# ANALIZA APLIKACIJA ZA UČENJE NA DALJINU IZ PERSPEKTIVE ZAŠTITE PRIVATNOSTI DJECE

Politiscope, siječanj 2021.

# UVOD

Tijekom prvog vala pandemije Korona virusa u Hrvatskoj, u razdoblju od ožujka do lipnja 2020. godine, sve škole u Hrvatskoj u potpunosti su prešle na model održavanja nastave na daljinu. Takav model podrazumijevao je i korištenje softverskih alata za održavanje nastave putem interneta, kako za gledanje snimljenih video lekcija, tako i za video-konferencijsku komunikaciju učenika s nastavnicima. U siječnju 2021., u klupe su se vratili učenici od prvog do četvrtog razreda osnovnih škola te maturanti s iznimkom onih u Istarskoj i Primorsko-goranskoj županiji. Ministar znanosti i obrazovanja Radovan Fuchs izjavio je da se nada kako će se svi učenici u škole vratiti početkom veljače, ako se epidemiološka situacija poboljša.

Izostanak standardiziranog pristupa u određenju alata za online održavanje nastave rezultirao je šarolikom primjenom alata koji se značajno razlikuju s aspekta zaštite privatnosti djece. Korištenjem tzv. big tech (Amazon, Apple, Google, Facebook, Microsoft) alata za nastavu, podaci učenika postaju dio nezakonitog i netransparentnog sustava stvorenog primarno za programirani sustav aukcija u svrhu prikaza reklama. Tako je, primjerice, Google 2019. godine platio 170 milijuna dolara u sklopu nagodbe u sporu koji je protiv njega pokrenut zbog nezakonitog prikupljanja i dijeljenja podataka djece putem servisa YouTube, bez pristanka roditelja.

Ministarstvo znanosti i obrazovanja, nadležne agencije i ustanove izdali su niz smjernica, uputa i drugih akata koji se tiču online održavanja nastave. No, iznimno je zabrinjavajuće što se niti jedan dokument ne osvrće na zaštitu privatnosti učenika u obrazovnom procesu smještenom u potpuno novo digitalno okruženje. Učenje na daljinu je trenutna potreba uzrokovana pandemijom Corona virusa, no nije nimalo nezamislivo da se u bližoj budućnosti, nakon završetka pandemije, određeni dio nastave održava online putem. Zbog toga je od iznimne važnosti ukazati na adekvatne mjere zaštite privatnosti i osobnih podataka djece i nastavnika prilikom korištenja različitih softverskih alata za video i glasovne pozive u svrhu provođenja nastave.

Ova analiza je namijenjena širokom krugu dionika koji sudjeluje u oblikovanju obrazovnog procesa na razini pojedinih škola (nastavnici, profesori, ravnatelji, roditelji i đaci) te donositeljima odluka i službenicima u izvršnim tijelima u području obrazovanja (ministarstva i nadležne agencije). Analiza će istražiti prakse provedbe nastave na daljinu u Hrvatskoj od ožujka do lipnja 2020. godine te analizirati pet najpopularnijih aplikacija iz perspektive zaštite privatnosti i osobnih podataka. Cilj ove analize je osvijestiti relevantne dionike o zaštiti privatnosti i osobnih podataka djece u digitalnom okružju, utjecati na odluke o odabiru alata za učenje na daljinu te dati provedive preporuke za unaprjeđenje postojećih praksi.

# UČENJE NA DALJINU U HRVATSKOJ

Nastava na daljinu u Hrvatskoj je započela 16. ožujka 2020. godine. U procesu koordinacije kojeg je vodilo Ministarstvo znanosti i obrazovanja (dalje u tekstu: MZO), sudjelovali su Hrvatska akademska i istraživačka mreža (dalje u tekstu: CARNET), Sveučilišni računski centar, Agencija za odgoj i obrazovanje, Agencija za strukovno obrazovanje i obrazovanje odraslih te Agencija za mobilnost i programe EU.

Akcijski plan za provedbu nastave na daljinu (dalje u tekstu: Akcijski plan) opširan je dokument MZO-a s popisom najvažnijih koraka i postupaka provedenih tijekom nastave na daljinu u školama i visokim učilištima (u periodu ožujak-lipanj 2020). Akcijski plan navodi da su u ožujku 2020. sljedeća tehnička rješenja dostupna putem platforme AAI@Edu.Hr preporučena školama za provedbu nastave na daljinu: Moodle, Teams, Yammer, Google Classroom, Edmodo.

CARNET je na podstranici "Nastava na daljinu" objavio informacije, savjete, preporuke i upute o odabiru i korištenju tehnoloških rješenja za provođenje nastave na daljinu. Osim toga, CARNET je objavio i dokument "Online sustavi za organizaciju i provođenje nastave na daljinu", u kojem objašnjavaju najvažnije značajke, prednosti i mane preporučenih alata. Dokument daje preporuke sljedećih alata za organizaciju i provođenje nastave na daljinu: Google Classroom (i pripadajući alat Google Meet), MS Teams, Yammer, CARNET Loomen i Zoom.

Preporučeno je da škola odabere platformu u kojoj će raditi i da u njoj rade svi nastavnici, odnosno učenici. Nacionalni raspored i videolekcije za osnovno i srednje obrazovanje kontinuirano su se objavljivali na stranici Škola za život.

Potrebno je istaknuti kako su se u provedbi nastave na daljinu koristile i brojne druge aplikacije osim onih preporučenih. Akcijski plan MZO-tako ističe brojne aplikacije koje su se koristile u nastavi hrvatskog jezika i kulture: razni programi za videokonferencije (BIGBLueButton, Skype), LearningApps, WordWall, Youtube, Socrative, Zoom, Firefox, Libre Office 6.4. Google docs (formulari u obliku nastavnog materijala), Google Forms, Jigsaw planet, LearningApps.org. i dr.

Odluka o izboru aplikacija za analizu donesena je na temelju gore istaknutih preprouka MZO-a i CARNET-a. Izbor aplikacija je dodatno korigiran nakon direktnih razgovora s manjim brojem nastavnika i ravnatelja koji imaju izravan uvid u najčešće korištene aplikacije. Izuzev aplikacija za koje je zaključeno da se najčešće koriste (Loomen, Microsoft Teams, Google Classroom, Zoom), u analizu smo uključili i BigBlueButton, aplikaciju za koju Akcijski plan MZO navodi da se koristila u nastavi hvatskog jezika i kulture, koja je ujedno i primjer dobre prakse u zaštiti privatnosti učenika.

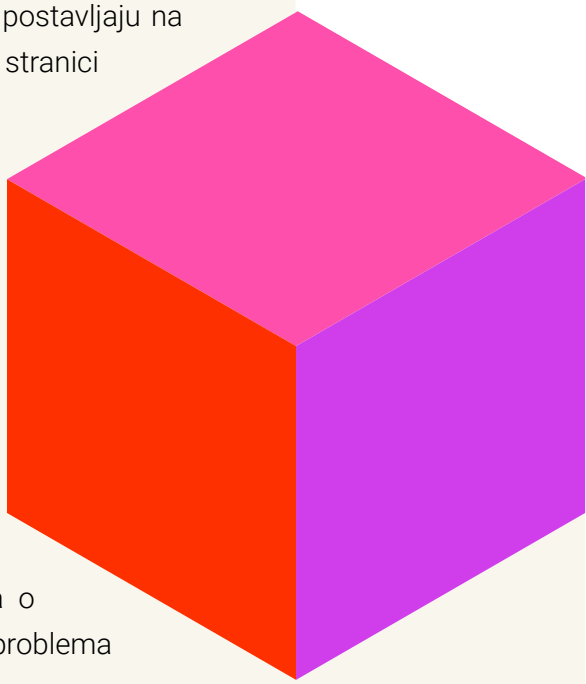
# UČENJE NA DALJINU I ZAŠTITA PRIVATNOSTI

U Akcijskom planu Ministarstva kategorizirane su potrebe nastavnika za buduća usavršavanja u različitim područjima te se među njima spominje i "zaštita podataka i provedba Opće uredbe o zaštiti podataka u nastavi na daljinu kad je riječ o maloljetnim osobama". Nije detaljnije objašnjeno kako će se nastavnici usavršavati u navedenom području, a riječ je ujedno o jedinom paragrafu u čitavih 38 stranica akcijskog plana u kojem se spominje zaštita osobnih podataka ili privatnosti učenika. U CARNET-ovom dokumentu "Online sustavi za organizaciju i provođenje nastave na daljinu" privatnost i zaštita podataka također nisu uzeti u obzir kao značajke bilo kojeg alata ili sustava.

S jedne strane, imamo neadekvatan pristup izvršnih vlasti u području obrazovanja koji je ponajviše vidljiv u izostanku edukacije nastavnog osoblja. Naime, navedene digitalne alate je potrebno podešavati za online nastavu, učenicima je potrebno objasniti osnove rada u novim alatima te ih upoznati s mjerama koje trebaju poduzeti s ciljem maksimalne zaštite vlastite sigurnosti i privatnosti. S druge strane, sasvim očekivano, izostalo je proaktivno djelovanje Agencije za zaštitu osobnih podataka (dalje u tekstu: AZOP). AZOP je propustio dati ciljane i jasne preporuke vezane uz nastavu na daljinu te kroz direktno uključenje pružiti podršku obrazovnim institucijama koje su koordinirale process. Ovaj propust institucionalne razine upravljanja rezultat je niske osviještenosti javnog sektora o privatnosti i digitalnim pravima građana.

Nije se dogodio niti najosnovniji minimum proaktivnog postupanja od strane institucija, koji bi potaknuo nastavnike da razmišljaju o nekim osnovnim pitanjima vezanima uz zaštitu privatnosti djece. Tko sve prilikom online učenja ima pristup podacima djece, kako se ti podaci koriste i s kim se dijele? Ostaju li primjerice video snimke, poslane poruke te podaci o korištenju određenog alata sačuvani i koliko dugo? Kombiniraju li se ti podaci s drugim podacima učenika s ciljem stvaranja profila?

Plastičan, ali vrlo jasan primjer nedostatka svijesti o privatnosti unutar hrvatskog obrazovnog sutava je web stranica **www.skolazazivot.hr**, koja je polazišna točka svakom učeniku za informacije i pristup sadržajima online nastave. Naime, stranica sadrži čak četiri trackera koji se bez davanja privole postavljaju na uređaj svakog posjetitelja te podatke o ponašanju učenika na stranici dijele s Facebookom, Googleom te tvrtkom ShareThis.



# ANALIZA APLIKACIJA

Za svaku od odabranih aplikacija provest će se analiza javno dostupnih obavijesti o privatnosti te informacija o opsegu podataka koje prikupljaju i dijele s trećim stranama, analiza korištenih tehnologija za praćenje korisnika, navoda o informacijskoj sigurnosti softvera te dosadašnjih propusta i problema povezanih sa zaštitom privatnosti.
Uz nalaze nastale prilikom korištenja aplikacija i analize javno dostupnih obavijesti o privatnosti, uključeni su i nalazi relevantnih analiza koje su proveli: **Privacy Common Sense**, **Freedom of the Press** te **nizozemsko nadzorno tijelo za zaštitu podataka**.

## 1. LOOMEN

**Prilikom izrade ove analize nažalost nismo imali priliku pristupiti sučelju za učenike CARNET-ove platforme Loomen te direktno proučiti način na koji funkcionira u praksi: koje osobne podatke prikuplja, sadrži li dodatne trackere, prenosi li podatke trećim stranama i slično. Proučili smo javno dostupnu Obavijest o privatnosti platforme, koja daje osnovne informacije o obradama podataka te ukazuje na niz problematičnih praksi te potencijalno kršenje nekoliko osnovnih načela Opće uredbe o zaštiti podataka. Analiza službene platforme CARNET-a doprinosi postojećem dojmu kako je javnim tijelima privatnost učenika potpuno irelevantna stvar.**

U nastavku ističemo neke od ključnih manjkavosti **Obavijesti o privatnosti platforme**:

- Kod stavke razdoblja pohrane osobnih podataka, ističe se kratka izjava: “Podaci o korisnicima su trajno pohranjeni u sustavu Loomen.” Nije jasno zašto bi se svi podaci trajno zadržavali: Zakon o odgoju i obrazovanju u osnovnoj i srednjoj školi te prateći pravilnici (poput Pravilnika o pedagoškoj dokumentaciji i evidenciji te javnim ispravama u školskim ustanovama) jasno definiraju periode zadržavanja za pojedine tipove dokumentacije – u navedenim zakonskim te podzakonskim aktima nismo pronašli zakonsku osnovu da svi podaci prikupljeni putem Loomena budu sačuvani zauvijek.

- Potencijalno je problematičan dio s korištenjem Google Drive sustava unutar aplikacije. U ovakvim situacijama postoji mogućnost direktnog prikupljanja podataka o korisniku iz Loomena, koje Google zatim može kombinirati s ostalim podacima koje posjeduje o pojedinom korisniku, u svrhu stvaranja profila za oglašavanje. U ovom trenutku ujedno je upitna i zakonitost takve obrade podataka, budući da korištenje Drivea podrazumijeva transfer podataka u SAD koji je nakon **Schrems 2 presude Suda Europske Unije** – nezakonit.

- Obavijest o privatnosti spominje samo jedan dio prava koje GDPR garantira ispitanicima – pa tako propušta navesti da korisnici u određenim situacijama imaju pravo na: ispravak netočnih podataka, brisanje osobnih podataka, ograničavanje obrade koji se odnose na ispitanika, prava na ulaganje prigovora na obradu te pravo na prenosivost podataka.

- Sama podstranica Loomena koja služi za prijavu u sustav koristi kolačiće Google Analyticsa koji se pokreću bez davanja privole – što je nezakonita praksa prema Zakonu o elektroničkim komunikacijama. Istovremeno, obavijest o privatnosti ne sadrži nikakve informacije o kolačićima ili drugim kategorijama trackera koje stranica sadrži.

Dakle, već sama analiza Obavijesti o privatnosti ukazuje da Loomen krši veći broj osnovnih načela Opće uredbe o zaštiti podataka (načelo transparentosti sigurno, a vrlo vjerojatno i načelo zakonitosti obrade podataka te načelo poštenosti). Uzimajući u obzir navedene manjkavosti, ne preporuča se korištenje platforme Loomen.

## 2. TEAMS

**Microsoftov Teams je pouzdan i siguran servis u smislu informacijske sigurnosti, no prikuplja preširok opseg osobnih podataka bez jasne svrhe te pravne utemeljenosti, a podatke kupuje i od trećih strana. Uz sve navedeno, koristi tehnologije za praćenje na vlasitim servisima, ali i tuđim web stranicama.**

Teams nudi dvofaktorsku autentifikaciju, jamči ugovorne sigurnosne zaštite, koristi najbolje dostupne prakse informacijske sigurnosti te ažurno obaviještava korisnike u slučaju incidenta s podacima. Platforma nudi enkripciju u prijenosu, no nema end-to-end enkripciju.

ŠTO JE END-TO-END ENKRIPCIJA?

End-to-end enkripcija (E2EE) najsigurnija je razina zaštite online komunikacije: kada se koristi, isključivo pošiljatelj i primatelj mogu pročitati, poslušati ili pogledati sadržaj koji je poslan – nitko drugi ne može pristupiti tom sadržaju, pa ni tvrtka koja je vlasnik određene aplikacije.
Kod usluga koje ne uključuju E2EE, tvrtka može pristupiti sadržaju komunikacije, budući da ima ključeve za "dekripciju" - kod E2EE, sadržaj razgovora je zaključan pomoću kriptografske šifre koju imaju isključivo pošiljatelj i primatelj. Enkripcija i dekripcija poslanog te primljenog sadržaja događaju se u potpunosti na uređaju korisnika.

Osim toga, Microsoft svojim korisnicima nudi *privacy dashboard* značajku (kontrolna ploča za privatnost), putem koje korisnici mogu kontrolirati dio podataka koje tvrtka obrađuje prilikom korištenja Microsoft računa. Microsoft općenito zadržava podatke korisnika 90 dana nakon brisanja računa – nakon čega je račun onemogućen i svi prateći podaci obrisani. Microsoft jamči ostvarenje svih GDPR-om zajamčenih prava ispitanika svojim korisnicima. Moguće je pristupiti sastanku na Teamsu bez izrade računa, što je primjer dobre prakse.

Unatoč kvalitetnoj informacijskoj sigurnosti i mogučnošću upravljanja privatnosti unutar aplikacije, najveći problem s ovom aplikacijom je količina osobnih podataka koja se prikuplja te izrada profila korisnika. **Obavijesti o privatnosti** ističe niz podataka koji se prikupljaju, iako nije uvijek potpuno jasno u koju svrhu: kontakti, demografski podaci, glasovni podaci, metapodaci o slikama. U određenim situacijama mogu se čak prikupljati i geolokacijski, zdravstveni te bihevioralni podaci. Dodatno tome, Microsoft kupuje podatke o svojim korisnicima od trećih strana i kombinira ih s podacima koje već posjeduje. Tako, na primjer, od *data brokera* kupuje demografske podatke svojih korisnika koje kombinira s vlastitim podacima u svrhu izgradnje što preciznijeg profila korisnika. Nije jasno da li tvrtka prikupljene podatke o vlastitim korisnicima ujedno prodaje trećim stranama.

U marketinške svrhe, Microsoft koristi tehnologije za praćenje (trackere) na vlastitim servisima, ali i web stranicama te servisima trećih strana, gdje ujedno prikazuje targetirane reklame korisnicima.

Iako se svi podaci brišu 90 dana nakon brisanja računa te postoji mogućnost upravljanja privatnošću unutar aplikacije, Teams nije servis koji može dobiti preporuku za korištenje iz perspektive zaštite privatnosti. Štoviše, zbog prikupljanja prevelike količine podataka, povezivanja s podacima kupljenih od trećih strana te zbog korištenja tehnologija za praćenje, Politiscope daje preporuku o potpunom izbjegavanju korištenja ove aplikacije.

# 3. GOOGLE CLASSROOM

**Google je dokazano jedan od najvećih kršitelja naše privatnosti u digitalnom okružju koji danas postoje. Iako možemo biti sigurni da mnogo ulažu u sigurnost svojih servera, ne čini se da namjeravaju prestati s nezakonitim praksama koje se odnose na prikupljanja prevelike količine podataka koje koriste za čitav niz netransparentnih svrha. Unatoč činjenici da njihovi servisi namijenjeni učenicima imaju dodatne kontrole privatnosti, važno je razumjeti da one vrijede isključivo za uži set aplikacija koje se koriste u obrazovanju. Ostali Google alati nastavljaju pratiti učenike, prikupljaju detaljne podatke o njihovom korištenju te ih profilirati u marketinške svrhe.**

Jedan od najvećih tehnoloških divova nedvojbeno ozbiljno ulaže u infrastrukturu te sigurnost vlastitih servera. Njihovi sistemi su među najsigurnijima, implementiraju najviše industrijske standarde i procedure kako bi osigurali najvišu razinu sigurnosti podataka korisnika te onemogućili neovlašteni pristup i korištenje podataka. Iako s visokom razinom povjerenja možemo tvrditi kako treće neovlaštene strane neće imati pristup podacima učenika, daleko je veći problem što s tim podacima radi sam Google.

Ne možemo zanemariti činjenicu da je riječ o jednom od najvećih kršitelja naše privatnosti uopće, tvrtki koja je dobila **najviše upravne novčane kazne** za kršenje Opće uredbe o zaštiti podataka otkad je Uredba stupila na snagu, i to zbog nedovoljne transparentnosti oko toga što radi s podacima te nezakonitog traženja privole. Osim toga, 2019. godine Google je i u SAD-u platio **170 milijuna dolara** kako bi se nagodio na sudu u tužbi prema kojoj je njihov servis YouTube neovlašteno prikupljao osobne podatke djece bez privole roditelja. Državni tužitelj američke savezne države New Mexico je u veljači podignuo **tužbu protiv tvrtke**, tvrdeći da Google prikuplja podatke o lokaciji učenika, njihove lozinke, povijest stranica koje su posjetili, pretrage na Googleu i Youtubeu, listu kontakata te glasovne zapise. Također tvrdi i da je Google do 2014. godine iščitavao sadržaj e-mailova učenika te tako izvučene informacije koristio za reklamne svrhe.

Classroom, kao servis namijenjen djeci, nudi nekoliko dodatnih kontrola te pravila koja se odnose na privatnost. Ono što znamo je da servis u određenim situacijama može prikupljati geolokacijske podatke korisnika, zdravstvene podatke, bihevioralne podatke te osjetljive kategorije podataka. Svi ovi podaci mogu biti korišteni za kreiranje profila učenika. Iako Google ističe kako "ne prikupljaju niti koriste podatke učenika za reklamne svrhe niti kreiranje reklamnih profila" – čini se da ta pravila vrijede isključivo za korištenje aplikacija u sklopu samog Classroma. Čim učenik koristi neki drugi servis, čak i dok je ulogiran u Google račun namijenjen edukaciji, njegovi podaci mogu biti prikupljani, sačuvani te profilirani u različite svrhe. Drugim riječima, učenik koji koristi YouTube, Google Maps ili Google Books više nije zaštićen strogim pravilima Google Classrooma. Naime, ti servisi prikupljaju podatke učenika, baš kao i bilo kojeg drugog korisnika, te ih obrađuju u svrhu stvaranja marketinškog profila kojem se serviraju targetirane reklame.

Dok Google u svojim obavijestima o privatnosti jasno navodi sva prava koja ispitanicima jamči GDPR, u praksi se ostvarenje tih prava pokazalo upitnim.

Zbog svega navedenog, Politiscope izdaje izričitu preporuku o nekorištenju aplikacije u provedbi nastave na daljinu.

# 4. ZOOM

**Najpopularniji video-konferencijski alat u 2020. godini imao je eksplozivni rast korisnika za vrijeme početka pandemije, uslijed kojeg su iskusili niz skandala vezanih uz ozbiljne propuste u zaštiti sigurnosti i privatnosti korisnika. U međuvremenu su se potrudili ispraviti neke od propusta i Zoom je danas nešto sigurniji za korištenje, no još uvijek ne ispunjava standarde potpune zaštite privatnosti korisnika.**

Zoom školama nudi mogućnost korištenja posebne verzije softvera – Zoom for Education, koja ima sigurnije prakse zaštite privatnosti koje su opisane u **K-12 School Privacy izjavi**. Ističemo kako korištenje standardne verzije softvera nudi značajno slabiju razinu zaštite privatnosti i sigurnosti učenika i nastavnika.

Zoom koristi neke od najboljih praksi industrije za zaštitu sigurnosti, dok su svi podaci u prijenosu enkriptirani. Nakon skandala oko lažnog marketinga end-to-end enkripcije, Zoom je odnedavno uveo upravo tu, najvišu razinu enkripcije svih razgovora. Iako je ograničena samo za neke verzije te ponekad zahtjeva dodatan trud prilikom podešavanja aplikacije, uvođenje end-to-end enkripcije treba pohvaliti kao pozitivan pomak.

Nije se pouzdano moglo utvrditi da li Zoom podatke svojih korisnika prodaje trećim stranama ili ne. Zoom plaćenim korisnicima, pa tako i korisnicima verzije za škole, omogućuje biranje servera putem kojih će se prenositi podaci tijekom njihovog razgovora, što omogućuje odabir servera u EU. Ovo omogućava izbjegavanje prijenosa podataka u SAD, koji je prema Schrems 2 presudi nezakonit, budući da prema američkim zakonima, državne sigurnosne agencije mogu imati pristup sadržaju komunikacije.

Tvrtka prikuplja podatke o geolokaciji, pozivima, kao i metapodatke načinjene tijekom korištenja aplikacije. Zoom tvrdi kako više ne dijele podatke korisnika s Facebookom i Linkedinom, dok izričito ističe da verzija softvera za škole ne koristi prikupljene podatke u marketinške ili reklamne svrhe. Isto, doduše, navode i za svoje intrenet stranice, iako sadrže

niz marketinških trackera koji se pokreću bez privole, stoga postoji ozbiljna sumnja u navedene tvrdnje.

Zoom je danas definitivno sigurniji za korištenje nego početkom 2020. godine, pogotovo nakon uvođenja najviše razine enkripcije svih razgovora. No, ostaju otvorene dvojbe oko dijeljenja podataka s trećim stranama u marketinške svrhe, zbog čega ga ne preporučamo za korištenje.

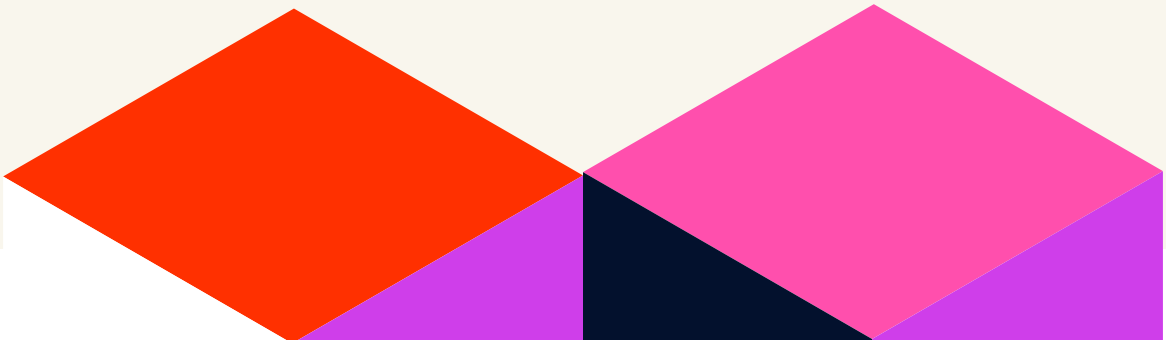
# 5. BIG BLUE BUTTON

**Open source rješenje Big Blue Button ujedno podrazumijeva uspostavljanje servisa na serveru škole (self-hostanje) - na ovaj način škole same kontroliraju koje podatke prikupljaju te pišu vlastitu politiku privatnosti. Dakle, privatnost učenika ne ovisi o niti jednoj trećoj strani. Uzimajući u obzir i jednostavnost korištenja aplikacije za učenike, BigBlueButton je jedina analizirana aplikacija kojoj Politiscope daje snažnu preporuku za korištenje u provedbi nastave na daljinu.**

Ovaj video konferencijski sustav otvorenog koda trebao bi biti postavljen na vlastite servere edukacijskih ustanova kako bi se koristio. Iako se radi o potencijalno kompliciranijem rješenju za provedbu školama, ono ujedno omogućuje kontrolu nad osobnim podacima i značajno veću mogućnost zaštite privatnosti. Škole mogu biti sigurne da softver ne obrađuje podatke djece u vlastite svrhe niti ih dijeli s trećim stranama. Istovremeno, za učenike je korištenje servisa iznimno jednostavno. Sve se odvija u njihovom internetskom pregledniku *(web browseru)* te za pristup nastavi ne moraju izvršiti posebne instalacije niti kreirati nove račune.

Open source kod osigurava maksimalnu transparentnost i povjerenje u softver jer osnovu javno dostupnog koda može pregledati bilo tko, bilo kada. Budući da postoji velika baza korisnika i angažiranih stručnjaka, kod je dubinski testiran i pouzdan, dok se sigurnosne rupe otklanjaju redovitim provjerama. Iako podržava enkripciju u prijenosu, platforma nema i najvišu razinu end-to-end enkripcije.

Kod softvera postavljenog na vlastitim serverima, škole ne ovise o pružatelju usluge, same imaju priliku odlučiti koje podatke o korištenju aplikacije žele zadržati te napisati vlastitu politiku privatnosti o načinu na koji su odlučili koristiti platformu. BigBlueButton zato ima našu preporuku.



# ZAKLJUČCI I PREPORUKE

Sumnje u alate IT divova, poput Googlea i Microsofta, posve su opravdane. Tvrtke su uronjene u niz skandala vezanih uz privatnost, dok je njihov osnovni model poslovanja stvorio kapitalizam nadzora – ekonomski model sazdan na procesu izvlačenja vrijednosti iz podataka koji su kreirani kao nusprodukt korištenja određene tehnologije. Primjenjene tehnologije praćenja te količina prikupljanih podataka, čak i kod softvera koji se koristi u edukacijske svrhe, su zabrinjavajući. Politiscope stoga preporuča da se Google Classrom i Microsoft Teams u potpunosti izbjegavaju u provedbi nastave na daljinu.

Dvije aplikacije dobile su nešto blažu ocjenu, no nisu preporučene za korištenje jer prepoznate manjkavosti pretežu nad prednostima alata – Loomen i Zoom. Iako je Zoom u odnosu na skandale u ožujku i travnju napravio snažne iskorake, još uvijek nije u potpunosti sigurno koja je razina praćenja korisnika u marketinške svrhe te prodaje podataka trećim stranama. Razočaravajuće je da CARNET-ov Loomen ima ozbiljne propuste detektirane analizom Obavijesti o privatnosti. Ipak, budući da je riječ o digitalnom rješenju javnog tijela, rizik za preširoko prikupljanje podataka te profiliranje u marketinške svrhe ipak je znatno niži nego kod softverskih alata big techa.

Politiscope daje snažnu preporuku za korištenje rješenja otvorenog koda koja ujedno omogućuju postavljanje alata na vlastite servere. Na ovaj način se ostvaruje potpuna kontrola privatnosti učenika. Politiscope stoga daje preporuku za korištenje servisa BigBlueButton u nastavi na daljinu. Dodatno tome, za manje video konferencijske razgovore Politiscope preporuča Jitsi Meet, također rješenje otvorenog koda koje se može postaviti na vlastiti server.

Jednako kao što građani ne smiju biti primorani da se odriču privatnosti ako koriste neki komercijalni servis, tako ni učenici i roditelji ne smiju biti prisiljeni žrtvovati temeljna ljudska prava kako bi dobili kvalitetnu edukaciju. Zaštita privatnosti djece nam uvijek mora biti prioritet.

U kriznoj situaciji hitnog prebacivanja kompletnog sustava obrazovanja na "nastavu na daljinu", može biti razumljivo da se nije istog trenutka razmišljalo o svim aspektima zaštite podataka učenika, no nedopustivo je da već gotovo godinu dana nisu zabilježeni neki konkretni pomaci u ovom smjeru. Ključno je što prije educirati učitelje koji na dnevnoj bazi rade s alatima za online nastavu - kako bi bili sposobni na primjeren način podešavati postavke alata te djeci objasniti osnove primjerenog rada u njima, kao i mjere koje trebaju poduzeti da maksimalno zaštite svoju sigurnost te privatnost. Između ostalog, podizanjem razine zaštite privatnosti u školama, djeca bi se ujedno po prvi put upoznala sa svojim digitalnim pravima te tako stekla kompetencije za život u suvremenom digitalnom okružju.

Nema sumnje kako je neadekvatan odgovor obrazovnog sustava na zaštitu privatnosti učenika u nastavi na daljinu jednim dijelom uzrokovan izostankom proaktivne uloge nadzornog tijela za zaštitu podataka -AZOP. Primjerice, nizozemsko nadzorno tijelo (Autoriteit Persoonsgegevens) u travnju 2020. izdalo je upute za obrazovne ustanove koje koriste glasovne ili video pozive te provode testove online putem. Nadzorno tijelo je potom pokrenulo istragu o korištenju softvera u nastavi na daljinu te su u prosincu objavili **obuhvatnu analizu** s jasnim uputama i preporukama. Upravo je navedeni dokument bio jedan od ključnih izvora u kreiranju preporuka za nastavu na daljinu za hrvatske škole.

Preporuke hrvatskim školama za tehničke i organizacijske mjera zaštite podataka te druge mjere zaštite privatnosti učenika prilikom korištenja aplikacija za nastavu na daljinu:

- Napraviti Procjenu učinka na zaštitu podataka za korištenje aplikacija za video/glasovne pozive, kojom bi bili ocijenjeni rizici za prava i slobode učenika te profesora prilikom korištenja pojedinog softverskog alata

- U suradnji s izvršnim tijelima u obrazovnom sustavu kreirati upute o korištenju aplikacija i rukovanju video snimkama, koje sadrže jasna pravila o izradi snimki, prikazivanju video zapisa učenika i nastavnika, obaviještavanju pojedinaca o najvažnijim stavkama vezanima uz obradu podataka, načinima sigurnosnog pohranjivanja, periode zadržavanja, određivanje djelatnika koji imaju pristup podacima, kao i osobu odgovornu za uništavanje podataka.

- U slučaju obrade podataka od strane trećih strana (Izvršitelja obrade) u sklopu nastave na daljinu, edukacijske institucije obvezne su i potpisati Ugovor o obradi podataka s Izvršiteljima obrade, kojim bi dodatno osigurali da Izvršitelj provodi adekvatne organizacijske i tehničke mjere zaštite podataka. Ovu preporuku bi trebalo primijeniti na najvećem broju aplikacija, jer rijetko koja omogućuje *self-hostanje* (postavljanje na vlastitom serveru)

- Preporuča se odabir pružatelja usluga smještenih u Europskoj Uniji. Naime, Sud Europske Unije je nadavno proglasio ništavnim odluku o adekvatnosti EU-SAD Privacy Shielda o razmjeni podataka, budući da navedeni mehanizam nije osiguravao adekvatnu razinu zaštite podataka. Navedena odluka prijenos podataka video-konferencijskih sustava u SAD čini nezakonitim.

- Škole moraju imati imenovane stručne službenike za zaštitu podataka, koji trebaju imati aktivnu ulogu u procesu organizacije nastave na daljinu, s ciljem osiguravanja zaštite podataka učenika i nastavnika

- Ukoliko se pohranjuju video zapisi, nužno je imati i dokumentirani razlog za pohranu te o tome informirati sve pojedince u video zapisu. Dakle, ako učenici imaju upaljene kamere tijekom lekcija, nije dopušteno pohranjivati video zapise učenika bez opravdanog i jasno definiranog razloga.

- Standardne postavke aplikacija, prethodno korištenju od strane učenika, trebaju biti postavljene na način koji minimizira obradu osobnih podataka

Iceland Liechtenstein Norway **Active citizens** fund

politiscope

Projekt "Privatnost u doba Corone" je podržan s 4.973 € financijske podrške Islanda, Lihtenštajna i Norveške u okviru EGP i Norveških grantova.

Kreiranje ove analize omogućeno je financijskom podrškom Islanda, Lihtenštajna i Norveške u okviru EGP i Norveških grantova. Sadržaj ove analize isključiva je odgovornost udruge Politiscope i ne odražava nužno stavove država donatorica i Upravitelja Fonda.