



RADOVAN DÁVID

vzdělávací společnost

si dovoluje Vás pozvat na seminář

„Alternativní způsoby dokazování v době digitalizace – od screenů po blockchain“

Instituce akreditovaná u Ministerstva vnitra ČR

Termín a místo konání: 9. dubna 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 exekutivnímu řádu)

Digitalizace proměnila způsob, jakým vznikají, uchovávají se a hodnotí důkazy. Elektronická komunikace, sociální sítě, chytré telefony či cloudové služby se staly hlavními zdroji informací o chování a jednání účastníků řízení. Tradiční pojetí listinných a svědeckých důkazů ustupuje a praxe čím dál častěji pracuje s „alternativními“ formami – screenshoty, metadaty, záznamy z kamer, sdílenými úložišti nebo daty z blockchainu. Právní řád přitom na tuto proměnu reaguje pomalu a zůstává otázkou, jak tyto důkazy získávat, ověřovat a hodnotit tak, aby obstály v soudním či správním řízení. Seminář přinese praktický přehled o tom, jaké digitální důkazy lze využívat ve správních a civilních řízeních, jak posuzovat jejich autenticitu a jak se bránit proti falzifikacím a manipulacím. Pozornost bude věnována také právní váze elektronických dokumentů, možnostem ověřování elektronické identity, principům důkazní hodnoty a řetězce důvěry. Účastníci se naučí rozpoznávat spolehlivé digitální důkazy, bezpečně je ukládat a předkládat, hodnotit jejich relevanci i rizika. Kurz zároveň otevře diskusi o budoucnosti dokazování – o využití umělé inteligence, prediktivních algoritmů a blockchainových úložišť jako prostředků ověřování pravosti informací.

Na konci programu bude absolvent schopen:

- orientovat se v právním rámci digitálních důkazů
- rozlišit jednotlivé typy elektronických důkazů a jejich právní váhu
- vyhodnotit autenticitu screenshotů, e-mailů a online komunikace
- znát zásady bezpečného získávání digitálních dat

- využívat elektronické podpisy a časová razítka
- porozumět principům řetězce důvěry a integrity důkazu
- pracovat s důkazy z cloudových a blockchainových úložišť
- odlišit originál, kopii a manipulovaný digitální důkaz
- zohlednit soulad s GDPR a právem na soukromí
- formulovat návrhy na provedení důkazu v elektronické podobě
- posoudit použitelnost důkazů v soudním a správním řízení
- využít moderní technologie pro dokumentaci skutkového stavu
- orientovat se v elektronických identitách a ověřování
- aplikovat zásadu přiměřenosti při dokazování online daty
- identifikovat etické a právní limity využívání AI při dokazování

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

Obsah kurzu:

1. Proměna důkazního prostředí v digitálním věku

- Přechod od listinných k digitálním důkazům
- Dopady digitalizace na dokazování
- Typické elektronické stopy a jejich zdroje
- Význam elektronických komunikací
- Vznik, uchování a ověřování dat
- Elektronická důvěra a integrita
- Mezinárodní trendy a judikatura
- Rizika manipulace s důkazy

2. Právní rámec elektronických důkazů

- Ústavní principy a OSŘ, ZŘS, správní řád
- Zákon o službách vytvářejících důvěru v elektronické transakce (eIDAS)
- GDPR a ochrana soukromí při dokazování
- Autenticita, integrita a prokazatelnost
- Zásada volného hodnocení důkazů
- Role elektronického podpisu a razítka
- Odpovědnost za pravost a úplnost důkazů
- Význam legislativních novinek po roce 2025

3. Screenshots, e-maily a komunikace na sítích

- Půžitelnost printscreenů v řízení
- Jak správně pořizovat a uchovávat screenshots
- Ověřování původu e-mailů a jejich hlaviček
- Chaty z WhatsAppu, Messengeru, Telegramu apod.
- Manipulace a falzifikace elektronické komunikace
- Znalecké posudky na autenticitu obsahu
- Dokumentace a řetězec důvěry
- Způsoby prezentace důkazů v řízení

4. Zvukové a obrazové záznamy

- Právní limity nahrávání a použití záznamů
- Rozdíl mezi souhlasným a skrytým záznamem
- Posouzení zásahu do soukromí

- Pravidla pro použití záznamů ve správním řízení
- Zásady proporcionality a účelnosti
- Hodnocení technické kvality a autenticity
- Ochrana osobních údajů nahrávaných osob
- Příklady z rozhodovací praxe soudů

5. Metadata a digitální stopy

- Co jsou metadata a jakou mají důkazní hodnotu
- GPS souřadnice, časová razítka, digitální podpisy
- Jak metadata chránit a interpretovat
- Řetězec důvěry a kontrola integrity
- Sběr a zajištění digitálních stop
- Znalectví v oblasti informatiky
- Úskalí přenosu a konverze dat
- Praktické využití v řízení

6. Cloud, úložiště a e-mail v prostředí třetích stran

- Sdílené disky, cloudové platformy, úložiště
- Ověření původu dat uložených v cloudu
- Právní vztah mezi uživatelem a poskytovatelem služby
- Přístup OSPOD, policie a soudů k datům
- Mezinárodní přeshraniční přenosy dat
- Uchování důkazů a jejich dostupnost
- Zásada legality a proporcionality
- Možnosti elektronické spolupráce institucí

7. Blockchain jako důkazní nástroj

- Princip fungování blockchainu
- Nezměnitelnost a transparentnost záznamů
- Využití pro ověřování autenticity dat
- Smart kontrakty a právní jistota
- Limity a nedostatky blockchainu v důkazním řízení
- Právní relevance záznamů z distribuovaných databází
- Ověřování digitální identity
- Možnosti budoucího využití ve veřejné správě

8. Elektronické podpisy, razítka a časová razítka

- Typy elektronických podpisů a jejich právní váha
- Kvalifikované prostředky podle eIDAS
- Ověření totožnosti a integrity dokumentu
- Elektronické razítko úřadu a soudní praxe
- Časová razítka a důkaz o okamžiku vytvoření
- Konverze dokumentů a autorizovaná konverze
- Právní jistota při digitální archivaci
- Postupy pro úředníky a právní zástupce

9. Umělá inteligence a automatizované analýzy

- AI jako nástroj zpracování důkazů
- Riziko zkreslení a chyb algoritmů
- Etické a právní limity využívání AI
- Automatické vyhodnocování obrazu a textu
- Transparentnost algoritmických rozhodnutí
- Zásada lidského dohledu
- Využití AI v digitální forenzice

- Odpovědnost za výsledky automatické analýzy

10. Ochrana osobních údajů a soukromí při dokazování

- Zpracování osobních údajů v rámci řízení
- Souhlas, veřejný zájem a právní titul
- Ochrana třetích osob na záznamech
- Anonymizace a pseudonymizace dat
- Práva subjektů údajů v důkazním procesu
- Proporcionalita zásahu do soukromí
- Zásady bezpečného uchování důkazů
- Prevence zneužití důkazního materiálu

11. Praktické kazuistiky a příklady

- Úspěšné využití digitálních důkazů v řízení
- Chyby při pořizování screenshotů a záznamů
- Ověřování elektronických podpisů v praxi
- Kazuistiky z praxe úřadů a soudů
- Manipulace s metadaty a její odhalení
- Příklady selhání důkazního řetězce
- Poučení z rozhodovací praxe NSS a ÚS
- Doporučení pro praxi úředníků

12. Diskuse a závěr školení