

DIGITALNA PRIVATNOST STUDENATA I PORODICE: ETIČKE DILEME I KRIVIČNOPRAVNA ZAŠTITA U ERI ONLINE OBRAZOVANJA

Dalibor Krstinić¹, Nenad Bingulac², Đorđe Sančanin³, Jelena Matijašević⁴, Sanja Škorić⁵

^{1,2,3,4,5} Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

¹dkrstinic@pravni-fakultet.info, ²nbingulac@pravni-fakultet.info, ³djordje.sancanin@pravni-fakultet.info, ⁴jelena@pravni-fakultet.info, ⁵sanja@pravni-fakultet.info

Kratak sadržaj: Digitalizacija visokog obrazovanja i razvoj online nastave doveli su do toga da se nastavni proces i provera znanja sve češće odvijaju u privatnom prostoru studenata. Time se otvaraju značajna pitanja zaštite digitalne privatnosti, ne samo studenata, već i članova njihove porodice, koji posredno mogu biti izloženi putem video-platформи, snimanja predavanja i sistema nadzora tokom ispita. Rad razmatra etičke dileme koje nastaju u vezi sa granicama institucionalne kontrole i očuvanjem dostojanstva ličnosti, kao i krivičnopravne mehanizme zaštite u situacijama kada povrede privatnosti prerastu u protivpravna snimanja, neovlašćeno objavljivanje podataka ili digitalno uznemiravanje. Zaključuje se da se kvalitet visokog obrazovanja u tehnološki intenzivnom okruženju ne može posmatrati isključivo kroz dostupnost i efikasnost, već i kroz standarde zaštite privatnosti, etičku legitimnost digitalnih praksi i delotvornu pravnu zaštitu studenata i njihove porodice.

Ključne reči: digitalna privatnost, online obrazovanje, studenti, porodica, etika, krivičnopravna zaštita

DIGITAL PRIVACY OF STUDENTS AND THEIR FAMILIES: ETHICAL DILEMMAS AND CRIMINAL LAW PROTECTION IN THE ERA OF ONLINE EDUCATION

Abstract: The digitalization of higher education and the expansion of online learning have increasingly shifted teaching and assessment processes into students' private homes. This development raises important questions regarding the protection of digital privacy, not only of students, but also of their family members, who may become indirectly exposed through video platforms, lecture recordings, and remote proctoring systems. The paper examines ethical dilemmas related to the limits of institutional control and the protection of human dignity, as well as criminal-law mechanisms applicable when privacy violations escalate into unlawful recording, unauthorized data disclosure, or digital harassment. It is argued that the quality of higher education in a technologically intensive environment cannot be assessed solely through accessibility and efficiency, but must also include privacy standards, ethical legitimacy of digital practices, and effective legal protection for students and their families.

Key Words: digital privacy, online education, students, family, ethics, criminal-law protection

1. UVOD

Digitalizacija visokog obrazovanja, naročito nakon pandemijskog perioda, dovela je do toga da se značajan deo nastave i provere znanja odvija u online okruženju. Time se obrazovni proces iz institucionalnog prostora prenosi u privatni dom studenta. Iako ovakav model povećava dostupnost, fleksibilnost i kontinuitet nastave, istovremeno otvara pitanje granica institucionalne kontrole, zaštite dostojanstva ličnosti i digitalne privatnosti.

Posebna specifičnost online obrazovanja jeste da članovi porodice, iako nisu učesnici nastavnog procesa, mogu postati posredno izloženi: kroz video-platформи, snimanje predavanja, deljenje ekrana, kao i kroz sisteme daljinskog nadzora ispita (remote proctoring). U tom smislu, digitalna privatnost postaje pitanje ne samo studentskih prava, već i zaštite porodičnog života.

2. DIGITALNA PRIVATNOST U ONLINE NASTAVI: OPSEG I RIZICI

Digitalna privatnost u visokom obrazovanju obuhvata zaštitu podataka o ličnosti, tajnost komunikacija, audio/video identitet, kao i pravo na nepovredivost privatnog i porodičnog života. U praksi, tokom online nastave i ispita obrađuju se identifikacioni podaci (ime, prezime, broj indeksa), kontakt podaci, podaci o uspehu, ali i audio/video snimci i podaci o uređaju i mreži. U pojedinim sistemima, naročito kod proctoring rešenja, mogu se obrađivati i biometrijski podaci (prepoznavanje lica).

Rizici po privatnost posebno su izraženi u situacijama kada kamera obuhvata deo doma: prostoriju, lične predmete, porodične fotografije, dokumenta ili prisustvo drugih osoba. Članovi porodice mogu biti snimljeni ili indirektno identifikovani, iako nisu dali pristanak. Ovo je naročito problematično kada se u pozadini nalaze maloletna deca, čime se

otvara pitanje najboljeg interesa deteta i zaštite porodičnog života.

3. ETIČKE DILEME: PROPORCIONALNOST, PRISTANAK I JEDNAKOST

Etika u visokom obrazovanju zahteva da se digitalne tehnologije koriste odgovorno, uz poštovanje dostojanstva studenata i principa jednakosti. Prva ključna dilema odnosi se na proporcionalnost: univerzitet ima legitiman interes da obezbedi integritet ispita, ali invazivne mere nadzora (snimanje, praćenje pogleda, skeniranje prostorije, detekcija zvuka) mogu biti prekomerne u odnosu na cilj. Time se student tretira kao potencijalni prekršilac, što narušava akademsko poverenje.

Druga dilema odnosi se na informisani pristanak. U praksi, student često nema realnu mogućnost izbora, jer je prihvatanje uslova platforme preduslov za polaganje ispita. Takav „pristanak“ ima formalni karakter i ne predstavlja slobodnu odluku. Treća dilema je pitanje jednakosti: ne poseduju svi studenti adekvatne uslove (miru prostoriju, stabilan internet, kvalitetnu opremu), pa se rizik povrede privatnosti neravnomerno raspodeljuje.

4. KRIVIČNOPRAVNA ZAŠTITA U SLUČAJEVIMA POVREDE PRIVATNOSTI

Kada povrede digitalne privatnosti prevaziđu nivo akademske ili građanskopravne odgovornosti, relevantna postaje krivičnopravna zaštita. U online obrazovanju mogu nastati situacije protivpravnog snimanja i objavljivanja sadržaja, neovlašćenog prikupljanja i obrade podataka, hakovanja platformi i curenja podataka, kao i digitalnog uznemiravanja studenata ili članova njihove porodice.

Krivični zakonik Republike Srbije predviđa više krivičnih dela koja mogu biti primenljiva, uključujući: neovlašćeno prisluškivanje i snimanje, neovlašćeno fotografisanje, neovlašćeno objavljivanje i prikazivanje tuđeg spisa, portreta i snimka, neovlašćeno prikupljanje ličnih podataka, kao i krivična dela protiv bezbednosti računarskih podataka. Digitalno uznemiravanje može se manifestovati kroz cyberbullying, doxxing ili širenje kompromitujućih snimaka, sa ozbiljnim posledicama po čast, ugled i mentalno zdravlje žrtava.

Posebno osetljive situacije nastaju kada kompromitujući sadržaj obuhvati članove porodice, naročito maloletnike. U takvim slučajevima, delotvorna pravna zaštita zahteva koordinaciju između visokoškolskih ustanova, nadležnih organa i regulatornih tela, kao i jasno definisane procedure prijavljivanja i reagovanja.

Uloga Poverenika za informacije od javnog značaja i zaštitu podataka o ličnosti je posebno značajna, jer studenti mogu tražiti zaštitu svojih prava, uvid u podatke, kao i brisanje ili ograničenje obrade u slučajevima kada se podaci obrađuju suprotno zakonu. Time se jača institucionalna kontrola nad praksama u online obrazovanju. [3]

Na nivou akademske etike, poželjno je da se pre uvođenja invazivnih proctoring rešenja sprovede procena uticaja na privatnost (DPIA), uz uključivanje studentskih predstavnika. Takav pristup povećava legitimnost odluke i doprinosi izgradnji poverenja u digitalnu transformaciju visokog obrazovanja. [3][4][5]

Jedan od važnih preventivnih mehanizama jeste tehnički dizajn sistema („privacy by design“). To podrazumeva da se od početka biraju platforme koje omogućavaju minimizaciju snimanja, isključenje nepotrebnih funkcija, lokalno čuvanje podataka i jasne administratorske logove. Na taj način se rizici smanjuju pre nego što dođe do povrede prava. [5]

U praksi se pojavljuje i pitanje sekundarne upotrebe snimaka. Iako se snimanje predavanja ili ispita formalno vrši radi nastavnog procesa, postoji rizik da se materijal koristi u druge svrhe (interni nadzor, disciplinski postupci, marketinška promocija, pa čak i neformalno deljenje u zatvorenim grupama). Upravo zbog toga, univerziteti moraju jasno ograničiti svrhu obrade i rokove čuvanja, uz strogu kontrolu pristupa. [3][5]

Evropski standardi zaštite privatnosti, posebno kroz praksu Evropskog suda za ljudska prava, naglašavaju da pravo na privatnost obuhvata i zaštitu identiteta, reputacije i porodičnog života. U tom okviru, svako zadiranje u privatni prostor mora biti zasnovano na legitimnom cilju, uz nužnost i proporcionalnost mere. Ovi standardi su relevantni i za visokoškolske ustanove koje uvode digitalne tehnologije. [6]

Sa stanovišta krivičnopravne zaštite, posebno je važno naglasiti da digitalni tragovi (snimci, screenshot-ovi, logovi) imaju trajni karakter i mogu biti distribuirani velikom brzinom. Čak i kratkotrajno objavljivanje kompromitujućeg sadržaja može izazvati dugoročne posledice po ugled studenta i njegove porodice. U tom smislu, krivično pravo zadržava ulogu ultima ratio, ali u digitalnom prostoru dobija na praktičnom značaju. [2]

U akademskoj zajednici, poverenje između nastavnika i studenata predstavlja pretpostavku etički održivog obrazovanja. Prekomerna kontrola i stalni nadzor mogu narušiti taj odnos, stvarajući atmosferu sumnje i straha. Stoga je potrebno razvijati modele provere znanja koji kombinuju integritet i zaštitu privatnosti, kao što su usmeni ispiti, projektni zadaci ili otvorene forme testiranja. [4]

U poređenju sa klasičnim ispitivanjem u prostorijama fakulteta, remote proctoring pomera teret organizacije na studenta: on obezbeđuje prostor, opremu, tišinu i tehničke uslove. Ovakav model može dovesti do indirektno diskriminacije studenata koji žive u većim porodicama, u manjim stanovima ili u socio-ekonomski nepovoljnijim uslovima. [1][4]

U praktičnom smislu, studenti u online okruženju često nisu svesni punog obima obrade podataka. Pored video-snimka, platforme mogu prikupljati i metapodatke (vreme pristupa, IP adresu, identifikatore uređaja, logove aktivnosti), što povećava rizik od profilisanja i sekundarne upotrebe podataka. Zbog toga je transparentnost obrade podataka ključni element kvaliteta digitalizovanog obrazovanja. [3][5]

5. ZAKLJUČAK

Digitalna transformacija visokog obrazovanja predstavlja važan korak ka modernizaciji i povećanju dostupnosti nastave, ali istovremeno donosi rizike po privatnost i etičku legitimnost obrazovnih praksi. Kvalitet visokog obrazovanja u tehnološki intenzivnom okruženju ne može se posmatrati samo kroz efikasnost i dostupnost, već mora uključiti i standarde zaštite digitalne privatnosti studenata i njihove porodice.

Neophodno je da visokoškolske ustanove primenjuju princip minimizacije podataka, obezbede transparentnost, realne alternative studentima i jasne politike privatnosti. Krivičnopravna zaštita postaje relevantna kada povrede privatnosti prerastu u protivpravna snimanja, neovlašćeno objavljivanje ili digitalno uznemiravanje. Samo uz ovakav pristup digitalna transformacija može biti održiva i etički prihvatljiva.

6. LITERATURA

- [1] *Ustav Republike Srbije*, Službeni glasnik RS, br. 98/06, 115/21.
- [2] *Krivični zakonik Republike Srbije*, Službeni glasnik RS, br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19, 27/21 – odluka US, 62/21, 16/23.
- [3] *Zakon o zaštiti podataka o ličnosti*, Službeni glasnik RS, br. 87/18.
- [4] *Zakon o visokom obrazovanju*, Službeni glasnik RS, br. 88/17, 27/18 – dr. zakon, 73/18, 67/19, 6/20 – dr. zakoni, 11/21 – autentično tumačenje, 67/21, 67/21 – dr. zakon, 76/23.
- [5] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016* (General Data Protection Regulation – GDPR).
- [6] *European Convention on Human Rights*, Article 8.