

LECHNER, T.: NAŘÍZENÍ EIDAS A ČESKÉ ADAPTAČNÍ ZÁKONY. RECENZE A ÚVAHA O POMĚRU ELEKTRONICKÉ IDENTIFIKACE A ELEKTRONICKÝCH PODPISŮ

ADAM JAREŠ¹

**LECHNER, T.: Nařízení eIDAS a české adaptační zákony. Komentář.
Praha: Wolters Kluwer ČR, 2023, 488 s., ISBN 978-80-7598-924-6**

1. ÚVOD

Oblastem úpravy nařízení eIDAS², tedy elektronické identifikace a služby vytvářející důvěru, není dlouhodobě v české právní literatuře věnována náležitá pozornost. To samé platí pro české právní předpisy upravující elektronické právní jednání, ať již jde o elektronické podepisování, identifikaci nebo doručování. S ohledem na probíhající digitální transformaci zrychlenou katalyzátorem v podobě různých lockdownů a omezení osobního styku či nutnými úsporami na straně státu i soukromého sektoru se tato situace začíná pomalu měnit a téma virtualizace právního jednání se dostává v právní literatuře větší pozornosti. Kniha Tomáše Lechnera tak do jisté míry splácí dluh spočívající buď ve zcela absentující literatuře či v doplnění k existujícím publikacím jako aktuální a velmi vítaný další zdroj poznání této oblasti.

¹ JUDr. Adam Jareš, Ph.D., Ústav práva a technologií Právnické fakulty Masarykovy univerzity, Digitální a informační agentura, kontaktní e-mail: adam.jares@mail.muni.cz.

² Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (dále jen „nařízení eIDAS“).

2. HODNOCENÍ A PŘÍNOS KNIHY

Význam knihy pro diskurz k tématu elektronického právního jednání je patrný již z jejího samotného názvu. Autor se totiž nezastavil pouze u nařízení eIDAS³, ale v návaznosti na předchozí výklad k tomuto nařízení komentuje také české adaptační předpisy – zákon o službách vytvářejících důvěru⁴ a zákon o elektronické identifikaci⁵. Velmi vhodně se autor věnuje také komentáři evropských prováděcích předpisů.⁶

Knihu jsem přivítal s očekáváním, jelikož některé předpisy nebyly v České republice vůbec komentovány nebo od vydání komentáře už uplynula delší doba. Knize se toto očekávání naplnit podařilo. Autor v ní odkazuje a čerpá z některých dříve publikovaných textů a své akademické či publikační praxe a zároveň výklad prokládá ryze praktickými úvahami, které navíc často přináší náhled daleko za hranice zájmu běžného právníka až k technologickému pozadí služeb vytvářejících důvěru či elektronické identifikace.

Ze všech částí knihy věnovaným různým předpisům je patrná autorova dlouholetá publikační a akademická praxe v oblastech působnosti těchto předpisů. Výklad je navíc doplněn řadou praktických příkladů a přehledů – například aktuálním přehledem oznámených systémů elektronické identifikace v Evropské unii, přehledem subjektů zodpovědných za zveřejnění důvěryhodného seznamu podle čl. 22 nařízení eIDAS nebo příklady využití důvěryhodných seznamů zveřejněných dle článku 22 Nařízení či kvalifikovaného časového razítka.

Pokud jde o výklad jiných oblastí, například ochrany osobních údajů, pak autor vhodně odkazuje na relevantní odborné publikace. U kome-

³ K nařízení eIDAS také srov. DONÁT, Josef; MAISNER, Martin a PIFFL, Robert. *Nařízení eIDAS: komentář*. Praha: C.H. Beck, 2017.

⁴ Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, Parlamentu České republiky.

⁵ Zákon č. 250/2017 Sb., o elektronické identifikaci, Parlamentu České republiky.

⁶ Prováděcí rozhodnutí Komise 2015/296, prováděcí nařízení Komise 2015/1501, prováděcí nařízení Komise 2015/1502, prováděcí rozhodnutí Komise 2015/1505, prováděcí rozhodnutí Komise 2015/1984 a prováděcí rozhodnutí Komise 2016/650.

tovaných článků nařízení eIDAS pak autor uvádí odkaz na konkrétní body odůvodnění nařízení.

3. KNIHA A AKTUÁLNÍ VÝVOJ NA ÚROVNI EVROPSKÉ UNIE

Kniha nereflexuje aktuální evropský legislativní proces revize nařízení eIDAS.⁷ Zdánlivě by se tak mohlo zdát, že kniha rychle zastará. Poznámku o absenci zohlednění revize nařízení eIDAS v textu komentáře však nelze vnímat jako výtku. Jde zřejmě spíše o pragmatické rozhodnutí autora, jelikož přijetí revize eIDAS, následná použitelnost či lhůta pro splnění některých povinností členskými státy se při přípravě komentáře mohla oprávněně jevit jako velmi vzdálená. Cesta k dohodě nad finálním textem revize byla navíc velmi složitá, a autor by tedy mohl pouze spekulovat nad tím, jaká varianta konkrétního článku bude nakonec přijata.

I s ohledem na to bude kniha velmi dobře použitelná ještě po delší dobu i po přijetí revize eIDAS. Vezměme navíc v úvahu, že komentář je dostupný také v právním informačním systému ASPI, přičemž nakladatelství Wolters Kluwer po autorech komentářů zpravidla vyžaduje, aby komentář v této formě pravidelně aktualizovali v případě změn komentovaných předpisů. Navíc se domnívám, že málokdo čte komentář právního předpisu jako celek od prvního do posledního ustanovení. Po přijetí revize eIDAS tak bude, doufejme, aktualizovaný komentář dostupný v ASPI.

4. ÚVAHA KE DVĚMA ČÁSTEM NAŘÍZENÍ

Kniha může čtenáře vést k různým úvahám. Jednu z nich vyvolává opakovaná zmínka, že nařízení eIDAS je rozděleno do dvou téměř disjunkčních částí – úpravě elektronické identifikace a služeb vytvářejících důvěru. Zde autor odkazuje primárně na práci Vojtěcha Kmenta, podle kterého sice může příležitostně dojít ke smíšení technických prostředků, ale v nařízení eIDAS k žádnému mísení ani k systémovým návaznostem nedochází. To

⁷ Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení rámce pro evropskou digitální identitu, [online] dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52021PC0281> [cit. 2023-11-03].

odůvodňuje odchylnou metodou regulace a různým vývojem právní úpravy obou oblastí.⁸

Kladu si v této souvislosti otázku, zda tyto dvě oblasti, které mohlo být do jisté míry možné vnímat jako oddělené v době přijetí nařízení eIDAS, je možné vnímat stejným způsobem i v roce 2023. Oddělenost obou oblastí lze sice zdůvodnit nejen autorem odkazovanou prací Vojtěcha Kmenta nebo přijetím dvou různých zákonů v České republice⁹. Odpověď na tuto otázku však není podle mého názoru tak jednoznačná a obě oblasti se postupně začínají stále více prolínat či se vzájemně alternovat.

Při veřejnoprávním elektronickém jednání klademe totiž v českém právním řádu obě oblasti v některých ohledech naroveň. Příklady budiž následující:

1. Zákon o právu na digitální služby¹⁰ dává na stejnou úroveň elektronicky podepsaná podání a podání učiněná po provedení elektronické identifikace. Uživatel digitální služby má podle tohoto zákona právo činit digitální úkon vůči orgánu veřejné moci prostřednictvím sítě elektronických komunikací dokumentem podepsaným uznávaným elektronickým podpisem či v některých případech uznávanou elektronickou pečetí. Stejně tak má uživatel právo digitální úkon vykonat za stanovených podmínek i prostřednictvím informačního systému veřejné správy umožňujícího prokázání totožnosti uživatele služby s využitím elektronické identifikace.¹¹

2. Podle zákona o informačních systémech veřejné správy se úkon, jehož náležitostí má být podpis, považuje za podepsaný, pokud byl učiněný prostřednictvím informačního systému veřejné správy, který umožňuje prokázání totožnosti s využitím elektronické identifikace.¹²

⁸ KMENT, V. Elektronické právní jednání. Praha: Wolters Kluwer, 2018. s. 108.

⁹ Dříve zmíněné zákony o elektronické identifikaci a o službách vytvářejících důvěru pro elektronické transakce.

¹⁰ Zákon č. 12/2020 Sb., o právu na digitální služby.

¹¹ Srov. § 4 odst. 1 zákona č. 12/2020 Sb.

¹² Srov. § 8 zákona č. 365/2000 Sb., o informačních systémech veřejné správy.

3. Do datové schránky se uživatel přihlásí po provedení elektronické identifikace a následně může činit úkon bez současného připojení elektronického podpisu. Úkon učiněný osobou oprávněnou k přístupu do datové schránky nebo pověřenou osobou prostřednictvím datové schránky má totiž podle zákona o elektronických úkonech stejné účinky jako úkon učiněný písemně a podepsaný.¹³

Kvalifikované prostředky také mohou umožňovat jak elektronickou identifikaci, tak vytváření elektronických podpisů. A to ať již půjde o české občanské průkazy s čipem či Evropské digitální peněženky, které má Evropská unie záměr zavést revizí nařízení eIDAS, nebo jiné prostředky.

Podpisy a identifikace spolu souvisí i tak, že kvalifikovaný poskytovatel služeb vytvářejících důvěru při vydávání kvalifikovaného certifikátu pro službu vytvářející důvěru (tedy i pro kvalifikovaný elektronický podpis) má povinnost ověřit pomocí vhodných prostředků totožnost osoby, které je kvalifikovaný certifikát vydáván. To může být za stanovených podmínek provedeno i na dálku s využitím prostředku pro elektronickou identifikaci.¹⁴ Po revizi nařízení eIDAS by mělo být možné o vydání certifikátu požádat i prostřednictvím Evropské peněženky digitální identity.

Lze si představit kombinaci elektronických podpisů a elektronické identifikace také v rámci soukromoprávního styku. V civilních sporech prvostupňové soudy často (nesprávně) vyžadují, aby elektronický podpis zajišťoval identifikaci jednající osoby a integritu dokumentu. Elektronický podpis nemusí defaultně poskytovat identifikaci podepisujícího. Ani vlastnoruční podpis bez dalšího podepisujícího neidentifikuje a tento požadavek na podpis nevyplývá ani z občanského zákoníku.

Právní jednání v elektronické podobě však musí zajistit identifikaci jednající osoby.¹⁵ Tento požadavek bude možné naplnit i kombinací elektronické identifikace a podpisu. Právní jednání v takovém případě bude

¹³ § 18 odst. 2 zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

¹⁴ Srov. čl. 24 nařízení eIDAS.

¹⁵ Srov. § 562 odst. 2 zákona č. 89/2012 Sb., občanský zákoník.

sice podepsáno nižší úrovní elektronického podpisu, nicméně podpis bude připojen v rámci systému, který nejprve provede elektronickou identifikaci s určitou úrovní záruky. V takovém systému pak může být zajištěna i archivace podepsaného dokumentu takovým způsobem, aby byla zajištěna také integrita dokumentu. Tak bude možné využít domněnku spolehlivosti záznamů údajů o právních jednáních v elektronickém systému, pokud budou záznamy provedeny systematicky, posloupně a chráněny proti změnám ve smyslu § 562 odst. 2 občanského zákoníku.

5. DISKUZE A ZÁVĚR K ÚVAZE

S předchozím odstavcem souvisí i to, zda při soukromoprávním jednání bude do budoucna větší prostor pro podepisování kvalifikovanými elektronickými podpisy, resp. jestli některé podpisové techniky nebudou nahrazeny elektronickou identifikací a archivací.

Tímto způsobem odkazoval Polčák před účinností současného občanského zákoníku na použití kontraktačních platforem, systémů pro vedení elektronické spisové služby či jiných datových uložišť. Pravost dokumentu se v takovém případě podle něj neprokazuje přímo, ale „prostřednictvím toho, že dokument ležel v příslušném standardně zabezpečeném úložišti“.¹⁶ Značný potenciál v § 562 odst. 2 občanského zákoníku, resp. v uchování dat v profesionálním elektronickém systému spisové služby vidí i Korbel s Melzerem.¹⁷ Podle Matejky s Güttlerem trend elektronického zpracování dokumentů vede k tomu, že jejich důkazní věrohodnost je zjišťována spíše kvalifikovaným způsobem a postupem, kterým byly vytvořeny nebo jsou dlouhodobě ukládány, než jednotlivými elektronickými podpisy v nich. Záruky tak mohou poskytovat funkční vlastnosti, architektura a design elektronického systému.¹⁸

¹⁶ POLČÁK, Radim. Praxe elektronických dokumentů. *Bulletin advokacie*. roč. 2011, č. 7–8, s. 59.

¹⁷ KORBEL, František a Filip MELZER. Písemnost, elektronický a biometrický podpis v elektronickém právním jednání. *Bulletin advokacie*. roč. 2014, č. 12, s. 36.

Domnívám se tedy, že oblasti elektronické identifikace a elektronického podepisování jsou vzájemně prostupné, úzce spolu souvisí či se v některých případech mohou vzájemně nahrazovat. To platí nyní a do budoucna může platit stále více.

Toto dílo lze užít v souladu s licenčními podmínkami Creative Commons BY-SA 4.0 International (<http://creativecommons.org/licenses/by-sa/4.0/legalcode>).

¹⁸ MATEJKA, Ján a Vojen GÜTLER. Electronic Written Documents and Biometric Options of Their Signing – Problem of Evidentiary Reliability and Personal Data Protection. *The Lawyer Quarterly*. roč. 2018, č. 1, s. 46.