# PLATO’S EU

Filozofsko učenje primijenjeno na online okruženja unutar EU

Nacrt i primjer

za PRP2 radionicu:

# “Moderni problem privatnosti:

# Što je moje pravo na privatnost u digitalnom dobu?”

Co-funded by the European Union

PLATO’s EU

| Version | Date | Comments |
|---|---|---|
| 1 | 6.2.2023. | *First draft of the workshop developed for PRP2, offered to partnership for revision.* |
| 2 | | |
| 3 | | |
| 4 | | |

| | |
|---|---|
| **Document title:** | *"Draft and example for 2nd Project Results Package 2 workshop"* |
| **Date of issue:** | *20.2.2022.* |
| **Author(s):** | *Filip Škifić* |
| **E-mail address:** | f.skifa123@gmail.com |
| **Contributors to document:** | |
| **Quality reviewer (if any)** | *n/a* |
| **Number of pages:** | *16* |
| **Confidentiality status:** | ***For internal use of project partnership only*** |



The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

# CONTENTS





The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

# 5th WORKSHOP:

# "Moderni problem privatnosti:

# Što je moje pravo na privatnost u digitalnom dobu?"



The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

## 1. UVOD U TEMU

Na početku radionice nastavnik/voditelj svojim učenicima ukratko opisuje tijek radionice. Učenicima objašnjava cilj naše radionice, a taj cilj se može sažeti kroz odgovore na ova pitanja:

- Što je pravo na privatnost?
- Što je digitalna privatnost?
- Gdje je granica između privatnog i javnog života?
- Je li čovječanstvo imalo više privatnosti prije digitalne revolucije?
- Je li sigurno dijeliti osobne podatke s cijelim svijetom?
- Mogu li se vaši osobni podaci zloupotrijebiti?

Što je pravo na privatnost?

Pravo na privatnost obuhvaća pravo na zaštitu nečije intime, identiteta, imena, spola, časti, dostojanstva, izgleda, osjećaja i spolne orijentacije. Pravo na privatnost može se ograničiti u interesu drugih pod uvjetom da interferencija međusobnih prava nije proizvoljna ili nezakonita

Digitalna privatnost odnosi se na zaštitu podataka pojedinca koji se koriste ili stvaraju tijekom korištenja interneta na računalu ili osobnom uređaju. Ova zabrinutost raste jer povijest pregledavanja i osobni podaci na mreži mogu biti ugroženi.



The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

## 2. PRESJEK LEKCIJE

Ova radionica je klasični sokratski dijalog sa stimulusom (poticajem) u digitalnom svijetu. (preporučeno vrijeme: 45 minuta).

Glavni ciljevi ove radionice su:

- pokazati kako su promjene u digitalnom svijetu utjecale na digitalnu privatnost

- ukazati na važnost razumijevanja ljudskog prava na privatnost i njegovu krhkost u suvremenom svijetu

- potaknuti učenike na korištenje vještina kritičkog mišljenja u digitalnom svijetu i razumijevanje granice između privatnog i javnog života

Materijali za korištenje uključuju:

- Mobilni telefoni (bilo bi idealno kada bi svaki učenik mogao koristiti svoj mobitel s internetskom vezom)

- Računalo

- Projektor

- Papir, olovka i ostali nužni edukacijski materijali.

Ishodi učenja koji će se postići kroz radionicu:

• razumjeti svoj digitalni identitet i svoju ulogu u digitalnom svijetu

• razumjeti svoja ljudska prava na privatnost i slobodu



The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

• razumjeti digitalno građanstvo kroz pristup pouzdanim i vjerodostojnim informacijama

## 3. RAZRADA LEKCIJE – AKTIVNOSTI RADIONICE

### 3.1. I. dio: Što je privatnost?

Učitelj počinje radionicu pitajući učenike znaju li što je privatnost? Ne postoji točan odgovor, ali poanta je uputiti učenike da naprave razliku između privatnih i javnih stvari. Nakon što shvate tu razliku i definiraju privatnost, nastavnik bi ih trebao pitati s kim sve dijele svoje osobne podatke. Učenici će vjerojatno odgovoriti da svoj osobni život dijele s obitelji i prijateljima. Taj je trenutak idealan za uvođenje pravog stimulusa. Nastavnik bi trebao potaknuti učenike da odu na svoje profile na društvenim mrežama (facebook, Instagram, twitter itd.) i pronađu informacije koje su tamo dostupne kao što su ime, datum i mjesto rođenja te gdje trenutno žive kao i neke druge informacije o njihovim interesima itd. Nakon toga, učitelj bi trebao prodiskutirati s učenicima što se smatra prekomjernim dijeljenjem.

**Što se smatra prekomjernim dijeljenjem na društvenim mrežama?**

Prekomjerno dijeljenje na društvenim medijima temelji se na izlaganju intimnih detalja o vašem osobnom životu kao što su odnosi, prijateljstva, obiteljske stvari ili vaša dnevna rutina. Neki primjeri uključuju:

• Redovito objavljivanje s kim ste



The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

• Objavljivanje intimnih detalja o vašim odnosima, prijateljstvima, članovima obitelji i osobnim problemima

• Omogućavanje geografske lokacije na svakoj objavi

• Neprekidno objavljivanje slika onoga što nosite

• Objavljivanje informacija vezanih uz posao

Nakon razgovora o prekomjernom dijeljenju na društvenim mrežama, učitelj kaže učenicima da napišu minimalno 2 moguće opasnosti koje se mogu dogoditi ako pretjerano dijele svoj osobni život. Dajte im oko 10 minuta i dopustite im da na internetu pretražuju neke slučajeve koji su se nedavno dogodili u vezi s online zlostavljanjem, krađom identiteta itd. Potaknite ih da razmišljaju kao inspektori i da razmišljaju izvan uobičajenih okvira tipičnih digitalnih prijetnji.

Mogući odgovori koji su zanimljivi za daljnju raspravu:

• Preuzimanje računa

o Kibernetički napad u kojem kriminalci koriste korisnička imena i lozinke koje su ukradeni kako bi preuzeli kontrolu nad online računima.

• Društveni inženjering

o Društveni inženjering je psihološka manipulacija koja se koristi kako bi se drugi natjerali da nešto učine ili otkriju privatne informacije. Ova se metoda često koristi putem e-poruka za krađu identiteta.

• Ugled

o Zaštita ugleda onoga tko ste u svom osobnom i profesionalnom životu mogla bi biti ugrožena ako previše dijelite na svojim računima.



The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

Nakon što učenici pročitaju što su napisali, nastavnik može započeti malu raspravu o tome tko može vidjeti njihove osobne podatke i što mogu učiniti s njima. Poželjno je potaknuti raspravu o prednostima i nedostacima dijeljenja našeg života na internetu, kao i usredotočiti se na neke određene loše prakse koje su učenici pronašli na internetu u vezi s krađom identiteta, zlostavljanjem itd.

Učitelj može spomenuti i kolačiće na web stranicama i objasniti učenicima na koji način se njima može manipulirati na internetu te upitati ih što oni misle o tome. Ideja koja stoji iza ovoga je poticaj učenika na kritičnije razmišljanje o svom digitalnom identitetu i stvarnim opasnostima pretjeranog dijeljenja osobnih podataka.

Rasprava bi trebala trajati deset do petnaest minuta, a nastavnik bi trebao biti moderator i ne bi trebao sam donositi zaključke. Također, važno je potaknuti učenike da podijele neka osobna negativna iskustva na internetu i da se osjećaju sigurno u razrednom okruženju. U ovom slučaju, važno je izgraditi čvrsto povjerenje u razredu i poticati razumijevanje bez osuđivanja bilo koga ili bilo čega. Zaključak u tom scenariju trebao bi ići prema razumijevanju toga da je dijeljenje njihovog iskustva u sigurnom okruženju poput učionice, s obitelji ili bliskim prijateljima bolje od dijeljenja osjetljivih informacija na internetu.

## 3.2. II. dio: Zašto imamo pravo na privatnost?

Nastavnik/voditelj predstavlja svojim učenicima kratak tekst o sustavu nadzora u Kini koji je postao popularna tema u zapadnim medijima:

*“Sigurnosne kamere automatski hvataju lica ljudi i povezuju ih s podacima o najmu kuća, zapisima u bolnicama, hotelima i školama te sažimaju dnevnik aktivnosti različitih skupina*



The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project’s national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

*ljudi. Sa svim prikupljenim informacijama i podacima stvorio bi se model alarma koji bi automatski identificirao abnormalne aktivnosti."*

*Još se ne zna kako će točno model biti implementiran. Ali u kombinaciji s postojećim kineskim sustavom nadzora, projekt Sharp Eyes mogao bi omogućiti zaposlenicima u zajednici da proaktivno odu na vrata pojedinaca kako bi istražili zločin koji još nije ni počinjen.*

*Njegov cilj je stvoriti sustav koji je doslovno namijenjen "sprječavanju zločina prije nego što se dogodi".*

Prvo, nastavnik mora dati učenicima malo vremena da razmisle o napisanom, a zatim bi trebao slijediti ovaj niz pitanja koja mogu potaknuti učenike na filozofsko razmišljanje o predmetu. Svako pitanje može dovesti do dodatnih pitanja i šire rasprave, ali treba slijediti ovu strukturu:

- Je li opravdano nadzirati pojedince radi višeg cilja i zašto tako mislite?

- U kojim slučajevima biste dopustili da vas država nadzire?

- Mislite li da bi to spriječilo da se nešto dogodi?

- Je li čovjeku važnije biti siguran ili slobodan?

- Možete li projicirati negativne utjecaje ovakvog sustava nadzora u bliskoj budućnosti?

- Mislite li da je društvo roblje tehnologije ili mislite suprotno?



The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

- Koliko ljudi može vidjeti vašu lokaciju ili vaše ponašanje na društvenim medijima?

- Je li vas ikada netko osudio na društvenim mrežama ili ste ikada čuli za nešto slično?

- Koja je razlika između novog kineskog sustava nadzora i svakodnevnog života zapadnog čovjeka?

- Znate li na koji se način mogu koristiti vaši osobni digitalni podaci?

- Jeste li ikada pročitali odredbe i uvjete na nekoj web stranici?

- Mislite li da je riskantno dopustiti tvrtkama da prate svaki vaš korak u digitalnom okruženju?

- Znate li koliko web stranica i mobilnih aplikacija ima vaše osobne podatke?

- Možete li imenovati neke od njih?

- Ima li moderni čovjek pravo na privatnost ili slobodu i ako ima, na koji način je može koristiti?

- Mogu li tehnologija, digitalno okruženje i umjetna inteligencija promijeniti ljudsku prirodu?

Svako pitanje može biti popraćeno skupom potpitanja kako bi se učenicima pomoglo da zagrebu dublje ili da ih se potakne na otkrivanje novih značenja iza pojmova s kojima su već upoznati. To je sokratska majeutička metoda u kojoj učitelj svojim učenicima ne daje



The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

definicije ili neke smislene zaključke, već ih pokušava potaknuti da se uhvate u koštac s već poznatim pojmovima i činjenicama koji ih okružuju i prema kojima djeluju i razmišljaju. Na primjer, mogu govoriti o suvremenom konceptu slobode ili mogu raspravljati o raznim društvenim problemima koji se tiču odnosa između čovjeka i stroja (umjetna inteligencija i sl.). Za uspjeh ovakvog pristupa radionicama nužan je otvoren dijalog.

## 4. RASPRAVA

Budući da je ova radionica u potpunosti izgrađena na nizu rasprava, sljedeća pitanja mogu se koristiti za proširenje tema koje su istražene tijekom radionice i usmjeravanje radionica prema različitim zaključcima i široj slici:

1. Što mislite kako će svijet izgledati za 10 godina ako umjetna inteligencija preuzme neki aspekt ljudskog života?

2. Mislite li da je čovječanstvo moćnije od tehnologije?

3. Kakav bi bio tvoj život bez društvenih mreža?

4. Zamislite jedan tjedan bez tehnologije i recite nam što biste mogli raditi taj tjedan?

5. Je li privatnost važnija od mira u svijetu?

6. Kad bi cijeli svijet bio pod nadzorom, mislite li da bi to bio bolji ili lošiji svijet za život?

7. Zašto ljudi previše dijele svoj osobni život?

8. Je li bolje biti tajanstven ili potpuno otvoren prema svijetu?



The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

9. Je li netko u razredu potpuno isključen iz društvenih mreža?

10. Smatrate li da su ljudi koji su stvarno aktivni na društvenim mrežama u nekoj prednosti ili nedostatku u odnosu na druge?

## 5. DODATNI IZVORI


- Online article “Digital privacy in education” [https://ecampusontario.pressbooks.pub/digitalprivacyleadershipandpolicy/chapter/digital-privacy-in-education/]
- Online article “Inside China's Surveillance State, Built On High Tech And A Billion Spies” [https://worldcrunch.com/culture-society/china-surveillance-cameras]
- Online article “How Oversharing on Social Media Affects Your Privacy“ [https://www.keepersecurity.com/blog/2022/12/23/how-oversharing-on-social-media-affects-your-privacy/]
- Online article “Four Takeaways From a Times Investigation Into China’s Expanding Surveillance State” [https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html]
- Online article “Surveillance State explores China's tech and social media control systems” [https://www.npr.org/2022/09/07/1118105165/surveillance-state-explores-chinas-tech-and-social-media-control-systems]
- Online article “7 Examples of Data Misuse in the Modern World” [https://www.invisibly.com/learn-blog/data-misuse-7-examples/]




The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project’s national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

- Online article “Philosophy and Digitization: Dangers and Possibilities in the New Digital Worlds” [https://www.degruyter.com/document/doi/10.1515/sats-2021-0006/html?lang=en]
- Book: Soames, S. *The World Philosophy Made: From Plato to the Digital Age* Princeton University PressOnline, 2019
- Youtube video “How China’s Surveillance Is Growing More Invasive | Visual Investigations” [https://www.youtube.com/watch?v=Oo_FM3mjBCY]

## 6. ANNEX

**Prijetnje vašim računima na društvenim mrežama:**

Vrijeme je da društvene mreže počnete shvaćati ozbiljno. Ispod su tri uobičajene prijetnje na koje pojedinci nasjedaju kada je u pitanju zaštita njihovih računa. Ako ste svjesni sljedećeg, možete smanjiti svoje šanse da postanete žrtva.

- **Javna Wi-Fi mreža**
    - Prijava na vaše račune društvenih mreža na nezaštićenoj javnoj Wi-Fi mreži dovodi vas u opasnost da netko presretne vaše podatke. Jedna od najistaknutijih kibernetičkih prijetnji javnom Wi-Fiju je napad „čovjeka u sredini“ (MITM). Ovaj se napad oslanja na mrežnu manipulaciju, odnosno stvaranje zlonamjernih mreža pod kontrolom kibernetičkih kriminalaca koji djeluju kao “posrednici” između pošiljatelja i primatelja informacija, mijenjajući promet i presrećući podatke.



The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project’s national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

- **Krađa identiteta**
  - Prijevare s krađom identiteta su prijevare u kojima vas kibernetički kriminalac uvjeri da mu date svoje podatke za prijavu tako što vam šalje poruke, obično putem e-pošte, koje izgledaju kao da su iz pouzdanog izvora tražeći da potvrdite svoje vjerodajnice za prijavu ili im date privatne podatke. Na primjer, „phishing prijevara“ može izgledati kao da dolazi s platforme kao što je Instagram i od vas traži da poništite svoju lozinku pomoću zlonamjerne veze.
  - Klikanje na poveznice u e-pošti ili porukama koje su nepoznate ili neočekivane, čak i ako se čini da su iz pouzdanog izvora, treba uvijek izbjegavati.
- **Slabe lozinke**
  - Ako koristite slabu lozinku za sve svoje račune, kibernetičkom kriminalcu je mnogo lakše pogoditi je na temelju osobnih podataka koje ste pretjerano podijelili, kao što je ime vašeg psa ili datum rođenja. Uvijek koristite jaku lozinku kako biste zaštitili svoju privatnost.

### Što možete učiniti da spriječite prekomjerno dijeljenje na društvenim mrežama?

Možete spriječiti prekomjerno dijeljenje na društvenim mrežama ako budete pažljiviji i slijedite različite sigurnosne najbolje prakse. Treba se uvijek zapitati je li nešto prikladno za javno objavljivanje ili je bolje poslati tu informaciju kao privatnu poruku. Također je važno razlikovati platforme koje želite koristiti privatno i profesionalno, jer vam to omogućuje objavljivanje odgovarajućeg sadržaja bez ugrožavanja vašeg profesionalnog ugleda.



The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.

Preporučujemo da prijeđete na privatne račune kada je to moguće i uključite potvrdu u 2 koraka kako biste dodatno zaštitili svoje račune. Pobrinite se da prihvaćate zahtjeve za prijateljstvo samo ako doista poznajete tu osobu i utvrdite je li prikladno da ona vidi vaš sadržaj bez izlaganja sebe ikakvom riziku.

**Osobni digitalni podaci koriste se na jedan od tri načina:**

- Osobni podaci prikupljaju se i analiziraju kako bi nam pružili prilagođenije oglase.
- Osobni podaci se bilježe i procjenjuju za istraživanje i razvoj.
- Osobni podaci prodaju se brokeru za podatke.



The creation of this publication has been co-funded by the Erasmus+ grant program of the European Union under project **no. 2021-1-SK01- KA220-SCH-000034395**. This publication reflects the views only of the author. Neither the European Commission nor the project's national funding agency are responsible for the content or liable for any losses or damage resulting of the use of this publication.