within the domains assessed.

The validity of the developed instrument was confirmed on three key grounds: (1) theoretical grounding of the constructs, based on relevant models of digital literacy and privacy mediation in children; (2) satisfactory internal consistency, confirmed by reliability coefficients ($\alpha > .70$) for all indices and (3) empirical confirmation through intercorrelations of composite variables in accordance with the stated hypotheses.

To assess the internal consistency reliability of these constructs, Cronbach's alpha coefficients were calculated using data from the full sample ($N = 240$). The results confirmed satisfactory reliability across all five indices: the *Level of Independence in AI Use* yielded an alpha of .72; the *Privacy Awareness Index* showed an alpha of .81; *Communication with Adults* reached .76; *Teacher Support Index* recorded .79 and *Parental Support Index* demonstrated the highest reliability with an alpha of .83. All coefficients exceeded the conventional threshold of .70, indicating acceptable internal consistency for each construct. It is acknowledged that reliability estimates for two-item scales such as "Communication with Adults" and "Level of Independence in AI Use" should be interpreted with caution, as Cronbach's alpha is less stable for such constructs; nonetheless, both indices exceeded .70 and reflected conceptually coherent dimensions (Eisinga et al., 2013).

These composite variables were subsequently used to examine the relationships among key dimensions of the study, as well as to evaluate the proposed hypotheses. Preliminary evidence of construct validity was obtained through correlation analysis among the composite variables, which revealed statistically significant relationships in expected directions.

The construct validity of the composite variables was supported by both theoretical justification and empirical evidence derived from intercorrelations. The index of autonomy in using AI applications was significantly negatively associated with parental monitoring ($\rho = -.189, p < .01$), while the index of parental support also showed a significant negative correlation with students' awareness of privacy ($\rho = -.163, p < .05$). In contrast, the index measuring communication with adults did not exhibit a statistically significant relationship with students' understanding of privacy ($\rho = .052, n. s.$), suggesting thematic differentiation between the constructs. Furthermore, the Wilcoxon test confirmed statistically significant differences in students' perception of parental versus teacher support ($Z = -3.397, p < .01$), thereby strengthening the internal validity of the defined indices.

Although the instrument was not adapted from pre-existing scales, its coherent thematic structure, clearly defined indicators and consistent empirical patterns provide strong support for its adequacy in assessing students' attitudes and experiences regarding the use of AI tools, awareness of data privacy, as well as the role of adult support.

Data Analysis

All survey responses were numerically coded (1 – 5) and aggregated to produce composite scores for each latent variable. The distribution of variables was tested for normality using the Kolmogorov–Smirnov and Shapiro–Wilk tests. As none of the variables followed a normal distribution, nonparametric statistical methods were employed, including Spearman's rank correlation coefficient (to assess relationships among variables) and the Wilcoxon Signed-Rank test (in order to compare paired responses, particularly between teacher indicators and parental support indicators).

Results

Spearman's rho correlation (Table 1) shows a statistically significant negative correlation between the frequency of AI application use and parental supervision at home ($\rho = -.189, p < .01$), confirming the hypothesis (H1) that students who use AI applications more frequently are less supervised by their parents. In addition, parental supervision shows a negative correlation with the level of privacy awareness ($\rho = -.163, p < .05$), indicating that students under greater parental supervision have a lower level of understanding regarding privacy in AI tools. Students under strict parental control are not likely to have the opportunity to independently explore AI tools and gain experience in understanding privacy. On the other hand, the frequency of AI use did not have a significant correlation with the level of privacy awareness ($\rho = .106$), nor with the level of communication with adults ($\rho = .013$), suggesting that the autonomy in the AI environment is not directly connected with understanding privacy or conversations with adults. The conclusion that higher frequency of AI application use is significantly associated with lower parental supervision supports the hypothesis as correct. Therefore, hypothesis H1 is fully confirmed.

Table 1

Correlation between frequency of AI use, parental supervision, privacy awareness and communication with adults (N = 240)

Variable	Frequency of AI Use	Parental Supervision	Level of Privacy Awareness	Level of Communication with Adults
Frequency of AI Use	1	-.189**	.106	.013
Parental Supervision		1	-.163*	.052
Level of Privacy Awareness			1	.052
Level of Communication with Adults				1

Note. **Correlation is significant at the .01 level (2-tailed). *Correlation is significant at the .05 level (2-tailed).

The influence of students' communication with adults on their understanding of privacy in AI tools (H2) was evaluated using Spearman's rank correlation. As shown in Table 2, the correlation between communication with teachers and privacy awareness was weak and statistically insignificant ($\rho = .096$, $p = n. s.$). Communication with parents showed an even weaker, slightly negative relationship ($\rho = -.010$, $p = n. s.$). In contrast, overall communication with adults was strongly correlated with communication with teachers ($\rho = .739$, $p < .01$) and parents ($\rho = .735$, $p < .01$), indicating that students who communicate with one adult source often communicate with the other adult source as well. However, this combined communication did not translate into a significant improvement in privacy awareness, suggesting that such interactions, even when frequent, may not address data protection topics in meaningful or structured ways.

For H2.1, a weak and statistically non-significant correlation was found between communication with teachers and privacy awareness ($\rho = .096$, $p = n. s.$). This suggests that teacher–student conversations have little impact on students' understanding of digital privacy. A plausible explanation is that privacy-related topics are not sufficiently emphasized in the school curriculum, or that teachers may lack the training to effectively address these issues.

For H2.2, the correlation between communication with parents and privacy awareness was extremely weak and slightly negative ($\rho = -.010$, $p = n. s.$), indicating no meaningful association. This implies that students either do not receive relevant information from their parents or do not perceive such conversations as applicable to their AI-related activities. A likely explanation is that many parents are not adequately informed about AI privacy concerns, thus failing to communicate accurate or comprehensive information.

H2.3 explored whether overall communication with adults (combined parent and teacher interaction) would be a stronger predictor of privacy understanding. Although strong correlations were observed between general communication with adults and the two specific sources (teachers: $\rho = .739$, parents: $\rho = .735$, $p < .01$), the direct correlation between overall communication and privacy awareness remained weak and non-significant ($\rho = .052$, $p = n. s.$). This suggests that while students may engage in conversations with both parents and teachers, these interactions likely focus on general aspects of technology use rather than data protection or privacy.

The results indicate that communication with teachers and parents does not significantly influence students' awareness of data privacy. While a strong and significant correlation exists between teacher and parent communication ($\rho = .739$ and $\rho = .735$, $p < .01$), these interactions do not translate into higher levels of student privacy understanding.

H2.1 and H2.2 are not supported, as neither teacher nor parent conversations show a statistically significant effect on privacy awareness. H2.3 is only partially supported: although combined communication with adults correlates strongly with its individual components, it does not significantly predict students' privacy understanding. These findings suggest that students may acquire most of their knowledge about data protection through personal experience rather than through conversations with adults. Consequently, the overall hypothesis H2 is not confirmed. This points to the need for more explicit and structured education regarding data privacy, both in schools and at home.

Table 2

Association between level of privacy awareness, communication with teachers, parents and the level of communication with adults (N=240)

Variable	Level of privacy awareness	Communication with teachers	Communication with parents	Level of communication with adults
Level of privacy awareness	1.000	.096	-.010	.052
Communication with teachers		1.000	.106	.739**
Communication with parents			1.000	.735**
Level of communication with adults				1.000

Note. **Correlation is significant at the .01 level (2-tailed).

The Wilcoxon Signed Ranks Test results (Table 3) support Hypothesis H3, showing that students perceive parental support for AI tool use as significantly more developed than teacher support. H3.1 is supported: Students report that parents give permission to use AI tools more frequently than teachers do ($Z = -2.579, p < .05$). H3.2 is not supported: No significant difference was found in AI supervision levels between parents and teachers ($Z = -1.072, p = .284$), indicating comparable supervision at home and school. H3.3 is supported: Students perceive parents as more knowledgeable about data safety than teachers ($Z = -1.901, p < .05$). A strong and statistically significant difference in overall support was found in favor of parents ($Z = -3.397, p < .01$). These findings confirm that parental support is generally more developed than school support in guiding children's use of AI applications, thereby fully supporting hypothesis H3. The results indicate that parents play a key role in supporting students in the use of AI tools, while teachers have limited influence, likely due to insufficient adaptation of the curriculum and approach to this topic.

Table 3

Test Statistics of the Wilcoxon Signed Ranks Test for teacher and parental support in the use of AI tools and applications (N = 240)

Teacher and parental support	Permission from teachers at school – parents at home to use AI tools and applications	Use of AI tools only under teacher supervision at school – parental supervision at home	Teachers – parents are informed about data safety in AI tools and applications	Level of teacher – level of parental support
Z	-2.579	-1.072	-1.901	-3.397
Asymp. Sig. (2-tailed)	.010	.284	.039	.001

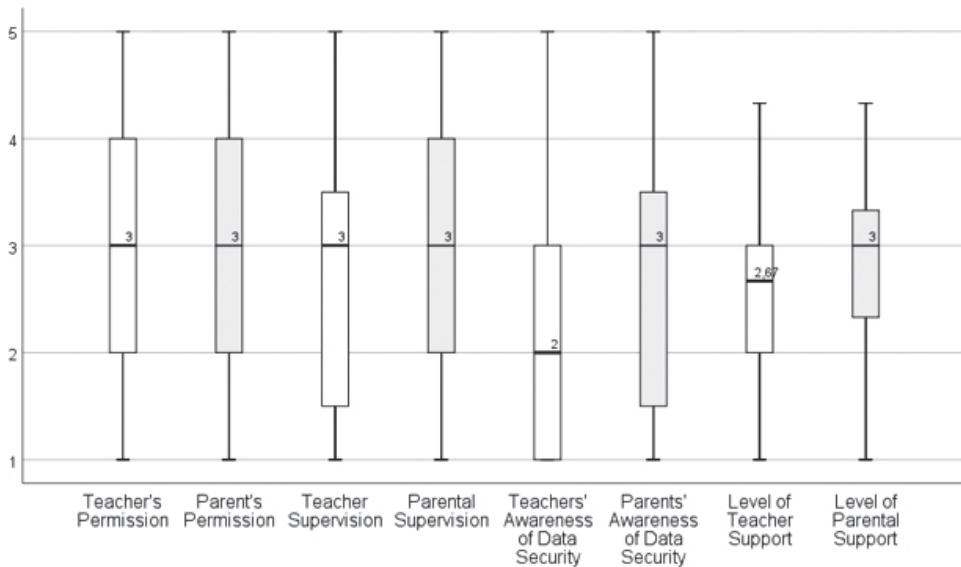
Note: A negative Z-value indicates that all values for parents are higher than those for teachers.

Graph 1 visually confirms previous conclusions that parents provide a higher level of support to students in all aspects of AI tool usage, including permission to use AI tools and applications, supervision by teachers and parents and their awareness of data safety. The graph shows that the median value for teacher support remains lower across

all categories, except in the supervision segment, where the difference is not statistically significant. Awareness of data safety shows a notable difference, as students believe parents are better informed about data privacy protection than teachers. The largest gap appears in the level of support, where parental support is significantly more prominent than teacher support (median 3 vs. 2.67). These findings confirm that students rely more on parental than teacher support when using AI tools and applications, suggesting a need for improved educational initiatives within the school system.

Graph 1.

Comparison of teacher and parental support in the use of AI tools



Discussion

The results of this study show that adult mediation — whether from parents or teachers — has only a modest link to primary students' understanding of data privacy. Parental involvement showed a slightly stronger correlation than teacher engagement, but both effects were weak (e.g., parental supervision and privacy awareness ($p = -.163$, $p < .05$). This challenges the common belief that the mere presence of adults, without training or institutional backing, is sufficient to ensure safe digital practices.

Adult guidance in this context appears limited in both form and content. As Matović and Žunić-Pavlović (Matović i Žunić-Pavlović, 2020) note, many Serbian parents rely on restrictive controls rather than encouraging open discussion. Such strategies may create dependency instead of independence, leaving students poorly prepared to deal with privacy risks in AI-based tools. Our findings also support Nešić's (Nešić, 2023) observation that verbal communication, without practical tools or concrete examples, rarely helps children identify or assess online risks. Even when adults try to intervene, the language is often abstract, the examples are too general and the impact is minimal.

At the same time, the statistically significant correlation between parental oversight and privacy awareness must be treated with care. The data show a link but not its direction. One possibility is that restrictive parental strategies may suppress children's ability to think critically about privacy, producing dependence instead of autonomy. But another, equally plausible explanation is that children who already possess greater awareness of data protection seek more independence and therefore face less parental intervention. A third, confounding factor — such as the parents' own digital literacy or socioeconomic background — may influence both their approach and the child's understanding. Long-term or mixed-method studies are needed to clarify these possibilities.

Teachers, despite their formal role, had little measurable influence on students' privacy awareness. This is consistent with the lack of tools or training in Serbia to help them address privacy and AI ethics in classrooms (Danaj et al., 2024; Ignjatović, 2024). As Škobo and Šović (Škobo & Šović, 2025) stress, teacher readiness to use AI is limited not only by missing resources but also by policy delays, infrastructure gaps and weak institutional support. Students exposed to AI tools in schools are rarely able to explain how their data might be used, indicating that classroom integration remains superficial and ethically underdeveloped.

Part of this outcome may reflect the developmental stage of the students. Piaget's model suggests that learners aged 11 to 14 are only beginning to engage with abstract reasoning (McLeod, 2009). Our findings confirm that students often give formal answers without showing deeper understanding. This suggests that teaching strategies need to be carefully scaffolded. If adult support does not match children's developmental level — with simple language, visuals and real-life examples, as Vygotsky's ZPD framework suggests — learning is unlikely to be meaningful. Children may complete surveys filled with technical or legal terms without really knowing what is being asked, pointing to the need for age-appropriate and accessible materials.

Addressing this challenge requires change at both family and school levels. Occasional lessons or abstract talks are not enough to build lasting data literacy. Schools should integrate privacy and ethics into everyday teaching. For example, abstract topics like consent or data sharing can become more relatable through activities such as acting out digital dilemmas (role-plays), discussing common app use situations or walking through the adjustment process of privacy settings in tools students already use. Teachers need training in how to design lessons that make these issues clear, engaging and age-relevant. They should be supported through access to ready-made lesson templates, scenario cards and opportunities to share materials through school networks or online forums.

Parents also have a central role, but they often lack the confidence or knowledge to provide constructive guidance. They need support from schools, policymakers and digital platforms. Schools can provide illustrated guides, short video explainers and conversation starters in order to help families discuss key issues like app permissions, online consent and what it means to "share too much." Home activities might include reviewing app settings together, making a 'family digital contract,' or watching and discussing short clips about online safety. Schools could dedicate part of each parent-teacher meeting to modeling how to talk with children about these issues in a supportive and practical way.

This study has several limitations. First, the sample was drawn from a small number of urban and semi-urban schools in Serbia, so the findings may not apply to rural or ethnically

diverse settings, where access to technology and adult guidance around AI can differ. Second, the findings are based on students' self-reports; although responses were anonymous, younger participants may have misunderstood some questions, given socially desirable answers, or lacked the words to fully explain their experiences. Thirdly, since the study was cross-sectional, the data offer only a snapshot in time. They do not show how children's understanding of privacy might grow or shift as they get older or use AI tools more regularly. Finally, although the questionnaire was carefully designed and showed solid internal consistency, it was not based on existing international scales. This design choice reflected local needs and language but limits comparability with studies from other countries.

Future research should employ longitudinal or mixed-method designs to track how children's views about privacy change as they mature and how sustained adult involvement shapes this process. Qualitative methods such as interviews and group discussions with children might reveal how they understand adult guidance and what kind of advice actually makes sense to them. It would also be useful to test new types of teaching materials that are designed with this age group in mind—short animated videos, simple interactive games or illustrated guides that explain things like consent or data sharing in everyday terms. Teachers might, for example, use storybooks or role-playing games to introduce ideas like digital footprints or online safety. These discussions can be tied to everyday classroom topics using familiar fictional characters or situations — such as a cartoon figure who accidentally overshares online — rather than relying on abstract legal terms. Therefore, collaboration between educators and families, which includes translating abstract concepts into terms that make sense to children — things they encounter in their daily lives — should be prioritized. When done well, this approach could help connect digital literacy with critical thinking, responsible online behavior and even early forms of civic awareness.

Conclusion

This study confirms that the safe and meaningful use of AI in primary education cannot rely on occasional lessons and short-term initiatives. What is needed is a more grounded, long-term approach that combines thoughtful curriculum changes, practical teacher support and meaningful collaboration with families. Although many students do talk with adults about digital tools and risks, these conversations are often too shallow or inconsistent to give them the confidence they need—particularly when it comes to complex issues like data privacy. Digital literacy must be fully integrated into the regular curriculum, not treated as a single topic or limited to IT classes. For younger learners especially, teaching materials need to match their age, language and cognitive development.

At the institutional level, schools need more than just technical checklists. Teachers should have clear, usable guidance on how to choose AI tools responsibly and handle student data safely. But beyond that, schools should promote a shared understanding of what responsible digital behavior looks like, by also making these values visible in the classroom, not just on paper.

The success of AI-related education also depends on treating children as active participants. They should be invited to ask questions, express concerns and reflect critically on their own digital behavior. This kind of digital empowerment, especially when supported at home and in class, is essential for building long-term resilience — not just technical skill.

At the same time, the Serbian education system still faces structural limits. Outdated curricula, gaps in infrastructure and a lack of teacher training in digital ethics make it hard to turn good ideas into everyday practice. Teachers should not be expected to carry this responsibility alone — they must be provided with real preparation, shared resources and institutional trust to take the lead.

References

- Andrić, V. (2025, June 29). Digitalna prava dece: Šta podrazumevaju i ko ih najčešće krši? *Danas*. <https://www.danas.rs/vesti/drustvo/digitalna-prava-dece-sta-podrazumevaju-i-ko-ih-najcesce-krsi/>
- Andries, V. & Robertson, J. (2023). Alexa doesn't have that many feelings: Children's understanding of AI through interactions with smart speakers in their homes. *Computers and Education: Artificial Intelligence*, 5, 1-17. <https://doi.org/10.1016/j.caeai.2023.100176>
- CoSN (2025). *2025 National Student Data Privacy Report*. Consortium for School Networking. <https://www.cosn.org/wp-content/uploads/2025/03/2025-CoSN-National-Student-Data-Privacy-Report-Part-1-Final-031825.pdf>
- Danaj, A., Škorić, J. & Galetin, M. (2024). Comparative analysis of the legal frameworks of the Republic of Serbia and Republic of Albania: The application of Artificial Intelligence and child protection. In M. Počuča (Ed.), *XXI međunarodni naučni skup „Pravnički dani-Prof. dr Slavko Carić „Odgovori pravne nauke na izazove savremenog društva, (Radovi) (pp. 413-425)*. Faculty of Law for Commerce and Judiciary, University of Novi Sad. <https://doi.org/10.5937/PDSC24413D>
- Eisinga, R., Grotenhuis, M.t. & Pelzer, B. (2013). The reliability of a two-item scale: Pearson, Cronbach, or Spearman-Brown?. *International Journal of Public Health*, 58, 637–642. <https://doi.org/10.1007/s00038-012-0416-3>
- Gao, L., Blinder, E. B., Barnes, A., Song, K., Clegg, T., Vitak, J. & Chetty, M. (2025). Creating and Evaluating Privacy and Security Micro-Lessons for Elementary School Children. *arXiv preprint arXiv:2503.07427*. <https://doi.org/10.48550/arXiv.2503.07427>
- Guo, Y. (2021). The Cultural Implications and Ethical Risks of Algorithm Society. *Chinese Book Review*, 9, 45-53. <https://doi.org/10.3969/j.issn.1002-235X.2021.09.006>
- Hao, X., Wang, F. & Qi, C. (2019). The current status and developmental trends of educational artificial intelligence. *Modern Educational Technology*, 2, 12-18.
- Hillman, V., Manolev, J., Johnston, S.K., Kumar, P.C., Martin, F., Zeide, E., Vladova, G. & Lai, R. (2024). Children, Education, and Technologies: Current Debates, Key Concerns, and Future Directions Around Data Privacy, Surveillance, and Datafication. In D. A. Christakis & L. Hale (Eds.), *Handbook of Children and Screens* (pp. 557-567). Springer. https://doi.org/10.1007/978-3-031-69362-5_76
- Hoofnagle, C. J., Van Der Sloot, B. & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1), 65-98. <https://doi.org/10.1080/13600834.2019.1573501>
- Huang, L. (2023). Ethics of artificial intelligence in education: Student privacy and data protection. *Science Insights Education Frontiers*, 16(2), 2577-2587. <https://doi.org/10.15354/sief.23.re202>
- Ignjatović, G. (2024). AI TECHNOLOGIES IN EDUCATION: Regulatory frameworks at the international, regional and national level. *Zbornik radova Pravnog fakulteta u Nišu*, 63(103), 235-260. <https://doi.org/10.5937/zrpf1-55374>
- Jia, K. & Jiang, Y. (2017). Three basic issues of artificial intelligence governance: Technical logic, challenges, and public policy making. *Chinese Public Administration*, 10, 40-45. <https://doi.org/10.3782/j.issn.1006-0863.2017.10.07>

- Li, L., Valdez, J.P.M. & Du, Y. (2025). Digital citizenship education at the early childhood level: how is it implemented? A systematic review. *International Journal of Child Care and Education Policy* 19, 13. <https://doi.org/10.1186/s40723-025-00153-2>
- Liu, S., Liu, S., Sun, J., Shen, X., & Liu, Z. (2021). Key issues in the development of intelligent education. *Distance Education in China*, 4, 69-76. <https://doi.org/10.13541/j.cnki.chinade.2021.04.001>
- Livingstone, S. M. & Blum-Ross, A. (2020). *Parenting for a digital future: How hopes and fears about technology shape children's lives*. Oxford University Press.
- Lupton, D. & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society*, 19(5), 780-794. <https://doi.org/10.1177/1461444816686328>
- Matović, M. & Žunić-Pavlović, V. (2020). Povezanost restriktivnih strategija roditeljskog nadzora i digitalnog nasilja u adolescenciji. *CM: Communication and Media*, 15(47), 35-56. <https://doi.org/10.5937/cm15-27100>
- McLeod, S. (2009). Piaget's Theory and Stages of Cognitive Development. *Simply Psychology*. <https://doi.org/10.5281/zenodo.15241970>
- Muammar, S., Hashim, K. F. B. & Panthakkan, A. (2023). Evaluation of digital competence level among educators in UAE Higher Education Institutions using Digital Competence of Educators (DigComEdu) framework. *Education and Information Technologies* 28, 2485-2508. <https://doi.org/10.1007/s10639-022-11296-x>
- Nešić, A. (2023). Zaštita podataka o deci na internetu. *Savremene studije bezbednosti*, 16(1), 29-48. <https://doi.org/10.5937/ssb202301029N>
- Nguyen, A., Ngo, H. N., Hong, Y., Dang, B. & Nguyen, B. P. T. (2023). Ethical principles for artificial intelligence in education. *Education and Information Technologies*, 28(4), 4221-4241. <https://doi.org/10.1007/s10639-022-11316-w>
- Shi, Y. & Zhou, X. (2022). The debate on the "right to be forgotten" in the era of big data: To be remembered or forgotten? *Editorial Friends*, 12, 88-99. <https://doi.org/10.13786/j.cnki.cn14-1066/g2.2022.12.012>
- Shouli, A., Barthwal, A., Campbell, M. & Shrestha, A. K. (2025). Ethical AI for Young Digital Citizens: A Call to Action on Privacy Governance. *arXiv preprint arXiv:2503.11947*. <https://doi.org/10.48550/arXiv.2503.11947>
- Solberg, J. (2023). Privacy in Early Childhood Education and Care: The Management of Family Information in Parent-Teacher Conferences. *Human Studies*, 47, 367-388. <https://doi.org/10.1007/s10746-023-09683-5>
- Stoilova, M., Livingstone, S. & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age*. Research findings. London School of Economics and Political Science.
- Škobo, M. & Šović, M. (2025). Teachers' perspectives on Chatbots and AI agents in primary and secondary education. *International Journal on Studies in Education*, 7(2), 410-442. <https://doi.org/10.46328/ijonse.352>
- UNESCO. (2022). *Recommendation on the Ethics of Artificial Intelligence*. Available at: <https://unesdoc.unesco.org/ark:/48223/pf0000381137>
- Vartiainen, H., Pope, N., Kahila, J., López-Pernas, S. & Tedre, M. (2025). Classroom Activities and New Classroom Apps for Enhancing Children's Understanding of Social Media Mechanisms. *arXiv preprint arXiv:2501.16494*. <https://doi.org/10.48550/arXiv.2501.16494>
- Wang, Z. (2016). American student data privacy protection legislation and governance frameworks in the era of big data. *International and Comparative Education*, 11, 28-33.

- Wang, G., Zhao, J. & Shadbolt, N. (2019). Are children fully aware of online privacy risks and how can we improve their coping ability? *arXiv preprint arXiv:1902.02635*. <https://doi.org/10.48550/arXiv.1902.02635>
- Williamson, B. (2017). *Big data in education: The digital future of learning, policy and practice*. SAGE.
- Williamson, B. (2019). Datafication of education: a critical approach to emerging analytics technologies and practices. In H. Beetham & R. Sharpe (Eds.), *Rethinking pedagogy for a digital age* (pp. 212-226). Routledge.
- Xue, L. & Zhao, J. (2019). Paths to agile governance: The development of emerging industries and regulatory models. *Chinese Public Administration*, 8, 28-34. <https://doi.org/10.19735/j.issn.1006-0863.2019.08.02>
- Yeşilyurt, E. & Vezne, R. (2023). Digital literacy, technological literacy, and internet literacy as predictors of attitude toward applying computer-supported education. *Education and Information Technologies*, 28(8), 9885-9911. <https://doi.org/10.1007/s10639-022-11311-1>
- Yim, I. H. Y. & Su, J. (2025). Artificial intelligence literacy education in primary schools: a review. *International Journal of Technology and Design Education*, 35, 2175-2204. <https://doi.org/10.1007/s10798-025-09979-w>
- Zhao, H., Jiang, Q. & Zhao, W. (2016). The security of big data-based learning analytics and privacy protection. *Modern Educational Technology*, 26(3), 5-11. <https://doi.org/10.3969/j.issn.1009-8097.2016.03.001>
- Zhao, Z., Xu, F., Gao, F., Li, F., Hou, H. & Li, M. (2021). An evaluation of ethical risks in artificial intelligence. *China Soft Science*, 6, 1-12.

Article received: 22.07.2025.

Updated version received: 07.10.2025.

Accepted for publishing: 08.10.2025.

Milena Škobo

Faculty of Philology, Sinergija University, Bijeljina, Bosnia and Herzegovina
<https://orcid.org/0000-0001-8427-2051>

Milena Šović

Faculty of Economics and Engineering Management, University Business Academy in Novi Sad, Novi Sad, Serbia
<https://orcid.org/0009-0009-5774-5672>



This work is published under the Creative Commons Attribution 4.0 International (CC BY 4.0). It is permitted to copy and distribute the work in all media and formats, to remix, transform, and build upon it for any purpose, including commercial purposes, provided that the original authors are properly credited, a link to the original license is included and it is indicated whether the work has been modified. Users are required to provide a full bibliographic citation of the article published in this journal (authors, title of the work, journal title, volume, issue, pagination), as well as its DOI identifier, and in the case of electronic publication, they are also required to provide an HTML link.