



RADOVAN DÁVID
vzdělávací společnost

si dovoluje Vás pozvat na seminář

„Digitální forenzika pro sociální pracovníky“

Akreditace Ministerstva práce a sociálních věcí

Akreditace Ministerstva vnitra České republiky

Termín a místo konání: 14. listopadu 2025 od 9:00

online

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

lektor na právnických fakultách (Brno a Bratislava), šestnáctiletá praxe asistenta soudce Ústavního soudu, 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 exekutivnímu řádu)

Digitální forenzika, tedy odborné zajišťování, uchovávání, analýza a prezentace elektronických důkazů, se stále častěji stává součástí práce sociálních pracovníků, zejména v oblasti sociálně-právní ochrany dětí (OSPOD). Elektronické stopy mohou hrát klíčovou roli při odhalování kyberšikany, groomingového chování, domácího násilí či zanedbávání péče, a také při prokazování či vyvracení tvrzení účastníků řízení.

Pro pracovníky OSPOD je zásadní porozumět **právním limitům** při získávání a uchovávání digitálních důkazů, umět rozlišit, kdy a jak mohou sami zajistit digitální stopy, a kdy je nutné přizvat specializovaného experta či policii. Současně musí dbát na **ochranu soukromí dítěte**, dodržování zásad GDPR a na procesní použitelnost takto získaných informací.

Školení nabídne srozumitelný úvod do principů digitální forenziky, praktické postupy přizpůsobené roli OSPOD a doporučení, jak spolupracovat s dalšími subjekty, aby digitální důkazy obstály v soudním a správním řízení.

Na konci vzdělávacího programu bude účastník schopen:

- vysvětlit základní principy digitální forenziky
- rozpoznat, jaké digitální stopy mohou být relevantní v případech SPOD
- znát právní rámec zajišťování digitálních důkazů
- dodržet zásady ochrany osobních údajů při práci s elektronickými stopami
- vyhodnotit, kdy postupovat sám a kdy zapojit odborníka/policii
- zajistit uchování integrity digitálních důkazů
- dokumentovat a řádně popsat získané digitální stopy
- spolupracovat s IT specialisty, znalci a orgány činnými v trestním řízení
- připravit podklady pro soudní řízení tak, aby byly procesně použitelné

Obsah kurzu:

1. Úvod do digitální forenziky pro OSPOD

- Co je digitální forenzika a její využití v praxi SPOD
- Typické situace vyžadující digitální důkazy (kyberšikana, grooming, domácí násilí)
- Zdroje digitálních důkazů (mobilní telefony, počítače, sociální sítě, e-maily)
- Rozdíl mezi neformálním zajištěním a forenzním zajištěním
- Role sociálního pracovníka vs. role policie a znalců
- Základní pojmy (hash, metadata, řetězec důkazní stopy)
- Rizika neodborného zásahu do důkazů
- Mezinárodní doporučení k ochraně dětí v digitálním prostředí
- Příklady z praxe

2. Právní rámec práce s digitálními důkazy

- Občanský zákoník – ochrana osobnosti a soukromí
- Zákon o SPOD – pravomoci OSPOD při zajišťování důkazů
- GDPR a zvláštní ochrana osobních údajů dětí
- Trestní zákoník – trestné činy související s digitálními daty
- Trestní řád – získávání a zajišťování elektronických důkazů
- ZŘS – předkládání a hodnocení důkazů v civilních řízeních
- Správní řád – podklady pro rozhodování
- Zásada proporcionality a nezbytnosti zásahu
- Mezinárodní úmluvy (Úmluva o právech dítěte, Budapešťská úmluva o kyberkriminalitě)

3. Druhy digitálních důkazů relevantních pro OSPOD

- Textová komunikace (SMS, chat, e-maily)
- Fotografie a videa
- Záznamy hovorů
- Metadata (čas, GPS poloha, typ zařízení)
- Aktivita na sociálních sítích
- Protokoly z online platform a her
- Digitální školní záznamy a elektronické žákovské knihy

- Historie prohlížení internetu
- Záznamy z kamerových systémů

4. Postupy zajištění digitálních důkazů

- Okamžitá identifikace relevantního důkazu
- Pořízení kopie obrazovky (screenshot) a její dokumentace
- Export komunikace z aplikací
- Uložení digitálních souborů v původním formátu
- Zachování metadat bez jejich změny
- Použití hash funkcí k ověření integrity
- Zabezpečené ukládání důkazů
- Označení a popis důkazního materiálu
- Předání důkazů policii nebo znalci

5. Spolupráce s odborníky a policií

- Kdy je nutné zapojit policii ihned
- Postup při podezření na trestný čin
- Jak komunikovat s IT specialisty a znalci
- Společné zajištění důkazů s policií
- Pravidla předávání elektronických důkazů
- Uchování kopie pro účely SPOD
- Koordinace s právníky při přípravě podkladů
- Ochrana identity dítěte při spolupráci s externími subjekty
- Sdílení informací v souladu s právem

6. Ochrana soukromí a práv účastníků

- Právo dítěte na soukromí v digitálním prostředí
- Limity monitoringu online aktivit dítěte pracovníkem OSPOD
- Zásady minimalizace shromažďovaných dat
- Informovaný souhlas, pokud je vyžadován
- Povinnost mlčenlivosti a její limity
- Zajištění, aby získané důkazy nebyly zveřejněny
- Postup při incidentu úniku dat
- Balanc mezi ochranou dítěte a ochranou práv ostatních osob
- Etické zásady při práci s digitálními důkazy

7. Dokumentace a uchovávání důkazů

- Vedení spisu s elektronickými důkazy
- Chronologické zaznamenávání úkonů
- Popis okolností získání důkazů
- Připojení důkazů k úředním záznamům
- Zajištění dlouhodobé čitelnosti dat
- Archivace dle interních směrnic a zákonných povinností

- Likvidace dat po uplynutí doby uchování
- Přístup k důkazům oprávněným osobám
- Zajištění přezkoumatelnosti v soudním řízení

8. Hodnocení důkazů v řízení

- Procesní použitelnost digitálních důkazů
- Hodnocení autenticity a integrity
- Důkazní síla různých typů digitálních stop
- Kombinace digitálních a jiných důkazů
- Rizika nesprávného hodnocení
- Vliv forenzních zpráv znalců
- Příklady soudních rozhodnutí
- Role OSPOD při prezentaci důkazů soudu
- Argumentace pro jejich přijetí

9. Praktická doporučení pro OSPOD

- Interní směrnice k práci s digitálními důkazy
- Školení pracovníků v základech digitální forenziky
- Používání standardizovaných formulářů pro popis důkazů
- Spolupráce s IT odborníky při každodenní práci
- Prevence ztráty či poškození digitálních důkazů
- Využití bezpečnostních technologií a šifrování
- Pravidelné vyhodnocování postupů v praxi
- Sdílení zkušeností s ostatními OSPOD
- Vytváření případových studií pro interní vzdělávání

10. Diskuse a závěr školení