PLATO'S EU

Philosophical Learning Applied To Online Surroundings in EU

"Moderné problémy súkromia: Aké je moje právo na súkromie v digitálnej dobe?"

Co-funded by the European Union

PLATO's EU

Verzia	Dátum	Komentáre
1	6.2.2023.	*Prvý návrh workshopu vyvinutý pre PRP2, ponúknutý partnerstvu na revíziu.*
2		
3		
4		

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

Názov dokumentu:	*„Návrh a príklad pre workshop 2. balíka výsledkov projektu 2“*
Dátum vydania:	*20.2.2022.*
Autor(i):	*Filip Škifić*
Emailová adresa:	f.skifa123@gmail.com
Prispievatelia do dokumentu:	
Recenzent kvality (ak existuje)	*n/a*
Počet strán:	*16*
Stav dôvernosti:	***Len na interné použitie projektového partnerstva***

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

OBSAH

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

WORKSHOP:

„Moderné problémy súkromia:
Aké mám právo na súkromie v digitálnej ére?

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

1. ÚVOD K TÉME

Na začiatku workshopu učiteľ/ka resp. facilitátor/ka stručne opíše svojim študentom/kám priebeh workshopu. Vysvetľuje študentom/kám cieľ nášho workshopu a tento cieľ možno zhrnúť do odpovedí na tieto otázky:

- Aké je právo na súkromie?

- Čo je digitálne súkromie?

- Kde je hranica medzi súkromným a verejným životom?

- Malo ľudstvo pred digitálnou revolúciou viac súkromia?

- Je bezpečné zdieľať osobné údaje s celým svetom?

- Môžu byť vaše osobné údaje zneužité?

Čo je právo na súkromie?

Právo na súkromie zahŕňa právo na ochranu intimity, identity, mena, pohlavia, cti, dôstojnosti, vzhľadu, citov a sexuálnej orientácie osoby. Právo na súkromie môže byť obmedzené v záujme iných za osobitných podmienok za predpokladu, že zásah nie je svojvoľný alebo nezákonný.

Digitálne súkromie sa vzťahuje na ochranu informácií jednotlivca, ktoré sa používajú alebo vytvárajú pri používaní internetu na počítači alebo osobnom zariadení. Táto obava narastá, pretože história prehliadania a osobné informácie online môžu byť ohrozené.

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

2. PREHĽAD LEKCIE

Tento workshop je klasickým sokratovským dialógom so stimulmi v digitálnom svete (odporúčaný čas: 45 minút).

Hlavnými cieľmi tohto workshopu sú:

- ukázať, ako zmeny v digitálnom prostredí ovplyvnili digitálne súkromie

- poukázať na dôležitosť pochopenia ľudského práva na súkromie a jeho krehkosti v súčasnom svete

- povzbudiť študentov/ky, aby používali zručnosti kritického myslenia v digitálnom svete a aby pochopili hranicu medzi súkromným a verejným životom

Medzi materiály, ktoré by sa mali použiť, patria:

- Mobilné telefóny (bolo by dobré, keby každý študent/ka mohol používať svoj mobilný telefón s pripojením na internet)

- Počítač

- Projektor

- Papier, ceruzka a ďalšie potrebné vzdelávacie materiály.

Vzdelávacie výsledky, ktoré sa prostredníctvom workshopu dosiahnu:

- pochopenie ich digitálnej identity a ich úlohy v digitálnom svete
- pochopenie ich ľudských práv na súkromie a slobodu

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

- pochopenie digitálneho občianstva prostredníctvom prístupu k spoľahlivým a dôveryhodným informáciám

3. ROZDELENIE HODINY – WORSKHOP AKTIVITY

3.1. Časť I. Čo je súkromie?

Učiteľ/ka začína workshop tým, že sa opýta svojich študentov/iek, či vedia, čo je súkromie? Neexistuje správna odpoveď, ale cieľom je viesť študentov/ky k tomu, aby rozlišovali medzi súkromím a verejnou záležitosťou, pokiaľ ide o osobné a verejné informácie. Po vykonaní tohto rozdelenia a definovaní súkromia by sa ich učiteľ/ka mal/a opýtať, s kým zdieľajú svoje osobné údaje. Študenti/ky pravdepodobne odpovedia, že zdieľajú svoj osobný život s rodinou a priateľmi/kami a to je čas, kedy začína skutočný stimul. Učiteľ/ka by mal/a povedať svojim študentom/kám, aby si prešli na svoje profily na sociálnych sieťach (Facebook , Instagram, Twitter atď.) a našli tam napísané informácie, ako je meno, dátum a miesto narodenia a ich aktuálna poloha, ako aj ďalšie informácie. o ich záujmoch atď. Potom by mal učiteľ/ka prediskutovať so študentmi/kami, čo sa považuje za nadmerné zdieľanie.

Čo sa považuje za nadmerné zdieľanie na sociálnych médiách?

Nadmerné zdieľanie na sociálnych sieťach je založené na odhalení intímnych detailov o vašom osobnom živote, ako sú vzťahy, priateľstvá, rodinné záležitosti alebo každodenná rutina. Niektoré príklady:

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

- Pravidelne uverejňujte, s kým ste
- Zverejňovanie intímnych detailov o vašich vzťahoch, priateľstvách, rodinných príslušníkoch a osobných drámach
- Povolenie geografickej polohy v každom príspevku
- Neustále uverejňujte obrázky toho, čo máte na sebe
- Uverejňovanie informácií súvisiacich s prácou na vašom účte

Po rozhovore o nadmernom zdieľaní na sociálnych sieťach učiteľ/ka povie študentom/kám, aby napísali 2 možné nebezpečenstvá, ktoré môžu nastať, ak budú príliš zdieľať svoj osobný život. Dajte im asi 10 minút a nechajte ich, aby si na internete vyhľadali nejaké problémy, ktoré sa nedávno vyskytli v súvislosti so šikanovaním online, krádežou identity atď. Povzbuďte ich, aby mysleli ako inšpektori/ky a mysleli mimo bežného rámca typických digitálnych hrozieb.

Možné odpovede, ktoré sú zaujímavé pre ďalšiu diskusiu:

- Prevzatie účtu
  - Kybernetický útok, pri ktorom kyberzločinci využívajú ukradnuté používateľské mená a heslá, aby získali kontrolu nad online účtami.
- Sociálne inžinierstvo
  - Sociálne inžinierstvo je psychologická manipulácia používaná na to, aby prinútila ostatných robiť veci alebo odhaliť súkromné informácie. Táto metóda sa často vyskytuje prostredníctvom phishingových e-mailov.
- Povesť

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

- Ochrana povesti toho, kto ste vo svojom osobnom a pracovnom živote, môže byť ohrozená, ak sa na svojich účtoch príliš podieľate.

Keď si študenti/ky prečítajú, čo napísali, učiteľ/ka môže začať malú diskusiu o tom, kto môže vidieť ich osobné údaje a čo s nimi môže robiť. Je naozaj dobré povzbudiť diskusiu o výhodách a nevýhodách zdieľania nášho života na internete, ako aj zamerať sa na niektoré konkrétne zlé praktiky, ktoré študenti/ky našli na internete v súvislosti s krádežou identity, šikanovaním atď .

Učiteľ/ka môže tiež spomenúť cookies na webových stránkach a vysvetliť im, akým spôsobom s nimi možno na internete manipulovať a zistiť, čo si o tom myslia. Myšlienkou je povzbudiť študentstvo, aby kritickejšie premýšľalo o svojej digitálnej identite a skutočných nebezpečenstvách nadmerného zdieľania osobných informácií.

Diskusia by mala trvať desať až pätnásť minút a učiteľ/ka by mal/a byť moderátor/ka a nemal/a by sám/sama robiť žiadne závery. Je tiež dôležité povzbudiť študentsvo, aby zdieľali niektoré osobné negatívne skúsenosti na internete a aby sa v prostredí triedy cítili bezpečne. V tomto prípade je dôležité budovať dôveru v triede a podporovať porozumenie bez toho, aby ste niekoho a čokoľvek odsudzovali. Záver v tomto prípade by mal smerovať k pochopeniu, že zdieľanie svojich skúseností v bezpečnom prostredí, ako je trieda, s rodinou alebo blízkymi priateľmi/kami, je lepšie ako zdieľanie citlivých informácií na internete.

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

3.2. Časť II. Prečo máme právo na súkromie?

Učiteľ / facilitátor predstavuje svojim študentom/kám krátky text o systéme sledovania v Číne, ktorý sa stal populárnou témou v západných médiách:

> *„Bezpečnostné kamery automaticky zachytávajú tváre ľudí a porovnávajú sa s informáciami o prenájme domu, záznamami v nemocniciach, hoteloch a školách a sumarizujú záznamy aktivít rôznych skupín ľudí. So všetkými zhromaždenými informáciami a údajmi by sa vytvoril model alarmu na automatickú identifikáciu abnormálnych aktivít."*
>
> *Zatiaľ nie je známe, ako presne bude model implementovaný. Ale v kombinácii s existujúcim čínskym systémom sledovania by projekt Sharp Eyes mohol umožniť komunitným pracovníkom proaktívne ísť k dverám jednotlivcov, aby vyšetrili zločin, ktorý ešte ani nebol spáchaný.*
>
> *Jeho cieľom je vytvoriť systém, ktorý má doslova „zabrániť zločinu skôr, ako k nemu dôjde“.*

Po prvé, učiteľ/ka musí dať študentom/kám krátky čas na premyslenie napísaného textu a potom by mal nasledovať súbor otázok, ktoré môžu študentov/ky podnietiť k filozofickému uvažovaniu o predmete. Každá otázka môže viesť k ďalším otázkam a širšej diskusii, ale mala by mať túto štruktúru:

- Je opodstatnené sledovať jednotlivcov pre väčšie blaho a prečo si to myslíte?

  - V ktorých prípadoch by ste dovolili svojmu štátu, aby vás sledoval?

  - Myslíte, že by to zabránilo tomu, aby sa niečo stalo?

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

- Je pre človeka dôležitejšie byť v bezpečí alebo slobodný?

- Viete načrtnúť negatívne vplyvy tohto druhu monitorovacieho systému v blízkej budúcnosti?

- Myslíte si, že spoločnosť je otrokom techniky alebo si myslíte opak?

- Koľko ľudí môže vidieť vašu vlastnú polohu alebo vaše správanie na sociálnych sieťach?

- Odsúdil vás niekedy niekto na sociálnych sieťach alebo ste už o niečom podobnom počuli?

- Aký je rozdiel medzi novým čínskym systémom sledovania a každodenným životom západného človeka?

- Viete, akým spôsobom možno použiť vaše osobné digitálne údaje?

- Už ste si niekedy skutočne prečítali zmluvné podmienky na akejkoľvek webovej stránke?

– Myslíte si, že je riskantné nechať spoločnosti sledovať každý váš krok v digitálnom prostredí?

- Viete, koľko webových stránok a mobilných aplikácií má vaše osobné údaje?

- Môžete menovať niektoré z nich?

- Má moderný človek právo na súkromie alebo slobodu a ak áno, akým spôsobom ich môže využiť?

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

- Môžu technológie, digitálne prostredie a umelá inteligencia zmeniť ľudskú povahu?

Po každej otázke môže nasledovať súbor podotázok, ktoré pomôžu študentom/kám posunúť sa ďalej alebo ich povzbudia, aby objavili nové významy pojmov, ktoré už poznajú. Ide o sokratovskú maieutickú metódu, pri ktorej učiteľ/ka nedáva svojim žiakom/kám definície alebo nejaké zmysluplné závery, ale snaží sa žiakov/ky podnietiť, aby pochopili už známe pojmy a fakty, ktoré ich obklopujú a podľa ktorých konajú a myslia. Môžu napríklad hovoriť o modernom poňatí slobody alebo môžu diskutovať o rôznych problémoch spoločnosti týkajúcich sa vzťahu medzi človekom a strojom (umelá inteligencia atď.). Pre úspech tohto prístupu k workshopom je nevyhnutný otvorený dialóg.

4. KONTROLNÁ DISKUSIA

Keďže tento workshop je úplne postavený na súbore diskusií, ďalšie otázky možno použiť na rozšírenie tém skúmaných v priebehu workshopu a viesť workshopy k rôznym záverom a širšiemu obrazu témy:

1. Ako si myslíte, že bude vyzerať svet o 10 rokov, ak umelá inteligencia prevezme nejaký aspekt ľudského života?
2. Myslíte si, že ľudstvo je mocnejšie ako technológia?
3. Aký by bol tvoj život bez sociálnych sietí?
4. Predstavte si jeden týždeň bez technológie a povedzte nám, čo by ste za ten týždeň mohli robiť?

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

5. Je súkromie dôležitejšie ako svetový mier?
6. Ak by bol celý svet pod dohľadom, myslíte si, že by bol lepší alebo horší svet na život?
7. Prečo ľudia nadmerne zdieľajú svoj osobný život?
8. Je lepšie byť tajomný alebo byť úplne otvorený svetu?
9. Je niekto v triede úplne mimo sociálnych médií?
10. Máte pocit, že ľudia, ktorí sú skutočne aktívni na sociálnych sieťach, sú v určitej výhode alebo nevýhode voči ostatným?

5. DODATOČNÉ ZDROJE

- Online článok „Digitálne súkromie vo vzdelávaní“ [https://ecampusontario.pressbooks.pub/digitalprivacyleadershipandpolicy/chapter/digital-privacy-in-education/]
- Online článok „Vo vnútri čínskeho dozorného štátu, postavený na špičkovej technológii a miliarde špiónov“ [https://worldcrunch.com/culture-society/china-surveillance-cameras]
- Online článok „Ako nadmerné zdieľanie na sociálnych médiách ovplyvňuje vaše súkromie“ [https://www.keepersecurity.com/blog/2022/12/23/how-oversharing-on-social-media-affects-your-privacy/]
- Online článok „Štyri poznatky z vyšetrovania Times do rozširujúceho sa štátu dohľadu v Číne“ [https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html]

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

- Online článok „Surveillance State skúma čínske systémy kontroly technológií a sociálnych médií“ [https://www.npr.org/2022/09/07/1118105165/surveillance-state-explores-chinas-tech-and-social-media-control -systémy]
- Online článok „7 príkladov zneužitia údajov v modernom svete“ [https://www.invisably.com/learn-blog/data-misuse-7-examples/]
- Online článok „Filozofia a digitalizácia: Nebezpečenstvo a možnosti v nových digitálnych svetoch“ [https://www.degruyter.com/document/doi/10.1515/sats-2021-0006/html?lang=en]
- Kniha: Soames, S. *The World Philosophy Made: From Plato to the Digital Age* Princeton University PressOnline , 2019
- Youtube video „Ako sa čínsky dohľad stáva invazívnejším | Vizuálne vyšetrovanie” [https://www.youtube.com/watch?v=Oo_FM3mjBCY]

6. PRÍLOHA

Hrozby pre vaše účty sociálnych médií:

Je čas začať brať sociálne siete vážne. Nižšie sú uvedené tri bežné hrozby, ktoré na jednotlivcov číhajú, pokiaľ ide o ochranu ich účtov. Uvedomenie si nasledujúceho môže znížiť vaše šance stať sa obeťou.

- **Verejná Wi-Fi**
    - Prihlásením sa do svojich účtov sociálnych médií na nezabezpečenej verejnej sieti Wi-Fi sa vystavujete riziku, že niekto zachytí vaše údaje.

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

Jednou z najvýznamnejších kybernetických hrozieb pre verejné Wi-Fi je útok typu man-in-the-middle (MITM). Tento útok sa spolieha na sieťovú manipuláciu alebo vytváranie škodlivých sietí pod kontrolou kyberzločincov, ktorí fungujú ako „sprostredkovatelia“ medzi odosielateľom a príjemcom informácií, menia prevádzku a zachytávajú údaje.

- **Phishingové podvody**
  - Podvody s neoprávneným získavaním údajov sú, keď vás kyberzločinec oklame, aby ste mu poskytli svoje prihlasovacie údaje tým, že vám pošle správy, zvyčajne prostredníctvom e-mailu, ktoré vyzerajú, že pochádzajú z dôveryhodného zdroja a žiadajú vás o potvrdenie vašich prihlasovacích údajov alebo o poskytnutie súkromných informácií. Napríklad phishingový podvod môže vyzerať tak, že prichádza z platformy, ako je Instagram, ktorý vás žiada o obnovenie hesla pomocou škodlivého odkazu.
  - Vždy by ste sa mali vyhýbať klikaniu na odkazy v e-mailoch alebo správach, ktoré nepoznáte alebo neočakávate, aj keď sa zdá, že pochádzajú z dôveryhodného zdroja.
- **Slabé heslá**
  - Ak používate slabé heslo pre všetky svoje účty, pre kyberzločinca je oveľa jednoduchšie ho uhádnuť na základe osobných informácií, ktoré ste nadmerne zdieľali, ako je meno vášho psa alebo dátum narodenia. Vždy používajte silné heslo, aby ste ochránili svoje súkromie.

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.

Čo môžete urobiť, aby ste zabránili nadmernému zdieľaniu na sociálnych sieťach ?

Nadmernému zdieľaniu na sociálnych sieťach môžete zabrániť tým, že budete viac rozmýšľať a budete postupovať podľa rôznych osvedčených postupov zabezpečenia. Dobrým pravidlom je zvážiť, či je niečo vhodné ako verejný príspevok alebo či je lepšie ako súkromná správa. Je tiež dôležité rozlišovať medzi platformami, ktoré chcete používať súkromne a profesionálne, pretože vám to umožňuje uverejňovať primeraný obsah bez toho, aby ste ohrozili svoju profesionálnu reputáciu.

Ak je to možné, odporúčame vám prejsť na súkromné účty a zapnúť verifikáciu v dvoch krokoch, aby ste ešte viac zabezpečili svoje účty. Uistite sa, že akceptujete žiadosti o priateľstvo iba vtedy, ak daného jednotlivca skutočne poznáte a určíte, či je vhodné, aby videl váš obsah bez toho, aby ste sa vystavili riziku.

Osobné digitálne údaje sa používajú jedným z troch spôsobov:

- Osobné údaje sa zhromažďujú a analyzujú, aby nám mohli poskytovať prispôsobenejšie reklamy.
- Osobné údaje sa zaznamenávajú a vyhodnocujú na účely výskumu a vývoja.
- Osobné údaje sa predávajú sprostredkovateľom údajov.

Vznik tejto publikácie bol spolufinancovaný z grantového programu Erasmus+ Európskej únie v rámci projektu **č. 2021-1-SK01-KA220-SCH-000034395** . Táto publikácia odráža iba názory autora. Európska komisia ani národná finančná agentúra projektu nezodpovedajú za obsah ani nezodpovedajú za žiadne straty alebo škody vyplývajúce z používania tejto publikácie.