(Ne)bezpečná digitální stopa

Digitální stopa a její dopady – pro pedagogy a ředitele škol

Lucie Kosová

CZ.NIC | SPRÁVCE DOMÉNY CZ

Úvod do tématu a přehled témat

- Digitální stopa – úvod do tématu
- Právní aspekty a odpovědnost školy
- Digitální stopa v kontextu školního prostředí
- Sociální sítě a rizika sdílení
- Role pedagogů při edukaci žáků v oblasti ochrany soukromí
- Prevence a vzdělávací přístup
- Doporučení a strategie pro školy
- Jak podporovat pozitivní digitální identitu i stopu
- Shrnutí a závěrečná doporučení

Co je digitální stopa a proč je důležitá?

nejrůznější informace, data, údaje **„digitální otisky“** v online prostředí

Existuje celá řada dělení digitálních stop, které jsou utvářeny:

- vědomě
- nevědomě
- veřejně
- neveřejně
- skryté (cookies, metadata)
- vlastní
- přáteli, cizími osobami

Trvalost digitální stopy

“Jednou na internetu, navždy na internetu“

Kde je možno se s ní setkat a kde ji využít nebo zneužít?

- **v online prostředí – kdekoliv**
- **v offline prostředí – škole, zaměstnání**
- v soukromí a volném čase
- personalistice
- marketingu
- při jejím zneužití: v trestně – právní rovině a **kybernetické kriminalitě**

Příklady reálných dopadů z praxe: (kyber)bezpečnost, škola, zaměstnání

- **rodiče** vytvoří svému dítěti virtuální videoalbum „vzpomínek“ na veřejném Youtube kanále. Dítě se tam nachází v situacích a polohách, které mu v dospělosti nemusí být vůbec příjemné. Mohou si ho zde najít přátelé, ale třeba i personalisté až se bude hlásit do svého prvního zaměstnání
- **děti/ žáci sami sobě**:

  -15 letá slečna si dá svůj polonahý snímek na Instagram

  - čerstvě 18 letá natáčí videoklipy pro platformu OnlyFans. O pár let později se hlásí na vysokou školu, chce si dodělat vzdělávání nebo se hlásí do zaměstnání, kde si personalisté mohou její digitální stopu z minulosti bez problémů vyhledat.

Příklady reálných dopadů z praxe: (kyber)bezpečnost, škola, zaměstnání

- **cizí osoby:** „kamarád/ka“ z online hry nabízí za intimní fotku odměny a bonusy navíc. Jakmile získá tuto digitální stopu a intimní materiál, začne ho zneužívat – pomlouvat, vyhrožovat, vydírat nebo virtuálně šířit po sítích.
- **„syntetický“ obsah a AI**: virtuální prostor začíná být zaplaven uměle generovaným obsahem prostřednictvím nástrojů AI (velkými jazykovými modely), mezi nimi můžeme narazit i na **deepnudes**, což mohou být pozměněné fotografie, které mohou využít například reálný obličej, ale přidat k němu jiné nebo uměle vygenerované „AI tělo“. Dotčené osoby se pak mohou stát oběťmi posměchu, **challenges a dalších rizikových jevů** nebo dokonce **kyberšikany, vydírání, groomingu, sextortionu** a podobně.

Právní vědomí, aspekty a odpovědnost školy

- žáci, pedagogové a další zaměstnanci by měli znát **práva i povinnosti**, která jsou s ochranou, bezpečností i nakládáním s digitální stopou spojená
- nutnost vzdělávání učitele a žáky – poskytovat pravidelná školení o rizicích digitální stopy a způsobech její ochrany
- zvyšovat povědomí o deepfake technologiích – jak lze AI zneužít k manipulaci s digitální identitou
- chránit osobní údaje a omezit veřejné sdílení informací: pečlivě zvažovat zveřejňování jmen, fotografií a dalších údajů na školních webech a sociálních sítích. Nastavit pravidla pro sdílení fotografií žáků a zajistit, aby k tomu rodiče vždy poskytli informovaný souhlas - dle GDPR i občanského zákoníku (NPI, 2025)

GDPR a ochrana osobních údajů ve škole

- škola jako správce osobních údajů potřebuje mít jasné **postupy a směrnice**
- zodpovídá za **uchovávání, shromažďování** i **zabezpečení** údajů, dat i metadat
- jedná se o:
  - jména, fotografie, známky, hodnocení, absence
  - práce žáků, záznamy z online hodin, IP adresy, metadata
  - citlivé údaje (zdravotní, sociální situace)

GDPR a ochrana osobních údajů ve škole: povinnosti školy

- minimalizujeme data - sbíráme jen to, co je opravdu nezbytně nutné
- zabezpečujeme údaje - hesla, přístupová práva, šifrování
- vhodně nakládáme se školní dokumentací, fotografiemi i dalšími audio-video materiály
- škola má jasně nastavena pravidla sdílení dat mezi pedagogy

GDPR a ochrana osobních údajů ve škole: práva žáků i rodičů

- právo na přístup k údajům
- právo na opravu nebo omezení osobních údajů
- právo na nesouhlas se zpracováním osobních údajů
- právo na „zapomenutí“ - po uplynutí lhůt (školský zákon, archivace, interní komunikace) možnost vymazání nepotřebných osobních údajů

GDPR a ochrana osobních údajů ve škole: práva žáků i rodičů

- právo na přístup k údajům
- právo na opravu nebo omezení osobních údajů
- právo na nesouhlas se zpracováním osobních údajů
- právo na „zapomenutí“ digitálních stop - po uplynutí lhůt (školský zákon, archivace, interní komunikace) možnost smazání nepotřebných osobních údajů

GDPR – doporučení pro školní praxi

- možnost pravidelného školení pro zaměstnance – ideálně jedenkrát ročně/jednou za dva roky
- jasně stanovit role – pověřenec, ICT koordinátor, metodik prevence
- používat bezpečné komunikační kanály – školní e-maily a intranet, bezpečné komunikační platformy – například Signal, Threema
- nesdílet jména nebo fotografie žáků na veřejných sociálních sítích bez informovaného souhlasu

Digitální stopa v kontextu školního prostředí

Každodenní prací žáků i pedagogů vznikají nové:

- záznamy o žácích (docházka, výsledky hodnocení, fotografie, správa zařízení)
- komunikace v systémech (Bakaláři, Teams/y/, G-classroom, EduPage…)
- digitální obsah žáků (prezentace, videa, projekty)

  Rizika:

  - nechtěné zveřejnění

  - únik dat,

  - sdílení bez souhlasu
- Silná role školy v ochraně a edukaci

Jak pracovat s osobními i školními daty bezpečně. Co rozlišovat?

osobní údaj × **citlivý údaj** × běžné školní informace

Bezpečné ukládání:

- Hesla
- Šifrování
- Zálohování

Vytvořit jednotnou **metodiku** a opřít se o školské směrnice

Ochrana soukromí žáků a učitelů

Důležité je důkladně chránit obrazový i audiovizuální materiál (fotky, videa a podobně)

- kdo smí ve škole fotit a kdy (např. školní fotograf, žáci v rámci úkolu ve vyučování)
- kde mohou nebo nemohou být fotky a videa zveřejněny (např. školní web pro registrované uživatele, uzavřená a bezpečná sociální platforma opatřená vícefaktorovým ověřením a end-to-end šifrováním, nástěnka ve školní třídě)
- ochrana digitální identity – online vyučování a e-maily, minimalizace digitální stopy pedagoga v komunikaci s rodiči a žáky – jasná a jednoznačná pravidla/vodítka pro komunikaci na sociálních sítích a platformách

Sociální sítě a rizika sdílení

Žáci:

- na sítích často **nevědomě** sdílí příliš mnoho informací

Škola a pedagogové:

Co o žácích sdílet?

- oficiální informace a data prostřednictvím informačních systému, doplňkově přes **bezpečné** a **zabezpečené** sociální sítě a platformy

Co o žácích (ne)sdílet?

- velmi citlivé informace, data, situace vždy „offline“ a vhodně komunikovat jen k „pověřeným osobám – rodičům, zákonným zástupcům, OSPOD, OČTŘ a podobně

Jak sociální sítě pracují s daty i digitální stopou a jak je využívají

Sociální platformy pracují s daty v rámci:

- profilování
- algoritmů (personalizovaných)
- metadat

Riziky jsou:

- manipulace s informacemi a daty
- kyberšikana, sextortion, sexting
- deepfake a syntetické obsahy

Co by měli učitelé vědět o online profilování, co digitální stopa utváří

- **profilování** může být automatizovaný proces vedoucí (k) vyhodnocování chování žáka
- **(personalizované) algoritmy** mohou ovlivňovat to, co žák vidí – obsahy, doporučení, reklamy – na tuto oblast a snížení dopadů se zaměřuje i Digital Services Act (DSA) – snaha o minimalizaci dopadu na děti/žáky v § 28, § 34, §35
- umět pomoci žákům vědomě utvářet i budovat bezpečnou digitální stopu ve školním prostředí
- pomoci bezpečně nastavit nejen školní zařízení, ale i vysvětlit rizika zranitelností a dopadů.

Role pedagoga při edukaci žáků v oblasti ochrany soukromí

- Pedagog je pro žáky vzorem v online komunikaci
- informuje žáky o principech utváření, budování, sdílení, trvalosti digitálních stop
- edukuje o ochraně, rizicích i dopadech digitální stopy v závislosti na ochraně soukromí, bezpečnosti a kritickém myšlení
- Vytváří **bezpečný prostor** (security) **a prostředí** (safety) **pro hlášení problémů**
- spolupracuje v případě potřeby i možnosti s rodiči

Prevence a vzdělávací přístup

- důležité je zapojení celého **týmu** – metodik prevence, ICT koordinátor, případně výchovný poradce, sociální pedagog, školní psycholog – v případě řešení problému, závažné události nebo incidentu vedení školy
- vytvářet a aktualizovat preventivní programy zaměřené na bezpečnost na internetu
- pracovat s: reálnými scénáři, kazuistikami – příklady dobré i méně dobré praxe, modelovými situacemi, formou zážitkové pedagogiky
- komplexně a dlouhodobě budovat pozitivní digitální návyky a bezpečnost i bezpečné prostředí
- informovat a trénovat o tom, jak reagovat na problém nebo incident – stanovit si stručný postup. Vědět na koho se je možno s důvěrou obrátit v případě problému.

Jak učit žáky o digitálních stopách: metodické materiály a nástroje

Praktické ukázky:

- vyhledávání vlastních digitálních stop na internetu a sociálních sítích
- analýza metadat u těchto stop
- ověřování informací – rozeznávání důvěryhodných a méně důvěryhodných zdrojů a autorit, licencí (zdroje např. CZ.NIC, SIC, E-Bezpečí, MVČR, NÚKIB, NPI, EDUin)
- seznámení s autorským zákonem a autorskými právy (důležité například pro oblast práce s AI/LLM – kdo je nebo není zodpovědný za deepfake a syntetický obsah)

„Najdi informaci, které by mohla být zneužitelná“

Jak a kde používat kritické myšlení i ověřování informací v kontextu digitálních stop

- ověřovat zdroje informací
- rozeznávání manipulace a zkreslení – ukazovat si příklady fake news, deepfakes
- AI obsah: deepfakes, deepnudes, syntetické obsahy i data
- probírat i sdílet s žáky, to, že digitální stopa může mít mnoho podob – nemusí být vždy „pravá“
- praktické nástroje pro ověřování (např. metodou OSINT – příběh Sáry – AI dětem)

Praktické tipy: co dělat, když se objeví problém?

- mít stanoveny praktické kroky, které použijeme při ohrožení nebo zneužití digitální stopy
- vytvořit si „plán B“ – když nevyjde jedna možnost řešení problému nebo situace, mít další „záložní“ možnost (evokuje pocit většího bezpečí i naděje na vyřešení)
- Vědět, jaká je **komunikační strategie** školy, **jak vhodně komunikovat v krizových situacích**
- **Kdy koho kontaktovat: rodiče, vedení školy, OSPOD, PČR**
- jak uchovávat „digitální“ i fyzické důkazy
- **podporovat toho, komu se problém stal** (oběti)
- **prevence** následných problémů nebo incidentů

Doporučení a strategie pro školy, zásady bezpečné komunikace

- vytvoření školní bezpečnostní politiky ochrany dat
- stanovení (z)odpovědností – ředitel, ICT koordinátor, třídní učitel, metodik prevence
- jasná a srozumitelná pravidla pro zveřejňování obsahu a fotografií
- bezpečná a etická komunikační „kultura“
- spolupráce s rodiči, participujícími i širší zapojovanou komunitou

Jak podporovat pozitivní digitální stopu žáků (digitální wellbeing, digitální i profesní identita)

- učit žáky co je to digitální wellbeing a jak s ním pracovat – provázení digi-well prostředím
- podpora vhodné digitální identity žáků – co je bezpečné a co ne, jak pracovat se školními zařízeními, jak bezpečně přistupovat k digitálním technologiím i tvorbě a volení procesů i produktů digitální identity
- budování digitální stopy pomocí soutěží, projektových dnů a projektů, prezentací, sdílení kreativních nápadů i výstupů k tématu
- učit se uvědoměle pracovat s „veřejnými“ profily i „neveřejnými“ informacemi
- Učit se, jak se prezentovat v online světě bezpečně, eticky a profesionálně

Shrnutí & závěrečná doporučení

- **digitální stopy** jsou zásadním tématem a je nutné se jím ve škole důkladně zabývat
- může ovlivnit fyzickou i kybernetickou bezpečnost, bezpečnost v online prostředí a na internetu žáků i celé školy
- je vhodné mít **celoškolní strategii** (v oblastech zaměřených na systémy a nástroje i v oblastech zaměřených na člověka a lidskou chybu) **jako prevenci pro zvládání rizik a varovných signálů,** které mohou vyústit v ohrožující incidenty nebo události
- **je potřebné prvořadě podporovat budování digitální identity i vědomé digitální stopy (nejen) žáků, ale i celého „ekosystému“ školy.**
- **digitální i online bezpečnost je celoživotní proces a živý organismus, proto je potřebné takto přistupovat i k budování bezpečnostního povědomí a k bezpečnému budování digitální identity (Moje ID) i digitální stopy (PČR a SIC ČR - Nebudujte svému dítěti digitální stopu)**

Zdroje:

https://digitalizace.rvp.cz/napric-predmety/kyberneticka-bezpecnost

https://policie.gov.cz/clanek/akce-a-projekty-nebudujte-svemu-diteti-digitalni-stopu.aspx

https://digitalizace.rvp.cz/clanky/digitalni-stopa-ve-skole

https://digitalizace.rvp.cz/files/kyberprevence-plakat-a4-zasady-zamestnance.pdf

https://digitalizace.rvp.cz/files/kyberprevence-plakat-a4-zasady-pro-rodice.pdf

https://osveta.nukib.gov.cz/local/dashboard/

https://portal.nukib.gov.cz/informacni-servis/podpurne-materialy/68666293c0ce8d07aa01b297

Zdroje:

https://edu.ceskatelevize.cz/video/7733-jak-na-internet-digitalni-stopa

https://clanky.rvp.cz/clanek/23705/DIGITALNI-STOPA.html

https://elearning.ecrime.cz/mod/resource/view.php?id=3259&forceview=1

https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/socialni-site/4609-digitalni-stopa-co-to-je-a-proc-je-dulezite-ji-chranit

https://padlet.com/pavelmatejicek/osint-a-cybersec-tooly-n77p8sipeuzf12n4

https://manena.info/2025/10/10/ucitel-in-digitalni-stopa-v-dobe-ai/

https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

https://nebudobet.cz/digitalni-stopa/

Děkuji vám za pozornost!

Lucie Kosová

CZ.NIC | SPRÁVCE DOMÉNY CZ