



Kurikulum k ochraně údajů

Pedagogická univerzita ve Freiburgu

leden 2025

Lucie Brzáková, Deborah Krzyzowski, Bernd Remmele a Zlatko Valentic



**Spolufinancováno
Evropskou unií**

Financováno Evropskou unií. Vyjádřené názory a stanoviska jsou pouze názory a stanoviska autora (autorů) a nemusí nutně odrážet názory a stanoviska Evropské unie nebo Evropské výkonné agentury pro vzdělávání a kulturu (EACEA). Evropská unie ani EACEA za ně nemohou nést odpovědnost.

Obsah

1. Úvod	3
2. Kompetence, na které se DataPro zaměřuje	4
3. Popis kompetencí	5
3.1 Data jako zboží	6
3.2 Soukromí jako lidské právo	8
3.3 Opatření na ochranu údajů	11
4. Vztahy mezi kompetencemi	12
5. Širší výsledky učení	14
6. Závěr pro pedagogy	15

1. Úvod

Digitální technologie se stávají součástí všech aspektů našeho soukromého i veřejného života, zároveň kapitalizace osobních informací dostupných online učinila ze soukromí cenný majetek, pro společnosti, vládu i jednotlivce¹. Zabezpečení osobních údajů pomocí zásad minimalizace údajů a opatření na jejich ochranu je v důsledku toho zásadním zájmem.

DataPro je projekt v rámci programu Erasmus Plus Evropské unie, který se zabývá potřebou rozvíjet porozumění mladých občanů hodnotě jejich údajů, jejich právům na soukromí a opatřením na ochranu údajů. Během tří let trvání projektu budou transdisciplinární partneři vyvíjet vzdělávací nástroje o ochraně údajů pro studenty. Tento výukový program se zaměří na tři zmíněné oblasti využívání a ochrany údajů a umožní učitelům a dalším partnerům seznámit se s koncepty obsaženými ve vzdělávacích nástrojích.

Širším cílem projektu DataPro je tedy podpořit učitele komplexním vzdělávacím rámcem, který pomůže studentům, aby se stali aktivními a autonomními digitálními aktéry. Základním záměrem výuky metod ochrany údajů je přesvědčit studenty o hodnotě jejich dat jako zboží a o hodnotě jejich vlastního soukromí pro fungování demokracie. Vzděláváním studentů v oblasti mnohostranné povahy využívání údajů a zásadního významu ochrany osobních údajů se projekt DataPro snaží vychovat dobře informované občany, kteří budou vybaveni k tomu, aby svá práva k údajům prosazovali a obhajovali.

Tyto učební osnovy stanovují konkrétní vzdělávací cíle. Tyto cíle mají být realizovány pomocí řady kompetencí, které zvyšují porozumění studentů složitosti ochrany údajů a chápání soukromí jako otázky lidských práv. Prostřednictvím strukturovaného přístupu zahrnujícího shromažďování, uzpůsobování a vývoj inovativních výukových nástrojů chce projekt DataPro propojit teoretické znalosti a praktické porozumění. Tato iniciativa se zaměřuje nejen na šíření těchto zdrojů mezi školami a zúčastněnými stranami v oblasti vzdělávání, ale klade důraz také na zahrnutí obav a zpětné vazby studentů a učitelů. Další výhodou výukových nástrojů je jejich podpora studentů v

¹ Viz "surveillance capitalism" in Zuboff, S. (2018) *The Age of Surveillance Capitalism: Zuboff, Shoshana: The Fight for a Human Future at the New Frontier of Power (Boj o lidskou budoucnost na nové hranici moci)*. Dostupné na: <http://archive.org/details/zuboff-shoshana-the-age-of-surveillance-capitalism-2019> (Přístup: 10. ledna 2025).

tom, aby se stali digitálními aktéry. V takové roli by byli vybaveni k tomu, aby dokázali identifikovat a chránit se před digitálními hrozbami. Například falešným ovlivňováním prostřednictvím digitálních dezinformací nebo koordinovanými datovými útoky využívajícími taktiky sociálního inženýrství. Kurikulum také zohledňuje dříve identifikované překážky učení, jako je desenzibilizační účinek každodenního používání internetu na online soukromí². Na základě aktuální anglické verze kurikula bude toto přeloženo pro cílové skupiny v příslušných zemích.

Začleněním těchto osnov do vzdělávacího prostředí si klademe za cíl vychovat generaci, která si bude nejen vědoma důležitosti ochrany údajů, ale bude také umět uplatňovat osvědčené postupy. Očekává se, že tyto základní znalosti podpoří společenský postoj studentů k ochraně údajů a právům na soukromí, aby se z nich stali informovaní a zodpovědní digitální občané.

2. Kompetence, na které se DataPro zaměřuje

Kurikulum k ochraně údajů informuje učitele a další partnery o základních znalostech, které mladí občané potřebují, aby se mohli orientovat ve složitých otázkách ochrany údajů. Ústředním bodem projektu jsou kompetence, které studenti potřebují k bezpečnému řešení digitálních výzev. Mladí lidé vyrůstají v prostředí, kde data hrají ústřední roli, ať už prostřednictvím sociálních médií, online učení nebo digitální komunikace. Mnozí z nich však nemají dostatečné povědomí o rizicích a právech spojených s používáním digitálních technologií. Cílem projektu DataPro je vyvinout pro studenty hravé a kreativní výukové nástroje, které jim pomohou vytvořit si mechanismus bezpečné správy vlastních dat.

Jak bylo řečeno v úvodu, předpokládané oblasti kompetencí jsou založeny na chápání údajů jako zboží; zahrnují například mechanismy zpracování dat, kapitalizaci osobních informací online, algoritmické doporučovací systémy a důsledky online chování. V další části učební plán nabízí komplexní schéma, které představuje důsledky existence dat jako zboží pro jednotlivce a společnost. Vzhledem k tomu, že data jsou zbožím, zahrnuje schéma také příslušné kompetence, které si studenti musí osvojit, aby mohli úspěšně chránit své údaje online.

² Krzyzowski, D. (2024) *Zpráva o kvantitativní analýze dat z průzkumu*. Freiburg: Pedagogická univerzita ve Freiburgu, s. 21-23.

Učební plán se orientuje na univerzální vzdělávací rámec DigComp³, přičemž při jeho vývoji bylo realizováno několik kol zpětné vazby s odborníky na vzdělávání. Byly získány poznatky od členů konsorcia, odborníků na ochranu údajů a zejména učitelů. To by mělo zajistit vhodnost vzdělávacích nástrojů pro cílovou skupinu, kterou jsou studenti středních škol.

Výchozím bodem učebních osnov je objasnění skryté ekonomické hodnoty osobních údajů. Na základě tohoto zásadního předpokladu je zdůrazněn význam práva na soukromí pro zdraví demokracie a ochrany údajů pro individuální autonomii občanů těchto společností. Kurikulum integruje tyto tři jmenované tematické oblasti tak, aby studenti získali dovednosti pro ochranu svého soukromí a zodpovědné jednání v digitálním prostoru. Vzájemná dynamika mezi těmito tématy týkajícími se ochrany údajů bude vysvětlena v oddíle 4., za pomoci vizualizace v schématu kompetencí (obrázek 1).

3. Popis kompetencí

Kompetence projektu DataPro jsou strukturovány do tří tematických oblastí, které pokrývají různé souvislosti spojené s digitálními daty:

1. **Data jako zboží:** „co“ projektu. Předmětem ochrany jsou osobní údaje online, které jsou komercializovány a se kterými poskytovatelé online služeb a online platformy nakládají jako s výměnným zbožím.
2. **Soukromí jako lidské právo:** „proč“ projektu. Společenský význam ochrany tohoto zboží vzhledem k zásadní roli, kterou soukromí jednotlivce hraje pro výkon základních práv v demokratické společnosti.
3. **Ochrana údajů:** „jak“ projektu. Po uživatelsky orientované senzibilizaci vůči výše uvedeným tématům v oblasti kapitalizace údajů a ochrany soukromí online lze studentům představit praktická opatření na ochranu jejich dat. Tato opatření jsou prostředkem pro větší autonomii na internetu a soběstačnost při uplatňování vlastních práv.

Konkrétní kompetence potřebné k orientaci v těchto vzájemně propojených tematických skupinách jsou popsány v následující části.

³ EU Science Hub a Evropská komise (2022) *DigComp Framework*. Dostupné [na: https://joint-research-centre.ec.europa.eu/scientific-activities-z/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp/digcomp-framework_en](https://joint-research-centre.ec.europa.eu/scientific-activities-z/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp/digcomp-framework_en).

3.1 Data jako zboží

"Data jako zboží" jsou důvodem vzestupu naléhavosti významu vzdělávání v oblasti ochrany údajů. Ochrana soukromí je předmětem politických debat od doby, kdy vlády a tisk začaly dokumentovat informace o svých občanech⁴, avšak algoritmická reklama a sběr dat pro účely podnikání učinily z údajů směnnou měnu za bezplatné online služby. Projekt DataPro se snaží vysvětlit takové mechanismy datového průmyslu, aby povzbudil studenty k využívání hodnoty jejich dat. Ekonomickou hodnotu dat je možné si uvědomit, když si studenti osvojí následující kompetence:

Skupina kompetencí A.	Praktická opatření
A.1 Přeměna dat na aktivum	<i>Zacházení s daty jako s online měnou</i> Pochopení hodnoty osobních údajů, stejně jako hodnoty peněz. To zahrnuje rozpoznání toho, kdy a jaké údaje jsou zpracovávány online službami, pochopení toho, jak mohou být osobní údaje zpeněženy, znalost rizik spojených se zneužíváním osobních údajů a informované rozhodování o sdílení údajů. <i>Povědomí o monetizaci</i> Seznámení se s hlavními způsoby, jak společnosti vydělávají peníze na osobních a souhrnných údajích, například prostřednictvím reklamních platform a zlepšování cílené reklamy (včetně politické reklamy). Uvědomění si, že mnoho bezplatných komunikačních služeb (jako jsou sociální média) a online obsah jsou placeny z reklamy nebo prodeje uživatelských dat. Tento ekonomický model se opírá o zpeněžování osobních údajů.
A.2 Rozlišování bezpečnostních rizik sdílení dat	<i>Veřejné sdílení</i> Uvědomění si, že vše, co je veřejně sdíleno online (např. obrázky, videa, zvuky), může být použito k trénování systémů umělé inteligence, což může zahrnovat nežádoucí sledovací funkce. Potřeba obezřetnosti, pokud jde o rozsah veřejného sdílení dat. <i>Praxe minimalizace údajů</i> Pravidelné zamýšlení se nad nutností uchovávání a sdílení osobních údajů. Osvojení si postupů, jako je poskytování pouze nezbytných informací a používání jednorázových e-mailových adres nebo telefonních čísel, je-li to vhodné. <i>Bezpečnostní opatření</i>

⁴ Historický vývoj diskurzu o právu na soukromí viz Warren, S.D. a Brandeis, L.D. (1890) "The Right to Privacy", *Harvard Law Review*, 4(5), s. 193-220. Dostupné na: <https://doi.org/10.2307/1321160>.

	Uvědomění si běžných útoků sociálního inženýrství (phishing) prostřednictvím různých komunikačních kanálů, aby se zabránilo podvodnému získávání (digitálního) majetku.
A.3 Zhodnocení záměrů, které stojí za monetizací dat	Kritické hodnocení Pravidelné zamyšlení se, kdo stojí za informacemi na internetu, zejména na sociálních sítích. Zjišťování, kdo může mít zájem na vytváření tzv. komnat ozvěn (bublin). Povědomí o kvalitě Pochopení, že dezinformace mohou být velmi přesvědčivé, zejména s využitím pokročilých technologií, jako je umělá inteligence, která dokáže vytvářet sofistikované vizualizace. Nezbytnost zjišťování kvality a zdroje informací.
A.4 Povědomí o kontrole chování	Povědomí o mechanismu Uvědomění si, že mnoho digitálních platforem používá k ovlivňování chování uživatelů psychologické taktiky, jako je například poštuchování, gamifikace a manipulace. Rozpoznání těchto taktik pro zamezení nepřiměřeného ovlivňování. Uvědomění si, že vzorce používání a související nástroje lze využít k optimalizaci online služeb a cílené reklamy. To zahrnuje sledování chování uživatelů za účelem poskytování personalizovaného obsahu. Kontrolní opatření Naučení se strategiím pro kontrolu a omezení rozsahu sledování chování, jako je úprava nastavení ochrany soukromí a používání technologií pro zvýšení ochrany soukromí. Rozvíjení strategie, jak tyto vlivy omezit, například stanovením osobních limitů využití a kritickým hodnocením konzumovaného obsahu.

3.2 Soukromí jako lidské právo

Z hlediska všeobecného vzdělávání zdůrazňuje téma "Soukromí jako lidské právo" význam soukromého života a informačního sebeurčení pro jednotlivce i demokracii. *Všeobecná deklarace lidských práv* chrání "soukromí, rodinu, domov nebo korespondenci" každého jednotlivce před jakýmkoli "svévolným zasahováním"⁵. Jako negativní příklad lze uvést závažné porušování těchto práv nelegitimním používáním špiónážního softwaru vládami, jak potvrdil případ *Pegasus*⁶. Téma *Soukromí jako lidské právo* pomáhá studentům dát si do souvislosti vlastní soukromí na internetu s životem občana (evropské) demokracie. Zvláštní postavení soukromí a soukromého života

⁵ Viz Článek 12 *Všeobecné deklarace lidských práv* OSN (1948). Organizace spojených národů. Dostupné [na: https://www.un.org/en/about-us/universal-declaration-of-human-rights](https://www.un.org/en/about-us/universal-declaration-of-human-rights).

⁶ Valné shromáždění OSN (2022) *Právo na soukromí v digitálním věku*. Zpráva Úřadu vysokého komisaře OSN pro lidská práva* A/HRC/51/17. Rada pro lidská práva, s. 2. Dostupné [na: https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf](https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf).

chráněného před zásahy státu a podniků by mělo také upozorňovat na hodnotu autonomie jednotlivce pro celou společnost. Soukromí je proto základním pilířem dalších hodnot demokracie, jako je svoboda projevu a informační sebeurčení. Pouze při absenci kontroly, ať už ze strany vlády, institucí nebo moci soukromého sektoru, si mohou jednotlivci vytvářet autonomní názory a vyjadřovat je v demokratickém diskurzu. Soukromí lze tedy chápat jako absenci zaznamenatelemých poznatků o jednotlivci, jako stav, kdy může zažívat skrytost svého já před úředníky a úřady.⁷

Skupina kompetencí B.	Praktická opatření
B.1 Pochopení rozsahu svobody	<i>Uznávání svobody</i> Uvědomění si důležitosti soukromí pro vlastní svobodu. Ochrana vlastního soukromí je ochranou možnosti svobodně vyjadřovat své názory a žít bez zbytečných zásahů. Pochopení, že pokud ostatní mohou pozorovat nebo kontrolovat vaše chování, může být vaše osobní svoboda ohrožena.
B.2 Porozumění sebeurčení	<i>Kontrola dat</i> Uvědomění si práva kontrolovat, jaké údaje jsou shromažďovány, zpracovávány a používány. Uplatňování tohoto práva pomáhá zachovat si osobní autonomii a mít svou digitální identitu pod kontrolou. <i>Ochrana automatizace</i> Uvědomění si, že ochrana údajů zahrnuje právo nebýt podroben plně automatizovaným rozhodovacím procesům, které mohou významně ovlivnit jednotlivce. <i>Prevence zneužití</i> Ochrana osobních údajů pomáhá chránit před nežádoucími sledováním, krádeží identity, diskriminací a dalšími formami zneužití osobních údajů. Uvědomění si běžných útoků sociálního inženýrství (phishing) prostřednictvím různých komunikačních kanálů, aby se zabránilo podvodnému získávání (digitálního) majetku.
B.3 Znalost práv na ochranu osobních údajů (GDPR)	<i>Práva na údaje a nutnost souhlasu</i> Znalost práv vůči společnostem, které používají osobní údaje, včetně práva na přístup k údajům, které o vás uchovávají, na opravu nepřesností, na vymazání údajů (právo být zapomenut) a na podání stížnosti u úřadů.

⁷ Srovnej s konceptualizací soukromí jako nejasnosti v Selinger, E. a Hartzog, W. (2016) "Obscurity and Privacy", *Spaces for the Future: A Companion to Philosophy of Technology* [preprint]. Dostupné na: https://scholarship.law.bu.edu/faculty_scholarship/3099.

	Uvědomění si, že společnosti obecně potřebují získat souhlas k nakládání s vašimi osobními údaji. Pravidelné vyhodnocování, zda je nutné takový souhlas udělit. Hodnocení souhlasu Časté posuzování nutnosti udělení souhlasu s použitím údajů pro ujištění se, že vaše osobní údaje nejsou zbytečně zneužívány.
B.4 Povědomí o lidských právech	Digitální odpovědnost Uvědomění si odpovědnosti za ochranu lidské důstojnosti, svobody, demokracie a rovnosti při jednání na internetu. To zahrnuje respektování soukromí a práv na údaje ostatních a prosazování odpovědných postupů při zpracování údajů.
B.5 Posouzení rizik pro soukromí jednotlivců	Úrovně rizika Pochopení, že s různými postupy při zpracování dat jsou spojeny různé úrovně rizika pro soukromí. Některé datové procesy, zejména ty, které zahrnují umělou inteligenci, s sebou nesou vyšší rizika. Rizika umělé inteligence Uvědomění si, že procesy a služby založené na umělé inteligenci mohou představovat různé úrovně rizika pro soukromí, často kvůli schopnosti zpracovávat velké množství dat a odvozovat citlivé informace.
B.6 Hodnocení potenciálu internetu	Rozpoznání duality internetu Je třeba si uvědomit, že internet vytváří nové možnosti zapojení do společnosti pro zranitelné skupiny, ale může také přispívat k izolaci těch, kteří jej nepoužívají.
B.7 Přezkoumání zásad ochrany osobních údajů	Hodnocení politik Rozvíjení schopnosti kriticky posuzovat zásady ochrany osobních údajů aplikací a služeb. To zahrnuje pochopení toho, jaké údaje jsou shromažďovány, jak jsou používány a jaká máte práva týkající se vašich údajů.

3.3 Opatření na ochranu údajů

"Ochrana údajů" je obecným cílem výuky v učebních osnovách. Tato dimenze vychází z pochopení tematických okruhů 1: Data jako zboží a 2: Soukromí jako lidské právo. Kompetence v rámci tematického okruhu 3. se vztahují k praktickým opatřením v oblasti ochrany údajů a kybernetické bezpečnosti, která mohou jednotlivci přijímat na každodenní bázi.

Kompetence C.	Praktická opatření
C.1 Správa identit	Povědomí o používání

	Pravidelné zamyšlení se, jak a kde bezpečně používat a sdílet osobní údaje. Porozumění rizikům spojeným se sdílením osobních údajů. Opatření pro anonymitu Používání opatření ke skrytí vlastní identity na internetu, jako jsou sítě VPN, šifrované komunikační nástroje a prohlížeče zaměřené na ochranu soukromí.
C.2 Zajištění bezpečnosti dat	Bezpečnostní opatření Používání standardních bezpečnostních postupů, jako je používání různých silných hesel pro různé online služby, vícefaktorové ověřování, biometrické zámky, pravidelné aktualizace softwaru a instalace ochranného softwaru. Bezpečná identifikace Naučení se zabezpečit elektronickou identifikaci pomocí metod, jako jsou silná, jedinečná hesla a dvoufaktorové ověřování.
C.3 Zkoumání sledovatelnosti online	Správa sledování Zavedení opatření k omezení a správě sledování vlastních aktivit na internetu, včetně používání rozšíření prohlížeče, která blokují sledovací zařízení a soubory cookies. Kontrola komunikace Znalost a používání opatření k zastavení přijímání nevyžádaných zpráv nebo e-mailů, jako jsou filtry spamu a pravidla pro e-maily.
C.4 Ověřování informací	Kontrola zdroje Připravenost ověřit si informace z více zdrojů. To pomáhá rozpoznat a pochopit různé úhly pohledu nebo zájmy, které se skrývají za konkrétními informacemi a zdroji dat. Rozpoznávání předsudků Naučení se rozpoznávat potenciální zkreslení informací a uvědomění si, že každý zdroj dat může být zkreslený na základě svého původu nebo účelu.
C.5 Vzájemná ochrana údajů	Úvahy o sdílení údajů Pravidelné zjišťování, zda jsou sdíleny osobní údaje jiných osob a zda nemohou být zneužity. Právní povědomí Uvědomění si, že sdílení informací o jiných osobách může mít závažné právní důsledky. Před sdílením cizích osobních údajů je třeba si vždy vyžádat souhlas.

4. Vztahy mezi kompetencemi

Kompetence potřebné pro samostatné a zodpovědné využívání online služeb lze rozdělit do tří představených tematických okruhů. Tyto klastry jsou vzájemně propojeny. *Data jako zboží* a *Soukromí jako lidské právo* se překrývají při zvažování (oprávněného) zájmu společností využívajících data a vlastního soukromí. Kurikulum se zabývá rovnováhou mezi zájmy podniků na využívání dat a právy na soukromí jednotlivce. To pomůže studentům pochopit širší důsledky ekonomiky dat, jako je informační asymetrie a nerovnováha moci mezi společnostmi, korporacemi a státem.⁸

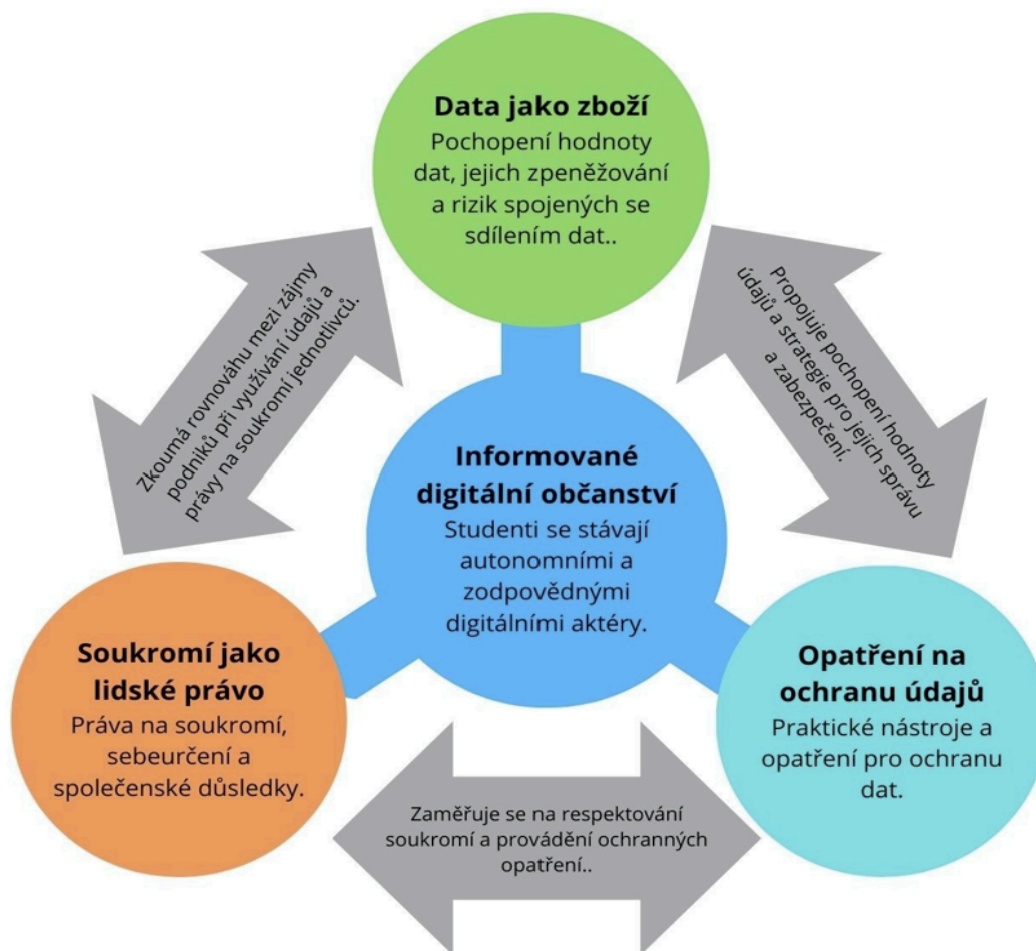
Opatření na ochranu údajů a *Soukromí jako lidské právo* se překrývají v pragmatických otázkách, jak chránit individuální údaje a zároveň zohlednit práva na soukromí ostatních. To znamená, že učební plán počítá nejen s tím, že bude jednotlivce učit, jak chránit své vlastní údaje, ale vštěpuje jim také respekt k soukromí údajů ostatních. Vzájemná praxe péče o osobní údaje pojímá soukromí jako vzájemně závislé dobro v rámci demokracií, nikoli jako pouhou osobní preferenci. Uznání vzájemné závislosti pomáhá studentům pochopit, že nestarání se o vlastní soukromí vede také k erozi práva na soukromí v širší společnosti a že udržování online soukromí pro ně samotné i pro ostatní posiluje demokracii.

Tuto tautologii doplňuje vztah mezi *Opatřeními na ochranu údajů* a *Údaji jako zbožím*. Tato témata se překrývají v pragmatice toho, jak využívat vlastní údaje s ohledem na informační asymetrii. Tento průsečík se zaměřuje na praktické dovednosti potřebné k odpovědnému a efektivnímu spravování a využívání osobních údajů v různých kontextech.

Dynamika a závislosti mezi jednotlivými dimenzemi vzdělávání v oblasti ochrany údajů jsou znázorněny v následujícím schématu kompetencí (*obrázek 1.*). Kurikulum nerozlišuje důležitost kompetencí z jednoho tématu oproti kompetencím z jiného tématu. Každá kompetence a její vzájemné působení s ostatními kompetencemi jsou považovány za stejně zásadní pro soběstačnost a svobodu jednotlivců v informační společnosti. Tyto základní dovednosti a základní porozumění

⁸ Viz například van de Waerdt, P.J. (2020) "Information asymmetries: recognizing the limits of the GDPR on the data-driven market", *Computer Law & Security Review*, 38, s. 105436. Dostupné [na adrese: https://doi.org/10.1016/j.clsr.2020.105436](https://doi.org/10.1016/j.clsr.2020.105436).

třem dimenzím ochrany údajů jsou považovány za nezbytné pro to, aby se jednotlivci mohli účinně a zodpovědně pohybovat v digitálně propojeném světě.



Obrázek 1: Schéma kompetencí. Diagram znázorňuje tři tematické skupiny ("Data jako zboží", "Soukromí jako lidské právo" a "Opatření na ochranu údajů"), které tvoří trojúhelník. Uprostřed je zastřešující cíl "Informované digitální občanství", který je propojen se všemi dimenzemi, což značí jeho integraci a závislost na jejich vzájemném působení.

5. Širší výsledky učení

Jedním z celkových cílů vzdělávání studentů v tom, aby jako digitální občané činili informovaná rozhodnutí, by mělo být nepřímé rozpoznání škodlivého chování na internetu. To může zahrnovat útoky na kybernetickou bezpečnost, jako je phishing nebo ransomware. Dále může být obtížnější rozlišit útoky na demokratickou svobodu a diskurz v podobě dezinformačních kampaní. Takové otázky nejsou ústředním tématem tohoto kurikula, přesto jsou považovány za přidružené výhody při osvojování si kompetencí v rámci projektu DataPro. Proto znalost toho, jak online platformy

profitují z pozornosti svých uživatelů, a to jak pozitivní, tak negativní, předpokládá uvědomění si tématu *Data jako zboží*. Takové znalosti by mohly studentům pomoci kriticky pohlížet na senzační titulky a zmanipulované informace a vybavit je nástroji pro identifikaci a nakládání s dezinformacemi na internetu. Propojení kompetencí ze skupiny A: *Data jako zboží* se skupinou B: *Soukromí jako lidské právo* proto podporuje demokratické povědomí a odolnost vůči útokům, jako jsou dezinformace.

Znalost mechanismů obchodování s údaji a uplatňování postupů minimalizace údajů pomáhá studentům chránit se před kontrolou jejich chování. Mechanismy kontroly chování jsou na online platformách všudypřítomné, např. v algoritmické reklamě a algoritmech, které se snaží vydělávat na pozornosti prostřednictvím zvyšování času stráveného na obrazovce služby. Vzájemná závislost mezi tématem A: *Data jako zboží* a tématem C: *Opatření na ochranu údajů* podporuje autonomii a sebeurčení studentů online.

Pokud jde o kybernetickou bezpečnost, prolíná se téma B: *Soukromí jako lidské právo* a téma C: *Opatření na ochranu údajů*. Propojení hodnoty soukromí na internetu s praktickými opatřeními na jeho ochranu pomáhá studentům vytvořit si odolnost vůči podvodným praktikám. Negativním příkladem nedostatku online soukromí je zneužívání osobních údajů např. autoritativními státy nebo organizovaným zločinem. Posílení studentů v boji proti podvodným praktikám znamená v celém rozsahu pochopení rizik ochrany soukromí a praktických způsobů, jak si soukromí na internetu uchovat s pomocí kompetencí ze skupiny C.

6. Závěr pro pedagogy

Aby si Žáci osvojili kritické povědomí o digitálních technologiích a podpořili jejich přínosné a efektivní využívání, je zásadní vyučovat kompetence z okruhů A, B a C. Na základě všeobecného rámce DigComp⁹, budou následující klíčové poznatky kurikula pro pedagogy orientačními body:

Ochrana zařízení a digitálního obsahu:

- Vzdělávejte studenty v oblasti ochrany digitálních zařízení před hrozbami, jako je malware a fyzické poškození, pomocí antivirového softwaru, pravidelných aktualizací a bezpečných hesel.
- Naučte studenty rozpoznat hrozby, jako je phishing, ransomware, krádež identity a kyberšikana, a reagovat na ně.

Porozumění bezpečnostním opatřením:

- Poučte je o bezpečném surfování na internetu, dvoufaktorovém ověřování a používání zabezpečených sítí, jako jsou sítě VPN.
- Zdůrazněte, že je důležité chránit osobní údaje, vědět, co sdílet online, a mít silná a jedinečná hesla.

Ochrana osobních údajů a soukromí:

- Zdůrazňujte, že je důležité vyhnout se sdílení citlivých informací na nezabezpečených webových stránkách a porozumět zásadám ochrany osobních údajů digitálních služeb.
- Naučte je, jak nastavit soukromí na sociálních sítích a dalších platformách.

Bezpečné používání a sdílení osobních údajů:

- Vzdělávejte je v oblasti bezpečného sdílení osobních údajů, šifrování citlivých dat a rozpoznávání možných škod způsobených nesprávným používáním dat.

Porozumění zásadám ochrany osobních údajů:

⁹ EU Science Hub a Evropská komise (2022) *DigComp Framework*. Dostupné [na: https://joint-research-centre.ec.europa.eu/scientific-activities-z/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp/digcomp-framework_en](https://joint-research-centre.ec.europa.eu/scientific-activities-z/education-and-training/digital-transformation-education/digital-competence-framework-citizens-digcomp/digcomp-framework_en).

- Vysvětlujte význam zásad ochrany osobních údajů v digitálních službách a naučte studenty je číst a porozumět jim, aby činili informovaná rozhodování.

Předcházení zdravotním rizikům:

- Poučte je o pokynech ke zmírnění zdravotních rizik plynoucích z dlouhodobého používání digitálních zařízení, jako je namáhání očí, špatné držení těla a dopady na duševní zdraví.

Ochrana před digitálním nebezpečím:

- Vzdělávejte je v oblasti rozpoznávání, předcházení a hlášení kyberšikany, online predátorů a dalšího škodlivého chování.

Podpora sociální pohody a začlenění:

- Zdůrazňujte pozitivní aspekty digitálních technologií při podpoře sociálních vazeb a inkluzivních postupů.

Povědomí o dopadech na životní prostředí:

- Učte o důsledcích digitálních technologií pro životní prostředí, včetně elektronického odpadu a spotřeby energie.

Monitorování a zajištění dobrých životních podmínek:

- Aktivně sledujte online aktivity, abyste zajistili pohodu, a v případě potřeby zasáhněte, abyste zabránili škodlivému chování.
- Buďte připraveni okamžitě zasáhnout proti hrozbám ohrožujícím blaho žáků, jako je například kyberšikana.

Umožnit žákům, aby si svých dat vážili jako peněz.

- Jedním z důležitých aspektů, kterým se rámec DigiCompEdu, konkrétně současné aktivity, nezabývá, je hodnota dat jako aktiv.