

si dovoluje Vás pozvat na seminář

„Digitální forenzika pro sociální pracovníky“

**Instituce akreditovaná u Ministerstva vnitra ČR
Akreditace Ministerstva práce a sociálních věcí**

**Termín a místo konání: 26. června 2026 od 9:00
online**

Lektor: JUDr. Ing. Radovan Dávid, Ph.D.

sedmnáctiletá praxe asistenta soudce Ústavního soudu, osmnáctiletá praxe lektora právnických fakult v Brně a Bratislavě, patnáctiletá praxe v oblasti vzdělávání úředníků, člen Světové organizace pro rodinné právo, čestný člen Profesní komory sociálně-právní ochrany dětí, člen redakční rady Juridical Analytical Journal, autor desítek článků, monografií (mimo jiné učebnice rodinného práva a civilního práva procesního) a komentářů (mimo jiné k občanskému zákoníku, občanskému soudnímu řádu, zákonu o zvláštních řízeních soudních a exekučnímu řádu)

Digitální stopy hrají stále větší roli při ochraně práv dětí i dospělých klientů. Sociální pracovníci se ve své praxi mohou setkat s případy, kde hrají klíčovou roli mobilní telefony, počítače, chatové aplikace, sociální sítě či cloudové služby. Tyto digitální stopy mohou sloužit jako důkaz šikany, týrání, sextortion, manipulace nebo finančního zneužívání. Zároveň je ale práce s nimi náročná – vyžaduje znalost toho, jak důkazy zajistit, uchovat a předat orgánům činným v trestním řízení tak, aby neztratily svoji hodnotu. Sociální pracovníci se navíc musí pohybovat na hranici mezi odbornou intervencí a právními limity: nesmějí suplovat práci policie, ale musejí vědět, co mohou a co naopak nesmí činit. Seminář účastníkům přiblíží základy digitální forenziky ve světě sociální práce: jaké druhy digitálních důkazů lze získat, jak je rozpoznat, jak se k nim chovat, co zaznamenávat a jak spolupracovat s policií, školami či dalšími institucemi. Důraz bude kladen na praktické dovednosti – od uchování screenshotů přes komunikaci s rodiči až po dokumentaci do spisu. Účastníci získají jistotu, jak jednat v situacích, kdy je digitální stopa klíčová pro ochranu dítěte nebo zletilého klienta.

Po absolvování programu bude účastník schopen:

- rozpoznat různé typy digitálních stop a důkazů
- vysvětlit základní principy digitální forenziky v sociální práci
- uchovávat a dokumentovat digitální důkazy přezkoumatelným způsobem
- rozlišit, co sociální pracovník smí a co nesmí provádět

- správně spolupracovat s policií a dalšími institucemi
- komunikovat s rodiči, dětmi i zletilými klienty o digitálních stopách
- chránit osobní údaje při práci s digitálním materiálem
- vyhodnotit relevanci digitálních stop pro vlastní šetření
- zapojit digitální forenziku do vyhodnocování ohrožení dítěte
- předcházet sekundární viktimizaci klienta při práci s důkazy
- využít metodické nástroje a kontrolní seznamy v praxi
- zpracovat doporučení do spisu nebo pro soud

Dotazy, na něž by měl být kurz především zaměřen, lze posílat na kontaktní e-mail radovandavid@radovandavid.cz.

Obsah kurzu:

1. Úvod do digitální forenziky

- základní pojmy a principy
- digitální stopa jako klíčový zdroj informací
- význam pro sociální práci a ochranu klienta
- rozdíl mezi forenzikou a běžným užíváním technologií
- typické situace z praxe OSPOD a sociálních služeb
- meze působnosti sociálního pracovníka
- spolupráce s IT odborníky a policií
- kazuistiky z českého i zahraničního prostředí
- etický rámec při práci s digitálními daty
- nejčastější omyly pracovníků v terénu

2. Typy digitálních důkazů

- komunikace v chatovacích aplikacích (WhatsApp, Messenger)
- sociální sítě (Facebook, Instagram, TikTok)
- fotografie, videa a metadata
- e-maily a elektronické dokumenty
- geolokační data a GPS stopy
- historii prohlížení a online nákupy
- cloudové služby a sdílené složky
- data z chytrých zařízení (hodinky, IoT)
- kyberšikana a online útoky jako digitální stopy
- příklady využitelných důkazů v praxi

3. Zásady práce s digitálními důkazy

- pravidla pro uchování integrity dat
- proč nepředávat originální zařízení
- využití printscreenů a jejich limity
- práce s digitální kopií a zálohou
- dokumentace řetězce předávání důkazů
- rizika manipulace s daty
- zásada minimálního zásahu do soukromí
- postup při nalezení digitálních důkazů v terénu
- spolupráce s IT specialisty
- příklady dobré a špatné praxe

4. Právní rámec

- zákon o sociálně-právní ochraně dětí a digitální důkazy
- GDPR a práce s osobními údaji
- povinnosti a limity sociálního pracovníka
- trestní řád a role policie při zajištění důkazů
- soudní praxe k digitálním stopám
- rozdíl mezi podnětem a důkazem v řízení
- právo dítěte a klienta na soukromí
- povinnost mlčenlivosti pracovníka
- mezinárodní rámec (Úmluva o právech dítěte, ESLP)
- riziko nezákonného zásahu do práv

5. Role sociálního pracovníka

- identifikace digitálních stop v praxi
- rozhodování, co zaznamenat a co předat
- hranice mezi šetřením a vyšetřováním
- prevence přetížení informacemi
- dokumentace a spisová praxe
- informování dítěte a rodičů o postupu
- respekt k důstojnosti klienta
- komunikace s institucemi (škola, zdravotnictví)
- předávání podkladů policii
- vlastní odpovědnost pracovníka

6. Nástroje a techniky v praxi

- jednoduché nástroje dostupné pracovníkům
- aplikace pro snímání obrazovky a archivaci
- uchování metadat (EXIF, časové značky)
- bezpečné ukládání a šifrování dat
- formuláře a checklisty pro práci v terénu
- školení pracovníků v základních technikách
- hranice mezi běžnou dokumentací a forenzikou
- rozdíly mezi amatérským a profesionálním zajištěním dat
- využití mobilních zařízení při dokumentaci
- příklady z terénní praxe

7. Spolupráce s policií a odborníky

- jak a kdy zapojit policii
- předávání digitálních důkazů bezpečným způsobem
- koordinace s IT specialisty a znalci
- důležitost řetězce předávání (chain of custody)
- příklady neuznatelných důkazů
- komunikace s rodinou při zapojení policie
- role státního zástupce a soudu
- ochrana dítěte při vyšetřování
- příklady dobré spolupráce z praxe
- prevence konfliktu kompetencí

8. Ochrana dítěte a prevence sekundární viktimizace

- práce s citlivými materiály (intimní fotografie)
- informování dítěte o účelu zajištění dat
- prevence stigmatizace a zahanbení

- bezpečné zapojení rodičů do procesu
- ochrana soukromí dítěte při dokumentaci
- zajištění podpory psychologa nebo krizového centra
- komunikace s dítětem o rizicích digitálních stop
- prevence opakovaného zkoumání téhož materiálu
- citlivé zacházení s oběťmi sextortion nebo grooming
- judikatura k ochraně dítěte při dokazování

9. Digitální forenzika a rodina

- role rodičů při předávání digitálních stop
- konflikt mezi rodiči ohledně využití důkazů
- hranice rodičovské kontroly a práv dítěte
- sdílení důkazů v rodinných sporech
- riziko manipulace digitálních stop rodiči
- práce s důkazy ve sporech o svěřeni dítěte
- zapojení opatrovníka ad hoc
- komunikace s rodiči o uchování materiálů
- právní odpovědnost rodiny
- příklady z rodinného práva

10. Etické a metodické otázky

- etika práce s digitálními materiály
- prevence neoprávněného šíření důkazů
- zásada „co není nezbytné, nesbírej“
- hranice profesionality v práci se soukromím
- metodická doporučení MPSV a OSPOD
- využití případových konferencí
- dilemata v ochraně soukromí vs. ochraně dítěte
- význam supervize a týmové podpory
- odpovědnost vedoucích pracovníků
- příklady etických selhání

11. Kazuistiky z praxe

- sextortion a role digitálních důkazů
- kyberšikana mezi žáky a předání důkazů škole
- grooming v online hře – chatová komunikace
- rodič manipulující digitální důkazy ve sporu
- neuznatelné důkazy kvůli špatnému postupu OSPOD
- úspěšná spolupráce s policií při dokumentaci
- případová konference nad digitálními stopami
- reakce dítěte na uchování jeho komunikace
- inspirace z judikatury
- poučení pro další praxi

12. Diskuse a závěr

- shrnutí hlavních principů
- doporučené postupy pro praxi OSPOD a sociálních služeb
- sdílení zkušeností účastníků
- reflexe etických a právních dilemat
- diskuse nad kazuistikami z praxe
- inspirace pro metodické standardy
- návrhy na rozvoj digitálních kompetencí

- doporučení pro další vzdělávání
- využití supervize v digitální agendě
- závěrečná reflexe účastníků