

32

REVUE PRO PRÁVO A TECHNOLOGIE

Ústav práva a technologií Právnické fakulty Masarykovy univerzity

ROČNÍK 16 / ROK 2025 / ČÍSLO 32

REVUE.LAW.MUNI.CZ

LL.M. v právu informačních a komunikačních technologií

CELOŽIVOTNÍ VZDĚLÁVÁNÍ NA
PRÁVNICKÉ FAKULTĚ MASARYKOVY
UNIVERZITY

Informace o zahájení a podmínkách přihlašování pro rok 2026:

Centrum dalšího vzdělávání na Právnické fakultě MU

Jana Buchalová

telefon: 731 591 249

email: jana.buchalova@law.muni.cz

www.llm.law.muni.cz

REVUE PRO PRÁVO A TECHNOLOGIE

ROČNÍK 16 | ROK 2025 | ČÍSLO 32

DISKUZE

Georgia Hejduková: Malware jako autorské dílo: Analýza ochrany a jejích limitů v evropském právu	3
Tomáš Lechner: Právní aspekty požadavků na datové formáty	21
Adam Žváček: Tracing pohledem autorského práva	49

ANOTACE

K. Akil, A. Blechová, M. Erlebach, Š. Chvojka, J. Harašta, P. Loutocký, J. Martínek, K. Mlčáková, O. Woznica: Přehled aktuální judikatury II/2025.....	107
---	-----

ESSAYS

P. Minima, O. Sukač: Essays II/2025	129
--	-----

RECENZE ZÁVĚREČNÝCH PRACÍ

K. Akil, O. Böhm, M. Erlebach, T. Mizerová, D. Palašta, F. Kasl: Recenze závěrečných prací II/2025	155
---	-----

RECENZE

Kristýna Akil: LEISER, M.: Dark patterns, deceptive design, and the law: AI's hidden influence on our digital experience	187
---	-----

TÉMA

Jakub Sauer, Stanislav Špaček, Patrik Fráňa, Denisa Drappanová, Jakub Harašta: Záznamy událostí: Stanovení doby uchování a implementace komplexních požadavků v organizaci	195
---	-----

Revue pro právo a technologie

Odborný recenzovaný časopis pro technologické obory práva a právní vědy zařazený na Seznamu recenzovaných neimpaktovaných periodik vydávaných v České republice a v databázi ERIH PLUS.

Recenzovány jsou příspěvky v sekci Diskuze a Téma.

Vychází dvakrát ročně. Toto číslo vyšlo 31. 12. 2025.

ISSN 1804-5383 (Print), ISSN 1805-2797 (Online), Ev. č. MK ČR E 19707

Vydává Masarykova univerzita, Žerotínovo nám. 9, 601 77 Brno, ČR, IČ 00216224

Šéfredaktor a kontaktní osoba: JUDr. Ing. František Kasl, Ph.D., Ústav práva a technologií Právnické fakulty Masarykovy univerzity, Veveří 70, 611 80 Brno, ČR, telefonní kontakt: +420 549 49 5545, kontaktní e-mail: frantisek.kasl@muni.cz | revue@law.muni.cz | <https://journals.muni.cz/revue>

Zástupce šéfredaktora: Jakub Stojan

Redakce: JUDr. Mgr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek, Ph.D.

Editoři: Mgr. Martin Erlebach, Adéla Dočkalová, Martin Plášek

Redakční rada: prof. JUDr. Radim Polčák, Ph.D. (čestný předseda), JUDr. Zuzana Adamová, Ph.D., prof. JUDr. Michael Bogdan, B.A., LL.M., jur. dr. (Lund), JUDr. Marie Brejchová, LL.M., JUDr. Jiří Čermák, prof. JUDr. Bc. Tomáš Gřivna, Ph.D., prof. JUDr. Josef Kotásek, Ph.D., JUDr. Bc. Zdeněk Kučera, Ph.D., Mgr. Ing. Zbyněk Loeb, LL.M., JUDr. Ján Matejka, Ph.D., prof. RNDr. Václav Matyáš, M.Sc., Ph.D., doc. JUDr. Matěj Myška, Ph.D., Mgr. Antonín Panák, LL.M., Mgr. Bc. Adam Ptašník, Ph.D., JUDr. Danuše Spáčilová, JUDr. Eduard Szattler, Ph.D., JUDr. Tomáš Ščerba, Ph.D.

Grafická úprava: Mgr. Martin Loučka, doc. JUDr. Matěj Myška, Ph.D.

Tisk: POINT CZ, s.r.o., Milady Horákové 20, 602 00 Brno

Vydání tohoto čísla časopisu Revue pro právo a technologie bylo financováno z projektu „Právo a technologie XIII“, MUNI/A/1739/2024.

Časopis © Masarykova univerzita, 2025

POKYNY PRO AUTORY

Revue pro právo a technologie je specializovaným odborným recenzovaným časopisem, který je zaměřen na technologické obory práva a právní vědy.

Časopis je zařazen od 1. 1. 2015 na Seznam recenzovaných neimpaktovaných periodik vydávaných v ČR a od 24. 6. 2015 do databáze ERIH PLUS.

Příspěvky zaslané do sekcí Téma a Diskuze jsou anonymně posuzovány minimálně dvěma nezávislými recenzenty a konečné rozhodnutí o publikaci příspěvků zaslaných do všech sekcí je v kompetenci redakční rady. Orientační doba recenze je jeden měsíc. Články neprochází jazykovou korekturou.

Příspěvky se podávají prostřednictvím redakčního systému dostupného na adrese <https://journals.muni.cz/revue>

DOPORUČENÝ ROZSAH PŘÍSPĚVKŮ:

Sekce Diskuze: 15 – 30 normostran

Sekce Anotace: 2 – 10 normostran

Sekce Essays: 5 – 10 normostran

Sekce Recenze závěrečných prací: 2 – 5 normostran

Sekce Recenze: 2 – 5 normostran

Sekce Téma: 30 – 50 normostran

(včetně mezer, poznámek pod čarou a seznamu použitých zdrojů)

CITAČNÍ STANDARD

Použité prameny je nutné citovat v souladu s citační směrnicí ČSN ISO 690:2022.

Způsob citování a praktické příklady jsou dostupné v interpretacích normy ISO 690:2022, které jsou dostupné např. na adrese <https://www.citace.com/CSN-ISO-690>

Na jednotlivé prameny se odkazuje v textu číslem poznámky psané horním indexem (metoda průběžných poznámek).

Autoři musí transparentně uvést užití generativního nástroje AI při vytváření textu.

TERMÍNY PRO DODÁNÍ PŘÍSPĚVKŮ

Do letního čísla: 28. února

Do zimního čísla: 31. srpna

Časopis se hlásí k politice otevřeného přístupu realizovaného zlatou cestou.

Časopis a příspěvky jsou dostupné na webových stránkách časopisu www.revue.law.muni.cz za veřejně dostupných licenčních podmínek Creative Commons Attribution-ShareAlike 4.0 International (dostupné on-line na adrese <http://creativecommons.org/licenses/by-sa/4.0/legalcode>).

Příspěvky jsou přebírány do příslušných elektronických právních informačních systémů společností Wolters Kluwer ČR, a. s. (ASPI), Nakladatelství C. H. BECK, s. r. o. (beck-online.cz) a ATLAS consulting spol. s r. o. (CODEXIS).

Detailní informace ohledně publikačního procesu, struktury a formálních náležitostí příspěvků, recenzního řízení a autorských práv jsou dostupné v sekci „Pro autory“ na webu časopisu <https://journals.muni.cz/revue/about/submissions> resp. Vám je na vyžádání ráda sdělí redakce (kontaktní e-mail: revue@law.muni.cz).

<https://doi.org/10.5817/RPT2025-2-1>

MALWARE JAKO AUTORSKÉ DÍLO: ANALÝZA OCHRANY A JEJÍCH LIMITŮ V EVROPSKÉM PRÁVU

GEORGIA HEJDUKOVÁ¹

ABSTRAKT

Ačkoliv malware může teoreticky požívat formální autorskoprávní ochrany, autor takového díla by při pokusu o její vymáhání čelil prakticky nepřekonatelným překážkám. Z procesního hlediska by se podáním žaloby doznal k trestné činnosti, zatímco z hmotněprávního hlediska by jakýkoli nárok paralyzovaly fundamentální právní principy, jako je zákaz zneužití práva či zásady nemo auditur. Současný právní rámec, opírající se o obecné zásady unijního i vnitrostátního práva, tak poskytuje dostatečnou ochranu činnosti antivirových společností a nevyžaduje zavedení nové, specifické legislativní úpravy.

KLÍČOVÁ SLOVA

Malware; autorské právo; reverzní inženýrství; antivirové programy; zneužití práva; evropské právo; kybernetická bezpečnost

ABSTRACT

Although malware may theoretically receive formal copyright protection, its author would face insurmountable obstacles in any attempt at enforcement. From a procedural standpoint, filing a claim would amount to a confession of criminal activity. From a substantive law perspective, any such claim would be neutral-

¹ Georgia Hejduková je studentkou magisterského studijního programu na Právnické fakultě Univerzity Karlovy. Odborně se dlouhodobě zaměřuje na problematiku ochrany lidských práv a práv menšin v kontextu českého ústavního práva i práva mezinárodního. Kontakt: georgia.hejdukova140@student.cuni.cz

ized by fundamental legal principles, such as the prohibition of the abuse of rights or the nemo auditur principle. Therefore, the existing legal framework, relying on the general principles of both EU and national law, provides sufficient protection for the activities of antivirus companies and does not necessitate the introduction of new, specific legislation.

KEYWORDS

Malware; Copyright Law; Reverse Engineering; Antivirus Software; Abuse of Rights; European Law; Cybersecurity

1. ÚVOD

Počítačová kriminalita představuje dlouhodobý fenomén, který časově předchází i samotnému vzniku internetu, jelikož podle některých autorů se první počítačový útok odehrál už v 70. letech,² kdy byl vytvořen jeden z prvních malwarů, který vznikl ještě na ARPANETu.³ Od té doby se z ní stal celosvětový fenomén, proti němuž se společnost snaží bojovat právními prostředky, ať už formou zákonů, mezinárodních smluv, či zřízením specializovaných institucí. Malware je dnes natolik všudypřítomný, že se z vývoje antivirových programů stal multimilionový trh a některé operační systémy antivirové programy „předinstalovávají“.

Autorské právo v otázce ochrany počítačových programů nezůstalo pozadu a dnes jsou počítačové programy chráněny jako autorská díla ve vnitrostátní i evropské legislativě. Cílem tohoto článku bude zjistit, zda se ochrana autorského práva u počítačových programů vztahuje i na malware a zda mohou antivirové programy, jejichž cílem je tyto programy v počítačových systémech odhalovat a zneškodňovat, svým fungováním, zejména analýzou virů, porušovat majetková práva autorů virů.

Pokud dojde tento článek k závěru, že antivirové programy zasahují do majetkových práv autorů virů, bude předmětem následné analýzy otáz-

² HILL, Joshua B. – MARION, Nancy E. *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*. New York: Bloomsbury Publishing USA, 2016.

³ ARPANET byl předchůdce internetu vyvinutý Ministerstvem obrany USA. Srov. ROSANNE WELCH a PEG A. LAMPHIER. *Technical Innovation in American History: An Encyclopedia of Science and Technology*. Santa Barbara: ABC-CLIO, 2019, s. 16.

ka, zda současný právní systém dokáže autorům antivirových programů poskytnout možnost, jak do práv autorů malwaru oprávněně zasáhnout a pokud současný právní systém záruky neposkytuje, jak by měla být legislativa upravena pro zajištění těchto záruk. Protože je autorské právo na úrovni Evropského hospodářského prostoru harmonizováno zejména pomocí směrnic, zaměří se analýza na tuto dimenzi.

Vzhledem k tomu, že evropské soudy zatím právní otázku ochrany autorských práv u malwaru neřešily, budou úvahy metodologicky vycházet především z heuristiky evropské legislativy, zejména směrnice upravující právní ochranu počítačových programů a dalších směrnic, včetně případné aplikace směrnice Evropské unie o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti, tam, kde se výklad týká užití malwaru v Evropském hospodářském prostoru.⁴

2. DEFINICE MALWARU A ANTIVIROVÉHO PROGRAMU

Pojem malware etymologicky vychází z anglických slov „malicious“ (zlovolný) a „software“.⁵ Označuje počítačový program, jehož primárním účelem je poškodit koncové zařízení uživatele nebo do něj získat neoprávněný přístup. Existuje celá řada typů malwaru, které se liší svými funkcemi a cíli, což se projevuje v různých důsledcích jejich činnosti v napadeném zařízení. Obecně lze však konstatovat, že cílem takového programu je provádět činnost, k níž by oprávněný uživatel neudělil souhlas. Tato definice našla svůj odraz v rozhodnutí Nejvyššího soudu⁶ a je reflektována i v trestním zákoníku ve skutkových podstatách trestných činů.⁷

Úmluva o počítačové kriminalitě, známá též jako Budapešťská úmluva, představuje klíčový mezinárodní dokument v této oblasti.⁸ Ukládá smluvním stranám povinnost kriminalizovat určené druhy jednání, jako je nezákonný přístup, nezákonný odposlech, zásah do dat, zásah do systému,

⁴ Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů, Úř. věst. OJ L 111, 5.5.2009.

⁵ AYCOCK, John. *Computer Viruses and Malware*. New York: Springer US, 2006.

⁶ Rozsudek Nejvyššího soudu ze dne 27.01.2011, sp. zn. 4 Tz 79/2010.

⁷ § 230 až § 232 zákona č. 40/2009 Sb., trestní zákoník.

⁸ Smlouva č. 104/2013 Sb. m. s Úmluva o počítačové kriminalitě.

zneužití zařízení, počítačové padělání či počítačový podvod.⁹ Samotná Úmluva však neobsahuje legální definici pojmu malware. Pro jeho vymezení je proto nutné vycházet z odborné literatury či z navazující judikatury. Odborná literatura malware definuje například jako počítačový program, který zasahuje do jiného počítačového programu a způsobuje, že se jeho zamýšlená funkce odlišuje od té, která je skutečně vykonána.¹⁰

Oproti tomu antivirový software je určen k ochraně koncového zařízení před napadením malwarem.¹¹ Širším a v současnosti přesnějším termínem je antimalware,¹² který označuje software aktivně analyzující soubory v zařízení. Za využití metod, jako je reverzní inženýrství, analyzuje strukturu a fungování škodlivého kódu. Získané informace a signatury následně uchovává ve svých databázích, aby byl schopen malware efektivně detekovat.¹³ Tento proces umožňuje neustálé zdokonalování ochrany a zajištění vyšší úrovně bezpečnosti pro uživatele.

3. LIMITY AUTORSKOPRÁVNÍ OCHRANY MALWARU

3.1 OBECNÁ VÝCHODISKA OCHRANY PRO POČÍTAČOVÉ PROGRAMY

Ačkoliv je účelem malwaru zpravidla protiprávní činnost, z hlediska autorského práva se může jednat o standardní počítačový program. Pokud takový program splňuje obecné pojmové znaky autorského díla, požívá právní ochrany jak v České republice, tak v celém Evropském hospodářském prostoru. Tuto ochranu harmonizuje směrnice o právní ochraně počí-

⁹ GRÍVNA, Tomáš, DVOŘÁK, Marek. § 230 In: ŠÁMAL, Pavel a kol. *Trestní zákoník*. 3. vydání. Praha: C. H. Beck, 2023, s. 2949.

¹⁰ KRAMER, Simon – BRADFIELD, Julian C. A general definition of malware. *Journal in Computer Virology*. 2010, roč. 6, č. 2., ISSN s. 105.

¹¹ NAYAK, Umesha. Malicious Software and Anti-Virus Software. In: *The InfoSec Handbook*. Apress, 2014. ISBN 9781430263838. Dostupné z: https://doi.org/10.1007/978-1-4302-6383-8_7 s. 156.

¹² ROSENCRANCE, Linda. What is antimalware? *TechTarget* [online] [cit. 2024-03-28]. Dostupné z: <https://www.techtarget.com/searchsecurity/definition/antimalware>.

¹³ LUNDE, Jeremy S. *COPYRIGHT PROTECTION FOR VIRUS AUTHORS: Establishing Protection for Authors Irrespective of the Merits of Their Creation*. 2010, Diplomová práce, University of Oslo s. 40.

tačových programů.¹⁴ Uvedená směrnice vymezuje podmínky ochrany, stanovuje dovozené způsoby zásahu do autorských práv tvůrců a definuje mechanismy pro zajištění této ochrany v rámci EHP¹⁵.

3.2 LIMITY OBECNÝCH VÝCHODISEK PRO ANTIVIROVÉ PROGRAMY

3.2.1 ZÁKONNÉ LICENCE A JEJICH APLIKACE NA MALWARE

Vycházíme-li z premisy, že i malware jako počítačový program požívá autorskoprávní ochrany,¹⁶ vyvstává zásadní otázka, zda by tato ochrana neměla být limitována s ohledem na jeho protiprávní účel. Tuto kolizi mezi individuálním autorským právem a veřejným zájmem lze posuzovat optikou již existujících omezení autorského práva. Prvním příkladem takových omezení jsou zákonné licence, které autorský zákon výslovně upravuje.

Mezi zákonné licence patří například licence pro citační účely, pro využití díla ve prospěch osob se zdravotním postižením nebo pro účely vyučování a vědeckého výzkumu. Zásadní je rovněž licence umožňující užití díla v zájmu veřejné bezpečnosti. Pro další analýzu jsou relevantní pouze licence pro vyučování, vědecký výzkum a veřejnou bezpečnost, neboť ostatní zákonné licence nejsou pro posouzení autorskoprávní ochrany malwaru aplikovatelné.¹⁷

Uplatnění výjimky pro vědecký výzkum a výuku je limitováno požadavkem, aby daná činnost nesledovala přímý ani nepřímý hospodářský prospěch.¹⁸ Tato restrikce sice umožňuje analýzu malwaru v akademickém

¹⁴ Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů, Úř. věst. OJ L 111, 5.5.2009.

¹⁵ Evropský hospodářský prostor.

¹⁶ Obecně, pokud malware naplní znaky počítačového programu podle § 2. odst. 2 autorského zákona chráněn spíše je, nicméně autor nebude z důvodu aplikace § 6 občanského zákoníku (OZ) moci z této ochrany těžit. Viz HOLCOVÁ, I. a kol. *Autorský zákon a předpisy související (včetně mezinárodních smluv a evropských předpisů): komentář*, s. 525. Praha: Wolters Kluwer Česká republika, 2019.

¹⁷ Čl. 5 odst. 3 Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti.

¹⁸ LUNDE, Jeremy S. *COPYRIGHT PROTECTION FOR VIRUS AUTHORS*, s. 49.

prostředí, avšak výrazně omezuje její aplikační potenciál v praxi. Představuje totiž bariéru pro komerční subjekty, které hrají klíčovou roli v detekci a analýze kybernetických hrozeb.

Alternativním právním titulem by mohla být tzv. úřední licence, jež v rovině unijního práva zahrnuje i užití pro účely veřejné bezpečnosti.¹⁹ V podmínkách českého právního řádu je však subsumpce analýzy malwaru pod toto ustanovení vyloučena. Rozsah § 34 autorského zákona totiž nekryje veřejný zájem v jeho obecné rovině. Odborná literatura konzistentně dovozuje, že tuto zákonnou licenci lze aplikovat pouze na základě specifického zákonného zmocnění pro úřední účely.²⁰ Teleologickým východiskem této licence není ochrana veřejné bezpečnosti *per se*, nýbrž zajištění výkonu pravomocí orgánů veřejné moci.²¹ Z tohoto důvodu nelze úřední licenci pro účely reverzního inženýrství využít.

3.2.2 NELEGÁLNÍ JEDNÁNÍ AUTORŮ MALWARU JAKO DŮVOD PRO ODEPŘENÍ OCHRANY AUTORSKÝM PRÁVEM

Klíčový argument pro odepření autorskoprávní ochrany malwaru spočívá v rozporu s dobrými mravy a veřejným pořádkem. Tato fundamentální soukromoprávní zásada brání tomu, aby výkon subjektivního práva vedl k následkům, které jsou v příkrém rozporu se společensky uznávanými hodnotami. Poskytnutí soudní ochrany dílu, jehož primárním účelem je páchání protiprávní činnosti, by naplňovalo znaky zneužití práva (§ 8 občanského zákoníku). Právní řád nemůže legitimovat nástroje určené k jeho vlastnímu porušování, neboť by tím popřel svůj základní smysl a dostal se do neřešitelného vnitřního rozporu.

Opozici vůči morálnímu korektivu tvoří objektivní charakter autorskoprávní ochrany. Mezinárodní smluvní rámec (Bernská úmluva,

¹⁹ Viz § 34 autorského zákona či čl. 5 odst. 3 písm. e) směrnice o Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti.

²⁰ CHALOUPKOVÁ, Helena, HOLÝ, Petr. *Autorský zákon*. 6. vydání. Praha: C. H. Beck, 2023, s. 105. Srov. HOLCOVÁ, I. a kol. *Autorský zákon a předpisy související (včetně mezinárodních smluv a evropských předpisů)*: komentář, s. 339–353.

²¹ TELEČ, Ivo, TŮMA, Pavel. *Autorský zákon*. 2. vydání. Praha: C. H. Beck, 2019, s. 413.

Smlouva WIPO),²² neumožňuje odepřít ochranu dílu pouze na základě jeho protiprávního původu či účelu. Moderní autorské právo je ovládáno zásadou, že ochrana svědčí každému dílu *ex lege*, nehlédě na jeho estetickou či morální kvalitu.²³ Tento doktrinální rozpor lze demonstrovat na příkladu street artu. I v případech, kdy vznik díla naplňuje skutkovou podstatu trestného činu (např. sprejerství), zůstává autorskoprávní status nedotčen. Právní teorie důsledně odděluje vlastnické právo k hmotnému nosiči a nehmotný statek. Splňuje-li výtvar generální klauzuli autorského díla, požívá ochrany bez ohledu na protiprávnost jednání, které vedlo k jeho vzniku.²⁴

Princip ochrany dobrých mravů se promítl například do amerického případu *Villa v. Pearson Education*, který relativizoval neomezenou ochranu děl street artu. Ačkoliv soud v dané fázi řízení nerozhodl ve věci samé, připustil možnost, že autorům graffiti nemusí být autorskoprávní ochrana přiznána právě pro rozpor se zásadou zákazu těžit z vlastní nepoctivosti (*nemo auditur*).²⁵ V českém právním řádu plní obdobnou funkci generální klauzule obsažená v občanském zákoníku. Zejména § 6 odst. 2 OZ stanoví, že nikdo nesmí těžit z vlastního protiprávního činu.²⁶ Dle rozhodnutí Nejvyššího soudu se lze těchto obecných principů, jako je zásada poctivosti, dovolat vždy jako korektivu i tam, kde to zákon výslovně neuvádí.²⁷ Na úrovni Evropského hospodářského prostoru však podobné ustanovení nenajdeme. Lze tedy konstatovat, že z celoevropského hlediska neexistuje jednotná úprava.²⁸

Nicméně je nutné dodat, že využití malwaru nemusí být pouze protiprávní. Malware může být vyráběn například i pro vědecké účely či pro

²² LUNDE, Jeremy S. *COPYRIGHT PROTECTION FOR VIRUS AUTHORS*, s. 50.

²³ LUNDE, Jeremy S. *COPYRIGHT PROTECTION FOR VIRUS AUTHORS*, s. 50.

²⁴ ELIAS, Brittany M a GHAJAR, Bobby. *Street art: the everlasting divide between graffiti art and intellectual property protection*. 7. American Bar Association, 2015. ISSN 1942-7239, s. 48.

²⁵ ELIAS, Brittany M a GHAJAR, Bobby. *Street art: the everlasting divide between graffiti art and intellectual property protection*, s. 49.

²⁶ HOLCOVÁ, I. a kol. *Autorský zákon a předpisy související (včetně mezinárodních smluv a evropských předpisů): komentář*, s. 525.

²⁷ Rozsudek Nejvyššího soudu ze dne 18. 3. 2019, sp. zn. 26 Cdo 1984/2018.

²⁸ Směrnice Evropského parlamentu a Rady 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu, Úř. věst. OJ L 130.

účely testování antimalware programů. Tyto situace lze však označit za vysoce specifické. V takovém případě by ochrana na principu zneužití práva a dobrých mravů nemohla obstát a autor by se mohl své autorskoprávní ochrany domáhat standardním způsobem.²⁹ Takový scénář je však vysoce nepravděpodobný, jelikož vývoj tohoto softwaru se zpravidla odehrává interně v rámci jedné společnosti a kód není určen pro veřejnost. Dojde-li k úniku, bude se primárně řešit porušení obchodního tajemství, nikoliv otázka autorství.

3.3 OCHRANA ZÁKLADNÍCH PRÁV JAKO ODŮVODNĚNÍ MOŽNOSTI ZÁSAHU

3.3.1 OBECNÁ VÝCHODISKA VEŘEJNÉHO ZÁJMU V AUTORSKÉM PRÁVU
Východiskem celé analýzy je střet dvou protichůdných principů. Na jedné straně stojí formální autorskoprávní ochrana malwaru jako počítačového programu. Na straně druhé je činnost antivirových společností, která do tohoto práva z podstaty věci zasahuje reverzním inženýrstvím a dalšími analytickými metodami. Aby tato činnost, která je nezbytná pro ochranu společnosti, mohla být považována za legální, je nutné dospět k závěru, že výkon autorských práv tvůrce malwaru je v tomto specifickém případě omezen vyšším veřejným zájmem na kybernetické bezpečnosti.

Ochrana autorského práva je nedílnou součástí práva na ochranu majetku. Toto základní právo je zakotveno jak v čl. 11 Listiny, tak v čl. 1 Dodatkového protokolu k Evropské úmluvě o lidských právech (EÚLP).³⁰ Rozhodnutí Evropského soudu pro lidská práva (ESLP) připouští zásah do vlastnického práva, pokud je takový zásah v souladu se zákonem, sleduje legitimní cíl ve veřejném zájmu a je přiměřený sledovanému cíli.³¹

Právě judikatura ESLP představuje vhodný rámec pro analýzu této problematiky v kontextu Evropského hospodářského prostoru. Všechny

²⁹ Děkuji anonymnímu recenzentovi za upozornění na tuto situaci.

³⁰ Rozsudek velkého senátu ESLP ze dne 11.1.2007, *Anheuser-Busch Inc. proti Portugalsku*, č. 73049/01, § 63.

³¹ Rozsudek velkého senátu ESLP ze dne 13.12.2016, *Béláné Nagy proti Maďarsku*, č. 53080/13, § 71.

členské státy EU jsou totiž zároveň smluvními stranami EÚLP a judikatura ESLP k ochraně majetku je podstatně rozvinutější než judikatura Soudního dvora EU. Proto bude soulad zásahu do práv tvůrců malwaru posuzován optikou testu proporcionality, jak jej aplikuje ESLP.

3.3.2 ZÁSAH DO VLASTNICKÝCH PRÁV AUTORŮ MALWARU VE VEŘEJNÉM ZÁJMU

Judikatura ESLP uznává širokou škálu legitimních veřejných zájmů, které mohou odůvodnit omezení vlastnického práva. Od sociální spravedlnosti přes hospodářskou regulaci až po prevenci daňových úniků.³² Ačkoliv ESLP dosud výslovně neřešil otázku omezení autorských práv u děl vytvořených za účelem poškodit třetí stranu (jako je malware), argument pro takové omezení lze dovodit z jeho stávající judikaturní linie. Takový argument lze postavit nejen na analogii z konkrétních rozhodnutí, kde Soud připustil omezení práv v zájmu ochrany společnosti před jinými druhy hrozeb, ale i na aplikaci obecných principů, kterými ESLP vymezuje a limituje pojem „veřejný zájem“.

Z judikatury ESLP lze dovodit obecný princip, že ochranu majetku je možné omezit za účelem prevence trestné činnosti. Například v případě Butler proti Spojenému království Soud akceptoval zabavení peněz, které mohly sloužit k pašování drog,³³ a v případě *Hentrich proti Francii* shledal legitimním obdobný zásah v zájmu prevence daňových úniků.³⁴

Mezi těmito případy a problematikou malwaru nicméně existuje zásadní rozdíl. V citovaných kauzách se jednalo o dočasné omezení práv k legitimnímu majetku (penězům), který mohl být ke spáchání trestného činu teprve použit. Oproti tomu malware je nástroj, jehož samotná podstata a účel jsou protiprávní. Nejde zde tedy o dočasnou prevenci, ale o trvalou

³² Například eliminace sociální nerovnosti Srov. Rozsudek pléna ESLP ze dne 21.2.1986 *James a ostatní proti Spojenému království*, č. 8793/79, nacionalizace specifických průmyslů Srov. Rozsudek pléna ESLP ze dne 8.7.1986 *Lithgow a ostatní proti Spojenému království* č. 9006/80, 9262/8, 9263/81, 9265/81, 9266/81, 9313/81, 9405/81, nebo třeba prevence daňových úniků Srov. Rozsudek ESLP ze dne 22.9.1994, *Hentrich proti Francii*, č. 13616/88.

³³ Rozhodnutí ESLP ze dne 27.6.2002, *Butler proti Spojenému království*, č. 41661/98.

³⁴ Rozsudek ESLP ze dne 22.9.1994, *Hentrich proti Francii*, č. 13616/88, § 39.

potřebu společnosti bránit se nástroji určenému ke škodlivé činnosti. Nicméně i přesto, že se tyto případy liší, lze prevenci kriminality označit za legitimní veřejný zájem.

3.3.3 ZÁKONNOST ZÁSAHU DO PRÁV AUTORŮ MALWARU

Druhou podmínkou pro jakýkoli zásah do vlastnického práva je, že musí být v souladu se zákonem.³⁵ To znamená, že omezení práva musí mít oporu v platném právním předpise.

Na úrovni Evropského hospodářského prostoru sice neexistuje specifický zákon, který by tuto problematiku řešil, avšak dostatečný právní základ poskytují obecné principy. Jak již bylo zmíněno, jedná se zejména o zákaz zneužití práva, zakotvený v čl. 54 Listiny základních práv EU, který funguje jako univerzální korektiv.

Pro účely testu ESLP je však existence těchto obecných a univerzálně aplikovatelných zásad, jako je zákaz zneužití práva, dostatečným zákonným základem pro omezení ochrany.

3.3.4 PROPORCIONALITA

Posledním krokem testu je posouzení, zda je zásah do práv tvůrce malwaru přiměřený (proporcionální). To vyžaduje poměření dvou konkurenčních zájmů: na jedné straně veřejného zájmu na zajištění kybernetické bezpečnosti a ochraně majetku a soukromí milionů uživatelů, a na straně druhé majetkového zájmu autora v díle, jehož jediným účelem je tato práva porušovat.

Při konečném poměřování je zřejmé, že zájem společnosti na ochraně před protiprávními útoky musí převážet. Zásah do autorských práv tvůrce malwaru, který umožňuje se těmto útokům bránit, tak nejenže splňuje test proporcionality, ale je i opatřením nezbytným v demokratické společnosti.³⁶

Důvodem je, že malware nepředstavuje hrozbu jen pro osobní údaje jednotlivců, ale může způsobit i kolaps kritické infrastruktury, od nemocnic po energetické sítě, a to například prostřednictvím ransomwaru. Ochrana této infrastruktury je tak klíčovým bezpečnostním zájmem státu.

³⁵ Čl. 1 dodatkového protokolu č. 1 Úmluvy o ochraně lidských práva a základních svobod.

³⁶ Rozsudek velkého senátu ESLP ze dne 5.1.2000, *Beyeler proti Itálii*, č. 33202/96, § 107.

Tuto ochranu v praxi z velké části zajišťují soukromé společnosti (např. McAfee, Symantec), které investují značné prostředky do analýzy hrozeb.³⁷ Tyto společnosti sice z těchto komerčních aktivit mají nemalý zisk, lze ale argumentovat, že bez možnosti analyzovat malware pomocí reverzního inženýrství by jakákoliv iniciativa malware odhalovat a potlačovat, ať již státem organizovaná či soukromá, byla nemožná. Jejich činnost, ač komerční, je nepostradatelná. Bez možnosti analyzovat škodlivý kód pomocí reverzního inženýrství by byla jakákoliv efektivní obrana zcela iluzorní. Z tohoto důvodu je nepochybné, že veřejný zájem na kybernetické bezpečnosti musí mít přednost. Ochrana, kterou autorské právo formálně poskytuje tvůrcům malwaru, tak musí být prolomitelná, aby bylo možné zajistit funkčnost a bezpečnost digitální společnosti.

K bezpečnostnímu argumentu se navíc řadí i důvod ekonomický. Kyberkriminalita každoročně způsobuje globální ekonomice škody v řádech bilionů dolarů.³⁸ Pokud by antivirové společnosti nemohly malware efektivně analyzovat a neutralizovat, tyto již tak astronomické ztráty by dále exponenciálně rostly. Ochrana ekonomiky před těmito dopady je tak dalším pádným důvodem, proč musí veřejný zájem převážet nad formální autorskoprávní ochranou malwaru.

Součástí testu proporcionality je i posouzení, zda nelze sledovaného cíle dosáhnout méně invazivními prostředky.³⁹ V případě malwaru je toto kritérium splněno, neboť neexistuje jiný efektivní způsob jeho detekce než analýza jeho kódu a chování. Ačkoliv se plošné omezení autorského práva může jevit jako radikální, pro zajištění kybernetické bezpečnosti je nezbytné.

Je důležité zdůraznit, že autor malwaru neztrácí svá práva zcela. Omezení se vztahuje výhradně na úkony nezbytné pro analýzu a neutralizaci

³⁷ RODRIGUEZ, Miranda. All Your IP Are Belong to Us: An Analysis of Intellectual Property Rights as Applied to Malware. *Texas A&M Law Review*. 2016, roč. 3, č. 3. ISSN 2837-5165, s. 665.

³⁸ MORGAN, Steve. Cybercrime To Cost The World \$10.5 Trillion Annually By 2025. *Cybercrime Magazine* [online]. 8. 12. 2018 [cit. 2024-03-22]. Dostupné z: <https://cybersecurity-ventures.com/cybercrime-damages-6-trillion-by-2021/>.

³⁹ Rozsudek ESLP ze dne 11.2.2020, *Vaskrsić proti Slovinsku*, č. 31371/12, § 83.

hrozby. Jakékoli jiné užití díla (např. komerční reprodukce) by nadále vyžadovalo jeho svolení. Tvůrce softwaru určeného ke škodlivé činnosti však musí nést zvýšenou míru tolerance vůči zásahům, které slouží k ochraně společnosti.

Problematictější se může jevit skutečnost, že toto omezení dopadá i na tvůrce legitimního softwaru. Antivirový program z podstaty své funkce musí analyzovat všechny programy, nikoli jen ty škodlivé. Tento plošný zásah je však odůvodněn povahou hrozby. Potenciálně nebezpečný může být jakýkoli kód. Jde tedy o široké, avšak s ohledem na neexistenci alternativ proporcionální omezení.

Při konečném poměřování je zřejmé, že veřejný zájem na fungující a bezpečné digitální infrastruktuře jednoznačně převažuje nad zájmem na absolutní ochraně autorských práv k softwaru. Autorskoprávní ochrana v důsledku činnosti antivirových programů nemizí, je pouze v nezbytně nutné míře omezena ve prospěch vyššího celospolečenského cíle.

4. MALWARE A ANTIVIROVÉ PROGRAMY

Základní funkce antivirového softwaru spočívá v analýze malwaru. Tímto jednáním však nevyhnutelně dochází k užití cizího autorského díla ve smyslu § 12 a násl. autorského zákona. Pokud tedy přijmeme premisu, že malware je chráněným dílem, antivirové společnosti svou činností zasahují do majetkových práv jeho tvůrců.

Klíčovou metodou této analýzy je reverzní inženýrství,⁴⁰ definované jako proces dekonstrukce finálního produktu za účelem zjištění jeho vnitřního fungování. V kontextu softwaru to umožňuje odhalit charakteristiky a zamýšlené funkce škodlivého kódu.⁴¹ Cílem je identifikovat jeho chování nebo nalézt zranitelnost, která umožní jeho neutralizaci. Uplatňují se přitom dvě základní techniky.

⁴⁰ Reverzní inženýrství bylo předmětem právního sporu v USA, kde získalo definici jako „proces, kdy začneme s finálním produktem a pracujeme tím, že ho rozmontujeme a zjišťujeme, jak funguje a jak byl vyroben“ Srov. *Secure Services Tech. v. Time and Space Processing*, 722 F. Supp. 1354 (E.D. Va. 1989).

⁴¹ VIGNA Giovanni. *Static Disassembly and Code Analysis*, Christodorescu, Mihai. *Malware detection*. New York: Springer, 2006. ISBN 1-280-80436-X., s. 28.

První takovou technikou je dynamická analýza, která spočívá v monitorování běžícího programu a sledování příkazů, které zadává operačnímu systému a hardwaru. Druhou technikou je následně statická analýza, která představuje zkoumání samotného binárního kódu programu bez jeho spuštění.⁴²

Směrnice o právní ochraně počítačových programů⁴³ skutečně stanovuje určité výjimky z výlučného práva autora. Klíčový je čl. 5, který oprávněnému nabyvateli licence umožňuje bez dalšího svolení zkoumat, studovat a zkoušet funkčnost programu za účelem zjištění jeho základních myšlenek a zásad.⁴⁴ Stejně tak smí provádět úpravy nezbytné pro zamýšlené užití programu, včetně opravy chyb. Tato ustanovení však nelze vykládat extenzivně – neopravňují například k dekompilaci za účelem vytvoření konkurenčního produktu.

Nabízí se tedy otázka, zda se antivirové společnosti mohou této výjimky dovolat. Takový výklad je však neudržitelný, a to ze dvou klíčových důvodů. Za prvé se vztahují pouze na oprávněného nabyvatele licence. Antivirová společnost analyzující malware, který se šíří protiprávně, nikdy není v pozici oprávněného nabyvatele, s výjimkou případů, kdyby si nechala od autora udělit licenci. Toto si sice lze těžko představit, ale je to teoreticky možné. Za druhé samotným cílem antivirové analýzy je malware neutralizovat a zničit, nikoliv ho užívat k zamýšlenému účelu či dosáhnout interoperability. Taková činnost jde zjevně nad rámec účelu, pro který směrnice výjimky stanovila.⁴⁵

Pokud však odhlédneme od této formálněprávní roviny, je nepředstavitelné, že by se autor malwaru u soudu úspěšně domohl ochrany. Jeho případný nárok by byl vyloučen fundamentálními principy soukromého práva. Jakýkoli soud by takovou žalobu s největší pravděpodobností zamítl s odkazem na zákaz zneužití práva a obecnou zásadu, že nikdo nesmí těžit

⁴² VIGNA Giovanni. *Static Disassembly and Code Analysis*, s. 29.

⁴³ Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů, Úř. věst. OJ L 111, 5.5.2009.

⁴⁴ Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů, Úř. věst. OJ L 111, 5.5.2009.

⁴⁵ LUNDE, Jeremy S. *COPYRIGHT PROTECTION FOR VIRUS AUTHORS*, s. 14.

z vlastního protiprávního činu. I přesto, že autor tak formálně svůj nárok neztrácí a teoreticky jej může licencovat, tak je takové právo jen těžko před orgány veřejné moci vymahatelné.

5. DOSTATEČNOST SOUČASNÉ LEGISLATIVNÍ ÚPRAVY A ÚVAHY DE LEGE FERENDA

Tato kapitola posuzuje, zda je současná unijní legislativa dostatečná pro omezení autorských práv tvůrců malwaru. Jak bylo ukázáno, evropské směrnice s existencí děl vytvořených za protiprávním účelem výslovně nepočítají, což ponechává řešení na aplikaci obecných právních principů, jako je zákaz zneužití práva.⁴⁶ Vystává proto otázka, zda by bylo vhodnější přijmout explicitní legislativní úpravu.

První zvažovanou možností je rozšíření stávajících zákonných licencí, což by muselo být v souladu s tzv. třístupňovým testem Bernské úmluvy.⁴⁷ Konkrétně by šlo o extenzivní výklad úřední licence zakotvené v informační směrnici.

Tento přístup by nevyžadoval novelizaci směrnice, nýbrž změnu výkladu Soudního dvora EU. Soud by musel dovodit, že licenci mohou využít i soukromé subjekty (antivirové společnosti), pokud tím prokazatelně chrání veřejný zájem. Proti takovému výkladu však stojí značné riziko zneužití. Šlo by o široký průlom do systému licencí kvůli relativně úzkému problému, což by mohlo narušit právní jistotu a otevřít dveře pro nepředvídatelné aplikace v jiných oblastech.

Druhou teoretickou možností je zavedení nové generální klauzule, která by umožnila omezit autorskoprávní ochranu v případě rozporu s veřejným zájmem. Klíčovou otázkou však zůstává, zda je taková legislativní změna nezbytná. V praxi neexistují případy, kdy by se autor malwaru úspěšně domáhal ochrany svých autorských práv proti antivirové společnosti. Historicky je sice znám pokus autorů Zetus Rootkitu zakázat reverzní inženýrství

⁴⁶ Konkrétně čl. 54 Listiny základních práv Evropské unie, který zakazuje zneužití práva.

⁴⁷ Třístupňový test Bernské úmluvy je test, který vychází z čl. 9 odst. 2 Bernské úmluvy a stanovuje limity na výjimky z ochrany majetkových práv autora k dílu.

a analýzu jejich kódu prostřednictvím licenčních podmínek (EULA),⁴⁸ avšak vymahatelnost takových podmínek je považována za čistě hypotetickou.⁴⁹ Autor malwaru by se navíc podáním žaloby fakticky sebeobvinil z trestné činnosti.

Především však platí, že nástroje pro řešení takové situace již existují, a to na národní i unijní úrovni. Jakýkoli pokus o zneužití autorského práva k ochraně malwaru by narazil na již zmiňovaný § 6 OZ,⁵⁰ a v právu Evropské unie na Listinu základních práv EU.⁵¹ Z těchto důvodů lze konstatovat, že stávající právní rámec, opírající se o obecné právní zásady, je pro ochranu činnosti antivirových společností plně dostačující.

Ačkoliv se může zdát myšlenka žaloby podané tvůrcem malwaru absurdní, nelze ji zcela vyloučit. Spory vedené autory street artu ukazují, že i díla na hraně legality si mohou nárokovat ochranu. Přesto by takový pokus v případě malwaru narazil na dvě takřka nepřekonatelné překážky.

První je procesní povahy: žalobce by se podáním žaloby fakticky doznal k jednání, které je ve většině jurisdikcí klasifikováno jako trestný čin, a vystavil by se tak riziku trestního stíhání. Druhá překážka je hmotněprávní: i kdyby soud formální ochranu dílu přiznal, samotný výkon práva by byl znemožněn fundamentálními právními principy, jako jsou právě výše zmíněné zásady zákazu těžit z vlastní nepoctivosti (zásada *nemo auditur*), či zjevného zákazu zneužití práva.

Lze tedy shrnout, že ačkoliv specifické autorskoprávní směrnice EU postrádají výslovnou výjimku pro analýzu malwaru, současný právní rámec je plně dostačující. Ochranu antivirovým společnostem poskytují obecné zásady a korektivy obsažené jak v primárním právu EU, tak v národních občanských zákonících. Vzhledem k hypotetické povaze těchto sporů není

⁴⁸ RODRIGUEZ, Miranda. *All Your IP Are Belong to Us*. s. 665-666.

⁴⁹ DOCTOROW, Cory. *Malware gets a EULA. Boing Boing* [online]. 28. 4. 2008 [cit. 2024-03-27]. Dostupné z: <https://boingboing.net/2008/04/29/malware-gets-a-eula.html>. KDAW-SON. *EULAs For Malware. Slashdot* [online]. 28. 4. 2008 [cit. 2024-03-27]. Dostupné z: <https://slashdot.org/story/08/04/29/0057236/eulas-for-malware>.

⁵⁰ Viz HOLCOVÁ, I. a kol. *Autorský zákon a předpisy související (včetně mezinárodních smluv a evropských předpisů): komentář*, s. 525.

⁵¹ Listina základních práv Evropské unie ze dne 26.10.2012, Úř. věst. OJ C 202, 7.6.2016.

nutné přijímat novou legislativu; stávající právní řád si s tímto problémem dokáže efektivně poradit prostřednictvím soudního výkladu.

6. ZÁVĚR

Předkládaný článek analyzuje způsobilost malwaru být předmětem autorskoprávní ochrany a kolizi této ochrany s činností bezpečnostního softwaru (antimalware). Text konstatuje, že malware, jakožto počítačový program, naplňuje definiční znaky díla dle autorského zákona, a tudíž požívá ochrany bez ohledu na svou škodlivou povahu.

Autorka však zároveň dovozuje, že faktická vymahatelnost těchto subjektivních práv je nulová. Soudní vymáhání by nutně vedlo k sebeobvinění autora z trestné činnosti a nárok by byl s vysokou pravděpodobností zamítnut na základě zákazu zneužití práva či zásady *nemo auditur*.

V kontextu antivirových programů článek potvrzuje, že dochází k užití cizího autorského díla, které nelze subsumovat pod stávající zákonné licence. Tento zásah je však legitimizován převažujícím veřejným zájmem na ochraně kybernetické infrastruktury. Závěrem je konstatováno, že ačkoliv jsou úvahy *de lege ferenda* možné, stávající judikатурní nástroje a obecné právní principy poskytují pro řešení těchto hypotetických sporů dostatečný rámec.

7. SEZNAM POUŽITÝCH ZDROJŮ

- [1] AYCOCK, John. Computer Viruses and Malware. New York, NY: Springer US, 2006. ISBN 1-280-71620-7. Dostupné z: <https://doi.org/10.1007/0-387-34188-9>.
- [2] DOCTOROW, Cory. Malware gets a EULA. *Boing Boing* [online]. 28. 4. 2008 [cit. 27.03.2024]. Dostupné z: <https://boingboing.net/2008/04/29/malware-gets-a-eula.html>.
- [3] MICROSOFT. Does Windows 11 Need Antivirus on Laptops? | Microsoft Surface. In: *Microsoft* [online] [cit. 2024-03-28]. Dostupné z: <https://www.microsoft.com/en-us/surface/do-more-with-surface/does-windows-11-need-antivirus-on-laptops> > .
- [4] ELIAS, Brittany M a GHAJAR, Bobby. *Street art: the everlasting divide between graffiti art and intellectual property protection*. 7. American Bar Association, 2015. ISSN 1942-7239.
- [5] GRÍVNA, Tomáš, DVOŘÁK, Marek. § 230. ŠÁMAL, Pavel a kol. *Trestní zákoník*. 3. vydání. Praha: C. H. Beck, 2023.
- [6] HILL, Joshua B. – MARION, Nancy E. *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*. New York: Bloomsbury Publishing USA, 2016 .

- [7] HOLCOVÁ, Irena; KŘEŠŤANOVÁ, Veronika; DOBŘICHOVSKÝ, Tomáš; CÍSAŘOVÁ, Zuzana; ŽIKOVSKÁ, Petra et al. Autorský zákon a předpisy související (včetně mezinárodních smluv a evropských předpisů): komentář. Praha: Wolters Kluwer Česká republika, 2019. ISBN 978-80-7598-049-6.
- [8] CHALOUPKOVÁ, Helena, HOLÝ, Petr. *Autorský zákon*. 6. vydání. Praha: C. H. Beck, 2023.
- [9] KRAMER, Simon a Julian C. BRADFIELD. A general definition of malware. *Journal in Computer Virology*. 2010, roč. 6, č. 2. ISSN 1772-9890.
- [10] LUNDE, Jeremy S. *Copyright protection for virus authors*. Establishing Protection for Authors Irrespective of the Merits of Their Creation. Oslo, 1.12.2010, 65, Diplomová práce, University of Oslo.
- [11] MORGAN, Steve. Cybercrime To Cost The World \$10.5 Trillion Annually By 2025 In: *Cybersecurity ventures* [online]. 2018 [cit. 22.03.2024]. Dostupné z: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>.
- [12] NAYAK, Umesha. Malicious Software and Anti-Virus Software. *The InfoSec Handbook*. Apress, 2014. ISBN 9781430263838.
- [13] RODRIGUEZ, Miranda. All Your IP Are Belong to Us: An Analysis of Intellectual Property Rights as Applied to Malware. *Texas A&M Law Review*. 2016, roč. 3, č. 3. DOI: 10.37419/LR.V3.13.7. ISSN 2837-5165
- [14] ROSENCRANCE, Linda. What is antimalware? In: *TechTarget* [online] [cit. 28.03.2024]. Dostupné z: <https://www.techtarget.com/searchsecurity/definition/antimalware>.
- [15] VIGNA Giovanni. Static Disassembly and Code Analysis CHRISTODORESCU, Mihai. *Malware detection*. New York: Springer, 2006. ISBN 1-280-80436-X.
- [16] Listina základních práv Evropské unie ze dne 26.10.2012, Úř. věst. OJ C 202, 7.6.2016.
- [17] Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti, Úř. věst. OJ L 167, 22.6.2001.
- [18] Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů, Úř. věst. OJ L 111, 5.5.2009.
- [19] Smlouva č. 104/2013 Sb. m. s. Úmluva o počítačové kriminalitě.
- [20] Smlouva č. 209/1992 Sb. m. s. Úmluva o ochraně lidských práv a základních svobod ve znění protokolů č. 1, 2, 4, 6, 7.
- [21] Rozhodnutí ESLP ze dne 27.6.2002, *Butler proti Spojenému království*, č. 41661/98.
- [22] Rozsudek ESLP ze dne 11.2.2020, *Šeiko proti Litvě*, č. 82968/17, § 30.
- [23] Rozsudek ESLP ze dne 22.9.1994, *Hentrich proti Francii*, č. 13616/88.
- [24] Rozsudek Nejvyššího soudu ze dne 18. 3. 2019, sp. zn. 26 Cdo 1984/2018.
- [25] Rozsudek Nejvyššího soudu ze dne 27.01.2011, sp. zn. 4 Tz 79/2010.

[26] Rozsudek pléna ESLP ze dne 21.2.1986, *James a ostatní proti Spojenému království*, č. 8793/79.

[27] Rozsudek pléna ESLP ze dne 8.7.1986, *Lithgow a ostatní proti Spojenému království*, č. 9006/80, 9262/8, 9263/81, 9265/81, 9266/81, 9313/81, 9405/81.

[28] Rozsudek velkého senátu ESLP ze dne 11.1.2007, *Anheuser-Busch Inc. proti Portugalsku*, č. 73049/01.

[29] Rozsudek velkého senátu ESLP ze dne 13.12.2016, *Béláné Nagy proti Maďarsku*, č. 53080/13.

[30] Rozsudek velkého senátu ESLP ze dne 5.1.2000, *Beyeler proti Itálii*, č. 33202/96.

[31] *Secure Services Tech. v. Time and Space Processing*, 722 F. Supp. 1354 (E.D. Va. 1989).

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>).

<https://doi.org/10.5817/RPT2025-2-2>

PRÁVNÍ ASPEKTY POŽADAVKŮ NA DATOVÉ FORMÁTY

TOMÁŠ LECHNER¹

ABSTRAKT

Příspěvek představuje elektronický dokument jako důležitou entitu, která je nositelem zaznamenané informace anebo alespoň zaznamenaného obsahu. Z pohledu své elektronické formy má elektronický dokument určité atributy, mezi které patří také datový formát. Na některé právní úkony, zejména v oblasti veřejné správy, jsou kladeny specifické požadavky na tento formální atribut elektronického dokumentu. V příspěvku jsou tyto požadavky diskutovány a srovnávány včetně toho, jaké dopady má jejich nedodržení na uvedené úkony. Z toho jsou pak identifikována konkrétní rizika spojená s tvorbou a použitím elektronických dokumentů v kontextu volby datových formátů. V diskusi je také zmíněn vliv datového formátu na dlouhodobou čitelnost elektronických dokumentů a udržení jejich důkazní hodnoty v kontextu připravované nové kvalifikované služby elektronické archivace dle nařízení Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu.

KLÍČOVÁ SLOVA

Elektronický dokument; datový formát; podání; doručování; zveřejňování smluv; konverze datových formátů; archivace dokumentů

¹ Mgr. Tomáš Lechner, Ph.D. Vysoká škola ekonomická v Praze, Národohospodářská fakulta, katedra práva. Kontakt: tomas.lechner@vse.cz

ABSTRACT

The paper deals with the electronic record as a significant entity that serves as a carrier of recorded information, or at least recorded content. From the perspective of its electronic form, an electronic record possesses specific attributes, which also include the data format. Particular acts, especially in the area of public administration, impose explicit requirements on this formal attribute of the electronic records. These requirements are discussed and compared in the paper, including an analysis of the consequences arising from non-compliance with such formal requirements in relation to the acts concerned. Based on this analysis, some risks associated with the creation and use of electronic documents in the context of data format selection are identified. The discussion further addresses the impact of data format on the long-term readability of electronic records and the preservation of their evidentiary value, with reference to the forthcoming qualified electronic archiving service under the Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024, amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

KEYWORDS

Electronic Records; Data Format; Application; Delivery; Publication of Contracts; Conversion of Data Formats; Record Archiving

1. ÚVOD

Elektronický dokument byl v českém právu dlouho definován jako podmnožina dokumentu, kterým je dle § 2 písm. e) zákona č. 499/2004 Sb., o archivnictví a spisové službě,² každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena. Vymezení dokumentu jen na původce je poplatné zaměření citovaného zákona, nicméně stěžejní

² Všechny právní předpisy jsou citovány ve stavu účinném k 1. září 2025.

je obecná podstata definice, že jde o zaznamenanou informaci. Podle sémiotických přístupů má mít informace tři základní relevance:³

- syntaktickou, což znamená, že subjekt, jemuž je informace určena, musí být schopen této informaci porozumět,
- sémantickou, což znamená, že subjekt, jemuž je informace určena, musí vědět, co znamená, tedy co vypovídá o něm a o jeho okolí,
- pragmatickou, což znamená, že informace musí mít pro subjekt, jemuž je určena, nějaký konkrétní význam.

Znamená to, že všemi těmito relevancemi by měl oplývat také dokument, i když na druhou stranu jejich striktní vyžadování by mohlo vést ke ztrátám dokumentů, u nichž některá z nich absentuje, a přesto jsou z určitých hledisek zajímavé a důležité. Norma ISO 15489-1 dokument definuje jako „*informace vytvořené, získané a spravované organizacemi nebo osobami jako doklady a/nebo vzniklé při plnění jejich právních povinností nebo při jejich činnosti*“,⁴ čímž se zdůrazňuje jejich vztah k právním úkonům a jejich důkazní role, kdy dokument vlastně dokáže konzervovat právní stav v čase.

Aktuální definice přímo elektronického dokumentu je obsažena v 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 a o zrušení směrnice 1999/93/ES, známého jako nařízení eIDAS. Tento předpis definuje elektronický dokument jako jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka,⁵ aniž tedy vyžaduje, aby tím obsahem byla informace.⁶ Obdobně dokument definuje též směrnice Evropského parlamentu a Rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru jako jakýkoli obsah na jakémkoli nosiči (v listinné či elektronické

³ Blíže viz ŠLAPÁK, O. Data, informace, znalosti. *E-LOGOS. Electronic journal for philosophy*. [online] 2003, roč. 10, č. 1, [cit. 26. 9. 2025], s. 1.

⁴ Viz ISO 15489-1:2001 – Information und Dokumentation, 3.15. record, s. 3.

⁵ Viz čl. 3 odst. 35 nařízení eIDAS.

⁶ Detailní diskuse k tomuto rozporu je v publikaci POLČÁK, Radim a kol. *Právo informačních technologií*. 2. vyd. Praha : Wolters Kluwer, 2024, s. 472-474.

podobě nebo jako zvuková, vizuální nebo audiovizuální nahrávka) nebo jakákoli část takového obsahu.⁷

Elektronický dokument tak již není jen podmnožinou dokumentu, ale má určitý přesah z hlediska volnějšího obsahu, čímž se v praxi komplikují některé přístupy, zejména v oblasti spisové služby.⁸

2. DATOVÝ FORMÁT

Elektronické dokumenty mají svá specifika z různých hledisek, například:

- Z principu je lze přenášet elektronickými prostředky jako jsou datové schránky nebo e-mail.
- Pro jejich zobrazení lidsky vnímatelným způsobem potřebujeme technické (hardware) a programové (software) nástroje.
- Péče o elektronické dokumenty je péčí o data a je významně odlišná od péče o listinné dokumenty, při které chráníme zejména nosič.⁹

Jedním z atributů elektronického dokumentu je způsob jeho kódování označovaný jako datový formát, na který bychom mohli také nahlížet jako na návod, jakým způsobem mají technické a programové nástroje elektronický dokument převést do lidsky vnímatelné podoby. Sumarizací informací o těchto návodech, tedy popisů a znaků datových formátů, se dlouhodobě zabývá Národní archiv Spojeného království, který buduje databázi označovanou jako PRONOM.¹⁰ Vývoj této databáze byl inspirován tím, že dostupnost informací o datových formátech je v dnešním rychle se vyvíjejícím technologickém prostředí velmi zranitelná, a je tedy významným rizikem z pohledu správy elektronických dokumentů. S ohledem na to je

⁷ Viz čl. 2 odst. 6 písm. a) a b) směrnice 2019/1024.

⁸ Viz KUNT, M., LECHNER, T. *Spisová služba. 3. aktualizované vyd.* Praha: Leges, 2022. s. 74-78 a s. 81-83.

⁹ Viz CUBR, L. *Dlouhodobá ochrana digitálních dokumentů.* Praha: Národní knihovna České republiky, 2010, s. 10-14.

¹⁰ UK NATIONAL ARCHIVES. *The technical registry PRONOM [online].* [cit. 3. 6. 2025]. Dostupné z: <https://www.nationalarchives.gov.uk/PRONOM/>

databáze PRONOM dále rozvíjena a aktualizována o nově vznikající datové formáty.

Mají-li elektronické dokumenty sloužit svému účelu a být nositeli obsahu a informací, je třeba se jejich datovým formátem zabývat, aby tento obsah či tyto informace zůstaly budoucím adresátům dostupné. Z právního pohledu jde o zachování jejich důkazní hodnoty, což je jedním ze stěžejních smyslů dokumentů.

A proto si zde klademe následující výzkumné otázky:

- Jakým způsobem jsou kategorizovány datové formáty, tedy jinými slovy, jaké mohou mít vlastnosti, kterými je vhodné se zabývat z pohledu udržení jejich důkazní hodnoty?
- Jaké požadavky na datové formáty elektronických dokumentů jsou kladeny ve specifických úkonech, jako je například podání, doručování anebo zveřejňování smluv?

3. STRUKTURA ELEKTRONICKÝCH DOKUMENTŮ

Z pohledu spisové služby, která je zejména v oblasti veřejnoprávní základním nástrojem pro správu všech forem dokumentů, a tedy i těch elektronických, je na dokument nahlíženo jako na logickou jednotku, která může mít vnitřní strukturu. Základní stavební jednotkou elektronického dokumentu je podle národního standardu pro elektronické systémy spisové služby, který vydává Ministerstvo vnitra na základě zmocnění v zákoně č. 499/2004 Sb., komponenta. Ta je v citovaném standardu definována jako jednoznačně vymezený proud bitů tvořící datový soubor charakterizovaný zpravidla formátem datového souboru, běžně zpracovávaným programovými aplikacemi, které umožňují provádět správu souborů, složek a disků tak, aby k nim bylo možné uživatelsky srozumitelně přistupovat a s nimi samostatně manipulovat.¹¹ Není pak překvapující, že týž standard definuje datový formát jako způsob kódování komponenty pro účely zpracování výpočetní technikou.¹²

¹¹ Viz MINISTERSTVO VNITRA. *Národní standard pro elektronické systémy spisové služby*. 6. verze. Věstník Ministerstva vnitra, částka 85/2024, s. 9.

¹² *Ibid*, s. 7.

Protože elektronický dokument se skládá alespoň z jedné komponenty a každá má svůj datový formát, může to znamenat, že dokument tak může mít více datových formátů, což v žádném případě není neobvyklé. Je tedy otázkou, jak posuzovat formát elektronického dokumentu z pohledu zákonných požadavků na něj kladených, když těchto formátů může mít jeden dokument najednou více, protože se může skládat z více komponent s různými datovými formáty.

Určitým vodítkem k řešení této otázky může být přístup aplikovaný v oblasti spisové služby. Inspirovat se lze také strukturou datové zprávy přenášené informačním systémem datových schránek. V obou případech se komponentám přisuzují různé role. Jen jedna z nich je hlavní, ostatní mají charakter příloh. To znamená, že můžeme datový formát dokumentu chápat jako datový formát hlavní komponenty, a z pohledu zákonných požadavků na datové formáty je vztahovat jen k hlavní komponentě elektronického dokumentu bez ohledu na datové formáty příloh.

3.1 ELEKTRONICKÝ DOKUMENT A DATOVÁ ZPRÁVA

V případě diskuse o elektronických dokumentech se z hlediska pojmosloví použitého v zákoně č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, a k němu prováděcím předpisům,¹³ nelze nezmínit o souvisejícím pojmu, kterým je datová zpráva. V uvedených předpisech se lze setkat s konstrukcí typu „dokument obsažený v datové zprávě.“

Rozboru pojmu datová zpráva se věnuje Stanovisko Nejvyššího soudu k podáním činěným v elektronické podobě a k doručování elektronicky vyhotovených písemností soudem, prováděnému prostřednictvím veřejné datové sítě (Plsň 1/2015) publikované pod č. 1/2017 ve Sbírce soudních rozhodnutí a stanovisek. V něm je přímo uvedeno, že elektronické dokumenty mají podobu datové zprávy anebo že dokumenty jsou obsaženy v datové zprávě. Tím vznikají dva pohledy na datovou zprávu:

¹³ Konkrétně jde o vyhlášku č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů, a vyhlášku č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek.

- Na datovou zprávu v užším slova smyslu lze pohlížet jako na elektronický dokument mající podobu datové zprávy, což z pohledu naší diskuse znamená vlastně jednu komponentu, která je charakterizována jedním datovým formátem.
- Na datovou zprávu v širším slova smyslu lze pohlížet jako na elektronický nosič neboli obálku či kontejner, v nichž je obsažen samotný elektronický dokument jako příloha. Takovou datovou zprávou může být e-mail, datová zpráva přenášená informačním systémem datových schránek, nebo třeba SIP balíček ukládaný do národního archivu. Z technického pohledu taková datová zpráva má opět vlastní datový formát,¹⁴ což ale není datový formát dokumentu v ní obsaženém. Nicméně se tím může komplikovat diskuse podmínek kladených na datové formáty, protože nemusí být jasné, zda je také vztáhnout na datovou zprávu v širším slova smyslu.

4. KATEGORIZACE DATOVÝCH FORMÁTŮ

Než přistoupíme k rozboru požadavků kladených na datové formáty, je dobré je nějakým způsobem kategorizovat.

4.1 KONTEJNEROVÉ DATOVÉ FORMÁTY

Národní standard pro elektronické systémy spisové služby definuje jednu specifickou podmnožinu datového formátu, kterou je kontejnerový datový formát. Kontejnerové datové formáty jsou formáty komponent obsahující alespoň jednu další komponentu.¹⁵ Problém s uchopením vnitřní struktury elektronického dokumentu, který znamená, že elektronický dokument může mít najednou více datových formátů, pokud se skládá z více komponent s různými datovými formáty, se tím prohlubuje na otázku, zda u případů, kdy se jedna komponenta skládá z více komponent, pohlížet na datový for-

¹⁴ Např. e-mail má datový formát EML (E-Mail Message) a datová zpráva přenášená informačním systémem datových schránek má formát ZFO (602XML Filler dokument).

¹⁵ MINISTERSTVO VNITRA. *Národní standard pro elektronické systémy spisové služby*. 6. verze. Věstník Ministerstva vnitra, částka 85/2024, s. 9.

mát celku, tedy kontejneru, nebo na datové formáty v kontejneru vložených komponent.

Otázka souvisí s pojetím výše zmíněné datové zprávy, neboť ve stanovisku Nejvyššího soudu PlsN 1/2015 je přímo kontejner uveden, jako příklad datové zprávy v širším slova smyslu. Avšak v době vydání tohoto stanoviska, ještě nebylo možné prostřednictvím informačního systému datový schránek přenášet datový formát ZIP, který v tomto případě znamená vnořenou datovou zprávu v širším slova smyslu do jiné datové zprávy v širším slova smyslu. Domnívám se, že rekurzivní přístup původního rozboru provedeného v citovaném stanovisku zde nelze automaticky aplikovat na tuto novou situaci.

Z mého předchozího výzkumu kontejnerových datových formátů¹⁶ vyplynulo, že nejsou ucelenou skupinou, ale mají různorodé vlastnosti, z nichž pro diskutovaný problém datových formátů je asi nejdůležitější to, zda jsou pouhou obálkou obalující skupinu vložených komponent (např. datový formát ZIP či ASIC), nebo zda kromě vložených komponent mají ještě i vlastní obsah (např. datový formát PDF/A-3 či ZFO).¹⁷

4.2 VÝSTUPNÍ DATOVÉ FORMÁTY

Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby, rozlišuje datové formáty podle obsahu komponenty na

- datové formáty pro statické textové komponenty,
- datové formáty pro statické obrazové komponenty,
- datové formáty pro statické kombinované textové a obrazové komponenty,
- datové formáty pro dynamické obrazové komponenty,
- datové formáty pro dynamické zvukové komponenty
- datové formáty pro databáze a datové věty,

¹⁶ Výsledky tohoto výzkumu jsem publikoval v příspěvku LECHNER, Tomáš. Právní pohled na kontejnerové datové formáty. In: PÁNKOVÁ, K. (ed.). *Sborník 27. ročníku konference ISSS* [online]. Hradec Králové, 12.05.2025 – 13.05.2025. Praha: Triada, 2025, s. 39–45.

¹⁷ *Ibid*, s. 44 a 45.

- datové formáty pro specifické kategorie dokumentů jako je třeba elektronická faktura.¹⁸

Pro všechny tyto kategorie dle charakteru obsahu vyhláška definuje odpovídající datové formáty, které označuje jako výstupní. Toto pojmenování je poněkud nešťastné, protože spíše poukazuje na procesní okamžik tvorby, než na smysl takto určených datových formátů. Podle § 23 odst. 1 citované vyhlášky se výstupním datovým formátem rozumí:

- a) datový formát výstupu z elektronického systému spisové služby,
- b) datový formát komponenty ukládané ve spisovně, která je součástí elektronického systému spisové služby,
- c) datový formát pro předávání do digitálního archivu.

Avšak smysl těchto datových formátů není v tom, aby byly jen na výstupu spisové služby, ale jedná se o takové datové formáty, u kterých je předpoklad dlouhodobé čitelnosti. To znamená, že s velkou pravděpodobností dokument ve výstupním datovém formátu budeme schopni zobrazit lidsky vnímatelným způsobem v delším časovém horizontu, čímž bude zachována jeho důkazní hodnota, alespoň z pohledu čitelnosti. Kromě toho tyto formáty jsou rozšířené a oplývají určitou univerzálností, což lze do jisté míry chápat jako naplnění práva na technickou neutralitu.¹⁹

To, že takto definované výstupní datové formáty, by se neměly vztahovat jen k elektronickým systémům spisových služeb, ale mají díky své užité hodnotě být jakýmsi standardem pro elektronické veřejné listiny dokládá též aktuální ustanovení § 69a odst. 5 zákona č. 499/2004 Sb., které hovoří o tom, že ve výstupním datovém formátu mají vyhotovovat elektronické dokumenty všichni veřejnoprávní původci bez ohledu na to, v jakém informačním systému tato tvorba probíhá. Vymezení veřejnoprávních původců²⁰ je poněkud užší než orgán veřejné moci či orgán veřejné správy,

¹⁸ Konkrétní datové formáty jsou specifikovány v § 23 vyhlášky š. 259/2012 Sb. a dále diskutovány v publikaci KUNT, M., LECHNER, T. *Spisová služba. 3. aktualizované vyd.* Praha: Leges, 2022, s. 182-184.

¹⁹ Toto právo také svým způsobem definuje § 13 zákona č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, byť zde spíše ve smyslu zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

²⁰ Viz § 3 odst. 1 zákona č. 499/2004 Sb.

ale i tak se tím dostáváme do většího zobecnění, než je výstup z elektronického systému spisové služby, navíc je tato povinnost specifikována přímo zákonem a nikoliv jen vyhláškou, jak bylo uvedeno výše.

4.3 STROJOVĚ ČITELNÝ A OTEVŘENÝ DATOVÝ FORMÁT

Další přívlasky u datového formátu, které jsou použity v právních předpisech, jsou strojově čitelný formát a otevřený formát. Aktuální definice těchto přívlasků jsou součástí zákona č. 106/1999 Sb., o svobodném přístupu k informacím, který v § 3a stanoví, že:

- Strojově čitelným formátem se rozumí formát datového souboru s takovou strukturou, která umožňuje programovému vybavení snadno nalézt, rozpoznat a získat z tohoto datového souboru konkrétní informace, včetně jednotlivých údajů a jejich vnitřní struktury.
- Otevřeným formátem se rozumí formát datového souboru, který není závislý na konkrétním technickém a programovém vybavení a je zpřístupněn veřejnosti bez jakéhokoli omezení, které by znemožňovalo využití informací obsažených v datovém souboru.

Tyto definice jsou transpozicí směrnice Evropského parlamentu a Rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru.²¹ Na rozdíl od definice výstupních datových formátů, není v České republice žádnou prováděcí normou uveden ani přesný výčet požadovaných konkrétních datových formátů, ani kategorizace z pohledu charakteru obsahu. Odst. 35 preambule citované směrnice připouští, že strojově čitelné formáty mohou být otevřené nebo chráněné vlastnickým právem. A dále uvádí, že mohou být formálně normalizované, avšak vždy by měl být při navrhování technických řešení pro opakované použití dokumentů zohledněn evropský rámec pro řešení interoperability. To znamená, že členské státy by měly podporovat používání unijních nebo mezinárodně uznávaných otevřených, strojově čitelných formátů, pokud je to možné a vhodné. V České republice nebyl zatím přístup

²¹ Transpozice doslovně odpovídá překladu směrnice, kde jsou tyto definice v čl. 2 odst. 13) a 14).

prostřednictvím formální standardizace prováděcím předpisem zvolen, čímž se otevírá cesta pro různé diskuse o naplnění těchto definic.

V komentáři k zákonu č. 106/1999 Sb. publikovaném v roce 2023 Jitka Jelínková a Miloš Tuháček uvádějí následující příklady:²²

- Pro otevřené formáty jsou přípustné formáty TXT, PDF, RTF, RDF, XML, HTML/XHTML, JPEG nebo CVS, ale nikoli formát DOC.
- Pro strojově čitelné formáty, které umožňují další automatické zpracování datových souborů, jsou přípustné formáty RDF, CSV, XML a částečně XTML, ale nikoli formáty PDF, TXT, RTF.

Pokud tento příklad srovnáme s aktuálním stanoviskem Ministerstva vnitra pro kombinovanou podmínku otevřeného strojově čitelného formátu, byť pro účely zákona č. 35/2021 Sb., o Sbírce právních předpisů územních samosprávných celků a některých správních úřadů, ale odkazujícího se na stejnou definici, vidíme jasný posun. Ministerstvo vnitra ve spolupráci s Digitální a informační agenturou dochází k závěru, že nejvhodnějším formátem je ODT, přípustné je pak i použití formátu DOCX.²³

4.4 DATOVÉ FORMÁTY PŘENÁŠENÉ INFORMAČNÍM SYSTÉMEM DATOVÝCH SCHRÁNEK

Určitou samostatnou skupinou datových formátů jsou ty, které mohou být přeneseny prostřednictvím informačního systému datových schránek a které jsou specifikovány vyhláškou č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek.²⁴

²² JELÍNKOVÁ, Jitka, TUHÁČEK, Miloš. *Zákon o svobodném přístupu k informacím. Praktický komentář*. 3. vydání. Praha: Wolters Kluwer, 2023, s. 48-49.

²³ MINISTERSTVO VNITRA. Stanovisko Odboru veřejné správy, dozoru a kontroly Ministerstva vnitra zpracované ve spolupráci s Digitální a informační agenturou č. 2/2025: Podmínky otevřeného a strojově čitelného formátu v souvislosti s vyhledáváním právních předpisů ve Sbírce právních předpisů územních samosprávných celků a některých správních úřadů [online]. 2025. [cit. 26. 9 2025]. Dostupné z: <https://sbirkapp.gov.cz/blob/obsah/stanovisko-2-2025-final.pdf>.

²⁴ K pravidlům pro datové schránky viz MATES, Pavel, SMEJKAL, Vladimír. *E-Government v České republice: Právní a technologické aspekty*. 2., podstatně přepracované a rozšířené vydání. Praha: Leges, 2012, s. 200 a násl.

Taxativní určení těchto datových formátů zahrnuje jednak výstupní datové formáty a jednak obecné i specifické potřeby komunikace přes datové schránky např. při budování základních registrů, zejména RUIAN²⁵. Při tom je zohledněno kritérium kybernetické bezpečnosti, které se promítá jak do volby těchto formátů, tak do upřesňujících pravidel jejich dalších specifik, např. z hlediska velikosti anebo verze.

4.5 SUMARIZACE KATEGORIZACE DATOVÝCH FORMÁTŮ

Sumární přehled přívlasků datových formátů uváděných a používaných v různých právních předpisech je v následující tabulce, která je tak shrnutím celé výše rozebírané kategorizace datových formátů.

Pojmenování	Předpis, kde je definováno	Účel	Charakter definice
Kontejnerový	Národní standard pro elektronické systémy spisových služeb	Dva různé účely: čistě technický, např. komprimace dat, nebo funkční, např. spojení příloh s hlavním dokumentem do jednoho celku	Není taxativně určeno, navíc velmi různorodá skupina
Výstupní	Vyhláška č. 259/2012 Sb.	Dlouhodobá čitelnost, technologická nezávislost	Je taxativně určeno
Strojově čitelný	Zákon č. 106/1999 Sb.	Umožňuje opakované použití	Není taxativně určeno

²⁵ Viz FORMÁNEK Jiří. *Zavedení volebních okrsků do RUIAN* In: Konference ISSS 2013. [online] 2013. [cit. 2. 9. 2025]. Dostupné z: https://archiv.issc.cz/archiv/2013/download/prezentace/cuzk_formanek.pdf. A vyhláška č. 422/2010 Sb., kterou se mění vyhláška č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek.

		informací ve- řejného sektoru	
Otevřený	Zákon č. 106/1999 Sb.	Není chráněn vlastnickým právem a není závislý na konkrétním tech- nickém a programovém vybavení	Není taxativně ur- čeno
Otevřený strojově či- itelný	Zákon č. 106/1999 Sb.	Kombinuje vlastnosti otevřeného a strojově či- itelného formátu pro snadné opa- kované použití informací ve- řejného sektoru	Není taxativně ur- čeno
Přenositelné prostřednictvím datových schránek (ne- mají konkrétní poj- menování)	Vyhláška č. 194/2009 Sb.	Technické možnosti ISDS, kybernetická bezpečnost	Je taxativně ur- čeno

Tab. 1. Vlastnosti datových formátů definované v právních předpisech.

5. POŽADAVKY NA DATOVÉ FORMÁTY

V určitých procesech či právních úkonech jsou specifikovány formální požadavky na datové formáty. Některé z nich zde rozebereme, zejména podání, doručování, zveřejňování smluv a zveřejňování předpisů ve Sbírce

právních předpisů územních samosprávných celků a některých správních úřadů.

5.1 PODÁNÍ

Pravidla pro podání jsou určitým způsobem upřesněna ve většině procesních právních předpisů, které se z hlediska elektronizace vesměs omezují na povinné komunikační kanály jako jsou datové schránky nebo elektronická pošta (e-mail). Pouze ve výjimečných případech jsou uvedeny konkrétní formáty, které ale mají charakter datové věty, jako např. formulářové podání podle § 72 odst. 2. písm. c) zákona č. 280/2009 Sb., daňový řád, které je možné povést jen ve formátu a struktuře zveřejněné správcem daně.

Pokud tedy není v procesních předpisech specifikace datového formátu uvedena, měl by se v takových případech použít *lex specialis*, kterým pro příjem podání bude zákon č. 499/2004 Sb., který v § 64 odst. 1 stanoví, že určení původci zajistí příjem alespoň v datových formátech stanovených jako výstupní datové formáty nebo formáty dokumentů, které jsou výstupem z autorizované konverze dokumentů obsažených v datové zprávě. Skupina určených původců je ještě užší než skupina veřejnoprávních původců, což znamená, že zde zůstává skupina orgánů veřejné moci, např. obce vykonávající jen základní rozsah přenesené působnosti, školy a školská zařízení, pro které není žádné minimum akceptovaných datových formátů stanoveno. Pro veřejnoprávní původce pak platí, že pokud umožní příjem dokumentů v digitální podobě také v dalších datových formátech, musí to zveřejnit na úřední desce a internetových stránkách. Opět se tato povinnost vztahuje jen na veřejnoprávní původce, což je podmnožina orgánů veřejné moci, byť širší než určení původci.²⁶

Pokud je učiněno podání v jiném datovém formátu než je přípustné, je to považováno za vadu podání, což je např. explicitně uvedeno v § 74 daňového řádu. Vyhláška č. 259/2012 Sb. k tomu dále přidává, že je-li doručen dokument v jiném datovém formátu, než v jakém veřejnoprávní původ-

²⁶ K vymezení pojmů veřejnoprávní původce a určený původce viz např. KUNT, M., LECHNER, T. *Spisová služba. 3. aktualizované vyd.* Praha: Leges, 2022, s. 93-96.

ce přijímá dokumenty v digitální podobě, vyrozumí původce odesílatele o zjištěné vadě dokumentu a stanoví další postup pro její odstranění.²⁷ K uvedené problematice je také poměrně obsáhlá judikatura.

V Nálezu Ústavního soudu čj. I. ÚS 226/20²⁸ je uvedeno, že nezdaří-li se orgánu veřejné moci zobrazit či otevřít podání nebo přílohy účastníka řízení či jeho zástupce, učiněné v elektronické podobě formou datové zprávy doručené do datové schránky, je tento orgán povinen o takové skutečnosti danou osobu alespoň vyrozumět a poskytnout jí prostor pro nápravu tak, aby nebyla jen pro tento nedostatek krácena na svých právech. Znamená to, že volba datového formátu, který daný orgán veřejné moci nepřijímá, neanuluje samotný úkon, neboť je vadou podání, kterou lze v přiměřeně poskytnuté lhůtě napravit. Na datový formát tak není v procesu podání nahlíženo jako na podmínku nezbytnou k uskutečnění podání.

Obdobně vyznívají rozhodnutí Nejvyššího správního soudu ČJ 6 Afs 206/2020-37 ze dne 25. 11. 2020 a ČJ 8 Afs 93/2020 ze dne 21. ledna 2021, z nichž vyplývá, že za žalobu, byť blanketní, je za daných okolností nutno považovat samotnou datovou zprávu, nikoli až její přílohu v nepřijímaném formátu, která byla k datové zprávě připojena. V obou případech šlo o podání učiněné prostřednictvím datové schránky, kdy tedy datový formát datové zprávy je zcela přehlížen, neboť není ani výstupním datovým formátem, ani formátem, který byl zveřejněn příslušnými orgány jako přípustný formát pro podání, ale v tomto případě dostává přednost povinnost příjmu podání prostřednictvím datové schránky vyplývající ze zákona č. 300/2008 Sb. Tím spíše se ukazuje, jak je důležité rozlišovat datovou zprávu v širším a užším slova smyslu, kdy z pohledu podání se posuzuje pouze datový formát datové zprávy v užším slova smyslu, tedy datový formát dokumentu.

Na tuto diskusi lze navázat rozbořem aktuální problematiky datového formátu ZIP, který může být od 1. ledna 2023 také obsažen v datové

²⁷ Teprve, pokud se nepodaří veřejnoprávnímu původci tuto vadu doručeného dokumentu ve spolupráci s jeho odesílatelem odstranit, veřejnoprávní původce dokument dále nezpracovává.

²⁸ Publikováno ve Sbírce nálezů a usnesení Ústavního soudu České republiky Svazek 99 / ročník 2020 II. díl.

zprávě, kterou je informační systém datových schránek schopen dodat.²⁹ Pokud bychom z pohledu vyhlášky č. 194/2009 Sb. aplikovali doslovně, že jde o přípustný formát datové zprávy dodávané do datové schránky,³⁰ pak by mohl zahrnovat i datovou zprávu v širším slova smyslu, protože tím není vyloučena. Znamenalo by to, že bude-li v datové zprávě přípustný formát ZIP podle pravidel citované vyhlášky, který je beze sporu kontejnerem, pak by se z hlediska posuzování přípustnosti pro podání mělo aplikovat až ověření jeho obsahu. Na druhou stranu se domnívám, že nelze automaticky aplikovat rekurzivní přístup, protože i další popisy včetně vlastní definice podmínek pro přístupnost formátu ZIP jej vylučují. Praxe je v tomto ohledu jednoznačně roztržštěná a nezbývá než případně čekat na vhodný judikát.

Z pohledu osob, které činí podání je asi největším problémem ne-jednotnost přípustných datových formátů u různých orgánů veřejné moci. Sice existuje určitý společný základ, nicméně povinnost jeho akceptace je omezena jen na určené původce, ale v ostatních případech (jiných než určených původců a dalších datových formátů) je třeba vždy vyhledat příslušné informace na webových stránkách konkrétních orgánů veřejné moci. Řešením by jednoznačně byla novelizace zákona č. 300/2008 Sb., která by umožnila rozšířit informace evidované o datové schránce orgánu veřejné moci a seznam přijímaných datových formátů, který by zahrnoval společný základ zejména v podobě výstupních datových formátů nebo jiné vhodné množiny a dále nastavení dalších přípustných datových formátů.³¹ Alespoň v případě podání prostřednictvím datové schránky by podatel získal potřebnou informaci dopředu a nebylo by třeba řešit případné vady podání v podobě nevhodně zvoleného datového formátu.

²⁹ Příloha č. 3 k vyhlášce č. 194/2009 Sb. k tomu v bodě V. dodává, že formát ZIP je přípustným datovým formátem pokud: a) obsah datové zprávy není zašifrovaný, b) datovou zprávu tvoří alespoň jeden soubor ve formátu, který by bylo možné samostatně vložit do datové zprávy, c) datovou zprávu tvoří soubor v jiném formátu než ve formátu, který by bylo možné samostatně vložit do datové zprávy, d) datovou zprávu tvoří nejvýše 1 000 souborů a adresářů, e) maximální úroveň vnoření adresářů do sebe činí 4 a f) maximální velikost dekomprimovaného obsahu činí 3 GB.

³⁰ Viz § 4 vyhlášky č. 194/2009 Sb.

³¹ Obdobný návrh, ale z hlediska velikosti přijímané datové zprávy, zazněl v diskusích na konferenci ISSS 2023, ale nedočkal se dosud ztvárnění do podoby legislativního návrhu novely citovaného zákona č. 300/2008 Sb.

5.2 DORUČOVÁNÍ

Stejně jako pro podání, tak ani pro doručování se procesní předpisy nezabývají technickou stránkou obsahu v podobě datového formátu doručovaného elektronického dokumentu. I zde je tedy třeba použít *lex specialis* v podobě zákona č. 499/2004 Sb., který v § 69a odst. 5 stanoví, že vyhotovuje-li veřejnoprávní původce v informačním systému dokument v digitální podobě obsahující text, musí dokument opatřit strojově čitelným textem a metadaty³² ve strojově čitelném formátu odpovídajícími obsahu dokumentu ve výstupním datovém formátu, což tedy znamená, že vyhotovovaný elektronický dokument musí být ve výstupním datovém formátu, pokud obsahuje text, a to bez ohledu na to, v jakém informačním systému dokument vzniká. Prováděcí vyhláška k tomuto zákonu stanoví povinnost použití výstupního datového formátu, pokud dokument vzniká ve spisové službě. Z toho vyplývá, že pokud elektronický dokument vzniká v jiném systému, než je elektronický systém spisové služby, a zároveň neobsahuje text, nejsou pro něj nyní stanovena žádná formátová pravidla.

V této souvislosti bych rád zmínil vlastní analýzu využívání výstupních datových formátů ve veřejné správě a dodržování formátových pravidel v období od ledna 2017 do března 2023, ze které vyplynulo, že na začátku analyzovaného období bylo ve výstupních formátech pouze 20 % elektronických dokumentů odesílaných orgány veřejné moci prostřednictvím informačního systému datových schránek, přičemž do roku 2023 tento podíl velmi zvolna stoupal až na necelých 60 % na konci analyzovaného období.³³ Jednoznačně to ukazuje na nedodržování formátových pravidel při doručování, jehož příčinu lze spatřovat zejména v složitých podmínkách výše uvedených pravidel ještě komplikovaných střetem s otevřenými a strojově čitelnými datovými formáty, jejichž použití zase požaduje § 13 zákona č. 12/2020 Sb. pro výstupy digitálních služeb.

³² Schéma pro strojově čitelnou vrstvu zveřejňuje podle § 69a odst. 7 zákona č. 499/2004 Sb. Digitální a informační agentura na svých internetových stránkách.

³³ LECHNER, Tomáš. Development of the Quality of Electronic Records within Public Administration. In: VAŇKOVÁ, Ivana (ed.). Proceedings of the 15th International Scientific Conference Public Economics and Administration 2023 [online]. Ostrava, 05.09.2023. Ostrava: VSB – Technical University of Ostrava, 2023, s. 189–198.

Základní komplikací je účel zmíněných definic datových formátů. Zatím co výstupní datové formáty jsou odvozovány z analýz udržitelnosti dlouhodobé čitelnosti,³⁴ tak otevřené ani strojově čitelné datové formáty toto hledisko nezohledňují. Z právního pohledu je jednoznačně důležitější to, zda dokument zůstane čitelný a důvěryhodný, což znamená zachování jeho důkazní hodnoty, než zda lze jeho obsah technicky zpracovat v rámci opakovaného použití informací veřejného sektoru, jak se o něm vyjadřuje směrnice Evropského parlamentu a Rady (EU) 2019/1024.

Navíc vyhláška č. 259/2012 Sb. připouští, aby veřejnoprávní původce použil pro výstup z elektronického systému spisové služby současně také jiný datový formát. V praxi to ale znamená, že jsou vlastně odeslány dvě různé podoby téhož. Z pohledu spisové služby se jedná o dva stejnopisy dokumentu, u nichž musí být zachován shodný obsah a liší se právě jen a pouze použitým datovým formátem. Nicméně i to lze vnímat jako komplikaci jak na straně odesílatele, tedy orgánu veřejné moci, který musí vytvářet dvě ztvárnění téhož, tak na straně příjemce, který musí rozpoznat, že se jedná o dvě varianty téhož obsahu, neboť současná struktura datové zprávy přenášené informačním systémem datových schránek neumožňuje uvedený vztah vyjádřit. V praxi se tak lze s tímto postupem setkat jen velmi výjimečně.

Z pohledu judikatury se domnívám, že zatím nebyl řešen případ, kdy použití nevhodného datového formátu pro doručovaný elektronický dokument by bylo zjevnou příčinou škody, aby bylo možné aplikovat pravidla pro nesprávný úřední postup podle zákona č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád).

5.3 ZVEŘEJŇOVÁNÍ SMLUV

Zákon č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru

³⁴ Viz též UK NATIONAL ARCHIVES. The technical registry PRONOM [online] [cit. 3. 6. 2025]. Dostupné z: <https://www.nationalarchives.gov.uk/PRONOM/>

smluv), stanoví uveřejnění smlouvy jako nezbytnou podmínku platnosti vybraných typů smluv,³⁵ a to tak, že nebyla-li smlouva, na niž se vztahuje povinnost uveřejnění prostřednictvím registru smluv, uveřejněna prostřednictvím registru smluv ani do tří měsíců ode dne, kdy byla uzavřena, platí, že je zrušena od počátku.³⁶

Podle § 5 odst. 1 citovaného zákona dále platí, že uveřejněním smlouvy prostřednictvím registru smluv se rozumí vložení elektronického obrazu textového obsahu smlouvy v otevřeném a strojově čitelném formátu a rovněž potřebných metadat. Dodržení otevřeného a strojově čitelného formátu je tedy v tomto případě nezbytnou podmínkou naplnění dikce zákona v povinnosti uveřejnění smlouvy. O to více je překvapující, že na rozdíl od výstupních datových formátů, které jsou taxativně uvedeny v prováděcí vyhlášce, nejsou otevřené a strojově čitelné datové formáty předpisem obdobného charakteru upřesněny. V praxi se tak vychází pouze z definic uvedených v zákoně č. 106/1999 Sb.³⁷

Vilém Podešva a kol. komentují, že pro naplnění podmínky otevřeného a strojově čitelného datového formátu musí být smlouva „*uveřejněna ve formátu umožňujícím fulltextové vyhledávání v celém jejím textu s tím, že bude možné rozpoznat vnitřní strukturu textu, např. určit, jaký obsah má určitá buňka tabulky, co je nadpis kapitoly, co je poznámka pod čarou atd.*“³⁸ V citovaném komentáři k zákonu se dále uvádí, že novelizačním zákonem č. 177/2019 Sb. bylo postaveno najisto, že formát PDF (a tím ani výstupní datový formát PDF/A) není otevřeným a strojově čitelným formátem, nýbrž otevřeným formátem umožňujícím úplné strojové zpracování textového obsahu právě proto, že není možné jednoznačně rozpoznat jeho vnitřní strukturu.³⁹

³⁵ K povinnosti, které smlouvy musí být takto uveřejněny, viz PODEŠVA, Vilém a kol. *Zákon o zadávání veřejných zakázek. Zákon o registru smluv*. Komentář. 2. vydání. Praha: Wolters Kluwer, 2023, s. 1397-1407.

³⁶ Viz § 7 odst. 1 zákona č. 340/2015 Sb.

³⁷ Viz kapitolu „*Strojově čitelný a otevřený datový formát*“.

³⁸ PODEŠVA, Vilém a kol. *Zákon o zadávání veřejných zakázek. Zákon o registru smluv*. Komentář. 2. vydání. Praha: Wolters Kluwer, 2023, s. 1397.

³⁹ *Ibid.*

Tím se vytváří střet mezi požadavky na dlouhodobou čitelnost, které upřednostňuje legislativa týkající se spisové služby a archivnictví, s požadavky na strojové zpracování. Určitým východiskem by mohlo být ustanovení § 69a odst. 5 zákona č. 499/2004 Sb., které zavádí tzv. „*strojově čitelnou vrstvu*“. Kdyby byla tato povinnost vytváření strojově čitelné vrstvy v elektronických dokumentech doprovázena zveřejněním příslušného schématu popisných dat Digitální a informační agenturou podle § 69a odst. 7 citovaného zákona pro dokumenty obsahující smlouvu, byl by tím, dle mého názoru, naplněn požadavek na strukturu, která umožňuje programovému vybavení snadno nalézt, rozpoznat a získat z tohoto datového souboru konkrétní informace, včetně jednotlivých údajů a jejich vnitřní struktury.⁴⁰ Avšak tento přístup by musel být vhodně koordinován mezi předpisy, které se týkají opakovaného použití informací veřejného sektoru, a pravidly, která jsou motivována dlouhodobou čitelností.

V souvislosti s tím si můžeme položit otázku, zda je skutečně nezbytné, aby text smlouvy zveřejněné v registru byl v podobě, která umožňuje programovému vybavení snadno nalézt, rozpoznat a získat z tohoto datového souboru konkrétní informace, aniž je garantována úspěšnost tohoto rozpoznání, a zda by naopak nemělo být toto zveřejnění doprovázeno adekvátní sadou popisných dat v souladu s principy otevřených dat vtělenými do zákona č. 106/1999 Sb.⁴¹ Nicméně stěžejní je fakt, že v případě zveřejňování smluv je volba správného datového formátu nezbytnou podmínkou provedení tohoto úkonu a následné platnosti smlouvy, aniž je tato volba usnadněna taxativním uvedením přípustných datových formátů v prováděcím předpisu, čímž se rozhodně snižuje právní jistota pro tento úkon.

⁴⁰ Viz § 3a odst. 1 zákona č. 106/1999 Sb.

⁴¹ Podle § 8a odst. 5 zákona č. 106/1999 Sb. se otevřenými daty rozumí informace zveřejňované způsobem umožňujícím dálkový přístup v otevřeném a strojově čitelném formátu, jejichž způsob ani účel následného využití není povinným subjektem, který je zveřejňuje, omezen a které jsou evidovány v národním katalogu otevřených dat. Z této definice lze vyzdvihnout zejména požadavek na neomezené využití.

5.4 SBÍRKA PRÁVNÍCH PŘEDPISŮ ÚZEMNÍCH SAMOSPRÁVNÝCH CELKŮ

Obdobné přístupy pro zveřejňování, jaké byly rozebrány pro některé typy smluv, jsou užity v zákoně č. 35/2021 Sb., o Sbírce právních předpisů územních samosprávných celků a některých správních úřadů. Tento zákon ukládá povinnost územním samosprávným celkům a správním úřadům, které vydaly právní předpis, zasílat text právních předpisů do této Sbírky v otevřeném a strojově čitelném formátu. I zde je uveřejnění podmínkou platnosti předpisu, obdobně jako tomu bylo u smluv, a i zde platí tedy stejné závěry, jaké byly učiněny v předchozí kapitole.

Ministerstvo vnitra ve spolupráci s Digitální a informační agenturou vytvořilo rozbor pro podmínky otevřeného a strojově čitelného formátu v souvislosti s vyhlášováním právních předpisů ve Sbírce právních předpisů územních samosprávných celků a některých správních úřadů, ve kterém se přiklání k tomu, že nejvhodnějším formátem pro uveřejnění je ODT, přípustné je pak i použití formátu DOCX.⁴² Nicméně ani jeden z těchto formátů nespadá do vymezené skupiny výstupních datových formátů, čímž je střet povinností plynoucí ze zákona č. 499/2004 Sb. a vyhlášky č. 259/2012 Sb. s povinnostmi použití otevřených strojově čitelných datových formátů plně vyhrocen.

Z pohledu uvedených rozborů se klade pro zveřejnění předpisů ve Sbírce právních předpisů územních samosprávných celků a některých správních úřadů větší důraz na strojové zpracování, než na přístup běžných adresátů práva, kteří ale jednoznačně mají mít možnost se plně s platnými předpisy seznámit. Domnívám se, že toto jednostranné upřednostnění technických přístupů před přístupem adresátů těchto právních předpisů není správné.

⁴² MINISTERSTVO VNITRA. Stanovisko Odboru veřejné správy, dozoru a kontroly Ministerstva vnitra zpracované ve spolupráci s Digitální a informační agenturou č. 2/2025: Podmínky otevřeného a strojově čitelného formátu v souvislosti s vyhlášováním právních předpisů ve Sbírce právních předpisů územních samosprávných celků a některých správních úřadů [online]. 2025. [cit. 26. 9 2025]. Dostupné z: <https://sbirkapp.gov.cz/blob/obsah/stanovisko-2-2025-final.pdf>.

5.5 SHRNUÍ A DISKUSE PODMÍNEK NA DATOVÉ FORMÁTY

Z provedeného rozboru jasně plyne, že v případech úkonů, kdy volba nevhodného datového formátu může být řešena vhodnými opravnými prostředky, jsou tyto formáty vesměs taxativně definovány a jedinými problémem může být dostupnost těchto informací roztržštěná do webových stránek jednotlivých orgánů veřejné moci. Naopak v případech, kdy volba nevhodného datového formátu znamená striktní nenaplnění nezbytných podmínek úkonu a kdy nejsou stanoveny žádné vhodné a jednoduché opravné prostředky, jsou tyto formáty pouze obecně popsány a výklad uvedených popisů není jednoznačný. Ukazuje to, že důležitost datového formátu jako formálního atributu elektronických dokumentů není dosud vhodně doceněna a přístup k jeho specifikování i aplikování je roztržštěný.

Důvodem pro uvedenou roztržštěnost je jistě také různý účel příslušných ustanovení. Z právního pohledu si dovoluji tvrdit, že zachování dlouhodobé čitelnosti a důvěryhodnosti pomocí elektronických zabezpečovacích prvků, jako je elektronický podpis, elektronická značka a elektronické časové razítko⁴³ je důležitější než strojová čitelnost a opakované automatické zpracování. Nicméně správné by asi bylo hledat cestu sjednocení uvedených požadavků, které by naplnilo jak zachování důkazní hodnoty a čitelnosti, tak otevřenosti a strojové čitelnosti, která má pozitivní vliv na automatizaci a efektivitu digitalizovaných procesů.⁴⁴

Když byla v roce 2009 zavedena autorizovaná konverze dokumentů prostřednictvím aplikace CzechPOINT,⁴⁵ znamenalo to mimo jiné zvýšení užité hodnoty elektronických dokumentů, které tím mohou být v oprávněných případech důvěryhodně konvertovány do listinné podoby, a naopak zvýšení možností provádění úkonů v elektronické podobě, pro které mohou být listinné podklady zase konvertovány do elektronické podoby. Podmínky

⁴³ K těmto atributům elektronických dokumentů viz např. POLČÁK, Radim a kol. *Právo informačních technologií*. 2. vyd. Praha: Wolters Kluwer, 2024, s. 493 a násled.

⁴⁴ Obecně k efektivitě digitalizace ve veřejné správě viz např. ŠPAČEK, D. *eGovernment – cíle, trendy a přístupy k jeho hodnocení*. Praha: C. H. Beck, 2012.

⁴⁵ Blíže k této konverzi viz např. MATES, Pavel, SMEJKAL, Vladimír. *E-Government v České republice: Právní a technologické aspekty*. 2., podstatně přepracované a rozšířené vydání. Praha: Leges, 2012, s. 227 a násled.

pro provádění autorizované konverze dokumentů jsou upřesněny vyhláškou č. 193/2009 Sb. V příloze č. 1 k této vyhlášce je uvedeno, že konvertovat je možné pouze elektronický dokument, který je v datovém formátu PDF (Portable Document Format) verze 1.3 a vyšší nebo PDF/A (Portable Document Format/Archive), což je právě výstupní datový formát a nikoliv podle aktuálních názorů otevřený strojově čitelný datový formát. Tento fakt podporuje prezentovaný názor, že zachování dlouhodobé čitelnosti a důvěryhodnosti je z právního pohledu důležitější, než strojová čitelnost a opakované automatické zpracování, protože výstupní datových formát PDF/A je nezbytným předpokladem možnosti autorizované konverze dokumentu.

5.6 ROZŠÍŘENÍ O DISKUSI ZMĚNY DATOVÉHO FORMÁTU

Datový formát jako způsob kódování komponenty je danou vlastností elektronického dokumentu, kterou nelze jednoduše změnit. Jediný důvěryhodný způsob změny datového formátu, jaký je v současné době popsán v právních předpisech, může být prováděn pouze orgány veřejné moci pro jejich vnitřní potřebu, tedy z moci úřední.

Proces důvěryhodné změny datového formátu je popsán v § 69a zákona č. 499/2004 Sb. Pravidla jsou inspirována autorizovanou konverzí dokumentů, nicméně na rozdíl od autorizované konverze zde neexistují žádná vstupní ani výstupní formátová omezení. Je pouze stanoveno, že tento postup mohou provádět určení původci, a to způsobem zaručujícím věrohodnost původu dokumentu, neporušitelnost obsahu, čitelnost dokumentu a bezpečnost procesu změny datového formátu.⁴⁶

Znamená to, že jak soukromoprávní subjekty, tak další orgány veřejné moci, kteří nejsou určenými původci, nemohou změnu datového formátu provádět takovým způsobem, který by zachoval důkazní hodnotu a zároveň byl popsán odpovídajícím předpisem, o který by se tento postup mohl opřít. Tím více se ukazuje, jak závažné dopady může mít nesprávná volba datového formátu dokumentu při jeho tvorbě.

⁴⁶ Viz § 69a odst. 1 zákona č. 499/2004 Sb.

6. KVALIFIKOVANÁ SLUŽBA ELEKTRONICKÉ ARCHIVACE

Z pohledu dlouhodobé důvěryhodnosti elektronických dokumentů jsou důležité kvalifikované služby vytvářející důvěru pro elektronické transakce, které popisuje nařízení eIDAS.⁴⁷ Toto nařízení bylo novelizováno nařízením Evropského parlamentu a Rady (EU) 2024/1183 ze dne 11. dubna 2024, kterým se mění nařízení (EU) č. 910/2014, pokud jde o zřízení evropského rámce pro digitální identitu. Tímto předpisem byl rozšířen výčet služeb vytvářejících důvěru o kvalifikovanou službou elektronické archivace.

Pojmenování této služby bylo zvoleno poněkud nešťastně, protože evokuje souvislost s uchováním archiválií, ale ve skutečnosti se týká zachování důvěryhodnosti elektronických dat a elektronických dokumentů bez ohledu na to, zda a jakou mají archivní hodnotu. Kvalifikovanou službou elektronické archivace se dle čl. 2 odst. 48 a 49 novelizovaného nařízení eIDAS rozumí služba, kterou poskytuje kvalifikovaný poskytovatel služeb vytvářejících důvěru a která zajišťuje přijímání, uchovávání, zpřístupnění a výmaz elektronických dat a elektronických dokumentů s cílem zajistit jejich trvanlivost a čitelnost, jakož i zachovat jejich integritu, důvěrnost a důkaz původu po celou dobu uchovávání.

Tato služba musí splňovat požadavky stanovené v čl. 45j novelizovaného nařízení eIDAS, mezi kterými lze z pohledu zaměření tohoto příspěvku zdůraznit zajištění trvanlivosti a čitelnosti po zákonně či smluvně stanovenou dobu. Aby mohla být zajištěna zejména čitelnost, je třeba dbát správné volby datového formátu. Pokud by totiž ke zvolenému datovému formátu přestal existovat nástroj pro jeho dekodování a uživatelské zobrazení, ztratil by elektronický dokument svou čitelnost. Z pohledu analýz datových formátů realizovaných Národním archivem Spojeného království a publikovaných v databázi PRONOM,⁴⁸ by bylo vhodné vstupy této služby omezit na takové datové formáty, které vyhláška č. 259/2012 Sb. označuje jako výstupní datové formáty.

⁴⁷ Ke službám vytvářejícím důvěru pro elektronické transakce viz např. KMENT Vojtěch. *Elektronické právní jednání*. Praha: Wolters Kluwer, 2018, s. 107 a násl.

⁴⁸ UK NATIONAL ARCHIVES. *The technical registry PRONOM [online]* [cit. 3. 6. 2025]. Dostupné z: <https://www.nationalarchives.gov.uk/PRONOM/>

Nicméně podrobnosti pro kvalifikovanou službou elektronické archivace stanoví až prováděcí předpis, který do okamžiku přípravy tohoto příspěvku nebyl dosud přijat. Nicméně v návrhu zatím nejsou žádná specifická vymezení nebo doporučení pro datový formát takto uchovávaných elektronických dokumentů, což se zdá být přinejmenším zvláštní. Navržený předpis se pouze soustředí na způsob, jakým bude oprávněným spoléhajícím se stranám umožněno obdržet automatizovaným způsobem zprávu, která potvrzuje, že u elektronických dat a elektronických dokumentů získaných z kvalifikovaného elektronického archivu platí předpoklad integrity dat od začátku doby uchovávání do doby jejich zpřístupnění.

Na druhou stranu je poměrně optimistické, že zde taková služba může v budoucnu vzniknout a nabídnout kvalitní zajištění udržení důkazní hodnoty elektronických dokumentů, což jistě významně prospěje praktickému použití elektronických dokumentů.

7. SHRUTÍ A ZÁVĚREČNÁ DOPORUČENÍ

Z provedené analýzy při hledání odpovědí na položené výzkumné otázky vyplynulo, že datový formát je důležitý formální atribut elektronického dokumentu, který má vliv na možnosti provedení právních úkonů a v některých případech je dokonce jeho správná volba jejich nezbytným předpokladem. Ukazuje se, že přístup k definování datových formátů pro různé účely je roztržštěný a že účely aktuálních definic výstupního a otevřeného strojově čitelného datového formátu nejsou v současné době vzájemně kompatibilní.

V návaznosti na provedenou diskusi lze formulovat následující doporučení:

- Za prvé by bylo dobré realizovat změnu zákona č. 300/2008 Sb., která by otevřela cestu, aby orgány veřejné moci mohly ve své datové schránce nastavit pro podatele viditelné informace o přijímaných datových formátech. Tím by ten, kdo činí podání vůči tomuto orgánu, byl dopředu informován o přípustných formátech pro podání a předešlo by se tak potřebě následných náprav vad podání

spočívajících ve volbě nevhodného datového formátu, jak bylo diskutováno v kapitole „*Podání*“.

- Za druhé by bylo dobré formálně normalizovat otevřené a strojově čitelné datové formáty, aby se předešlo důsledkům nevhodně zvolených formátů, které mohou zapříčinit neplatnost smluv zveřejněných v registru smluv a neplatnost předpisů zveřejněných ve Sbírce právních předpisů územních samosprávných celků a některých správních úřadů, jak bylo diskutováno v kapitole „*Zveřejňování smluv*“.
- Za třetí by bylo dobré zkvalitnit tvorbu elektronických dokumentů orgány veřejné moci bez ohledu na informační systém, v němž tyto dokumenty vznikají, tím, že pravidla pro datový formát elektronických dokumentů budou definována bez složitých podmínek a s jasným účelem zachování důkazní hodnoty takto vznikajících elektronických dokumentů, jak bylo diskutováno v kapitole „*Doručování*“. Jako nejvhodnější se jeví umístit tato přesná pravidla do zákona č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, který adaptuje nařízení eIDAS právě v oblasti služeb vytvářejících důvěru.
- A konečně za čtvrté by bylo dobré hledat cesty, jak vyřešit rozpor mezi dlouhodobou čitelností a udržením důkazní hodnoty elektronických dokumentů na jedné straně a otevřeností a strojovou čitelností motivovanou opakovaným použitím informací veřejného sektoru na straně druhé, jak bylo diskutováno v kapitole „*Shrnutí a diskuse podmínek na datové formáty*“.

8. SEZNAM POUŽITÝCH ZDROJŮ

[1] CUBR, L. Dlouhodobá ochrana digitálních dokumentů. Praha: Národní knihovna

[2] České republiky, 2010. 154 s. ISBN: 978-80-7050-588-5.

[3] FORMÁNEK Jiří. *Zavedení volebních okrsků do RÚIAN* In: Konference ISSS 2013. [online] 2013. [cit. 2. 9. 2025]. Dostupné z: https://archiv.issc.cz/archiv/2013/download/prezentace/cuzk_formanek.pdf.

[4] JELÍNKOVÁ, Jitka, TUHÁČEK, Miloš. *Zákon o svobodném přístupu k informacím. Praktický komentář*. 3. vydání. Praha: Wolters Kluwer, 2023. 376 s. ISBN 978-80-7676-695-2.

- [5] KMENT Vojtěch. *Elektronické právní jednání*. Praha: Wolters Kluwer, 2018. 460 s. ISBN 978-80-7552-815-5.
- [6] KUNT, M., LECHNER, T. *Spisová služba. 3. aktualizované vyd.* Praha: Leges, 2022. 412 s. Praktik. ISBN 978-80-7502-616-3.
- [7] LECHNER, Tomáš. Development of the Quality of Electronic Records within Public Administration. In: VAŇKOVÁ, Ivana (ed.). *Proceedings of the 15th International Scientific Conference Public Economics and Administration 2023* [online]. Ostrava, 05.09.2023. Ostrava: VSB – Technical University of Ostrava, 2023, s. 189–198. eISBN 978-80-248-4698-9. DOI: 10.31490/9788024846989. Dostupné z: <https://dokumenty.vsb.cz/docs/files/cs/63524dd3-8e13-4f31-916a-02dfbd4e0f91?prevPage=true>.
- [8] LECHNER, Tomáš. Právní pohled na kontejnerové datové formáty. In: PÁNKOVÁ, K. (ed.). *Sborník 27. ročníku konference ISSS* [online]. Hradec Králové, 12.05.2025 – 13.05.2025. Praha: Triada, 2025, s. 39–45. eISBN 978-80-907164-7-6. Dostupné z: https://issc.cz/wp-content/uploads/2025/05/ISSS2025_sbornik.pdf.
- [9] MATES, Pavel, SMEJKAL, Vladimír. *E-Government v České republice: Právní a technologické aspekty. 2., podstatně přepracované a rozšířené vydání*. Praha: Leges, 2012, 464 s. ISBN 978-80-87576-36-6.
- [10] MINISTERSTVO VNITRA. *Národní standard pro elektronické systémy spisové služby. 6. verze*. Věstník Ministerstva vnitra, částka 85/2024.
- [11] MINISTERSTVO VNITRA. Stanovisko Odboru veřejné správy, dozoru a kontroly Ministerstva vnitra zpracované ve spolupráci s Digitální a informační agenturou č. 2/2025: Podmínky otevřeného a strojově čitelného formátu v souvislosti s vyhledáváním právních předpisů ve Sbírce právních předpisů územních samosprávných celků a některých správních úřadů [online]. 2025. [cit. 26. 9. 2025]. Dostupné z: <https://sbirkapp.gov.cz/blob/obsah/stanovisko-2-2025-final.pdf>.
- [12] NEJVYŠŠÍ SOUD. Stanovisko Nejvyššího soudu k podáním činěným v elektronické podobě a k doručování elektronicky vyhotovených písemností soudem, prováděnému prostřednictvím veřejné datové sítě (Plsn 1/2015) publikovaného pod č. 1/2017 ve Sbírce soudních rozhodnutí a stanovisek
- [13] PODEŠVA, Vilém a kol. *Zákon o zadávání veřejných zakázek. Zákon o registru smluv. Komentář. 2. vydání*. Praha: Wolters Kluwer, 2023. s. 1488. ISBN 978-80-7676-554-2.
- [14] POLČÁK, Radim a kol. *Právo informačních technologií. 2. vyd.* Praha : Wolters Kluwer, 2024. 955 s. ISBN 978-80-286-0059-4.
- [15] ŠLAPÁK, O. Data, informace, znalosti. *E-LOGOS. Electronic journal for philosophy*. [online] 2003, roč. 10, č. 1, [cit. 26. 9. 2025], s.1-6. Dostupné z: <https://e-logos.vse.cz/pdfs/elg/2003/01/11.pdf>
- [16] ŠPAČEK, D. *eGovernment – cíle, trendy a přístupy k jeho hodnocení*. Praha: C. H.
- [17] Beck, 2012, 258 s. ISBN 978-80-7400-261-8.

[18] UK NATIONAL ARCHIVES. *The technical registry PRONOM [online]* [cit. 3. 6. 2025].
Dostupné z: <https://www.nationalarchives.gov.uk/PRONOM/>

*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>).*

<https://doi.org/10.5817/RPT2025-2-3>

TRACING POHLEDEM AUTORSKÉHO PRÁVA¹

ADAM ŽVÁČEK²

ABSTRAKT

Článek se zabývá analýzou tracingu, tj. netradiční odvozená tvorba, a dílem vytvořeným pomocí tracingu, načež se snaží o jejich pragmatickou subsumpci, spolu s jejich případnými zásahy do práv původního autora, do autorského zákona, a to na základě využití logické falzifikace a doktríny autorskoprávní individuality. Dále jsou analyzovány aplikovatelné výjimky a omezení autorského práva pro tracing, spolu s návrhem řešení, jak případně vyrovnat vzniklou nerovnováhu základních práv původního autora a uživatele tracingu.

KLÍČOVÁ SLOVA

Tracing; odvozené dílo; výtvarné dílo; autorskoprávní individualita; obecný fond; výjimky a omezení

ABSTRACT

The article analyses tracing, i.e. non-traditional derivative creation, and works created using tracing, while attempting to pragmatically subsume them, together with their possible infringements of the rights of the original author, into Czech Copyright Code, based on the use of logical falsification and the doctrine of

¹ Článek vychází a je obsahově založen na diplomové práci autora *Autorskoprávní aspekty tracingu*, která byla obhájena v roce 2025 na Právnické fakultě Masarykovy univerzity. Oproti diplomové práci byl pozměněn termín užívaný k označení osoby využívající tracing na „uživatele tracingu“, a to k lepšímu reflektování judikatury SDEU týkající se uživatelů v kontextu autorského práva.

² Mgr. Adam Žváček je absolvent Právnické fakulty Masarykovy univerzity. Kontaktní e-mail: 508863@mail.muni.cz

author's individuality. Furthermore, applicable exceptions and limitations to copyright law for tracing are analysed, together with a proposal of solution to balance the possible imbalance between the fundamental rights of the original author and the user of tracing.

KEY WORDS:

Tracing; Derivative Work; Artistic Work; Individuality of Author's Work; Public Domain; Exceptions and Limitations

1. ÚVOD

Přesunem z čistě analogové autorské či uživatelské tvorby na digitální, mnohdy odehrávající se přímo na internetu, musí autorské právo na mezinárodní i národní úrovni být flexibilně interpretováno, aby čelilo těmto výzvám, neboť původní autorskoprávní statuty již zcela nemusí reflektovat potřeby aktuální doby. Příkladem relativně nové a známé tvorby, která je ve svých aspektech netradiční a nejsou na ni tak přímo použitelné autorskoprávní normy, je například *appropriation art* nebo *sampling*.³

Tracing je jedním z těchto netradičních způsobů tvorby děl, který právě díky digitalizaci získává na popularitě, neboť přístup k potřebným technologiím je pro *prosumera* jednodušší, a tak je i jeho následné tvoření.⁴ Tracing avšak není pouze záležitost pro *prosumera*, ale i světově ekonomicky silný videoherní či komiksový průmysl, což dále poukazuje na důležitost vyřešení otázky oprávněnosti nebo protiprávnosti tracingu, který se stále pohybuje v „šedé zóně“ práva.⁵ Z povahy tracingu v digitálním prostředí a jeho následném využití pak vyplývá, že je jednoduché, aby došlo k mezinárodnímu přesahu (např. zásahem práv původního autora), a tak i v určitých případech k využití českého autorského práva ke klasifikaci tracingu.

Článek, vycházející z hlavních zjištění diplomové práce autora, se pragmaticky zaměřuje na poznání a subsumpci tracingu, díla vytvořeného po-

³ Oprávněnost *samplingu* na základě výjimek a omezení v podobě pastiše stále není zcela vyřešena, viz žádost o rozhodnutí o předběžné otázce ze dne 25. 9. 2023 ve věci C-590/23, Pelham II, o které by měl SDEU nejspíše již brzy, v roce 2025, rozhodnout.

⁴ Více o pojmu *prosumer* viz TOFFLER, Alvin. *The Third Wave*. New York: William Morrow & Company, Inc., 1980, s. 282.

mocí tracingu a tracingem zasažených autorských práv původního autora za pomoci deskripce do českého autorského zákona (dále jen „AutZ“), a to za užití relevantní judikatury, právních předpisů a odborné literatury.⁶ Článek dále analyzuje aplikaci výjimek a omezení autorského práva použitelných pro tracing, načež v tomto kontextu navrhuje právní úpravu k vybalancování základních práv autora a uživatele. Cílem článku je čtenáře obecně seznámit s tracingem a jeho pozicí v českém autorském právu, a také poukázat na případné problémy spojené s nedostatečnou či přímo neexistující regulací tohoto fenoménu netradičních způsobů tvorby děl.

Na závěr úvodu je nutné podotknout, že prezentovaná zjištění v tomto článku týkající se kvalifikace tracingu, a tak i možné následky navazující na klasifikaci, vycházejí z doktríny autorskoprávní individuality, jak o ní hovoří Koukal a Knap.⁷ V důsledku judikaturní praxe Soudního dvora Evropské unie (dále jen „SDEU“) totiž můžeme začít hovořit o snížení standardu (statistické) jedinečnosti na úroveň původnosti, a tak pojímat autorskoprávní individualitu jako „*vlastní duševní výtvor autora*“, což může pomoci i dílům s nižšími nároky na autorskoprávní individualitu k „přiznání“ autorskoprávní ochrany.⁸ Tato doktrína je pro účely kvalifikace doplněna o logickou falzifikaci pocházející z judikaturní praxe SDEU, o které Polčák hovoří, jakožto o činnosti soudů, které pro kvalifikaci díla musí nejdříve zkusit vyvrátit přítomnost pojmových znaků autorských děl v samotném dí-

⁵ Příkladem využití údajného tracingu v těchto průmyslech může být případ týkající se videohry *Fortnite* ze Spojených států amerických, viz *Hanagami v. Epic Games, Inc.*, 85 F.4th 931 (9th Cir. 2023). United States Court of Appeals, Ninth Circuit nebo případ týkající se *otome* ilustrací manga z Japonska, viz 東京地方裁判所民事第29部判決令和5年10月13日、令和2年(ワ)第25439号と令和3年(ワ)第1631号 [Rozsudek Tokijského okresního soudu (občanskoprávní oddělení 29) ze dne 13. 10. 2023, sp. zn. 2020(wa)25439 a sp. zn. 2021(wa)1631]. Analýza obou těchto rozhodnutí viz ŽVÁBEK, Adam. *Autorskoprávní aspekty tracingu*. Online, magisterská diplomová práce. Brno: Masarykova univerzita, Právnická fakulta. 2025, [cit. 10. 7. 2025] s. 72–86. Dostupné z: <https://is.muni.cz/th/r71x2/>.

⁶ Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů.

⁷ Více o autorskoprávní individualitě viz KOUKAL, Pavel. *Autorské právo, public domain a lidská práva*. 1. vydání. Brno: Masarykova univerzita, 2019, s. 440; KNAP, Karel. Užití autorského díla. In: KNAP, Karel (ed.) *Aktuální otázky práva autorského, práv průmyslových a práva soutěžního*. Praha: Univerzita Karlova, 1975, s. 42.

le, neboť do doby případného vyvrácení těchto znaků se předpokládá, že se jedná o autorské dílo.⁹

2. TRACING JAKO ČINNOST

Slovníková definice tracingu z *Cambridge Dictionary* uvádí, že se jedná o překreslení původního výkresu nebo vzoru přes tenký kus průhledného papíru, kterým vzniká kopie původního díla.¹⁰ Tato definice tak obsahuje analogový přístup a mimo jiné z ní vyplývá, že tracing je činnost, kterou osoba koná vědomě, tedy dopouští se úmyslného jednání.¹¹

Obecně se s rozvojem technologií objevují nové způsoby užití autorského díla, dokonce i nové druhy autorských děl.¹² Toto platilo pro minulé století s rozvojem televizí a fotografií, ale domnívám se, že pro současnost je tento fakt ještě citelnější s digitalizací a rozvojem počínaje internetem, konče umělou inteligencí. Fenomén tracingu je tak díky postupnému pokroku technologií možné sledovat i mimo zmíněnou analogovou definici, a to v digitálním prostředí, kdy je tenký kus průhledného papíru nahrazen například rastrovým grafickým editorem.¹³ Domnívám se, že důvod častější-

⁸ HUSOVEC, Martin. Judikátorná harmonizácia pojmu autorského diela v úijnom práve. *Bulletin slovenskej advokácie*. 2012, roč. 18, č. 12, s. 16–17. Ke stejnému závěru se po reko-difikaci slovenského autorského práva roku 2015 přiklání slovenská doktrína se svým vymezením pojmových znaků autorského díla, viz ADAMOVÁ, Zuzana a HAZUCHA, Branislav. § 3 Dielo. In: ADAMOVÁ, Zuzana a HAZUCHA, Branislav. *Autorský zákon: komentár*. 1. vydání. Bratislava: C. H. Beck SK, 2018, s. 32–34.

⁹ Více o logické falzifikaci viz POLČÁK, Radim. § 2 Autorské dílo. In: POLČÁK, Radim; KOUKAL, Pavel; LEŠKA, Rudolf; MYŠKA, Matěj; HRABÁNEK Jiří et al. *Autorský zákon: Praktický komentář s judikaturou*. Praha: Leges, 2020, s. 38–40.

¹⁰ Tracing. In: *Cambridge Dictionary*. [online]. [cit. 23. 10. 2024]. Dostupné z: <https://dictionary.cambridge.org/dictionary/english/tracing>

¹¹ Kvalifikace volní složky se stává relevantní zejména v kontextu porušení norem trestního práva při způsobení nikoli nepatrného neoprávněného zásahu na straně nositele autorských práv.

¹² KNAP. *Užití autorského díla*, s. 21. Také viz KNAP, Karel. Quo vadis současného autorského práva. In: KNAP, Karel (ed.) a KUNZ, Otto (ed.). *Aktuální otázky práva autorského a práv průmyslových*. Praha: Univerzita Karlova, 1986, s. 10.

¹³ Ostatně tento přístup je frekventovaně skloňován v japonském diskursu o tracingu, viz Explaining Illustration Tracing and Copyright Law Amidst the Frequent Plagiarism Controversies. In: *Monolith Law*. [online]. 2023. [cit. 23. 10. 2024]. Dostupné z: <https://monolith.law/en/internet/copy-plagiarize-tracing>

ho využívání digitálního přístupu k tracingu tkví ve zjednodušení vytvoření díla a lehkosti následného nakládání s dílem. Lze tedy uvažovat o této formě jako o virtualizaci analogového přístupu.



フルートレインで画像検索（個人様のブログから）



屋根の厚みと奥行きは変えてある
細かいディテールは省略
他は大体一致

Obr. 1 Ukázka dokazování tracingu na vlaku¹⁴

Levá fotografie je z osobního blogu uživatele. Pravá ilustrace je dílo vytvořené pomocí tracingu. Dole jsou oba obrázky uživatelem マスオ[masuo] přeloženy přes sebe k demonstraci tracingu.

¹⁴ マスオ. 【マサオ氏トレス疑惑】乗るしかない このピックアップに！ [MASUO. (Údajný tracing pana Masua) Musíme se svést na této velké vlně!]. In: *Pixiv*. [online]. 2012. [cit. 15. 11. 2024]. přeloženo pomocí DeepL. Dostupné z: <https://www.pixiv.net/en/artworks/26867576>

Pomyslné rozdělení přístupů k tracingu na dvě kategorie může napomoci s nasměrováním, do jakých práv původního autora může být případně zasazeno.¹⁵ Digitálním přístupem k tracingu tak může spíše dojít ke sdělování veřejnosti nežli rozšiřování díla, které může být dominantní u analogového přístupu. Avšak oba tyto případy se *apriori* vzájemně nevylučují, neboť záleží, jak bude s dílem vytvořeným pomocí tracingu dále nakládáno. Článek se ve svém zbytku zaměří zejména na dopady tracingu v digitálním prostředí.

V praxi se obvykle jedná o případy uměleckých děl, kdy je část autorova díla tracingem úmyslně převzata do díla nového osobou, která neměla a nemá od původního autora svolení k tracingu.¹⁶ Zároveň nedojde k uvedení jména nebo pseudonymu původního autora a nové dílo je vydáváno jako nová práce uživatele tracingu. Tato díla obvykle vznikají za dosažením přímého nebo nepřímého zisku a jsou často nahrávána na sociální sítě, kde je obsah možné zpeněžit, nebo jsou například rovnou prodávána jako potisk na tričko.¹⁷ Původní autor si v tuto chvíli není vědom, že ztrácí zisk a vzniká mu újma způsobená tracingem jeho díla. Mimo benefity v ekonomické sféře se tracing zpravidla dotýká i sociální sféry, kde je tak možné získat nové podporovatele či fanoušky a obecně získat na popularitě.

V poslední době se objevují případy, kdy původní autor využil svých sociálních sítí a označil osobu, která vytvořila dílo pomocí tracingu, za pachatele protiprávní činnosti, případně činnosti hluboce nemorální.¹⁸ Přesvědčení, které původní autor má o zásahu do jeho autorských práv se však ne-

¹⁵ Mimo kontext autorského práva mohou další dopady tracingu ležet i v odlišných právních odvětvích, jako například v soutěžním právu, právu k průmyslovému vlastnictví nebo právu na ochranu osobnosti.

¹⁶ Příkladem může být případ Hanamura Mai v. Juiga Satoru, viz rozsudek Tokijského okresního soudu (občanskoprávní oddělení 29) ze dne 13. 10. 2023, sp. zn. 2020(wa)25439 a sp. zn. 2021(wa)1631. Analýza případu viz ŽVÁČEK. *Autorskoprávní aspekty tracingu*, s. 78–83, 85–86.

¹⁷ *Explaining Illustration Tracing and Copyright Law Amidst the Frequent Plagiarism Controversies* [online].

¹⁸ トレバク指摘は要注意！知っておくべき著作権侵害の境界線 [Buďte opatrní, když obviňujete z plagiátorství! Hranice porušení autorských práv, které byste měli znát]. In: *Copyright Topics*. [online]. 2024. [cit. 23. 10. 2024]. přeloženo pomocí DeepL. Dostupné z: <https://copyright-topics.jp/topics/be-careful-when-pointing-out-trade-related-issues/>

musí shodovat s realitou věci, o které mohou rozhodovat pouze soudy. Údajnému uživateli tracingu může vzniknout škoda z titulu poškození dobrého jména nebo pomluvy.¹⁹ Veškeré záležitosti by měly být spíše komunikovány napřímo mezi stranami sporu bez přítomnosti veřejnosti, aby se původní autor nevystavoval situaci vzájemné žaloby.

Domnívám se, že základním problémem tracingu je fakt, že dochází k převzetí pouze vybraných prvků díla, kterými obvykle jsou obrysy, črty nebo tvary. Nové dílo v konečném důsledku obsahuje jak části získané tracingem, tak i části vlastní. Kvantita a kvalita převzatých prvků z původního díla je proto základním ukazatelem, zda bylo zasaženo do autorských práv autora původního díla, což musí být i *ad hoc* prokázáno soudy, neboť případ od případů se liší.²⁰ Je nutné podotknout, že nikoli tracing bude nakonec odhalen, neboť povahově se spíše jedná o činnost, se kterou není původní autor obeznámen.

Pokud opustíme tracing výtvarných děl (tracing *stricto sensu*), tak je možné aplikovat získané poznatky i na jiné druhy uměleckých děl (tracing *largo sensu*). Ačkoliv je to neobvyklé, tak se lze setkat i s případy, kdy dojde k tracingu jiného díla nežli díla výtvarného, a to například díla choreografického. Demonstrativním příkladem může být taneční video, kdy přichází v úvahu tracing choreografie po jednotlivých snímcích zachycených na hmotném nosiči, které se podobají tracingu jednotlivých ilustrací v řadě tvořících jeden celek.²¹ Výsledné dílo se na základě použité techniky neliší od obvyklého tracingu výtvarného díla. Tyto postupy jsou „tradičnímu“ tracingu velmi podobné, a proto se domnívám, že spadají do stejné kategorie (tracing) a bude tak s nimi nadále zacházeno.

¹⁹ *Buďte opatrní, když obviňujete z plagiátorství! Hranice porušení autorských práv, které byste měli znát* [online].

²⁰ イラストや画像のトレスは違法？ 企業が対策すべき著作権侵害 [Je tracing ilustrací a obrázků nezákonný? Porušování autorských práv, proti kterému by společnosti měly přijmout opatření]. In: *Verybest Law Offices Kagoshima*. [online]. 2022. [cit. 31. 10. 2024]. přeloženo pomocí DeepL. Dostupné z: https://kagoshima.vbest.jp/columns/general_corporate/g_ip/6774/

²¹ Příkladem může být případ Hanagami v. Epic Games, viz *Hanagami v. Epic Games, Inc.*, 85 F.4th 931 (9th Cir. 2023). United States Court of Appeals, Ninth Circuit. Analýza případu viz ŽVÁBEK. *Autorskoprávní aspekty tracingu*, s. 72–77, 84–85.



Obr. 2 Ukázka dokazování tracingu na emote²²

Obrázek je složen autorem článku ze snímku z citovaného videa. Polovina levé části vyobrazuje registrovanou choreografii od choreografa Kyla Hanagamiho. Druhá polovina levé části (modré pozadí) vyobrazuje emote z videohry Fortnite od společnosti Epic Games. Napravo je emote překreslen (bíle) a přeložen přes choreografii zachycenou na videu, demonstrující shodu pohybů. Jedná se o důkazní materiál tracingu předložený Hanagamim v případě Hanagami v. Epic Games.

²² HECHT, David. Fortnite Infringement of Kyle Hanagami Choreography. In: Youtube. [online]. 2022. [cit. 15. 11. 2024]. Dostupné z: https://www.youtube.com/watch?v=vXYDr9o_FJY

Kapitola se nadále bude zabývat porovnáváním tracingu vůči činnostem, které se na první pohled mohou fakticky nebo povahově tracingu podobat.

2.1 VYMEZENÍ VŮČI TRADIČNÍM ČINNOSTEM

Nejdříve budou analyzovány vybrané činnosti autorskému právu již dlouho známe, které budou následně porovnány s tracingem k zjištění, zdali a jak moc si jsou podobné nebo jestli se případně nejedná o činnost totožnou. Vybrané činnosti, kterými jsou kopírování, spojení, změna a inspirace nebo jejich výsledky, se totiž mohou tracingu podobat, a proto je podstatné zjistit, zdali tracing nemůže být pouze jejich digitalizovaná verze ve sféře uměleckých děl.

2.1.1 KOPÍROVÁNÍ

Mechanickým kopírováním nebo přesným manuálním kopírováním dáváme vzniknout úplné reprodukci původního díla, kterým inherentně vzniká rozmnoženina, v tomto případě rozmnoženina identická.²³ Na druhou stranu, tracingem jednoznačně identická kopie nemůže nikdy vzniknout, neboť jsou z díla původního převzaty jen vybrané prvky. Protiargument, že bychom pohlíželi na převzatý vybraný prvek jako samostatný celek, může být validní pouze, kdyby tento „stavební blok“ autorského díla požíval stejné ochrany jako dílo celé.²⁴

Avšak všechny rozmnoženiny nejsou 1 : 1 totožné, a tak je možné uvažovat o rozmnoženinách neidentických, které již zasahují do problematiky odvozené tvorby.²⁵ Napodobenina (neidentická rozmnoženina) v sobě obsahuje „autorský otisk“ napodobitele, kterým se začíná blížit faktickému stavu tracingu. Můžeme tak mluvit o „nedokonalé kopii“, ale i zde se domnívám, že podstatou rozmnožení je stále snaha zachovat vše z původního

²³ TELEC, Ivo a TŮMA, Pavel. § 13 Rozmnožování. In: TELEC, Ivo a TŮMA, Pavel. *Autorský zákon. Komentář*. 2. vydání. Praha: C. H. Beck CZ, 2019, s. 180.

²⁴ Obdobně rozsudek SDEU (čtvrtého senátu) ze dne 16. 7. 2009 ve věci C-5/08, Infopaq International, bod 45–47 nebo rozsudek Nejvyššího soudu ze dne 24. 3. 2021, sp. zn. 27 Cdo 2023/2019, bod 31, 33.

²⁵ TELEC, Ivo a TŮMA, Pavel. § 30 Volná užití. In: TELEC, Ivo a TŮMA, Pavel. *Autorský zákon. Komentář*. 2. vydání. Praha: C. H. Beck CZ, 2019, s. 390.

díla, tedy všechny smysly vnímatelné znaky.²⁶ Oproti tomu platí pro napodobeninu argument stejný jako pro rozmnožování identické. Tracingem jsou převzaty pouze vybrané části původního díla a nedokonalostí v procesu vytvoření napodobeniny představené zásahem člověka se zmíněným typům rozmnoženin blíží tracing pouze v některých pojmových znacích.

Dosud bylo argumentováno proti úplným rozmnoženinám (kopiím), ale rozmnoženinou je i její neúplná varianta. Poměrně vzdálenou od exaktní kopie, ale stále relevantní v kontextu rozmnožování díla, je neúplná napodobenina. Setkáváme se s ní v případech, kdy je převzata pouze vybraná část původního díla a lidský faktor v procesu způsobuje její nedokonalost. Může se tak stát pouze v případě, pokud je samotná vybraná část původního díla schopna naplnit pojmové znaky autorského díla.²⁷ Rozdílným vůči tracingu je ale fakt, že neúplná napodobenina postrádá přidanou hodnotu ve formě zakomponování vybrané části původního díla jako jedné části v díle nově vzniklém.

To ovšem neznamená, že se nemůže neúplná napodobenina objevit v průběhu tracingu. Dokonce se domnívám, že rozmnoženina (neúplná napodobenina) musí vzniknout v průběhu tracingu vždy, pokud se přebírají prvky s autorskoprávní individualitou, avšak sama o sobě není konečným výsledkem (novým dílem).²⁸ Nelze tedy říct, že se tracing rovná rozmnožování, avšak rozmnožování je inherentní součástí tracingu.

2.1.2 SPOJENÍ

Doposud je uváděno, že tracingem jsou v sobě *de facto* sloučeny část původního díla a část vlastní od uživatele tracingu. Spojená díla, jako součást děl hromadných, se obecně také pojí s původně na sobě nezávislými díly, které mohou společně vytvořit jeden celek, který má spojeným užitím širší

²⁶ KOUKAL, Pavel. § 13 Rozmnožování. In: POLČÁK, Radim; KOUKAL, Pavel; LEŠKA, Rudolf; MYŠKA, Matěj; HRABÁNEK Jiří et al. *Autorský zákon: Praktický komentář s judikaturou*. Praha: Leges, 2020, s. 118.

²⁷ TELEČ; TŮMA. § 13 *Rozmnožování*, s. 181.

²⁸ Z povahy tracingu, kdy si jeho uživatel nevědomě vybírá prvky z původního díla, totiž dojde nejspíše k převzetí jak prvků s autorskoprávní individualitou, tak i prvků obecného fondu. Naopak v nepravděpodobném případě převzetí pouze prvků bez autorskoprávní individuality, tedy využití prvků obecného fondu, nemůže dojít k rozmnožování.

možnost využití nebo vyšší ekonomický potenciál.²⁹ Například videohra na fyzickém nosiči, která ve svém balení obsahuje mapu videoherního světa.

Výsledek spojení nikdy nemůže být nové dílo, ani nevzniká nové autorské právo ke spojeným dílům, neboť zde chybí pojmové znaky uspořádání či zpracování, zejména pak tvůrčí činnost.³⁰ Z toho vyplývá, že díla i autorská práva stojí vedle sebe a na sobě nezávisle. V opačném případě bychom nemohli hovořit o spojených dílech, ale o vzniku souborného nebo odvozeného díla.

Tracingem ale vzniká dílo nové, které v sobě nese prvky obou, namísto spojení dvou na sobě nezávislých děl z jednotlivých částí tvořících jeden celek. Kdybychom došli k závěru, že tracing je spojení, tak se domnívám, že bychom snížili právní ochranu původního autora, neboť spojená díla a některé právní poměry z nich plynoucí nejsou explicitně upraveny v AutZ.³¹ Dále by to implikovalo, že tracingem není možné vyjádřit autorskoprávní individualitu vlastní tvůrčí činností.

Nejbližším k tracingu se jeví situace, kdyby spojení dvou děl vykazovalo tvůrčí činnost (zpracování) a vzniklo tak odvozené dílo.³² V tuto chvíli se již ale jedná o problematiku děl odvozených a zpracování.

2.1.3 ZMĚNA

Dalším případem, kdy je dílo využito v jiné než své původní podobě, je změna. Změna se může projevit jako tvůrčí, například jako zpracování, nebo jako netvůrčí.³³ Domnívám se, že právě zde je možné tracing zařadit.

²⁹ TELEEC, Ivo a TŮMA, Pavel. § 2 Autorské dílo. In: TELEEC, Ivo a TŮMA, Pavel. *Autorský zákon. Komentář*. 2. vydání. Praha: C. H. Beck CZ, 2019, s. 60–61.

³⁰ Ibidem.

³¹ Autoři se musí spolehnout na relativní úpravu vztahů, kterou jim poskytuje soukromé právo, a sjednat si práva a povinnosti na základě § 2358 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

³² Vznikem nového díla spojením se zpracovatelskou činností nelze nadále toto dílo považovat za součást děl hromadných dle § 2 odst. 5 AutZ. Avšak úprava souborného díla se velmi neliší od zpracování, kdy v obou případech jde o vyjádření „*tvůrčí schopnosti originálním způsobem prostřednictvím rozhodnutí učiněných na základě své tvůrčí svobody*“, viz rozsudek SDEU (třetího senátu) ze dne 1. 3. 2012 ve věci C-604/10, Football Dataco, bod 38.

Tracingem se původní dílo ocitá ve změněné podobě, nejspíše jako díle odvozené, působením tvůrčí činnosti, čímž mohou být narušeny oprávněné zájmy původního autora. Jako příklad poslouží kontroverze kolem *skinu* na zbraň M4A4 ve videohře *Counter-Strike: Global Offensive* (dnes „*Counter-Strike 2*“), od společnosti Valve, nesoucí název „Howl“. V případě se jedná o převzetí části ilustrace (vlka) od původního autora tracingem do nového díla, kde byla tvůrcem *skinu* (člen videoherní komunity) převzatá část lehce pozměněna a zakomponovaná jako středobod *skinu* *Howl* na zbraň M4A4.³⁴ Společnosti Valve obdržela od původního autora ilustrace DMCA (*Digital Millennium Copyright Act*) *takedown notice* na základě zásahu do jeho autorského práva, načež Valve na vlastní náklady *skin* pozměnila, aby neobsahoval protiprávní prvky, zakázala jeho další rozmnožování a tvůrce *skinu* potrestala.³⁵ V roce 2023 se společnost Valve na základě předchozích zkušeností vypořádala s obdobným případem na *skinu* „*Doodle Lore*“ na zbraň AWP způsobem, který již velmi neovlivní trh se *skiny* (např. navýšení ceny *skinu* o tisíce eur), a to tak, že *skin* úplně odstranila z videohry a nahradila ho novým se jménem „*Duality*“.³⁶

Stejně jako naplnění pojmových znaků autorského díla musí být soudy zkoumáno *ad hoc*, tak i povaha změny přísluší k rozhodnutí soudům.³⁷

³³ TELEČ, Ivo a TŮMA, Pavel. § 12 Právo dílo užít. In: TELEČ, Ivo a TŮMA, Pavel. *Autorský zákon. Komentář*. 2. vydání. Praha: C. H. Beck CZ, 2019, s. 165.

³⁴ Tyto *skiny* může hráč do svého videoherního inventáře získat například nákupem za „skutečné“ peníze a následně s nimi obchodovat (nejen) na integrovaném online tržišti na platformě *Steam*.

³⁵ Aby se společnost Valve vyhnula případným soudním sporům, tak požaduje po tvůrcích originalitu v dílech (*skinech*), které jsou dostupné na její platformě *Steam*. Případy tracingu tak „skončí dříve, nežli začnou“, když společnost Valve na své platformě působí jako „*judge, jury and executioner*“ pro nalézání pojmových znaků autorských děl. Respecting Intellectual Property. In: *Steam Community*. [online]. 2014. [cit. 30. 10. 2024]. Dostupné z: <https://steamcommunity.com/games/CSGO/announcements/detail/1751086783896069815>

³⁶ PATTERSON, Calum. New CSGO skins accused of stealing art for AWP and M4A4 in Revolution case. In: *Dexerto*. [online]. 2023. [cit. 28. 2. 2025]. Dostupné z: <https://www.dexerto.com/csgo/new-csgo-skins-accused-of-stealing-art-for-awp-and-m4a4-in-revolution-case-2059091/>

³⁷ TELEČ, Ivo. *Pojmové znaky duševního vlastnictví*. Praha: C. H. Beck CZ, 2012, s. 41.

V případě nalezení pojmových znaků na straně změny se bude v kontextu tracingu nejspíše jednat o zpracování.

Při vzniku odvozeného díla je obecně důležitým faktorem tvůrčí svoboda.³⁸ Ta může být v jistých případech omezena natolik, že je ze zákona vyloučeno, aby se tato odvozená tvorba kvalifikovala jako autorské dílo, neboť není „originální v tom smyslu, že je autorovým vlastním duševním vytvořením“.³⁹

Naopak neprokázáním splnění pojmových znaků ve zpracování původního díla by se jednalo o změnu netvůrčí povahy, kterou vznikne jinak změněné dílo zasahující do výlučných práv původního autora.⁴⁰ Domnívám se, že stejné závěry jsou vhodné i pro tracing.

2.1.4 INSPIRACE

K dokreslení právního rámce, ve kterém se tracing pohybuje, potřebujeme zmínit inspiraci. Inspirace je důležitým zdrojem k možnosti uměleckého vyjádření a může k ní dojít i bez toho, aniž by si to osoba autora uvědomovala. Tracing je důležitý při rozvoji umělce, kdy ho umělec může využít k učení a zdokonalování své kresby.⁴¹ Umělec si takto vnitřně přisvojí části technik jiných autorů, které ho nadále, i nevědomky, provází při tvorbě. Autor je tak ovlivněn (inspirován) autorskými díly, které při tracingu užívá.

Zejména umělecká díla obsahují „stavební bloky“, které mohou být předurčeny formou a obsahem díla, a proto se mohou různá díla v některých částech shodovat.⁴² Na příkladu kresby lidského obličeje ve stylu manga je autorovi značně omezena volnost v jeho tvůrčím vyjádření, a tak se mohou oči postav různých autorů shodovat v jejich tvaru a usazení

³⁸ POLČÁK. § 2 *Autorské dílo*, s. 56.

³⁹ Rozsudek SDEU (velkého senátu) ze dne 4. 10. 2011 ve spojených věcech C 403/08 a C 429/08, *Football Association Premier League*, bod 97, 98.

⁴⁰ TELEČ; TŮMA. § 2 *Autorské dílo*, s. 51.

⁴¹ *Explaining Illustration Tracing and Copyright Law Amidst the Frequent Plagiarism Controversies* [online].

⁴² Obdobně rozsudek Nejvyššího soudu ze dne 24. 3. 2021, sp. zn. 27 Cdo 2023/2019, bod 33.

na obličejí.⁴³ Autor je pak omezen nejen lidskou anatomií, ale i stylem kreslení manga, který může být abstraktním výsledkem tvůrčí duševní činnosti.⁴⁴ Obdobné shody v dílech můžeme spatřit, i když se autor inspi-ruje.⁴⁵ Inspirace a omezená autorská svoboda tak vykazují paralely. Na druhou stranu ani není vyloučeno, aby za působení inspirace vzniklo odvozené dílo.⁴⁶

Extenzivním výkladem by bylo možné hovořit o inspiraci jako o převzetí části původního díla, která obsahuje prvky z obecného fondu jako například myšlenku.⁴⁷ Poté taková ideální část původního díla sama o sobě nesplňuje pojmové znaky autorského díla, a proto nemůže dojít k jejímu zpracování a může být oprávněně převzata.⁴⁸

⁴³ KOMOTO, Akihiro. Release regarding Mai Hanamura's "trace false accusation" trial. In: *Komoto Sato Legal and Tax Partners*. [online]. 2023. [cit. 29. 10. 2024]. Dostupné z: https://ksltp.com/wp-content/uploads/2023/11/hanamura_231109_en.pdf

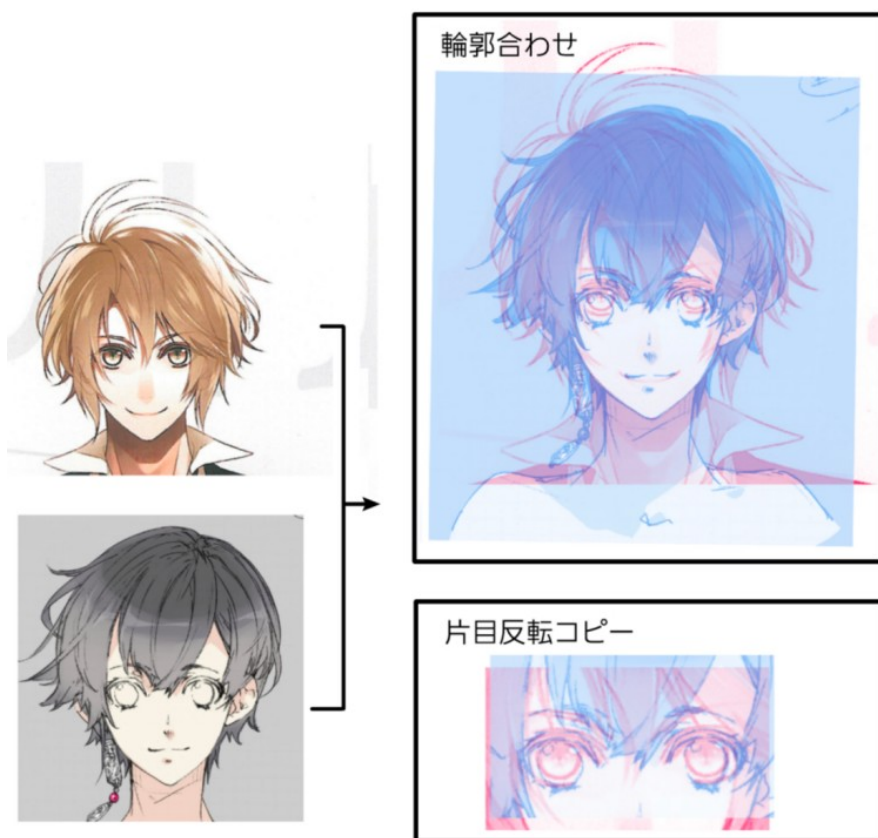
⁴⁴ KOUKAL. *Autorské právo, public domain a lidská práva*, s. 60.

⁴⁵ ŠALOMOUN, Michal. *Ochrana názvů, postav a příběhů uměleckých děl*. 2. vydání. Praha: Nakladatelství C. H. Beck CZ, 2009, s. 57.

⁴⁶ KOUKAL. *Autorské právo, public domain a lidská práva*, s. 151.

⁴⁷ Zákonem stanovený demonstrativní výčet součástí obecného fondu je zakotven v § 2 odst. 6 AutZ, avšak mnohé dovozuje i odborná literatura a judikatura, přičemž je možné, aby se prvky relevantní pro tracing v budoucnu objevily v obecném fondu. K zjištění, zdali se ještě jedná o inspiraci (obecný fond) nebo již zásah do autorských práv, může sloužit *abstractions test*, viz KOUKAL. *Autorské právo, public domain a lidská práva*, s. 219–221.

⁴⁸ ŠALOMOUN. *Ochrana názvů, postav a příběhů uměleckých děl*, s. 57–58.



Obr. 3 Ukázka dokazování tracingu na obličejích⁴⁹

Levá horní ilustrace patří Hanamura Mai (modře). Levá spodní ilustrace patří Juiga Satoru (červeně). Napravo jsou obě ilustrace položeny přes sebe s odlišnými barvami, aby demonstrovaly shodné linky. Pravé spodní přeložení pak vyobrazuje obličej s kopií jednoho oka dle osově souměrnosti. Jedná se o důkazní materiál tracingu předložený Juiga Satoru v případě Hanamura Mai v. Juiga Satoru.

Avšak z podstaty tracingu, kdy jde o převzetí explicitně vyjádřených částí děl na hmotném nosiči, si nemyslím, že bychom ho mohly řadit na úroveň inspirace. Tracingem již přebíráme vnější vyjádření myšlenky

⁴⁹ KOMOTO. Release regarding Mai Hanamura's "trace false accusation" trial [online].

původního díla, které za pouhé převzetí ideje můžeme těžko pokládat, a je tak možné se dopustit zásahu do autorského práva.⁵⁰ Proto se domnívám, že se různé úrovně inspirace v kontextu tracingu sice nachází, ale nejedná se o samostatnou definici tracingu jako činnosti.

2.2 VYMEZENÍ VŮČI NETRADIČNÍM ČINNOSTEM

Autorské právo zná dříve zmíněné vybrané kategorie činností, ale v průběhu svého působení se objevily činnosti, které jsou natolik specifické či kontroverzní, že se pro ně začala využívat vlastní terminologie. Příkladem může být *appropriation art*, *fan fiction* a *fan art*, *sampling* nebo *torepaku*. Domnívám se, že tracing má povahově ke každému z těchto typů tvorby více či méně blízko, ať už se jedná o samotnou nejednotnou definici, spornou otázku klasifikace nově vzniklých děl, typu zásahu do autorských práv anebo užití výjimek a omezení. Proto se domnívám, že by poznatky získané z následující analýzy těchto zákonem nepojmenovaných činností mohly být inspirativně, případně až analogicky, užitečné pro tracing.

2.2.1 APPROPRIATION ART

Appropriation art je jeden ze stylů moderního umění, který se týká užití nebo zpracování autorských děl bez souhlasu původních autorů.⁵¹ Do povědomí širší veřejnosti se *appropriation art* dostal až s nárůstem jeho trhu a jeho vysokými cenami, které začaly způsobovat nerovnost mezi ekonomickými pozicemi původních autorů a tvůrců *appropriation art*.⁵² Typickým příkladem tohoto stylu *pop art* je Andy Warhol s jeho sítotiskem fotografií anebo Roy Lichtenstein s jeho kopírováním a kombinací komiksové tvorby.⁵³ Díky svojí kontroverznosti se odborná literatura ze Spojených států

⁵⁰ Jedná se o obecné vyjádření doktríny *idea-expression dichotomy* z anglosaského práva zakotvené v mezinárodních smlouvách týkajících se autorského práva.

⁵¹ HAZUCHA, Branislav. Pop art z pohledu autorského práva. In: MOLNÁR, P. a kol. (ed.) *Košické dni súkromného práva IV. Pocta profesorovi Vojčíkovi*. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2022, s. 382.

⁵² Ibidem, s. 383.

⁵³ Ibidem.

amerických neshoduje na jednotném řešení oprávněnosti *appropriation art*.⁵⁴

Jednotlivá řešení jsou na pomyslné škále, a to počínaje vyjmutím výtvarného umění z autorskoprávní ochrany, *a priori* uplatnění výjimek a omezení (*fair use*) pro *appropriation art* nebo využití licence pouze pro vybrané případy a konče poměrným rozdělením zisku s nositelem práv k původnímu dílu.⁵⁵ Tyto přístupy se mimo problematickou majetkovou sféru snaží vyřešit i osobnostní sféru v podobě potřeby souhlasu ke změně původního díla.⁵⁶ Obecně tak lze problematiku *appropriation art* shrnout jako tvorbu odvozených děl za užití podkladových děl bez souhlasu původního autora.

2.2.2 FANFICTION A FAN ART

Fanfiction je volné pokračování původních děl fanoušky, kteří dotvářejí nedokončený příběh nebo zasazují například postavy, místa a děj do vlastních příběhů.⁵⁷ Obecně přijímaná definice *fanfiction* je tříprvková a říká, že se jedná o tvůrčí psaní, ve kterém je možné spatřit část pop kultury, přičemž je tato psaná tvorba vytvořena „neprofesionálem“.⁵⁸ Postupem času se z některých neprofesionálů ale stali profesionální autoři a *fanfiction* začala být tvořena za majetkovým ziskem.⁵⁹ Příkladem může být „*Fifty Shades of Grey*“ nebo „*Twilight*“, které byly vytvořeny bez licence od původního autora, avšak existují i případy licencované *fanfiction*.⁶⁰

Fan art je pak umělecká obdoba *fanfiction* v literatuře. Oba termíny popisují fanouškovskou tvorbu odvozených děl založenou na ději a postavách

⁵⁴ Ibidem, s. 386.

⁵⁵ Ibidem, s. 386–388.

⁵⁶ Případem, kdy došlo k úpravě fotografií s následným užitím bez souhlasu nositele práv, se zabýval Vrchní soud v Praze, jako odvolací soud, kdy shledal užití fotografií jako neoprávněné užití díla a potvrdil vznik bezdůvodného obohacení, viz rozsudek Vrchního soudu v Praze ze dne 19. 4. 2022, č.j. 3 Co 170/2021-211.

⁵⁷ KOUKAL. *Autorské právo, public domain a lidská práva*, s. 173.

⁵⁸ LIPTON, Jacqueline. D. Copyright and the Commercialization of Fanfiction. *Houston Law Review*. 2014, roč. 52, č. 2, s. 435.

⁵⁹ Ibidem, s. 438.

⁶⁰ Ibidem, s. 439.

původních děl, na jejíž oprávněnost nepanuje, jako v již zmíněných zákonem nepojmenovaných činnostech, jednotný názor.⁶¹

2.2.3 SAMPLING

Sampling je činnost zahrnující zakomponování původních zvukových nahrávek nebo jejich částí (melodie nebo text) do nové zvukové nahrávky.⁶² Specifickou povahou *samplingu* je jeho omezení na hudební díla, čímž se rozšiřuje okruh možných nositelů práv, u kterých může dojít k jejich zásahu. Tyto případy zahrnují zásah do práv autora k jeho dílu, práv výkonného umělce k jeho uměleckému výkonu, ale i právo výrobce zvukového záznamu k jeho záznamu.⁶³ Opět se jedná o užití díla bez souhlasu původního nositele práv, které se zakomponováním stává součástí nového díla jako odvozené dílo. Stejně jako *appropriation art*, otázka, jak se se *samplingem* vypořádat, stále není jasná, neboť rozhodnutí soudů v různých jurisdikcích jsou odlišná a soudy také postupem času své názory mění.

Například soudy ve Spojených státech amerických na počátku vždy dovozovaly potřebu licence pro každý *sampling*, poté připustily možnost využití výjimky a omezení *de minimis* a později i *fair use*.⁶⁴ Na druhou stranu SDEU rozhodl, že se nejedná o rozmnožování pouze v případě, kdy není převzata zvuková nahrávka jako celek nebo její podstatná část, přičemž *sample* nemusí vůbec být v pozměněné podobě.⁶⁵ Toto rozhodnutí plyne z „*Metall auf Metall ságy*“, která se řeší v Německu více než 15 let, což vyvrcholilo v předložení předběžné otázky k SDEU, ale jak se zdá, tak rozhodnutí SDEU tento případ ještě neuzavřelo.⁶⁶ Pravděpodobně konečnou odpověď na otázku *samplingu* se SDEU bude zabývat v nově podané

⁶¹ MORGAN, Rachel. Conventional Protections for Commercial Fan Art Under the U.S. Copyright Act. *Fordham Intellectual Property, Media and Entertainment Law Journal*. [online]. 2021, roč. 31, č. 2, [cit. 24. 11. 2024], s. 525.

⁶² CHALLIS, Ben. The Song Remains the Same: a Review of the Legalities of Music Sampling. *WIPO Magazine*. 2009, č. 6, s. 16.

⁶³ Ibidem.

⁶⁴ MEZEI, Péter. Thou Shalt (Not) Sample? New Drifts in the Ocean of Sampling. *Journal of Intellectual Property Law*. [online]. 2019, č. 2, [cit. 29. 11. 2024], s. 172–180.

⁶⁵ Rozsudek SDEU (velkého senátu) ze dne 29. 7. 2019 ve věci C 476/17, Pelham I, bod 46, 47.

předběžné otázce z případu *Metall auf Metall*, která řeší užití pastíše jako výjimky a omezení pro *sampling*.⁶⁷

2.2.4 TOREPAKU

Torepaku, volně přeloženo jako „krádež tracingem“, je činnost specifická pro Japonsko, která se zejména objevuje na sociálních sítích, kde se tento slangový výraz často skloňuje spolu s ilustracemi z anime a manga, neboť právě v Japonsku je trh s komiksy (manga), kreslenými filmy nebo seriály (anime) dlouhodobou předností země a vývozním artiklem.⁶⁸ Příkladem může být případ Hanamura Mai v. Juiga Satoru, který se týkal údajného tracingu ilustrací *otome* a na něj navazující nařčení z *torepaku*.⁶⁹ Tento termín je pak využíván, jak již bylo zmíněno, pro tracing v protiprávním kontextu, což může způsobovat stigma i vůči „oprávněnému“ tracingu.

V tomto kontextu je avšak zvláštní, že odvozená fanouškovská tvorba (dóždžinši) specifická pro Japonsko, jenž je také součástí zmíněné kultury, obvykle není díky implicitní kolektivní shodě společností hájících zájmy autorů a autory samotnými perzekuována stejně jako *torepaku*.⁷⁰ Obě díla jsou tvořena za účelem zisku, ale u fanouškovské tvorby je explicitně nebo implicitně přiznáno, o jaké původní dílo, tak i o jakého původního autora, se jednalo. Konsensus se také týká odlišnosti trhů, kdy fanouškovská tvorba údajně nezasahuje do původního trhu, a dokonce na něj může mít stimulační efekt.⁷¹ Díla vytvořená pomocí tracingu jednoznačně nemohou sdílet

⁶⁶ MEZEI, Péter; JÜTTE, Bernd Justin; SGANGA, Caterina; PASCAULT, Léo. Oops, i Sampled Again ... the Meaning of “Pastiche” as an Autonomous Concept Under EU Copyright Law. *International Review of Intellectual Property and Competition Law*. [online]. 2024, roč. 55, [cit. 30. 11. 2024], s. 1227–1228.

⁶⁷ Žádost o rozhodnutí o předběžné otázce ze dne 25. 9. 2023 ve věci C-590/23, Pelham II.

⁶⁸ Pejorativní termín トレパク [*torepaku*] vznikl z japonského トレース [*torésu*] – „obkreslit“ a パクする [*pakuru*] – „krást“.

⁶⁹ Rozsudek Tokijského okresního soudu (občanskoprávní oddělení 29) ze dne 13. 10. 2023, sp. zn. 2020(wa)25439 a sp. zn. 2021(wa)1631. Analýza případu viz ŽVÁČEK. *Autorskoprávní aspekty tracingu*, s. 78–83, 85–86.

⁷⁰ MEHRA, Salil K. Copyright and Comics in Japan: Does Law Explain Why All the Cartoons My Kid Watches are Japanese Imports?. *Rutgers Law Review*. [online]. 2002, roč. 55, [cit. 5. 12. 2024], s. 39.

⁷¹ *Ibidem*, s. 54.

stejný trh jako tato fanouškovská tvorba, když se vydávají za absolutně nová díla. Domnívám se, že proto, i přes konsensus japonské většiny o odvozené tvorbě, se tato forma (tracing) vymyká standardnímu pojetí přijatelného společností a je proto do této míry odsuzována jako zavrženíhodná.⁷²

2.3 POJMOVÉ ZNAKY TRACINGU

Z poznatků předchozích porovnání vůči činnostem, které jsou autorským právem tradičně předvídaný, ale i nepředvídaný, a příkladů si dovolím shrnout, že tracing je (i) úmyslná činnost (ii) tvůrčí povahy (iii) spočívající v převzetí (iv) vybraných prvků původního díla (v) a následném zakomponování těchto prvků (vi) do nově vznikajícího díla.

Ad (i) Ať již jde o přeložení papíru nebo vytvoření vrstvy v rastrovém grafickém editoru přes původní dílo, osoba, která se připravuje na tracing, si je vědoma toho, že použije nějaké podkladové dílo, zejména když si tato díla nevybírá nahodile, tedy i s předchozím rozmyslem.

Ad (ii) Domnívám se, že každý tracing v sobě ukrývá jistý rozměr tvůrčí činnosti ve smyslu „autorského otisku“, neboť je v procesu převzetí a zakomponování přítomen lidský faktor. Umělecké nadání či kvalita, které je uživatel tracingu schopen dosáhnout, je irelevantní, stejně tak jako umělecká hodnota díla nemůže být pojmovým znakem.

Ad (iii) Prvním bodem, kde je možné spatřit tvůrčí činnost, je převzetí původní části díla. Tvůrčí činnost tak může spočívat například v rozmyslu, které části původního díla převzít nebo jak budou tyto části změněny v novém díle (velikost, styl, barva atd.). Převzetím se v obecném kontextu, tak i zde, má namysli vytvoření rozmnoženiny původního díla, přesněji neúplné napodobeniny (neidentické rozmnoženiny). Vznik rozmnoženiny je inherentní mezikrok, bez kterého není možné tracing realizovat.

Ad (iv) Autorskoprávní analýzou původního díla můžeme přijít na jednotlivé prvky, které takové dílo tvoří. Prvky obsahující au-

⁷² V Japonsku přibývá případů, kdy je osoba nejen nařčena z neoprávněného tracingu, ale i případů, kdy se jedná pouze o křivé obvinění z tracingu. Takové případy se pak označují termínem *トレパク冤罪* [torepaku enzai], viz TOMORI, Subaru. *エセ著作権事件簿* (False Copyright Claim Casebook). Japonsko: Publib LLC, 2022.

torskoprávní individualitu a prvky, které jsou součástí obecného fondu. Jinak řečeno, prvky autorskoprávně chráněné a nechráněné. Uživatel tracingu si z těchto prvků (nevědomky) vybírá, které z nich převzít.

Ad (v) Část původního díla, tedy vybrané prvky, fungují jako podkladové dílo k vlastní tvorbě uživatele tracingu. Dříve, nežli můžeme hovořit o vzniku nového díla, musíme část původního díla (rozmnoženinu) a část vlastní uživateli tracingu zakomponovat do sebe. V zakomponování tak jde o další bod, ve kterém se projevuje tvůrčí činnost, která může být spatřena ve vytvoření kompozice nebo například v rozhodnutí, jak velkou váhu a důraz bude mít převzatá část v konečném díle.

Ad (vi) Po „dokončení předchozích kroků“ tracingu, činnost bez pochyb vyústí ve vznik něčeho nového, tedy něčeho, co se liší od díla původního. Domnívám se, že bychom měli na výsledky této tvorby pohlížet obdobně jako na výsledky *appropriation art* nebo *samplingu*, tedy že jedná se o autorská díla, dokud není prokázán opak.⁷³ K podání ucelené definice tracingu je tak zvoleným termínem „dílo“ namísto „výtvoru“.

Tracing je především vykonáván za účelem majetkového nebo osobního zisku uživatele tracingu, což může být využito jako ukazatel při soudním řízení pro výpočet újmy, dovoluje-li to daná jurisdikce.⁷⁴ Tomuto nahrává i absence zmínky o původním díle nebo původním autorovi, společně s absencí jakékoliv licence mezi stranami. Tracing je složité obecně klasifikovat, neboť části převzaté z původního díla jsou více či méně pozměněny a doplněny částmi vlastními. Dále se na složitosti klasifikace podílí to, jaké části původního díla jsou převzaty, kolik jich bylo, a jak velkou část tvoří v novém díle vytvořeném pomocí tracingu. Nakonec je ale klasifikace tracingu jako činnosti *ad hoc* na soudech, a proto povahu tracingu nelze s přesností v obvyklých případech dopředu určit.

Domnívám se, že tracing není inherentně spjat s protiprávním jednáním, avšak skrývá negativní podtón plynoucí z medializovaných kauz, které od-

⁷³ Podrobnostmi klasifikace díla vytvořeného pomocí tracingu se bude zabývat následující kapitola.

⁷⁴ Dle § 40 odst. 4 AutZ by se v České republice aplikovala licenční analogie k tomuto výpočtu.

suzují jeho nemorálnost a spíše se vůči tracingu vymezují.⁷⁵ Považovat *de lege* tracing jako protiprávní by nás mohlo vést až k závěrům o „kvazimonopolizaci“ autorského práva, neboť se domnívám, že existují případy, kdy je tracing oprávněný.⁷⁶

2.4 SUBSUMPCE TRACINGU DO ČESKÉHO AUTORSKÉHO ZÁKONA

Teze, že tracing je úmyslná činnost kreativně přeměňující část původního díla za následným jedinečným zakomponováním těchto prvků do díla nového, nás může dovést k následujícímu závěru pro subsumpci v AutZ.

Pragmaticky bychom měli na tracing nahlížet jako na faktický způsob vytváření odvozené tvorby dle § 2 odst. 4 AutZ. Avšak v případě nenalezení tvůrčí činnosti a autorskoprávně individuálních prvků soudy je možné konstatovat, na základě § 12 odst. 1 a § 11 odst. 3 AutZ, tracing jako zákonem nepojmenovanou *sui generis* změnu díla zasahující do práva dílo užít a do práva na nedotknutelnost díla původního autora. *Tertium non datur*. Je nutné podotknout, že v obou pragmatických případech je mezikrokem rozmnožení dle § 13 AutZ, ke kterému dochází při převzetí části původního díla.

3. DÍLO VYTVOŘENÉ POMOCÍ TRACINGU

V návaznosti na činnost tracingu a jeho výsledku musí být nejdříve položena otázka, zdali nově vzniklé dílo má vůbec povahu autorského díla dle § 2 odst. 1 AutZ a může být chráněno autorským právem. Musíme tak zkoumat přítomnost jednotlivých pojmových znaků autorského díla v nově vzniklém díle vytvořeném pomocí tracingu. Avšak ještě před tím je nutné podotknout, že hodnocení umělecké hodnoty díla subjektivním pohledem nemá na autorskoprávní posouzení vliv, naopak objektivní hodnocení vliv má, a ten se se projevuje v kategorizaci děl.⁷⁷ Pojmové znaky autorského dí-

⁷⁵ Zejména japonské kauzy a jejich dopady, viz TATSUMI, Kenji. For Japan illustrators, easy software heightens danger of false 'trace-copying' accusations. In: *The Mainichi*. [online]. 2024. [cit. 23. 10. 2024]. Dostupné z: <https://mainichi.jp/english/articles/20240819/p2a/00m/0et/010000c>

⁷⁶ Oprávněným tracingem na základě výjimek a omezení se bude zabývat kapitola 5.

⁷⁷ KNAP. *Užití autorského díla*, s. 30–31.

la obsahuje dílo vytvořené pomocí tracingu, pokud je (i) součástí kategorie umění, literatury nebo vědy, přičemž musí být (ii) kreativní jako výsledek tvůrčí činnosti autora a (iii) jedinečné ve smyslu autorskoprávní individuality a zároveň musí být i (iv) objektivně vnímatelné smysly.⁷⁸

Je důležité si uvědomit, že takové dílo je složeno *de facto* ze dvou děl, a to převzaté části a nové (vlastní) části, ale *de iure* je hodnoceno jako dílo jediné. Díky tomu stačí, aby jedna část nového díla naplnila všechny pojmové znaky. Na druhou stranu, je potřebné vědět, která část (nebo obě) naplnila pojmové znaky, neboť nás může přivést k odlišnému závěru u klasifikace nově vzniklého díla.

Ad (i) Naplnění prvního pojmové znaku by nemělo být v kontextu tracingu sporné, neboť tracing zachovává stejnou kategorii děl, jakou má původní dílo, nejčastěji uměleckou kategorii. Výjimku mohou tvořit například fotografie nebo některá díla dle § 3 AutZ, která povahově mohou být tvůrčí činností zpracována do nového díla.⁷⁹

Ad (iv) Objektivní vnímatelnost smysly je bezesporu jednoduché v díle vytvořeném pomocí tracingu naplnit. Ostatně jako kategorii chráněných děl, tak i podobu díla totiž diktuje dílo původní. Jediná změna může nastat v podobě objektivně vnímatelného vyjádření. Například z analogové do digitální podoby, která může mít v odlišných jurisdikcích dopady na kvalifikaci.

Ad (ii, iii) Problematickými pojmovými znaky autorského díla ze strany jejich naplnění jsou tvůrčí činnost a autorskoprávní individualita.⁸⁰ Domnívám se, že právě v tomto kroku dochází k diferenciaci děl vytvořených pomocí tracingu. Základní pojem je v tomto ohledu tvůrčí svoboda, která postupně krystalizuje v rozhodnutích SDEU. Dle SDEU je možné autorské právo „uplatnit pouze ve vztahu k předmětu, který je původní v tom smyslu, že je autorovým vlastním duševním výtvorem“.⁸¹ Stejně tak je důležité, aby tento

⁷⁸ § 2 odst. 1 AutZ.

⁷⁹ TELEČ; TŮMA. § 2 *Autorské dílo*, s. 50–51.

⁸⁰ POLČÁK. § 2 *Autorské dílo*, s. 38.

⁸¹ Rozsudek SDEU (čtvrtého senátu) ze dne 16. 7. 2009 ve věci C-5/08, Infopaq International, bod 37. Rozsudek SDEU (velkého senátu) ze dne 4. 10. 2011 ve spojených věcech C 403/08 a C 429/08, Football Association Premier League, bod 96–97.

předmět obsahoval „*prostor pro tvůrčí svobodu ve smyslu autorského práva*“.⁸² Vlastní duševní výtvor tak odráží osobnost autora, „*pokud mohl autor při realizaci díla vyjádřit své tvůrčí schopnosti prostřednictvím rozhodnutí učiněných na základě své tvůrčí svobody*“.⁸³ A contrario, když takový tvůrčí prostor neexistuje nebo nedojde k vyjádření autorových tvůrčích rozhodnutí, dílo postrádá odraz osobnosti autora, a tak nemůže být původní jako autorův vlastní duševní výtvor. Obdobně hovoří o autorskoprávní individualitě i Nejvyšší soud, který ji pojímá jako „*nejosobitější ztvárnění výtvoru na základě autorova svobodného výběru z tvůrčích možností*“ a „*tvůrčí činností nezaměnitelného osobitého rázu*“.⁸⁴ I zde platí, že pokud neexistuje dostatečný tvůrčí prostor pro autora, tak se nemůže jednat o autorské dílo, a to bez ohledu na hodnotu tohoto díla.⁸⁵ Základem autorskoprávní individuality je tedy tvůrčí činnost osoby autora, jejíž vlastnosti zapřičiňují osobitost díla, která se projevuje ve svobodném výběru z tvůrčích možností.

3.1 KLASIFIKACE DÍLA VYTVOŘENÉHO POMOCÍ TRACINGU

Esenciální částí celého procesu tvorby díla vytvořeného pomocí tracingu je uživatel tracingu, neboť právě jeho rozhodnutí a tvůrčí schopnosti mají silný vliv na právní kvalifikaci díla vytvořeného pomocí tracingu. Od předchozího úmyslu, kterou část nebo části původního díla převzít, až po to, jak velkou roli budou v novém díle hrát, jsou kroky předurčené rozmyslem této osoby. Schopnost přenést části původního díla v určité kvalitě se člověk od člověka liší, stejně tak při jejich zakomponování do díla nového. V tomto okamžiku dochází k projevům tvůrčí činnosti, která, byť někdy zvláště omezená, je podstatným pojmovým znakem vycházejícím z autora samotného.⁸⁶

Pomineme-li fakt, že dílo musí být součástí kategorie umění, literatury nebo vědy (tzv. „*doménový test*“) a být objektivně vnímatelné smysly, jedi-

⁸² Ibidem, bod 98–99.

⁸³ Rozsudek SDEU (třetího senátu) ze dne 1. 12. 2011 ve věci C-145/10, Painer, bod 89.

⁸⁴ Rozsudek Nejvyššího soudu ze dne 30. 4. 2007, sp. zn. 30 Cdo 739/2007.

⁸⁵ Rozsudek Nejvyššího soudu ze dne 24. 3. 2021, sp. zn. 27 Cdo 2023/2019, bod 37–40.

⁸⁶ Ostatně, důležitost tvůrčí svobody k naplnění pojmových znaků autorského díla je opakovaně judikována SDEU. Například rozsudek SDEU (třetího senátu) ze dne 22. 12. 2010 ve věci C-393/09, Bezpečnostní softwarová asociace, bod 48–50.

ným rozhodným kritériem pro klasifikaci díla vytvořeného pomocí tracingu je obecně (i) kvalita a (ii) kvantita převzatých částí díla a přítomnost (iii) tvůrčí změny v procesu jeho vytváření.⁸⁷

Ad (i) Kvalitou je myšlena autorskoprávní povaha převzaté části, a to, jestli byly převzaty prvky obsahující autorskoprávní individualitu, prvky obecného fondu anebo obojí. Toto rozdělení určuje, zdali došlo k zásahu do autorských práv původního autora či nikoli.⁸⁸ Zároveň je to i ukazatel, zdali vůbec můžeme uvažovat o zpracování a vzniku odvozeného díla, neboť převzetím prvků čistě z obecného fondu ke zpracování nemůže dojít.⁸⁹

Ad (ii) Kvantitou je myšleno, jak velkou část původního díla a zároveň jak velkou část nového díla tvoří převzaté části. Tento závěr je zejména vhodný pro Spojené státy americké, kde je sledována i kvantita u vzniku odvozených děl.⁹⁰ Řeč je o doktríně *de minimis*, která právě na kvantitě staví argumentaci zanedbatelného zásahu do práv původního autora.⁹¹ Není zcela jisté, zda je tato doktrína „prahové hodnoty“ využitelná v kontextu unijní autorskoprávní úpravy, avšak dle právního názoru tehdejšího generálního advokáta Szpunara tomu tak není.⁹² Za to ale můžeme nahlížet na kvantitu jako možnou tvůrčí svobodu, tedy kolik prostoru pro tvůrčí uvážení nám je zanecháno v tvorbě nového díla po převzetí částí z původní-

⁸⁷ „Doménový test“ nebyl SDEU doposud jednoznačně přijat jako kritérium při kvalifikaci autorských děl, viz HUGENHOLTZ, P. Bernt a QUINTAIS, João Pedro. Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output?. *International Review of Intellectual Property and Competition Law*. [online]. 2021, roč 52, [cit. 7. 1. 2025], s. 1194. Vybraná kritéria jsou poměrně vágně vymezena, aby poznatky mohly být aplikovatelné v různých jurisdikcích, například ve Spojených státech amerických, kde se odlišují druhy odvozených děl podle přítomnosti tvůrčí změny původního díla na transformativní a derivativní (*transformative and derivative*) díla, a to zejména pro případy aplikace doktríny *fair use*, viz DRASSINOWER, Abraham. Copyright is not about copying. *Harvard Law Review*. [online]. 2012, roč. 125, č. 7, [cit. 28. 11. 2024], s. 113–114.

⁸⁸ V tomto kontextu se naskytá otázka, zdali je generativní AI schopna ve svém vygenerovaném výstupu zasáhnout do práv původních autorů, když strojové učení probíhá v režimu obdobnému tracingu obecného fondu.

⁸⁹ TELEČ; TŮMA. § 2 *Autorské dílo*, s. 51.

⁹⁰ MANTA, Irina D.; BALGANESH, Shyamkrishna; WILKINSON-RYAN, Tess. Judging Similarity. *Iowa Law Review*. [online]. 2014, roč. 100, [cit. 28. 11. 2024], s. 274–275.

⁹¹ Ibidem.

⁹² Stanovisko generálního advokáta Macieje Szpunara ze dne 12. 12. 2018 ve věci C-476/17, Pelham I, bod 32, 33.

ho díla. Domnívám se, že velikost podílu částí k jejich patřičným dílům i podíl částí nových k původním v díle vytvořeném pomocí tracingu tak může být určujícím faktorem.

Ad (iii) Tvůrčí změnou je myšlena činnost měnící původní dílo takovým způsobem, aby mohlo vzniknout nové dílo, které splňuje pojmové znaky autorského díla. V případě vzniku odvozeného díla musí taková tvůrčí změna vykazovat i pojmové znaky zpracovatelské činnosti, či jiné činnosti, při které vzniká odvození díla.

Prvním možným závěrem o klasifikaci je vznik odvozeného díla, které svůj vznik povahově odvozuje od původního díla.⁹³ Aby mohlo být dílo odvozeným, musí být nové a jedinečné ve smyslu autorskoprávní individuality a musí být výsledkem osobitě tvůrčí zpracovatelské činnosti.⁹⁴ V tomto případě byly v částech původního díla autorskoprávně individuální prvky a nedošlo k vyvrácení přítomnosti tvůrčí činnosti při zpracování těchto částí do díla nového. V opačném případě, druhým závěrem, vznikne jinak změněné dílo, a to v důsledku přebrání částí původního díla, které obsahují autorskoprávně individuální prvky, ale již není dosaženo potřebné tvůrčí činnosti, pouze netvůrčí změny, při následném zpracování těchto částí do nového díla.

Extrémním případem pak může být vznik samostatného autorského díla, nebo naopak díla nesplňujícího pojmové znaky autorského díla. Snížením pomyslné „laťky“ ke klasifikaci díla jako autorského judikaturou SDEU se tato situace nejvíce pravděpodobnou. Nejdříve by musela převzatá část obsahovat pouze prvky z obecného fondu, čímž nemůže dojít k zásahu do autorských práv. Takovou část nelze ani tvůrčí činností zpracovat do nového díla jako odvozené dílo.⁹⁵ Pokud budou v autorově vlastní části nalezeny pojmové znaky autorského díla, vznikne nové autorské dílo, které je kompletně nezávislé od původního autora. V opačném případě vznikne výtvor, který bude od počátku součástí obecného fondu.⁹⁶ Uživatel tracingu se

⁹³ TELEČ; TŮMA. § 2 *Autorské dílo*, s. 49.

⁹⁴ Ibidem, s. 49–50.

⁹⁵ Ibidem, s. 51.

tak nemůže stát autorem takového díla a zároveň tímto dílem nemůže být zasaženo do autorských práv původního autora.

Upřesníme-li dříve zmíněná obecná kritéria ke klasifikaci díla vytvořeného pomocí tracingu, tak rozhodnými jsou prvky obsahující autorskoprávní individualitu, prvky obecného fondu a splnění pojmových znaků autorského díla. Základními u „vstupu“ jsou převzaté prvky obsahující autorskoprávní individualitu a u „výstupu“ naplnění pojmových znaků autorského díla.⁹⁶ Závěrem je nutné podotknout, že představené závěry se týkají ideálních případů, což umožňuje jednodušší proces klasifikace. V opačném případě bychom museli sledovat „sílu“ jednotlivých prvků, neboť *„čím slabší je individualita předmětu autorského práva, tím méně lze dovozovat, že došlo k užití autorského díla“*.⁹⁸ Dosud zmíněné poznatky lze přehledně shrnout ve formě tabulky.

⁹⁶ Vznik takového výtvoru tracingem je ještě složitější, neboť by muselo jít o rutinní, mechanické zpracování, které z definice neobsahuje autorskoprávní individualitu, viz KOUKAL. *Autorské právo, public domain a lidská práva*, s. 54. Složitost situace odvozují z teze, že uživatel tracingu spíše zanechává svůj „autorský otisk“ v díle vytvořeném pomocí tracingu.

⁹⁷ Shodnost prvků obecného fondu je u děl závislých nepodstatná, viz KNAP. *Užití autorského díla*, s. 39.

⁹⁸ KNAP. *Užití autorského díla*, s. 37.

Tab. 1 Klasifikace díla vytvořeného pomocí tracingu

Dílo vytvořené pomocí tracingu obsahuje			Klasifikace díla vytvořeného pomocí tracingu
Prvky z původního díla		Vlastní prvky	
Převzaté prvky autorskoprávně individuální	Využití prvky obecného fondu	Naplňující pojmové znaky autorského díla	
○	○	○	→ Odvozené dílo
○	×	○	→ Odvozené dílo
○	○	×	→ Jinak změněné dílo
○	×	×	→ Jinak změněné dílo
×	○	○	→ Autorské dílo
×	○	×	→ Výtvor

Tabulka vyobrazuje ideální situace pro klasifikaci díla vytvořeného pomocí tracingu. ○ = „ano“ × = „ne“

Obdobně s jednotlivými názory a přístupy k oprávněnosti a morálnosti *appropriation art*, tak i názory a přístupy k tracingu se mohou lišit nejen mezi veřejností a akademickou obcí, ale i navzájem uvnitř.⁹⁹ Domnívám se, že z doposud uvedených případů se tracing jeví spíše jako činnost v „šedé zóně“ práva. Obecně vzato, tracing s sebou nese negativní konotaci, která plyne z medializovaných kauz.¹⁰⁰ Příčinou může být jednak neexistence přímo aplikovatelných právních norem, jednak různě nastavené morální hodnoty jednotlivce či kultury jako celku. Cílem analýzy za ná-

⁹⁹ Více k přístupům k *appropriation art* viz kapitola 2.2.1.

¹⁰⁰ Například TATSUMI. *For Japan illustrators, easy software heightens danger of false 'trace-copying' accusations* [online].

slednou deskripci činnosti a vzniklého díla není tracing *a priori* odsoudit jako činnost protiprávní, ale zároveň ani obhájit jako činnost vždy oprávněnou. Cílem je naopak poukázat na existenci této právní „šedé zóny“, při současném návrhu řešení, jak postupovat při klasifikaci z dosud získaných poznatků v obdobných případech.

3.2 SUBSUMPCE DÍLA VYTVOŘENÉHO POMOCÍ TRACINGU DO ČESKÉHO AUTORSKÉHO ZÁKONA

Z dříve zmíněného zobecněného závěru, že tracingem pravděpodobně vznikne odvozené dílo nebo jinak změněné dílo, můžeme v českém autorském právu uvažovat o dvou možnostech kvalifikace.¹⁰¹

Nejdříve pragmatická subsumpce, pod vlivem rozhodovací praxe SDEU a českého Nejvyššího soudu, za využití Polčákovi logické falzifikace, jako odvozené dílo (tvůrčím způsobem změněné) dle § 2 odst. 4 AutZ, kdy musí dojít k převzetí prvků původního díla obsahujících autorskoprávní individualitu a vytvoření díla tvůrčí zpracovatelskou činností, které naplňuje pojmové znaky autorského díla.¹⁰² V případě vyvrácení naplnění pojmových znaků pak jako netvůrčím způsobem změněné původní dílo dle § 12 odst. 1 a § 11 odst. 3 AutZ, kdy musí dojít k převzetí prvků původního díla obsahujících autorskoprávní individualitu, ale už není přítomna tvůrčí činnost v průběhu tracingu. Opět je nutné podotknout, že v obou pragmatických případech je meziproduktem rozmnoženina dle § 13 AutZ, jako samostatná převzatá část původního díla.

Stejně jako pro subsumpci činnosti, tak i vzniklého díla, je problematické, že pouze soudům náleží určit, zdali je změna tvůrčí nebo netvůrčí povahy, tedy vzniká-li odvozené dílo nebo jinak změněné dílo.¹⁰³ V obou případech ale může dojít k zasažení stejných autorských práv.

¹⁰¹ Zaměříme-li se na výsledek tracingu, tak subsumpce tracingu jako činnosti výhradně pod § 13 AutZ není vhodná, neboť podstatou rozmnožování je pouze vytvoření rozmnoženiny. Mezitím tracingem se s rozmnoženinou nadále tvůrčí činností pracuje k vytvoření nového díla.

¹⁰² Více o logické falzifikaci viz POLČÁK. § 2 *Autorské dílo*, s. 38.

¹⁰³ TELEČ. *Pojmové znaky duševního vlastnictví*, s. 41.

4. ZASAŽENÁ PRÁVA PŮVODNÍHO AUTORA

Při hodnocení, zdali došlo k zásahu do autorských práv, je nejdříve nutné brát v potaz jednotlivé prvky autorského díla, a to prvky obsahující autorskoprávní individualitu a prvky z oblasti obecného fondu.¹⁰⁴ K užití autorského díla totiž může dojít pouze při užití částí obsahující autorskoprávní individualitu původního autora.¹⁰⁵

Prvky obsahující autorskoprávní individualitu jsou vlastním duševním výtvorem autora a vznikají za působení autorovy tvůrčí činnosti.¹⁰⁶ Obecně jsou tyto prvky výplodem osobnosti autora.¹⁰⁷ Právě tyto prvky dokážou naplnit pojmové znaky autorského díla, přičemž musí být zkoumány *ad hoc*. Autorskoprávní individualita se může projevit výběrem z několika málo alternativ nebo i tvůrčím uspořádáním prvků.¹⁰⁸

Obecný fond dle Koukala tvoří „(i) *abstraktní výsledky tvůrčí činnosti*, (ii) *skutečnosti existující nezávisle na lidském vědomí (objektivně existující skutečnosti)*, (iii) *vědecké myšlenky*, (iv) *principy a myšlenky, na kterých jsou postaveny počítačové programy*, (v) *volná díla*, a konečně (vi) *díla vyloučená z ochrany ve veřejném zájmu*“, přičemž stěžejním jsou abstraktní výsledky tvůrčí činnosti.¹⁰⁹ Domnívám se, že právě tyto abstraktní prvky můžeme považovat za „protipól“ k autorskoprávním individuálním prvkům v kontextu tracingu.¹¹⁰

K soukromoprávní ochraně osobnostních a majetkových práv autorských v AutZ slouží § 40 a násl. s demonstrativním výčtem možných žalobních návrhů.¹¹¹ Koncepce vztahu těchto autorských práv není v kontinentálním

¹⁰⁴ KOUKAL. *Autorské právo, public domain a lidská práva*, s. 366.

¹⁰⁵ KNAP. *Užití autorského díla*, s. 42.

¹⁰⁶ HUSOVEC. *Judikatórna harmonizácia pojmu autorského diela v únijskom práve*, s. 16–17.

¹⁰⁷ KNAP. *Quo vadis současného autorského práva*, s. 15.

¹⁰⁸ *Ibidem*, s. 19.

¹⁰⁹ KOUKAL. *Autorské právo, public domain a lidská práva*, s. 149.

¹¹⁰ Avšak tímto nejsou vyloučeny ostatní části obecného fondu. Je možné si představit například i volná díla nebo také díla vyloučená z autorskoprávní ochrany ve veřejném zájmu.

¹¹¹ Jmenovitě jsou pro zásah do autorských práv tracingem využitelné nároky na určení autorství, negatorní nároky spočívající ve zdržení se zásahu, požadování informací nezbytných k uplatnění dalších nároků, odstranění škodlivých následků, přiměřené zadostiučinění, náhradu škody a vydání bezdůvodného obohacení.

pojetí jednotná.¹¹² Německá a původní česká doktrína zastávají monistický přístup, který vnímá autorské právo jako „*vnitřně jednotné subjektivní právo absolutní povahy*“ s aspektem osobnostním a majetkovým.¹¹³ Naopak dnešní česká doktrína, nazývaná také „*kvazidualistická*“, se s novým autorským zákoníkem z roku 2000 vzdala monistického přístupu.¹¹⁴ Osobnostní a majetková autorská práva jsou tak od sebe oddělena. Z tohoto vyplývá, že protiprávně zasažena může být dokonce jen jedna z právních sfér autora, a proto budou jednotlivé sféry, do kterých může být tracingem zasaženo, představeny nezávisle na sobě. Dále uvedená práva, do kterých může být tracingem zasaženo, jsou založena na kvalifikaci tracingu jako faktickém způsobu vytváření odvozené tvorby.

Pro doplnění, veřejnoprávní část ochrany poskytuje jednak § 105a a násl. AutZ s odpovědností za přestupek, jednak § 270, § 271 trestního zákoníku (dále jen „TZ“) s odpovědností za trestný čin.¹¹⁵ Základem správněprávní odpovědnosti v případě tracingu pak bude neoprávněné užití autorského díla, které bude řešit v přenesené působnosti obecní úřad obce s rozšířenou působností, v jehož územním obvodu byl přestupek spáchán.¹¹⁶ Trestněprávní odpovědnost dle § 270 TZ pokrývá i odvozená díla, která při tracingu mohou vzniknout, avšak je-li použito prvků obecného fondu z původního díla, tedy není potřeba souhlasu původního autora k takové změně, nejedná se o neoprávněný zásah do práv k původnímu autorskému dílu a nemůže být dovozena trestněprávní odpovědnost.¹¹⁷ *A contrario*, jsou-li využity prvky autorskoprávně individuální a bylo neoprávněně zasaženo nikoli nepatrně, mohlo by se jednat o porušení autorského práva dle TZ.¹¹⁸ Naopak trestněprávní odpovědnost dle § 271 TZ nemůže při tracingu

¹¹² PRCHAL, Petr. *Limity autorskoprávní ochrany*. Praha: Leges, 2016, s. 22.

¹¹³ Ibidem.

¹¹⁴ KOUKAL. *Autorské právo, public domain a lidská práva*, s. 73.

¹¹⁵ § 270, § 271 zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

¹¹⁶ § 105c odst. 1 písm. a) AutZ.

¹¹⁷ Usnesení Nejvyššího soudu ze dne 16. 5. 2007, sp. zn. 5 Tdo 449/2007.

¹¹⁸ Ibidem. K výkladu „*neoprávněný zásah nikoli nepatrný*“ viz Šámal, Pavel. § 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi. In: ŠÁMAL, Pavel et al. *Trestní zákoník. Komentář*. 3. vydání. Praha: C. H. Beck CZ, 2023, s. 3573–3580.

vzniknout, neboť se nejedná o padělek nebo napodobení výtvarného projevu původního autora, který má být „*na místě díla původního a vydáván za originál*“.¹¹⁹ Tracingem je totiž spíše sledována snaha o změnu díla, aby se původnímu dílu natolik nepodobalo, případně není vůbec obvyklé, aby se uváděl autor původního podkladového díla.

4.1 ZASAŽENÁ OSOBNOSTNÍ PRÁVA AUTORSKÁ

Osobnostní práva autorská obecně slouží k udržení spojení mezi autorem a jeho dílem.¹²⁰ I v případě zcizení nebo úmrtí autora je stále, byť omezeně, poskytována ochrana osobnostním právům autorským.¹²¹ Tato práva vyplývají z autora jako středobodu autorského práva, neboť originální filozofická koncepce pobírá dílo jako projev autorovy osobnosti.¹²²

Domnívám se, že v kontextu tracingu bude do osobnostních práv zasaženo vždy, vyjma případů, kdy se nejedná o tracing částí díla obsahující prvky s autorskoprávní individualitou, avšak tyto případy se nezdají být obvyklé.¹²³ Druhou výjimkou jsou pak zákonné výjimky a omezení.¹²⁴

Z výčtu osobnostních práv autora v § 11 AutZ se obecně problematika odvozené tvorby pojí s právem na nedotknutelnost díla. Co se týče dalších osobnostních práv autora, tak k zásahu do práva rozhodnout o zveřejnění díla zpravidla nedochází, neboť se původní díla obvykle vyskytují volně přístupná (např. na internetu), avšak nelze takovou situaci předem vyloučit. K zásahu do práva osobovat si autorství může dojít pouze v případě nenalezení tvůrčí činnosti a autorskoprávně individuálních prvků v díle vytvo-

¹¹⁹ Šámal, Pavel. § 271 Padělání a napodobení díla výtvarného umění. In: ŠÁMAL, Pavel et al. *Trestní zákoník. Komentář*. 3. vydání. Praha: C. H. Beck CZ, 2023, s. 3590.

¹²⁰ BALDWIN, Peter. *The Copyright Wars*. United Kingdom: Princeton University Press, 2014, s. 37.

¹²¹ Ibidem.

¹²² POLČÁK, Radim. § 10 Obsah autorského práva. In: POLČÁK, Radim; KOUKAL, Pavel; LEŠKA, Rudolf; MYŠKA, Matěj; HRABÁNEK Jiří et al. *Autorský zákon: Praktický komentář s judikaturou*. Praha: Leges, 2020, s. 96.

¹²³ Naopak mimo autorské právo by bylo možné se domáhat ochrany i v případě využití části s autorskoprávně volnými prvky z oblasti obecného fondu, které nemohou být autorskoprávně chráněny, a to pomocí všeobecných osobnostních práv. KOUKAL. *Autorské právo, public domain a lidská práva*, s. 454.

¹²⁴ Více o výjimkách a omezeních aplikovatelných pro tracing bude pojednáváno v kapitole 5.

řeném pomocí tracingu, tedy situace, kdy proběhla pouhá netvůrčí změna původního díla.

Právo na nedotknutelnost díla v sobě demonstrativně zahrnuje právo udělit svolení ke změně či jinému zásahu do díla (integrita), právo na užívání díla způsobem nesnižujícím hodnotu díla (dehonestace) a právo na autorský dohled.¹²⁵

Integrita díla je zasažena jak změnou tvůrčí, tak i změnou netvůrčí povahy.¹²⁶ Tracingem, na základě dříve provedené subsumpce, proto bude integrita vždy zasažena, neboť odvozené dílo, tak i jinak změněné dílo, do této definice spadají. Zásahem do integrity se bude nejspíše jednat o změnu obsahu původního díla nebo připojení původního díla (zakomponování) do díla uživatele tracingu.

Dehonestace díla způsobuje snížení hodnoty díla, avšak nejedná se o hodnotu tržní, ale hodnotu uměleckou.¹²⁷ Dehonestace by tak v případě tracingu mohla například nastat, kdyby části původního díla byly zakomponovány v erotické, či dokonce pornografické tvorbě, ale pouze v případě, kdy se samotné původní dílo této tematiky nedotýká.

Autorský dohled spočívá v právu autora dohlížet na jednotlivé osoby, aby využívaly dílo způsobem nesnižující jeho hodnotu.¹²⁸ Je tak právem, vůči předchozím dvěma, komplementárním.

Také tracing volného díla bude mít za následek zásah do osobnostních práv autora, a to dojde-li k osobození autorství díla, užití snižující hodnotu původního díla a neuvedení jména autora je-li to obvyklé, neboť omezená ochrana je autorovi přiznána i *post mortem*.¹²⁹

¹²⁵ TELEČ, Ivo a TŮMA, Pavel. § 11 Osobnostní práva. In: TELEČ, Ivo a TŮMA, Pavel. *Autorský zákon. Komentář*. 2. vydání. Praha: C. H. Beck CZ, 2019, s. 149.

¹²⁶ Ibidem, s. 150.

¹²⁷ TELEČ; TŮMA. § 11 *Osobnostní práva*, s. 152–153.

¹²⁸ Ibidem, s. 154.

¹²⁹ § 28, § 11 odst. 5 AutZ.

4.2 ZASAŽENÁ MAJETKOVÁ PRÁVA AUTORSKÁ

V kontinentálním pojetí jsou majetková práva autora esenciální součástí autorského práva, díky kterým je autor schopen realizovat svou „osobnost a představy o štěstí“.¹³⁰ Majetková práva autora, jako výlučná práva, jsou zdrojem ekonomických příjmů, které pozitivně působí na autorovu možnost kreativního vyjádření nezávisle na vybraných vnějších faktorech. Ústavněprávní základ vlastnictví v čl. 11 Listiny základních práv a svobod zaručuje, aby autorskoprávní ochrana děl nebyla nastavena tak široko, že neumožňuje omezení těchto práv ve prospěch jiných právem chráněných zájmů, a například tak nezpůsobuje vytvoření monopolu a zpomalení vědeckého bádání.¹³¹

Demonstrativní výčet majetkových práv autorských nalezneme v § 12 a násl. AutZ. Právo dílo užít bude tracingem zpravidla vždy zasaženo, ale podoby zásahu se mohou měnit a vzájemně doplňovat vzhledem k situaci, ve které tracing proběhl. Zejména se jedná o právo na rozmnožování díla, právo na rozšiřování rozmnoženiny díla a právo na sdělování díla veřejnosti.

Právo na rozmnožování je zasaženo v každém případě, neboť způsob, jakým je dosažen vznik rozmnoženiny, není relevantní pro posouzení zásahu.¹³² Ať už analogově nebo digitálně, v procesu tracingu vzniká rozmnoženina na hmotném nosiči, přesněji neúplná napodobenina (neidentická rozmnoženina), která je esenciální k jeho dokončení.

Právo na rozšiřování rozmnoženiny díla je zasaženo pouze v souvislosti s převodem vlastnictví k rozmnoženině, který zatím může dosahovat formy nabídky.¹³³ Tracingem je mimo jiné sledován ekonomický zisk, a tak dříve či později vznikne nabídka k převodu práv k dílu vytvořenému pomocí tra-

¹³⁰ KOUKAL. *Autorské právo, public domain a lidská práva*, s. 408.

¹³¹ Čl. 11 ústavního zákon č. 2/1993 Sb., ve znění ústavního zákona č. 162/1998 Sb. a ústavního zákona č. 295/2021 Sb. KOUKAL. *Autorské právo, public domain a lidská práva*, s. 156–157.

¹³² TELEČ; TŮMA. § 13 *Rozmnožování*, s. 181.

¹³³ TELEČ, Ivo a TŮMA, Pavel. § 14 *Rozšiřování*. In: TELEČ, Ivo a TŮMA, Pavel. *Autorský zákon. Komentář*. 2. vydání. Praha: C. H. Beck CZ, 2019, s. 189–190.

cingu. Nabízení děl vytvořených pomocí tracingu k prodeji, například jako potisk na tričko, bude konstituovat zásah do práva na rozšiřování.¹³⁴

Právo na sdělování veřejnosti nemusí být zasaženo v každém případě. Je nutné naplnit pojmové znaky sdělování veřejnosti, tedy sdělení jako „zprostředkování autorských děl bez ohledu na technický prostředek nebo technický proces“ a novou veřejnost jako „veřejnost, již nositel autorského práva nebral v potaz při udělení svolení k prvotnímu sdělení“.¹³⁵ V častých případech, kdy jsou díla vytvořená pomocí tracingu umístěna na internet, je otázkou zásahu do práva na sdělování veřejnosti pouze konstatování nové veřejnosti. Pro tracing původních děl přístupných na internetu nemusí být konstatována nová veřejnost, avšak diferenciací na dílčí oblasti, jako je specifická internetová komiksová série nebo za poplatek přístupná vizuální novela, můžeme dojít k závěru, že se jedná o novou veřejnost i v případě zveřejnění díla vytvořeného pomocí tracingu na internetu.

V případě uplynutí doby trvání výlučných majetkových práv autora je užití díla zjednodušeno, neboť tato díla může každý bez dalšího volně užit.¹³⁶ Ostatně tak i pro tracing, při vzniku odvozeného díla nebo díla jinak změněného, nebude zapotřebí získat svolení k užití volného díla.

5. VÝJIMKY A OMEZENÍ APLIKOVATELNÉ PRO TRACING

Výjimky a omezení autorského práva jsou nezbytné k pokračování další tvorby a kulturního vývoje.¹³⁷ Na druhou stranu však „nesmí nikdy narušit normální využívání díla a působit neospravedlnitelnou újmu oprávněným zájmům autora“, tedy nesmí působit proti smyslu a účelu autorského práva.¹³⁸ Aby byl zachován užitečný účinek výjimek a omezení, musí být výkladem

¹³⁴ Úprava vyčerpání práv na rozšiřování se na tracing v tomto případě neaplikuje, neboť u tracingu se nejedná o oprávněný převod vlastnického práva k originálu nebo rozmnožení a zároveň jde o změnu původní díla, pro kterou se vyčerpání práv k původnímu dílu nebo jeho rozmnožení neaplikuje, viz TELEČ; TŮMA. § 14 Rozšiřování, s. 192–193.

¹³⁵ KOUKAL, Pavel. § 18 Obecná ustanovení. In: POLČÁK, Radim; KOUKAL, Pavel; LEŠKA, Rudolf; MYŠKA, Matěj; HRABÁNEK Jiří et al. *Autorský zákon: Praktický komentář s judikaturou*. Praha: Leges, 2020, s. 141–142.

¹³⁶ § 28 AutZ.

¹³⁷ KNAP. *Quo vadis současného autorského práva*, s. 28.

¹³⁸ Ibidem.

zajištěna přiměřená rovnováha základních práv a zájmů uživatele předmětu autorskopravní ochrany a nositele autorských práv.¹³⁹ Nositeli autorských práv jsou poskytována autorská práva pramenící z jeho základních práv, avšak uživateli tímto způsobem práva poskytována nejsou. Základní práva uživatele jsou totiž ztělesněna ve výjimkách a omezeních autorského práva nositele autorských práv, čímž je možnost hájení základních práv uživatele značně omezena.¹⁴⁰

K uplatnění výjimek a omezení je nutné, aby bylo původní dílo užito. Tracingem vzniká odvozené dílo, a proto dojde k zásahu do práva původního autora dílo užít v jiném zpracované či jinak změněné podobě.¹⁴¹ To znamená, že i v případě, kdy soud vyvrátí přítomnost pojmových znaků autorského díla a vzniklo tak jinak změněné dílo, je aplikace výjimek a omezení stále možná. Také veškerá následující užití díla odvozeného jsou vždy užitím i díla původního.¹⁴² Tato situace bez licence znamená, že jakékoliv užití díla vytvořeného pomocí tracingu je omezené na vůli původního autora. Obdobně jako majetková práva autorská, jsou zasažena i osobnostní práva autorská jako právo na nedotknutelnost díla.¹⁴³ Tracingem jsou tyto obě sféry práv autorských zasaženy, a aby výjimky a omezení byly v tomto případě schopny plnit svůj účel, domnívám se, že je nutné je vykládat tak, že zahrnují jak majetková, tak i osobnostní práva autorská.¹⁴⁴ Dle Myšky se tímto výkladem ale musíme držet limitů v podobě neužívání díla způsobem snižujícím jeho hodnotu a zachováním práva původního autora na osobování si autorství.¹⁴⁵ Zásah do integrity původního díla jeho

¹³⁹ Rozsudek SDEU (velkého senátu) ze dne 29. 7. 2019 ve věci C-469/17, Funke Medien NRW, bod 51, 53.

¹⁴⁰ Ibidem, bod 70.

¹⁴¹ § 12 odst. 1 AutZ.

¹⁴² TELEČ; TŮMA. § 12 *Právo dílo užít*, s. 166.

¹⁴³ Více o zasažených právech autorských viz kapitoly 5.1 a 5.2.

¹⁴⁴ Restriktivní výklad omezený na majetková práva autorská by znamenal, že každé dílo vytvořené pomocí tracingu zasahuje do osobnostních práv autorských a jeho vznik je tak *apriori* protiprávní.

¹⁴⁵ MYŠKA, Matěj. *Výjimky a omezení autorského práva v prostředí digitálních sítí*. Praha: Wolters Kluwer ČR, 2020, s. 61. Konkrétním případem, kdy se například jedná o užití díla způsobem snižujícím jeho hodnotu, může být tvorba děl vytvořených pomocí tracingu s pornografickým obsahem za podmínky, že původní dílo nesdílí stejnou tematiku.

změnou, například kolorováním v případech, kdy byl původním černobílým vyjádřením sledován umělecký účel, by se tímto výkladem překlenul.¹⁴⁶

Před využitím kterýchkoliv výjimek a omezení musí obecně dojít k aplikaci tříkrokového testu.¹⁴⁷ I pro případ, kdyby vznik díla vytvořeného pomocí tracingu pojmově spadal pod některou zákonnou výjimku a omezení, musí být splněn tříkrokový test, aby se předešlo zásahu do autorského práva původního autora. Musí zde tedy existovat zákonná licence, dále musí být splněna podmínka neexistence rozporu s běžným užitím díla a oprávněné zájmy původního autora nesmějí být nepřiměřeně dotčeny.

Běžným užitím díla je sledován hospodářský zisk nositele autorských práv a rozpor je myšlena alespoň potenciální ztráta tohoto zisku.¹⁴⁸ Podíváme-li se, na kterém trhu se dílo vytvořené pomocí tracingu a původní dílo nacházejí, zjistíme, že se většině případů bude jednat o trh totožný. I kdybychom například trh s ilustracemi dále diferencovali přes jednotlivé styly na jejich žánry až do ilustrací pro specifickou videohru, můžeme získat velmi odlišené trhy, avšak potenciální ztráta autora původní ilustrace stále není vyloučena. Na druhou stranu, čím větší podobnosti mezi díly jsou, tím spíše spolu budou soupeřit na totožném trhu, a tím větší rozpor s běžným užitím díla je možné vysledovat. Ke druhému kroku lze uzavřít, že dokud bude tříkrokový test takto nastaven anebo dokud nevznikne trh pro díla vytvořené pomocí tracingu, jako zvláštní trh s odvozenou tvorbou, bude pro tracing velice obtížné splnit druhý krok testu.¹⁴⁹

Oprávněné zájmy reflektují proporcionalitu zásahu, tedy aby zásah byl ve svém rozsahu odůvodněný a ospravedlnitelný vůči zájmům nositele práv.¹⁵⁰ Zájmy, které tracing reflektuje, jsou sociální a ekonomické zájmy uživatele tracingu, ale domnívám se, že mohou být reflektovány i zájmy

¹⁴⁶ GINSBURG, Jane C. a SIRINELLI, Pierre. Authors and Exploitations in International Private Law: The French Supreme Court and the Hustt and the Huston Film Colorization Contron Film Colorization Controversy. *Columbia-VLA Journal of Law & The Arts*. [online]. 1991, roč. 15, [cit. 10. 1. 2025], s. 154.

¹⁴⁷ § 29 odst. 1 AutZ.

¹⁴⁸ MYŠKA. *Výjimky a omezení autorského práva v prostředí digitálních sítí*, s. 70.

¹⁴⁹ Příkladem takového zvláštního trhu s odvozenou tvorbou může být trh s dódžinši, více viz kapitola 2.2.4.

¹⁵⁰ MYŠKA. *Výjimky a omezení autorského práva v prostředí digitálních sítí*, s. 71.

části společnosti jako takové. Tato tvorba odvozených děl totiž může být k prospěchu například spotřebiteli, který bude mít díky nižší nákladovosti tracingu přístup k většímu množství uměleckých děl ve formě komiksů. Tracingem také mohou vzniknout například ilustrované části nové videohry, což případně usnadní nebo urychlí proces videoherního vývoje. Pokud bychom tedy reflektovali i oprávněné zájmy třetích osob, případně kdybychom byli schopni nositelům práv efektivně poskytnout finanční náhradu, tak by tracing, jako způsob vytváření odvození tvorby, byl schopen splnit třetí krok testu.¹⁵¹ Avšak, jak bylo již zmíněno, je nepravděpodobné, že bychom se dostali až ke třetímu kroku, a to zásluhou pro tracing velice obtížného druhého kroku.

Tracing není nikde v zákoně výslovně upraven, což může zapříčinit značnou právní nejistotu ohledně jeho právní povahy. Domnívám se, že tracing, jako způsob vytváření odvozené tvorby, by za určitých podmínek mohl nalézt své místo v právní úpravě za pomoci aplikace výjimek a omezení. Avšak samozřejmě tento postup není vhodný pro každý tracing, neboť je z povahy této činnosti zřejmé, že se okolnosti případů liší, a tak i právní (a morální) posouzení tracingu. Počínaje úmyslem uživatele tracingu a sledováním jeho tvůrčí činnosti v zakomponování převzatých prvků, přes samotnou povahu těchto prvků (autorskoprávně individuální a obecného fondu), konče autorskoprávní kvalifikací díla vytvořeného pomocí tracingu obsahující jak převzaté, tak i vlastní prvky uživatele tracingu, se případ od případu liší. Jsme-li pak schopni rozlišit „negativní“ tracing, který pouze „parazituje“ na původním autorovi a „pozitivní“ tracing, který „přináší něco více“, získáme typ tracingu, který je vhodným adeptem pro aplikaci výjimek a omezení. Na základě těchto poznatků se domnívám, že v kontextu „pozitivního“ tracingu je vhodné prozkoumat zákonné licence AutZ v podobě citace, parodie a pastiše.¹⁵²

¹⁵¹ Čl 5.5 European Copyright Code. In: *The Institute for Information Law*. [online]. 2010. [cit. 11. 2. 2025]. Dostupné z: <https://www.ivir.nl/projects/copyrightcode/european-copyright-code/>

¹⁵² Oproti vyjmenovaným zákonným licencím se například volné užití díla pro osobní potřebu nebo nepodstatné vedlejší užití díla ve skutkové podstatě liší vůči pojmovým znakům tracingu. Stejně tak absence vědomí, tedy i souhlasu, původního autora o provedení tracingu vylučuje uzavření licence mezi stranami.

5.1 CITACE

První, ač na první pohled téměř neaplikovatelná zákonná licence, je citace.¹⁵³ Dle definice citace, jako autonomního pojmu unijního práva, je tato výjimka a omezení obecně aplikovatelná na tradiční díla, avšak za splnění poměrně nejasných podmínek SDEU zcela nevyloučil aplikaci citace v případě *samplingu*.¹⁵⁴ Jak již bylo dříve zmíněno, tracing a *sampling* vykazují paralely, jak po právní stránce kvalifikace, tak i po stránce svých pojmových znaků, které by mohly zapříčinit i obdobnou aplikaci práva.¹⁵⁵

Citace je použití části původního díla (i) k názornému dokreslení určitých výroku, obhájení určitého názoru nebo k intelektuální konfrontaci s dílem původním a těmito výroky, které doprovází (ii) záměr o zahájení interakce (*intention of entering into dialogue*) s původním dílem.¹⁵⁶ Není-li možné původní dílo rozeznat z díla, na které má být aplikována citace, nemůže ani dojít k této interakci.¹⁵⁷ Dále je nutné, aby bylo (iii) původní citované dílo oprávněně zpřístupněno veřejnosti, (iv) aby v novém díle byl uveden zdroj se jménem původního autora, přičemž užití nového díla musí být v (v) souladu s poctivými zvyklostmi a za sledováním konkrétního účelu, tedy pouze to, co je nezbytné k dosažení cíle citace.¹⁵⁸ Obě díla musí mezi sebou mít přímou a úzkou vazbu, aby došlo k dosažení cíle v podobě zejména kritiky nebo recenze, přičemž není nutné, aby díla v sobě byla neoddělitelně začleněna.¹⁵⁹

S tracingem narazíme hned na pár větší překážek, jako je cíl citace a soulad s poctivými zvyky, a menších překážek, jako je záměr o zahájení

¹⁵³ § 31 AutZ.

¹⁵⁴ Rozsudek SDEU (velkého senátu) ze dne 29. 7. 2019 ve věci C 476/17, Pelham I, bod 68, 72.

¹⁵⁵ Více o *samplingu* viz kapitola 2.2.3.

¹⁵⁶ Rozsudek SDEU (velkého senátu) ze dne 29. 7. 2019 ve věci C 476/17, Pelham I, bod 71.

¹⁵⁷ Ibidem, bod 73, 74. Na druhou stranu z případu řešícího *sampling* dále vyplývá, že není-li možné při poslechu rozpoznat pozměněné části původní díla v novém díle, nejedná se o rozmnožování, viz rozsudek SDEU (velkého senátu) ze dne 29. 7. 2019 ve věci C 476/17, Pelham I, bod 31.

¹⁵⁸ Ibidem, bod 67, 69.

¹⁵⁹ Rozsudek SDEU (velkého senátu) ze dne 29. 7. 2019 ve věci C 516/17, Spiegel Online, bod 79, 80.

interakce s původním dílem a uvedení zdrojového díla. V článku vyličený tracing přímo nesleduje stejný cíl jako citace, avšak takový případ není z povahy vyloučen. Také hodnocení souladu s poctivými zvyky je složité, neboť obdobná praxe (případy tracingu) se obvykle nevyskytuje a analogické hodnocení tracingu na obecném základě odvozené tvorby nemusí mít správný výsledek. Domnívám se, že právě posuzování a poměřování práv a zájmů původního autora s právy a zájmy uživatele tracingu je ale základním bodem pro aplikaci výjimek a omezení. Sleduje-li vágní pojem „záměr o zahájení interakce s původním dílem“ subjektivní pohled uživatele tracingu, tak potvrzení i vyvrácení tohoto záměru bude složité, a to i v případě, že je možné původní dílo rozeznat. Uvedení zdrojového díla u děl vytvořených pomocí tracingu by mohlo nabírat neobvyklých podob, neboť se jedná o uměleckou tvorbu. Autor původního díla by v tomto případě mohl být implicitně uveden skrze možnost rozpoznání jeho díla v díle vytvořeném pomocí tracingu, a to z převzatých částí.

Tyto poměrně složité podmínky pro aplikaci citace pro netradiční díla mohou svojí vágností zapříčinit interpretační potíže pro soudy.¹⁶⁰ Přidáme-li dokazování, můžeme se dostat se do sféry časově a finančně náročných soudních sporů, jejichž rozhodnutí nemusí být právně uspokojivá a zapříčiní tak pokles právní jistoty v otázce aplikace citace jako výjimky a omezení autorského práva. Domnívám se ale, že by tímto údělem bylo možné najít interpretaci soudu, která je schopna dát prostor pro aplikaci zákonné licence na citaci pro tracing. Pomineme-li tuto zanedbatelnou šanci, je z výše uvedených důvodů aplikace zákonné licence v podobě citace pro tracing nevhodná.

5.2 PARODIE

Další možnou aplikovatelnou zákonnou licencí je parodie (a karikatura). Ačkoliv je parodie obsažena ve stejném paragrafu jako pastiš, obě zákonné

¹⁶⁰ JÜTTE, Bernd Justin a QUINTAIS, João Pedro. The Pelham Chronicles: sampling, copyright and fundamental rights. *Journal of Intellectual Property Law & Practice*. [online]. 2021, č. 3, [cit. 15. 2. 2025], s. 220.

licence se od sebe svojí definicí mohou lišit, a proto jsou analyzovány samostatně.¹⁶¹

Parodie, jako autonomní pojem unijního práva, byla již závazně interpretována SDEU.¹⁶² Parodie musí být interpretována ve svém obvyklém smyslu, který určuje její podstatné znaky, jakožto (i) evokování již existujícího díla, přičemž se díla navzájem zřetelně liší, a (ii) komičnost nebo ironii.¹⁶³ Parodie dokonce nemusí vykazovat „původní osobitost“, neboť stačí zřetelného odlišení od parodovaného původního díla.¹⁶⁴

Právo duševního vlastnictví není právem nedotknutelným, a proto je také možné, aby autorské právo bylo omezeno základními právy (právem na svobodu projevu) v podobě výjimek a omezení.¹⁶⁵ Interpretace výjimek a omezení musí být restriktivní, přičemž zachovává užitečný účinek a úplný soulad se základními právy.¹⁶⁶ Pro oprávněnou parodii musí být *ad hoc* respektována přiměřená rovnováha mezi právy a zájmy zúčastněných stran s přihlédnutím ke všem okolnostem případu, v tomto případě práva a zájmy původního nositele autorských práv a svoboda projevu autora parodie.¹⁶⁷

V díle vytvořeném pomocí tracingu je možné spatřit prvky původního díla, a tak ho i evokovat, ale není to vždy jednoduché, zejména pokud se uživatel tracingu snaží tento fakt skrýt. Zřetelné odlišení obou děl pak lze spatřit ve faktu, že tracingem jsou převzaty pouze vybrané prvky, přičemž zbytek díla je vlastním počínáním dotvořen. Problematická je podmínka komičnosti nebo ironie, avšak pro aplikaci parodie není podstatné, zda bylo skutečně dosaženo tohoto účelu.¹⁶⁸ Je možné si představit, že by touto interpretací bylo možné překlenout požadavek komičnosti nebo ironie

¹⁶¹ § 38g AutZ.

¹⁶² Rozsudek SDEU (velkého senátu) ze dne 3. 9. 2014 ve věci C 201/13, Deckmyn and Vrijheidsfonds.

¹⁶³ Ibidem, bod 20.

¹⁶⁴ Ibidem, bod 21.

¹⁶⁵ Rozsudek SDEU (velkého senátu) ze dne 29. 7. 2019 ve věci C-469/17, Funke Medien NRW, bod 70–72.

¹⁶⁶ Ibidem, bod 69, 76.

¹⁶⁷ Rozsudek SDEU (velkého senátu) ze dne 3. 9. 2014 ve věci C-201/13, Deckmyn and Vrijheidsfonds, bod 27, 28.

¹⁶⁸ Rozsudek Nejvyššího soudu ze dne 28. 7. 2023, sp. zn. 23 Cdo 2178/2022, bod 62.

s odkazem na osobitý styl humoru uživatele tracingu, který zapříčinil, že reálně nebylo cíleného účelu dosaženo. Domnívám se ale, že by tento argument byl při dokazování poměrně rychle vyvrácen s odkazem například na výdělečnou povahu díla vytvořeného pomocí tracingu. Na druhou stranu, rozhodujícím při aplikaci parodie je tvůrčí záměr ve ztvárnění původního díla směřující k „*myšlenkovému vymezení se vůči obsahové či formální podstatě původního díla*“.¹⁶⁹ Zvratným bodem soudního řízení zabývajícího se aplikací parodie pro tracing by totiž bylo prokázání tohoto myšlenkového vymezení, neboť uživatel tracingu se vůči původnímu dílu nevymezuje, ale spíše se s dílem (jeho vybranými prvky) ztotožňuje. Proto se obecně domnívám, že až na výjimečné případy, kdy je tracingem opravdu sledován komický nebo ironický účel, není vhodné pro tracing aplikovat zákonnou licenci na parodii.¹⁷⁰

5.3 PASTIŠ

Poslední, ale nejvíce pravděpodobná varianta zákonné licence aplikovatelné pro tracing, je pastiš. V České republice se jedná o stále poměrně novou zákonnou licenci, která byla zavedena novelou AutZ z roku 2023, a protože její limity ještě nejsou plně prozkoumány, je vhodné zvážit právě možnost aplikace pastiše pro tracing.¹⁷¹

Pastiš je autonomní pojem unijního práva, avšak jeho definice nebyla unijním právem stanovena a také nebyla doposud SDEU závazně interpretována. Pro SDEU je v takových případech typický teleologický výklad, tedy výklad sledující cíl a záměr se zaměřením na užitečnost a efektivnost právní úpravy, díky čemuž je SDEU schopen odpovídat na dynamický roz-

¹⁶⁹ Rozsudek Nejvyššího soudu ze dne 28. 7. 2023, sp. zn. 23 Cdo 2178/2022, bod 62.

¹⁷⁰ Typickým příkladem mohou být tzv. *easter eggs*, což jsou nenápadné přímé nebo nepřímé odkazy různých podob na autory anebo jejich díla (například *creeper* a bloky z videohry *Minecraft* ukryty v dolech ve videohře *Borderlands 2*), které videoherní vývojáři umísťují do svých videoher pro jejich hráče, a to například k jejich pobavení nebo k navýšení jejich zájmu o videohru samotnou. Je možné se setkat i s takovými, které spíše plní funkci pocty (*hommage*) původnímu autorovi anebo jeho dílu, avšak ty se svojí podstatou blíží spíše pastiši.

¹⁷¹ § 38g AutZ.

voj unijního práva.¹⁷² Teleologický výklad společně s jazykovým výkladem pak tvoří základ pro odpověď na interpretační otázky vyvstávající z unijního práva, ke kterým ještě nebyla závazně stanovena definice.¹⁷³ Pastiš proto musí být jako pojem vykládán „v souladu s jeho obvyklým smyslem v běžném jazyce, s přihlédnutím ke kontextu, ve kterém je použit, a cílům, které sleduje právní úprava, jejíž je součástí“.¹⁷⁴

Definice pastíše byla historicky proměnlivá a jeho zákonná úprava pochází z Itálie a Francie.¹⁷⁵ Dnes se v běžném českém jazyce s pastišem setkáváme jako s napodobeninou stylu díla s možností přebrání nebo nepřebrání prvků tohoto díla, nebo přímo napodobením autora.¹⁷⁶ Dle důvodové zprávy je pastiš způsob uměleckého vyjádření, který je často přítomný v *online* prostředí na službách pro sdílení obsahu uživateli, kteří na těchto službách svá díla zveřejňují (*user-generated content*).¹⁷⁷ Poslední složkou k výkladu je cíl právní úpravy, kterým je snaha o zaručení svobody projevu uživatelů služeb pro sdílení obsahu *online*, zahrnující svobodu uměleckého projevu.¹⁷⁸

¹⁷² SEHNÁLEK, David; TÝČ, Vladimír et al. *Soudní dvůr EU a výklad práva Evropské unie*. 1. vydání. Brno: Masarykova univerzita, 2016, s. 106.

¹⁷³ Například rozsudek SDEU (velkého senátu) ze dne 3. 9. 2014 ve věci C-201/13, Deckmyn and Vrijheidsfonds, bod 19.

¹⁷⁴ Rozsudek SDEU (velkého senátu) ze dne 29. 7. 2019 ve věci C 476/17, Pelham I, bod 28, 70.

¹⁷⁵ MEZEI; JÜTTE; SGANGA; PASCAULT. *Oops, i Sampled Again ... the Meaning of "Pastiche" as an Autonomous Concept Under EU Copyright Law*, s. 1231–1233 [online].

¹⁷⁶ CHALOUPOKOVÁ, Helena a HOLÝ, Petr. § 38g Licence pro karikaturu, parodii nebo pastiš. In: CHALOUPOKOVÁ, Helena a HOLÝ, Petr. *Autorský zákon. Komentář*. 6. vydání. Praha: C. H. Beck CZ, 2023, s. 128.

¹⁷⁷ POSLANECKÁ SNĚMOVNA, 9. volební období, 2021, sněmovní tisk 31/0, 25. 10. 2021. Důvodová zpráva k vládnímu návrhu zákona o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, a další související zákony. In: *Poslanecká sněmovna Parlamentu České republiky*. [online]. 2021. [cit. 9. 2. 2025]. Dostupné z: <https://www.psp.cz/sqw/text/orig2.sqw?idd=199904>

¹⁷⁸ Bod 70 recitálu směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES. Obdobně bod 3 recitálu směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti.

Pro aplikaci pastíše bychom museli začít tracing brát jako zákonem nepojmenovaný způsob uměleckého vyjádření, což avšak není nemyslitelný závěr. Tracingem dojde k převzetí prvků původního díla, což znamená, že výsledné dílo vytvořené pomocí tracingu bude stylově podobné dílu původnímu (tracingem ilustrace stylu manga vznikne nová ilustrace stylu manga). Domnívám se, že tracing, na základě svých pojmových znaků, splňuje definici pastíše v běžném jazyce. Pokud tracing dokážeme interpretovat tak, že jeho uživatel uplatňuje své právo na svobodu uměleckého projevu, jakožto součást svobody projevu, je možné argumentovat splněním podmínek pro aplikaci pastíše. Avšak tento závěr o svobodě uměleckého projevu nemusí být shledán dostatečným k následování cílů právní úpravy. Odpověď na tento problém aplikace pastíše může obsahovat očekávané rozhodnutí SDEU.¹⁷⁹

Aktuálně před SDEU leží předběžná otázka zabývající se problematikou pastíše v případě *samplingu*.¹⁸⁰ Přesněji se první otázka týká existence limitů pastíše, tedy jestli musí být například komický, napodobovat styl nebo vzdávat poctu, a povahu pastíše, tedy je-li schopen být univerzálním ustanovením alespoň pro umělecké zapojení do již existujícího díla nebo jiného předmětu.¹⁸¹ Autonomní výklad tohoto pojmu je schopen změnit definice napříč všemi členskými státy, a to buď k lepšímu nebo horšímu. „Ustálená“ česká definice, podle které bychom mohli uvažovat o aplikaci pastíše pro tracing, může být rozhodnutím SDEU natolik změněna, že nebude možné o jeho aplikaci vůbec uvažovat. *European Copyright Society* podala k tomuto případu svůj názor, který říká, že pastiš (i) nemůže být omezen na pouhé napodobení stylu (prvek obecného fondu), (ii) neměl by vyžadovat explicitní interakci s původním dílem, (iii) neměl by být limitován na komické ztvárnění a (iv) nemusí být autorskoprávně individuální (*original*), ale ke své oprávněnosti musí obsahovat zřetelně odlišitelné převládající rysy od původního díla.¹⁸² Zároveň by pak jako „pružná limitace“ fungoval tříkrokový test, který by poměřoval kolidující zájmy v podobě zá-

¹⁷⁹ Žádost o rozhodnutí o předběžné otázce ze dne 25. 9. 2023 ve věci C-590/23, Pelham II.

¹⁸⁰ Ibidem.

¹⁸¹ Ibidem.

kladních práv.¹⁸³ Konečně zde nemusí být ani úmysl osoby pastiš vytvořit pro jeho aplikaci.¹⁸⁴ Názor *European Copyright Society* vychází z předchozích rozhodnutí SDEU, zejména *Pelham I* a *Deckmyn*, z důvodu, aby byla zachována rozhodovací praxe, ale aby na druhou stranu došlo k posílení práva na svobodu projevu a svobodu informací.¹⁸⁵ Vytvoření širokého pojetí pastíše pro různé tvůrčí „remixy“ jako „catch-all“ výjimka a omezení by mohlo být základem pro nalezení rovnováhy mezi právem na svobodu projevu tvůrčího uživatele a právem k duševnímu vlastnictví nositele autorských práv.¹⁸⁶

Takový pastiš by byl velice flexibilní výjimkou a omezením, která se vymyká pohledu SDEU, který je vykládá restriktivně. V důsledku nesouladu s rozhodnutím SDEU již dříve došlo ke zrušení § 24 německého autorského zákona (novelou ze dne 7. 6. 2021), který obsahoval výjimku a omezení jako otevřenou normu nazvanou „free use“ (*freie Benutzung*), která odporovala taxativnímu výčtu z čl. 5 směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti, protože by mohla narušit právní rovnováhu stanovenou taxativním výčtem výjimek a omezení vedoucím k narušení harmonizace unijního práva a právní jistoty.¹⁸⁷ Tato „free use“ norma umožňovala tvorbu nových nezávislých děl za

¹⁸² MEZEI, Péter; SENFTLEBEN, Martin; SGANGA, Caterina; GEIGER, Christophe. Opinion of the European Copyright Society on the Scope of the Pastiche Exception in EU Copyright Law (CG and YN v Pelham GmbH and Others, Case C-590/23). *International Review of Intellectual Property and Competition Law*. [online]. 2025, roč. 56, [cit. 20. 2. 2025], s. 8–9.

¹⁸³ Ibidem, s. 12.

¹⁸⁴ Ibidem.

¹⁸⁵ MEZEI; SENFTLEBEN; SGANGA; GEIGER. *Opinion of the European Copyright Society on the Scope of the Pastiche Exception in EU Copyright Law (CG and YN v Pelham GmbH and Others, Case C-590/23)*, s. 12 [online].

¹⁸⁶ Ibidem.

¹⁸⁷ § 24 Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Artikel 28 des Gesetzes vom 23. Oktober 2024 (BGBl. 2024 I Nr. 323) geändert worden ist. QUINTAIS, João Pedro a JÜTTE, Bernd Justin. Sample, sample in my song, can they tell where you are from? The Pelham judgment – Part II. In: *Kluwer Copyright Blog*. [online]. 2019. [cit. 28. 2. 2025]. Dostupné z: <https://copyrightblog.kluweriplaw.com/2019/11/19/sample-sample-in-my-song-can-they-tell-where-you-are-from-the-pelham-judgment-part-ii/>

„volného užití“ autorskoprávně chráněných děl uživateli.¹⁸⁸ Naproti tomu, že toto ustanovení bylo zrušeno, je názor *European Copyright Society* o pastiši svým reálným dopadem podobný této otevřené normě. Rozhodne-li SDEU v podobném duchu o interpretaci pastíše, jakého je názoru *European Copyright Society*, stane se pastiš přímo aplikovatelnou výjimkou a omezením pro tracing za předpokladu splnění tříkrokového testu.¹⁸⁹ Domnívám se, že v opačném případě, kdyby žádná z analyzovaných výjimek a omezení nebyla aplikovatelná pro tracing, je jednou z možností, jak tracing užívat oprávněně, zavedení nové výjimky a omezení, jejíž opodstatněním se bude zabývat následující kapitola.

6. DE LEGE FERENDA

Tracing je způsob vytváření odvozené tvorby netradičním způsobem, což způsobuje komplikace v jeho právním posouzení, od klasifikace tracingu jako činnosti, díla vytvořeného pomocí tracingu, práv tracingem zasažených až po aplikovatelné výjimky a omezení rezonující svobodu projevu. Článek na tyto vybrané autorskoprávní otázky poukázal a poskytnul na ně odpovědi, avšak v otázce aplikace výjimek a omezení pro tracing nemusí být řešení konečné, dokud se zákonodárce nerozhodne tracing výslovně právně regulovat nebo se závazné interpretace aplikovatelných výjimek a omezení pro tracing neujme soud. Na základě veškerých doposud učiněných poznatků o tracingu se domnívám, že bychom měli zvážit změnu právního pohledu na netradiční odvozenou tvorbu, jakou je právě tracing.

Právě zákonem nepojmenovaná odvozená tvorba, jakou je například *appropriation art* nebo *sampling*, vyvolává řadu právních i morálních otázek a způsobuje tak různé náhledy společnosti na oprávněnost nebo pro-

¹⁸⁸ Ibidem. V případě *samplingu* mohlo dojít k využití již zrušeného § 24 německého autorského zákona pouze v případě, kdy *sample* nemohl být uživatelem reprodukován, tedy kdy se nejednalo o pouhé ulehčení práce, viz MEZEL; JÜTTE; SGANGA; PASCAULT. *Oops, i Sampled Again ... the Meaning of "Pastiche" as an Autonomous Concept Under EU Copyright Law*, s. 1228 [online].

¹⁸⁹ Naopak právní názor generálního advokáta Nicholase Emilioua se spíše odklání od vymezení pastíše *Copyright Society* a zaujímá více restriktivní výklad oproti jejich „catch-all“ výjimce a omezení, viz stanovisko generálního advokáta Nicholase Emilioua ze dne 17. 6. 2025 ve věci C-590/23, *Pelham II*, bod 47, 48.

tiprávnost, společně s řešením tohoto fenoménu.¹⁹⁰ Hledáme-li rovnováhu autorského práva v době digitální, kdy se *prosumer* dostává do popředí autorské tvorby, domnívám se, že je nutné se tomuto faktu přizpůsobit a nebránit se netradičním způsobům odvozené tvorby, ale přijmout je.¹⁹¹ Tento přístup je dále vhodný, neboť se tak zvyšuje právní jistota nejen v otázce tracingu, ale i netradičního způsobu odvozené tvorby. Samozřejmě takové řešení neznamená vyloučení veškeré odpovědnosti uživatele tracingu za újmu původnímu autorovi, ale spíše by takové řešení mělo vést k podpoření tvorby obou autorů, přičemž se prospěch (finanční, ale i jiný) uživatele tracingu musí nějakým způsobem proporcionálně projevit i ve sféře původního autora.

Netradiční odvozená tvorba se právě nachází v pozici, kdy SDEU řeší aplikaci poslední možné výjimky a omezení pro případ *samplingu* v podobě pastíše.¹⁹² V případě kladného rozhodnutí bychom mohli uvažovat o aplikaci pastíše pro tracing.¹⁹³ Na druhou stranu je velmi nepravděpodobné, že by tracing prošel druhým a třetím krokem tříkrokového testu. Ke splnění tříkrokového testu by musela být změněna jeho interpretace tak, aby poskytnutí kompenzace nositeli autorských práv mohlo vést ke splnění testu, a zároveň byl brán ohled i na třetí osoby a jednotlivé kroky testu by byly posuzovány paralelně. Avšak tato situace se jeví velmi nepravděpodobnou, neboť by muselo dojít ke změně autorského práva na mezinárodní úrovni, k čemuž je zapotřebí nalézt širokou shodu mezi různě politicky orientovanými smluvními stranami mezinárodních autorskoprávních smluv obsahujících tříkrokový test.

Z výše uvedených důvodů je nevyhnutelně zapotřebí razantní změna nejen zákona, ale i smýšlení o (netradiční) odvozené tvorbě.¹⁹⁴ Spouštěčem změn obdobného měřítka může být pro autorské právo (nejen unijní) výzva

¹⁹⁰ HAZUCHA. *Pop art z pohledu autorského práva*, s. 386–388.

¹⁹¹ Více o pojmu *prosumer* viz TOFFLER. *The Third Wave*, s. 282.

¹⁹² Žádost o rozhodnutí o předběžné otázce ze dne 25. 9. 2023 ve věci C-590/23, Pelham II.

¹⁹³ Více o aplikaci pastíše pro tracing viz kapitola 5.3.

¹⁹⁴ Obdobně o aktuálním problému autorského práva hovoří i generální advokát Nicholas Emiliou, viz stanovisko generálního advokáta Nicholase Emilioua ze dne 17. 6. 2025 ve věci C-590/23, Pelham II, bod 130–133.

jménem generativní AI.¹⁹⁵ Není tak možné vyloučit další budoucí změny ve sféře autorského práva svojí modernizací, či dopady řešení týkající se generativní AI na odvozenou tvorbu.¹⁹⁶

Neodmyslitelnou součástí řešení je nalezení proporcionality mezi základními právy obou stran, která se projevují v autorském právu. Na jedné straně stojí vlastnické právo nositele autorských práv, na druhé straně stojí právo na svobodu projevu uživatele tracingu. Avšak k uplatnění svého práva na svobodu projevu při tracingu je možné využít pouze taxativně stanovené výjimky a omezení, které ještě navíc musí projít tříkrokovým testem, což může způsobovat omezení tohoto základního práva.¹⁹⁷ K dosažení rovnováhy na obou stranách by mohlo posloužit zavedení výjimky a omezení s reinterpetací tříkrokového testu, které tak přímo dovolí hájit základní práva uživatele tracingu. Dále představené navrhované řešení pro tracing v podobě výjimky a omezení přibližuje principy, na kterých se domnívám, že by tato právní úprava mohla stát.¹⁹⁸

6.1 ZÁKONNÁ LICENCE PRO TRACING

Zákonná licence pro tracing, obecně jako zákonná licence pro netradiční způsoby odvozené tvorby, jakými jsou například *appropriation art*, *sampling* nebo tracing, by mohla být výhodná pro všechny zúčastněné strany, avšak

¹⁹⁵ SENFTLEBEN, Martin. The Unproductive “Overconstitutionalization” of EU Copyright and Trademark Law – Fundamental Rights Rhetoric and Reality in CJEU Jurisprudence. *International Review of Intellectual Property and Competition Law*. [online]. 2024, roč. 55, [cit. 18. 2. 2025], s. 1507.

¹⁹⁶ Generativní AI by mohla sloužit jako nástroj uživatele tracingu, který může převzít nebo i vybrat prvky původního díla, které by následně také mohl zakomponovat do nového díla, což by v konečném důsledku mělo vliv na kvalifikaci díla vytvořeného pomocí tracingu, neboť by se tímto užitím omezoval prostor pro tvůrčí činnost při tracingu.

¹⁹⁷ SENFTLEBEN. *The Unproductive “Overconstitutionalization” of EU Copyright and Trademark Law – Fundamental Rights Rhetoric and Reality in CJEU Jurisprudence*, s. 1504–1505 [online].

¹⁹⁸ Domnívám se, že využití veřejných licencí typu *Creative Commons* není vhodné, neboť tracing ze své skutkové podstaty probíhá bez vědomí původního autora, tedy řešením této situace není získ explicitního souhlasu původního autora, který tyto licence poskytuje. Pouze při překročení rozsahu zákonné licence by souhlas původního autora mohl nahrazovat potřebné oprávnění, viz MYŠKA, Matěj; POLČÁK, Radim; ŠAVELKA, Jaromír; KYNCL, Libor; SVIRÁKOVÁ Iveta. *Veřejné licence v České republice*. verze 2.0. Brno: Masarykova univerzita, 2014, s. 139–140.

za splnění určitých zákonem stanovených podmínek.¹⁹⁹ Tato výjimka a omezení by mohla fungovat na modelu *liability rules*, který oslabuje roli absolutních práv nositele autorských práva, za kterou je mu ale poskytnuta náhrada, ve prospěch uživatele.²⁰⁰ K aplikaci musíme být schopni určit, že se opravdu jedná o odvozenou tvorbu vykazující tvůrčí činnost a autorskoprávní individualitu, jejíž výsledkem je autorské dílo. Dále musíme být schopni proporcionálně, vůči zisku uživatele tracingu, odměnit původního autora nebo prokázat přímý či nepřímý prospěch v jeho sféře. Tato výjimka a omezení by musela být zakotvena na unijní úrovni, neboť by její zavedení pouze v jednom členském státě mohlo dopadnout stejně jako dříve zmíněný § 24 německého autorského zákona, který odporoval taxativnímu výčtu výjimek a omezení v unijním autorském právu a obecně harmonizaci unijního práva, což nakonec vedlo k jeho zrušení. Konečně pak pro aplikaci výjimek a omezení, je nutné splnit i tříkrokový test.

Určení, že dílo vytvořené pomocí tracingu je autorským dílem, je přímočaré a vychází z analýzy převzatých a vlastních prvků díla, kde je zejména sledována autorskoprávní individualita. Soud dojde ke svému závěru na základě znaleckých posudků, které také mohou využít metodu přeložení děl k zjištění překryvu jejich linek.²⁰¹

Navrhovaná výjimka a omezení by ve své úpravě měla explicitně obsahovat povinnost poskytnout proporcionální odměnu původnímu autorovi od uživatele tracingu k aplikaci tohoto ustanovení.²⁰² Určení této proporcionální odměny by mohlo fungovat obdobně jako u mechanismu práva odměny při opětném prodeji originálu díla uměleckého, avšak s odlišnými para-

¹⁹⁹ Zařazení taxativně vymezené netradiční odvozené tvorby přímo do textu zákona by sice mohlo zvýšit právní jistotu, ale z povahy změny technologií a umění to není vhodné řešení. Více o *appropriation art* a *samplingu* viz kapitoly 2.2.1 a 2.2.3.

²⁰⁰ WOZNICA, Ondřej. Control or Compensation: Distorted Narrative and Aftermath of Article 17 CDSM. *GRUR International*. [online]. 2024, roč. 73, č. 7, [cit. 4. 3. 2025], s. 633.

²⁰¹ Domnívám se, že právě tato metoda může být nápomocná při kvalifikaci díla vytvořeného pomocí tracingu, a to za předpokladu, že dílo poskytuje alespoň malou možnost pro tvůrčí vyjádření autora v jeho svobodných rozhodnutích. Vyfiltrujeme-li všechny části, které jsou převzaté z původního díla (překrývající se části), zbude pouze vlastní část vytvořená uživatelem tracingu. V návaznosti na povaze vlastních prvků, tedy prvků obsahujících autorskoprávní individualitu a prvků obecného fondu, můžeme dílo vytvořené pomocí tracingu kvalifikovat. Příklady překrývání linek viz Obr. 1., Obr. 2., Obr. 3.

metry v podobě veškerého komerčního nakládání.²⁰³ Stejně tak by důležitou roli hrál kolektivní správce, který by se těmito odměnami zabýval.²⁰⁴ V zásadě by se pak jednalo o stejný mechanismus práva na odměnu jako je u zákonné licence týkající se užití zvukového záznamu uměleckého výkonu vydaného k obchodním účelům bez svolení výkonného umělce v § 72 AutZ, která stanoví výkon tohoto práva pouze prostřednictvím kolektivního správce.²⁰⁵ Stanovení odměny by mohlo probíhat na základě obdobných sazeb jako v příloze č. 1 AutZ určujících pevně stanovené odměny nebo *ad hoc* odměn určených na základě zjevného nepoměru zisku uživatele tracingu vůči původnímu autorovi, obdobných mechanismus jako v § 58 odst. 6 AutZ. K vynucování této odměny by musel být kolektivní správce zmocněn přímo zákonem.

Jsmo-li schopni reinterpretovat tříkrokový test tak, že rozpor s běžným užitím stačí proporcionálně kompenzovat dříve zmíněným ziskem ve sféře původního autora, přičemž oprávněné zájmy jsou schopny reflektovat nejen původního autora, ale i třetí osoby, tracing by splnil tříkrokový test a stal se oprávněným způsobem odvozené tvorby.²⁰⁶ Zároveň by situaci napomohlo, kdyby kroky testu byly posuzovány paralelně, nikoli sériově, aby splnění tříkrokového testu případně hned neztroskotalo na druhém kroku, který je pro tracing obtížný.²⁰⁷

Nepřímý projev prospěchu ve sféře původního autora by vyžadoval spíše změnu společnosti. Jedním z řešení by mohla být inspirace od japonskému

²⁰² V těchto nejasných nebo neregulovaných autorskoprávních otázkách může poskytnutí finanční náhrady být jedno z možných řešení, viz GERVAIS, Daniel J. Making Copyright Whole: a Principled Approach to Copyright Exceptions and Limitations. *University of Ottawa Law & Technology Journal*. [online]. 2008, roč. 5, č. 1–2, [cit. 27. 2. 2025], s. 40–41.

²⁰³ § 24 AutZ.

²⁰⁴ Právě role kolektivních správců v modelu *liability rules* je důležitá, neboť jsou jedním z orgánů napomáhajících model řídit, viz WOZNICA. *Control or Compensation: Distorted Narrative and Aftermath of Article 17 CDSM*, s. 641.

²⁰⁵ Tato zákonná licence již dříve existovala i v autorském právu do roku 1991, viz TELEČ, Ivo a TŮMA, Pavel. § 72 Úplatná zákonná licence. In: TELEČ, Ivo a TŮMA, Pavel. *Autorský zákon. Komentář*. 2. vydání. Praha: C. H. Beck CZ, 2019, s. 763.

²⁰⁶ Více o reinterpretaci tříkrokového testu viz MYŠKA. *Výjimky a omezení autorského práva v prostředí digitálních sítí*, s. 76–77.

²⁰⁷ *Ibidem*.

trhu s dódžinši, tedy východiskem pro společenský konsensus o přijetí tracingu jako morálně ospravedlnitelné tvorby je ho vnímat jako vzájemně výhodný jev, z něhož těží nejen samotní autoři, ale společnost jako celek.²⁰⁸ Na druhou stranu, stále existují tací, kteří se vůči tvorbě dódžinši právně brání.²⁰⁹ Ostatně i dosažení společenského konsensu ohledně tracingu je aktuálně nepravděpodobné, když je v Japonsku vnímán negativně vinou pejorativního termínu *torepaku* a autoři obecně mají snadno k dispozici podpůrné mechanismy k vymáhání svých práv.²¹⁰ Změnu společnosti tohoto měřítko je ovšem nutné budovat na vhodné právní úpravě, která dostatečně a transparentně ospravedlňuje svá řešení problémů.²¹¹

Tracing je bezpochyby fenomén, který neexistuje pouze ve vakuu autorského práva, ale rozléhá se do ostatních právních odvětví. Jsme-li schopni aplikovat výjimky a omezení pro tracing nebo jiným způsobem vyřadit autorské právo z hlavní role problému, neznamená to, že je původní autor naprosto bez jakékoliv právní obrany. Na výběr se namísto obrany autora například nabízí obrana účastníka soutěže soutěžním právem, případně obrana právem na ochranu osobnosti. Pointou navrhovaného řešení není zbavit původního autora jeho práv plynoucích z jeho tvorby děl, ale pouze je omezit v nezbytné míře, aby byla jednodušeji umožněna následná tvorba, která přidává ke splnění komunikační funkce autorského práva.²¹²

7. ZÁVĚR

Trend digitalizace je v autorském právu již znám, avšak nikoli každá výzva plynoucí z tohoto trendu má adekvátní řešení. Netradiční odvozená tvorba usnadněná technologickým pokrokem posledních desetiletí získává na popularitě, zejména u *prosumera*, ve videoherním a komiksovém průmyslu.

²⁰⁸ LESSIG, Lawrence. *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*. New York: Penguin Press, 2004, s. 26–27.

²⁰⁹ Ibidem.

²¹⁰ Příkladem může být mechanismus DMCA (*Digital Millennium Copyright Act*) fungující celosvětově na platformě YouTube jako *notice and takedown* nebo *notice and staydown*.

²¹¹ JÜTTE, Bernd Justin. What Is Sust[AI]nable Intellectual Property? *International Review of Intellectual Property and Competition Law*. [online]. 2023, roč. 54, [cit. 27. 2. 2025], s. 1314–1315.

²¹² KOUKAL. *Autorské právo, public domain a lidská práva*, s. 99–100.

Jedním z těchto způsobů odvozené tvorby, který z tohoto trendu těží, je tracing.²¹³

Odpověď na otázku tracingu pragmaticky tkví v odvozené tvorbě. Tracingem jsou úmyslně převzaty vybrané prvky původního díla, které jsou následně zakomponovány do nového díla (díla vytvořeného pomocí tracingu) obsahující i vlastní prvky uživatele tracingu. Hlavním ukazatelem, zdali došlo k zásahu do práv původního autora, je sledování autorskoprávní individuality v převzatých prvcích. Stejně tak je ale nutné sledovat autorskoprávní individualitu ve vlastních prvcích uživatele tracingu a tvůrčí činnost spojenou s tvorbou díla vytvořeného pomocí tracingu k její právní kvalifikaci. Tracing je tak netradiční způsob vytváření odvozené tvorby, podobný jiným populárním způsobům jako je *appropriation art* nebo *sampling*, který lze subsumovat pod § 2 odst. 4 AutZ, jehož výsledkem je odvozené dílo, není-li soudem vyvrácena přítomnost pojmových znaků autorského díla. Jednotlivé případy tracingu musí být řešeny *ad hoc*, a tak nelze jednoznačně říct, že by měl být každý tracing oprávněný nebo protiprávní. Naopak, je nutné pečlivě sledovat skutkovou podstatu každého případu, sledovat smysl a účel provedeného tracingu, a konečně poměřovat práva a zájmy uživatele tracingu (zejména právo na svobodu projevu) a původního autora (zejména vlastnické právo). Domnívám se, že jen a pouze poté je možné tracing správně posoudit.

De lege lata nejsou splnění tříkrokového testu a aplikace výjimek a omezení pro tracing pravděpodobné, a proto bude tracingem zpravidla zasazeno do osobnostních práv autorských (integrita díla) a majetkových práv autorských (užití díla zejména v podobě rozmnožování, rozšiřování rozmnoženiny díla, sdělování díla veřejnosti) původního autora. *De lege ferenda*, v zájmu ochrany svobody uměleckého projevu, který zprostředkovaně dává možnost většího výběru z autorských děl spotřebiteli, by tvůrčímu (oprávněnému) tracingu měla být udělena výjimka a omezení ze zásahu do autorských práv, a to při zachování proporcionality s původním autorem. Právě tento typ tracingu by měl být zákonem uznán za oprávněný.

²¹³ Více o pojmu *prosumer* viz TOFFLER. *The Third Wave*, s. 282.

8. SEZNAM ZDROJŮ²¹⁴

8.1 LITERATURA

- [1] ADAMOVÁ, Zuzana a HAZUCHA, Branislav. *Autorský zákon: komentár*. 1. vydání. Bratislava: C. H. Beck SK, 2018, 1127 s. ISBN 978-80-89603-58-9.
- [2] BALDWIN, Peter. *The Copyright Wars*. United Kingdom: Princeton University Press, 2014, 552 s. ISBN 978-0-691-16182-2.
- [3] DRASSINOWER, Abraham. Copyright is not about copying. *Harvard Law Review*. [online]. 2012, roč. 125, č. 7, s. 108–119. [cit. 28. 11. 2024]. Dostupné z: <https://ssrn.com/abstract=2069156>
- [4] GERVAIS, Daniel J. Making Copyright Whole: a Principled Approach to Copyright Exceptions and Limitations. *University of Ottawa Law & Technology Journal*. [online]. 2008, roč. 5, č. 1–2, s. 1–41. [cit. 27. 2. 2025]. Dostupné z: <https://ssrn.com/abstract=1825342>
- [5] GINSBURG, Jane C. a SIRINELLI, Pierre. Authors and Exploitations in International Private Law: The French Supreme Court and the Hustt and the Huston Film Colorization Conton Film Colorization Controversy. *Columbia-VLA Journal of Law & The Arts*. [online]. 1991, roč. 15, s. 135–159. [cit. 10. 1. 2025]. Dostupné z: https://scholarship.law.columbia.edu/faculty_scholarship/3725
- [6] HAZUCHA, Branislav. Pop art z pohľadu autorského práva. In: MOLNÁR, P. a kol. (ed.) *Košické dni súkromného práva IV. Pocta profesorovi Vojčíkovi*. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2022, s. 382–389. ISBN 978-80-574-0098-1.
- [7] HUGENHOLTZ, P. Bernt a QUINTAIS, João Pedro. Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output?. *International Review of Intellectual Property and Competition Law*. [online]. 2021, roč 52, s. 1190–1216. [cit. 7. 1. 2025]. Dostupné z: <https://doi.org/10.1007/s40319-021-01115-0>
- [8] HUSOVEC, Martin. Judikatórna harmonizácia pojmu autorského diela v únijnom práve. *Bulletin slovenskej advokácie*. 2012, roč. 18, č. 12, s. 16–20. ISSN 1335-1079.
- [9] CHALLIS, Ben. The Song Remains the Same: a Review of the Legalities of Music Sampling. *WIPO Magazine*. 2009, č. 6, s. 16–19. ISSN 1020-7074.
- [10] CHALOUPKOVÁ, Helena a HOLÝ, Petr. *Autorský zákon. Komentář*. 6. vydání. Praha: C. H. Beck CZ, 2023, 464 s. ISBN 978-80-7400-944-0.
- [11] JÜTTE, Bernd Justin a QUINTAIS, João Pedro. The Pelham Chronicles: sampling, copyright and fundamental rights. *Journal of Intellectual Property Law & Practice*. [online]. 2021, č. 3, s. 213–225. [cit. 15. 2. 2025]. Dostupné z: <https://ssrn.com/abstract=3775599>
- [12] JÜTTE, Bernd Justin. What Is Sust[AI]nable Intellectual Property? *International Review of Intellectual Property and Competition Law*. [online]. 2023, roč. 54, s. 1311–1315. [cit. 27. 2. 2025]. Dostupné z: <https://doi.org/10.1007/s40319-023-01368-x>

²¹⁴ Funkčnost hypertextových odkazů elektronických zdrojů byla zkontrolována k 25. 8. 2025.

- [13] KNAP, Karel. Quo vadis současného autorského práva. In: KNAP, Karel (ed.) a KUNZ, Otto (ed.). *Aktuální otázky práva autorského a práv průmyslových*. Praha: Univerzita Karlova, 1986, s. 9–34.
- [14] KNAP, Karel. Užití autorského díla. In: KNAP, Karel (ed.) *Aktuální otázky práva autorského, práv průmyslových a práva soutěžního*. Praha: Univerzita Karlova, 1975, s. 21–42.
- [15] KOUKAL, Pavel. *Autorské právo, public domain a lidská práva*. 1. vydání. Brno: Masarykova univerzita, 2019, 524 s. ISBN 978-80-210-9279-2.
- [16] LESSIG, Lawrence. *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity*. New York: Penguin Press, 2004, 345 s. ISBN 1-59420-006-8.
- [17] LIPTON, Jacqueline. D. Copyright and the Commercialization of Fanfiction. *Houston Law Review*. 2014, roč. 52, č. 2, s. 425–466. ISSN 0018-6694.
- [18] MANTA, Irina D.; BALGANESH, Shyamkrishna; WILKINSON-RYAN, Tess. Judging Similarity. *Iowa Law Review*. [online]. 2014, roč. 100, s. 267–290. [cit. 28. 11. 2024]. Dostupné z: <https://ssrn.com/abstract=2409811>
- [19] MEHRA, Salil K. Copyright and Comics in Japan: Does Law Explain Why All the Cartoons My Kid Watches are Japanese Imports?. *Rutgers Law Review*. [online]. 2002, roč. 55, s. 1–65. [cit. 5. 12. 2024]. Dostupné z: <http://dx.doi.org/10.2139/ssrn.347620>
- [20] MEZEI, Péter; JÜTTE, Bernd Justin; SGANGA, Caterina; PASCAULT, Léo. Oops, i Sampled Again ... the Meaning of “Pastiche” as an Autonomous Concept Under EU Copyright Law. *International Review of Intellectual Property and Competition Law*. [online]. 2024, roč. 55, s. 1225–1256. [cit. 30. 11. 2024]. Dostupné z: <https://doi.org/10.1007/s40319-024-01495-z>
- [21] MEZEI, Péter; SENFTLEBEN, Martin; SGANGA, Caterina; GEIGER, Christophe. Opinion of the European Copyright Society on the Scope of the Pastiche Exception in EU Copyright Law (CG and YN v Pelham GmbH and Others, Case C-590/23). *International Review of Intellectual Property and Competition Law*. [online]. 2025, roč. 56, s. 381–397. [cit. 20. 2. 2025]. Dostupné z: <https://doi.org/10.1007/s40319-025-01563-y>
- [22] MEZEI, Péter. Thou Shalt (Not) Sample? New Drifts in the Ocean of Sampling. *Journal of Intellectual Property Law*. [online]. 2019, č. 2, s. 170–198. [cit. 29. 11. 2024]. Dostupné z: <http://dx.doi.org/10.2139/ssrn.3360936>
- [23] MORGAN, Rachel. Conventional Protections for Commercial Fan Art Under the U.S. Copyright Act. *Fordham Intellectual Property, Media and Entertainment Law Journal*. [online]. 2021, roč. 31, č. 2, s. 514–573. [cit. 24. 11. 2024]. Dostupné z: <https://ir.lawnet.fordham.edu/iplj/vol31/iss2/4/>
- [24] MYŠKA, Matěj; POLČÁK, Radim; ŠAVELKA, Jaromír; KYNCL, Libor; SVIRÁKOVÁ Iveta. *Veřejné licence v České republice*. verze 2.0. Brno: Masarykova univerzita, 2014, 187 s. ISBN 978-80-210-7192-6.
- [25] MYŠKA, Matěj. *Výjimky a omezení autorského práva v prostředí digitálních sítí*. Praha: Wolters Kluwer ČR, 2020, 336 s. ISBN 978-80-7598-842-3.

- [26] POLČÁK, Radim; KOUKAL, Pavel; LEŠKA, Rudolf; MYŠKA, Matěj; HRABÁNEK Jiří et al. *Autorský zákon: Praktický komentář s judikaturou*. Praha: Leges, 2020, 864 s. ISBN 978-80-7502-391-9.
- [27] PRCHAL, Petr. *Limity autorskoprávní ochrany*. Praha: Leges, 2016, 272 s. ISBN 978-80-7502-141-0.
- [28] SEHNÁLEK, David; TÝČ, Vladimír et al. *Soudní dvůr EU a výklad práva Evropské unie*. 1. vydání. Brno: Masarykova univerzita, 2016, 188 s. ISBN 978-80-210-8396-7.
- [29] SENFTLEBEN, Martin. The Unproductive “Overconstitutionalization” of EU Copyright and Trademark Law – Fundamental Rights Rhetoric and Reality in CJEU Jurisprudence. *International Review of Intellectual Property and Competition Law*. [online]. 2024, roč. 55, s. 1471–1514. [cit. 18. 2. 2025]. Dostupné z: <https://doi.org/10.1007/s40319-024-01527-8>
- [30] ŠALOMOUN, Michal. *Ochrana názvů, postav a příběhů uměleckých děl*. 2. vydání. Praha: Nakladatelství C. H. Beck CZ, 2009, 180 s. ISBN 978-80-7400-097-3.
- [31] ŠÁMAL, Pavel et al. *Trestní zákoník. Komentář*. 3. vydání. Praha: C. H. Beck CZ, 2023, 4968 s. ISBN 978-80-7400-893-1.
- [32] TELEČ, Ivo a TŮMA, Pavel. *Autorský zákon. Komentář*. 2. vydání. Praha: C. H. Beck CZ, 2019, 1320 s. ISBN 978-80-7400-748-4.
- [33] TELEČ, Ivo. *Pojmové znaky duševního vlastnictví*. Praha: C. H. Beck CZ, 2012, 163 s. ISBN 978-80-7400-425-4.
- [34] TOFFLER, Alvin. *The Third Wave*. New York: William Morrow & Company, Inc., 1980, 544 s. ISBN 0-688-03597-3.
- [35] TOMORI, Subaru. *工セ著作権事件簿 (False Copyright Claim Casebook)*. Japonsko: Publib LLC, 2022, 544 s. ISBN 4908468605.
- [36] WOZNICA, Ondřej. Control or Compensation: Distorted Narrative and Aftermath of Article 17 CDSM. *GRUR International*. [online]. 2024, roč. 73, č. 7, s. 631–646. [cit. 4. 3. 2025]. Dostupné z: <https://doi.org/10.1093/grurint/ikae076>
- [37] ŽVÁBEK, Adam. *Autorskoprávní aspekty tracingu*. Online, magisterská diplomová práce. Brno: Masarykova univerzita, Právnická fakulta. 2025, 114 s. Dostupné z: <https://is.muni.cz/th/r71x2/>. [cit. 10. 7. 2025].

8.2 INTERNETOVÉ ZDROJE

- [38] European Copyright Code. In: *The Institute for Information Law*. [online]. 2010. [cit. 11. 2. 2025]. Dostupné z: <https://www.ivir.nl/projects/copyrightcode/european-copyright-code/>
- [39] Explaining Illustration Tracing and Copyright Law Amidst the Frequent Plagiarism Controversies In: *Monolith Law*. [online]. 2023. [cit. 23. 10. 2024]. Dostupné z: <https://monolith.law/en/internet/copy-plagiarize-tracing>

- [40] HECHT, David. Fortnite Infringement of Kyle Hanagami Choreography. In: *Youtube*. [online]. 2022. [cit. 15. 11. 2024]. Dostupné z: https://www.youtube.com/watch?v=vXYDr9o_FJY
- [41] KOMOTO, Akihiro. Release regarding Mai Hanamura's "trace false accusation" trial. In: *Komoto Sato Legal and Tax Partners*. [online]. 2023. [cit. 29. 10. 2024]. Dostupné z: https://ksltp.com/wp-content/uploads/2023/11/hanamura_231109_en.pdf
- [42] PATTERSON, Calum. New CSGO skins accused of stealing art for AWP and M4A4 in Revolution case. In: *Dexerto*. [online]. 2023. [cit. 28. 2. 2025]. Dostupné z: <https://www.dexerto.com/csgo/new-csgo-skins-accused-of-stealing-art-for-awp-and-m4a4-in-revolution-case-2059091/>
- [43] POSLANECKÁ SNĚMOVNA, 9. volební období, 2021, sněmovní tisk 31/0, 25. 10. 2021. Důvodová zpráva k vládnímu návrhu zákona o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, a další související zákony. In: *Poslanecká sněmovna Parlamentu České republiky*. [online]. 2021. [cit. 9. 2. 2025]. Dostupné z: <https://www.psp.cz/sqw/text/orig2.sqw?idd=199904>
- [44] QUINTAIS, João Pedro a JÜTTE, Bernd Justin. Sample, sample in my song, can they tell where you are from? The Pelham judgment – Part II. In: *Kluwer Copyright Blog*. [online]. 2019. [cit. 28. 2. 2025]. Dostupné z: <https://copyrightblog.kluweriplaw.com/2019/11/19/sample-sample-in-my-song-can-they-tell-where-you-are-from-the-pelham-judgment-part-ii/>
- [45] Respecting Intellectual Property. In: *Steam Community*. [online]. 2014. [cit. 30. 10. 2024]. Dostupné z: <https://steamcommunity.com/games/CSGO/announcements/detail/1751086783896069815>
- [46] TATSUMI, Kenji. For Japan illustrators, easy software heightens danger of false 'trace-copying' accusations. In: *The Mainichi*. [online]. 2024. [cit. 23. 10. 2024]. Dostupné z: <https://mainichi.jp/english/articles/20240819/p2a/00m/0et/010000c>
- [47] Tracing. In: *Cambridge Dictionary*. [online]. [cit. 23. 10. 2024]. Dostupné z: <https://dictionary.cambridge.org/dictionary/english/tracing>
- [48] イラストや画像のトレスは違法？企業が対策すべき著作権侵害 [Je tracing ilustrací a obrázků nezákonný? Porušování autorských práv, proti kterému by společnosti měly přijmout opatření]. In: *Verybest Law Offices Kagoshima*. [online]. 2022. [cit. 31. 10. 2024]. Dostupné z: https://kagoshima.vbest.jp/columns/general_corporate/g_ip/6774/; přeloženo pomocí DeepL.
- [49] トレパク指摘は要注意！知っておくべき著作権侵害の境界線 [Buďte opatrní, když obviňujete z plagiátorství! Hranice porušení autorských práv, které byste měli znát]. In: *Copyright Topics*. [online]. 2024. [cit. 23. 10. 2024]. Dostupné z: <https://copyright-topics.jp/topics/be-careful-when-pointing-out-trade-related-issues/>; přeloženo pomocí DeepL.
- [50] マスオ. 【マサオ氏トレス疑惑】乗るしかないこのピックアップに！ [MASUO. (Údajný tracing pana Masua) Musíme se svést na této velké vlně!]. In: *Pixiv*. [online]. 2012. [cit. 15. 11. 2024]. Dostupné z: <https://www.pixiv.net/en/artworks/26867576>; přeloženo pomocí DeepL.

8.3 JUDIKATURA A JINÉ ZDROJE

- [51] *Hanagami v. Epic Games, Inc.*, 85 F.4th 931 (9th Cir. 2023). United States Court of Appeals, Ninth Circuit.
- [52] Rozsudek Nejvyššího soudu ze dne 30. 4. 2007, sp. zn. 30 Cdo 739/2007.
- [53] Rozsudek Nejvyššího soudu ze dne 24. 3. 2021, sp. zn. 27 Cdo 2023/2019.
- [54] Rozsudek Nejvyššího soudu ze dne 28. 7. 2023, sp. zn. 23 Cdo 2178/2022.
- [55] Rozsudek Vrchního soudu v Praze ze dne 19. 4. 2022, č.j. 3 Co 170/2021-211.
- [56] Rozsudek SDEU (čtvrtého senátu) ze dne 16. 7. 2009 ve věci C-5/08, Infopaq International, ECLI:EU:C:2009:465.
- [57] Rozsudek SDEU (třetího senátu) ze dne 22. 12. 2010 ve věci C-393/09, Bezpečnostní softwarová asociace, ECLI:EU:C:2010:816.
- [58] Rozsudek SDEU (velkého senátu) ze dne 4. 10. 2011 ve spojených věcech C-403/08 a C-429/08, Football Association Premier League, ECLI:EU:C:2011:631.
- [59] Rozsudek SDEU (třetího senátu) ze dne 1. 12. 2011 ve věci C-145/10, Painer, ECLI:EU:C:2011:798.
- [60] Rozsudek SDEU (třetího senátu) ze dne 1. 3. 2012 ve věci C-604/10, Football Dataco, ECLI:EU:C:2012:115.
- [61] Rozsudek SDEU (velkého senátu) ze dne 3. 9. 2014 ve věci C-201/13, Deckmyn and Vrijheidsfonds, ECLI:EU:C:2014:2132.
- [62] Rozsudek SDEU (velkého senátu) ze dne 29. 7. 2019 ve věci C-469/17, Funke Medien NRW, ECLI:EU:C:2019:623.
- [63] Rozsudek SDEU (velkého senátu) ze dne 29. 7. 2019 ve věci C-476/17, Pelham I, ECLI:EU:C:2019:624.
- [64] Rozsudek SDEU (velkého senátu) ze dne 29. 7. 2019 ve věci C-516/17, Spiegel Online, ECLI:EU:C:2019:625.
- [65] Stanovisko generálního advokáta Macieje Szpunara ze dne 12. 12. 2018 ve věci C-476/17, Pelham I, ECLI:EU:C:2018:1002.
- [66] Stanovisko generálního advokáta Nicholase Emilioua ze dne 17. 6. 2025 ve věci C-590/23, Pelham II, ECLI:EU:C:2025:452.
- [67] Usnesení Nejvyššího soudu ze dne 16. 5. 2007, sp. zn. 5 Tdo 449/2007.
- [68] Žádost o rozhodnutí o předběžné otázce ze dne 25. 9. 2023 ve věci C-590/23, Pelham II.
- [69] 東京地方裁判所民事第29部判決令和5年10月13日、令和2年(ワ)第25439号と令和3年(ワ)第1631号 [Rozsudek Tokijského okresního soudu (občanskoprávní oddělení 29) ze dne 13. 10. 2023, sp. zn. 2020(wa)25439 a sp. zn. 2021(wa)1631].

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>).

<https://doi.org/10.5817/RPT2025-2-4>

PŘEHLED AKTUÁLNÍ JUDIKATURY II/2025

*KRISTÝNA AKIL, ANNA BLECHOVÁ, MARTIN ERLEBACH, ŠIMON
CHVOJKA, JAKUB HARAŠTA, PAVEL LOUTOCKÝ, JAN MARTÍNEK
KRISTÝNA MLČÁKOVÁ, ONDŘEJ WOZNICA*

1. SOUKROMÍ A OSOBNÍ ÚDAJE

NÁHRADA ÚJMY ZA ŠÍŘENÍ PORNOGRAFIE NA DARK WEBU

Soud: Ústavní soud
Věc: IV. ÚS 1323/25
Datum: 30. 7. 2025
Dostupnost: nalus.usoud.cz

Pachatel spáchal na stěžovatelce (dítěti) řadu trestných činů sexuální povahy. Mimo jiné šlo také o zneužití dítěte k výrobě pornografie a výrobu a jiné nakládání s dětskou pornografií.¹ Pachatel totiž stěžovatelku během sexuálních praktik fotil a natáčel, přičemž takto pořídil přes tisíc fotografií a desítky videí. Některé z nich následně sdílel na dark webu.² V rámci adhezního řízení obecné soudy přiznaly stěžovatelce odškodnění 200.000 Kč z jí požadovaných 600.000 Kč.³

Ústavní soud se v nálezu zabýval také otázkou, jak má být zohledněno šíření explicitního materiálu pachatelem na dark webu při stanovování náhrady újmy.

¹ § 192 odst. 3 a § 193 odst. 1 zákona č. 40/2009 Sb., trestní zákoník.

² Bod 3 anotovaného rozhodnutí.

³ Bod 5 anotovaného rozhodnutí.

Ústavní soud uvedl, že šíření takových materiálů prostřednictvím dark webu spadá pod „přitěžující“ kritérium při stanovování náhrady újmy, jelikož dochází k násobení účinků zásahu do práv jeho uváděním ve veřejnou známost.⁴ K tomu také připomněl specifika dark webu spočívající v absenci autority, která by šíření škodlivého obsahu účinně bránila (na rozdíl od běžného webu, kde je možné šíření částečně zamezit). Materiály se tak mohou nekontrolovatelně šířit na stránkách s dětskou pornografií, což představuje intenzivní pokračování zásahu do práv poškozené, a to i po ukončení trestné činnosti pachatele.⁵

Ústavní soud obecným soudům vytknul, že tuto rovinu případu zcela opomněly zohlednit. Přitom pachatel vytvořil velké množství materiálů zachycujících intimní partie poškozené. Část z nich poté sdílel na diskuzních fórech zaměřených na sadistickou dětskou pornografii a také s obchodníkem s dětskou pornografií. To představuje masivní zásah do práv poškozené, který je nadále násoben sdílením. S touto rovinou se bude muset vrchní soud řádně zabývat.⁶

Autor: ŠCH

KDO JE (VELMI VELKOU) ONLINE PLATFORMOU DLE DSA?

Soud: Soudní dvůr Evropské unie

Věc: T-348/23

Datum: 3. 9. 2025

Dostupnost: curia.europa.eu

Zalando, provozovatel retailové platformy pro prodej zejm. módních produktů, se obrátil na soud poté, co byl Komisí označen za velmi velkou online platformu dle DSA (dále jen „VLOP“).⁷ Při svém určení Komise vycházela z vlastního reportu Zalando, který deklaroval celkem 87 mil. měsíčních ak-

⁴ § 2957 zákona č. 89/2012 Sb., občanský zákoník; bod 24 anotovaného rozhodnutí.

⁵ Bod 25 anotovaného rozhodnutí.

⁶ Bod 25 anotovaného rozhodnutí.

⁷ Body 2-9 anotovaného rozhodnutí.

tivních příjemců (dále jen „PMP“).⁸ Současně však report dovedl, že pouze cca 30 mil. jsou PMP té části platformy, kde Zalando nabízí produkty jiných výrobců, a to s odkazem na 37% podíl této části produktů na celkových obrotech společnosti.

Podle čl. 33 DSA je VLOP taková online platforma, která má nad 45 mil. PMP. Zalando rozporuje, že je online platformou, neboť aktivně kontroluje a mění obsah třetích stran.⁹ Dále rozporuje závěr komise, že má celkem 87 mil. PMP.¹⁰

V prvním argumentu Zalando navazuje na dlouholetou judikaturu bezpečného přístavu dle eCommerce směrnice. V této judikatuře SDEU opakovaně dovozuje, že pro aplikaci bezpečného přístavu na hostingové platformy je zásadní, zda aktivně kontrolují a mění obsah nahraný uživateli. Jak však zdůrazňuje SDEU, tento závěr přispívá k tomu, zda se na hostingovou platformu uplatní bezpečný přístav, nikoliv zda se vůbec o hostingovou platformu jedná.¹¹ Jinými slovy SDEU zdůrazňuje rozdíl mezi klasifikací online platformy a aplikací výjimky z odpovědnosti pro některé online platformy. Pokud tedy Zalando aktivně monitoruje a mění obsah nahraný uživateli, může to mít dopad na aplikaci čl. 6 DSA, nikoliv však čl. 33 DSA.

Ve svém druhém argumentu se Zalando vrací ke svému výpočtu PMP dle poměru obrátů na platformě. SDEU však zdůrazňuje, že PMP je kdokoli, kdo je vystaven informací, a nejen ten, kdo provádí transakci.¹² SDEU dále zdůrazňuje, že je úkolem platformy správně identifikovat své PMP, a to dle vhodné metody, kterou si sama zvolí a která bude v souladu s DSA.¹³ Pokud však design platformy slívá vlastní obsah Zalando s obsahem třetích stran, je nutné za PMP považovat všechny uživatele platformy.

⁸ Bod 3 anotovaného rozhodnutí.

⁹ Bod 15 anotovaného rozhodnutí.

¹⁰ Bod 54 anotovaného rozhodnutí.

¹¹ Bod 38 a násl. anotovaného rozhodnutí.

¹² Bod 60 anotovaného rozhodnutí.

¹³ Bod 67-68 anotovaného rozhodnutí.

Závěrem Zalando napadá samotný koncept PMP, který dle Zalando podkopává právní jistotu, princip rovného zacházení a zásadu proporcionality Evropského práva.¹⁴ SDEU všechny argumenty odmítá, a to obecně s ohledem na nutnost aplikace obecné právní normy na kontext konkrétní online platformy.

Rozhodnutí tak vyjasňuje, že pro klasifikaci dle DSA je podstatné fungování konkrétní platformy a design uživatelského prostředí, nikoliv business model platformy. Současně SDEU vyjasňuje roli existující judikatury k eCommerce směrnici v kontextu DSA, kdy její dopad je omezen na překryv bezpečného přístavu dle obou právních předpisů. Z hlediska online platform pak je zásadní otázkou, zda se vyplatí designovat prostředí platformy tak, aby byly odděleny vlastní a cizí obsahové prvky.

Autor: OW

ZDRŽENÍ SE PROTIPRÁVNÍHO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ A NÁHRADA NEMAJETKOVÉ ÚJMY

Soud: Soudní dvůr Evropské unie

Věc: C-655/23

Datum: 4. 9. 2025

Dostupnost: curia.europa.eu

V původním sporu žádal uchazeč o zaměstnání svého potenciálního zaměstnavatele, společnost Quirin Privatbank, o určité mzdové ohodnocení. Společnost Quirin Privatbank jeho žádost v e-mailu odmítla a nabídla mu jiné mzdové ohodnocení. Tento e-mail však byl zaslán třetí osobě, které se přijímací řízení netýkalo. Tato třetí osoba uchazeče o zaměstnání znala a kontaktovala ho s dotazem, zda shání práci.¹⁵

Uchazeč se žalobou domáhal toho, aby se společnost Quirin Privatbank zdržela veškerého zpracování jeho osobních údajů v souvislosti s jeho žádostí o pracovní místo, které by znovu vedlo k jejich neoprávněnému zve-

¹⁴ Bod 71 a násl. anotovaného rozhodnutí.

¹⁵ Bod 23 anotovaného rozhodnutí.

řejnění, a dále aby mu byla vyplacena náhrada nemotné újmy, kterou utrpěl sdílením obsahu e-mailu se třetí osobou.¹⁶

Proti rozsudku, který uchazeči o zaměstnání vyhověl, se společnost odvolala. Odvolací soud částečně vyhověl uchazeči a částečně společnosti, což vedlo k soudnímu řízení v další instanci,¹⁷ kde soud položil Soudnímu dvoru Evropské unie šest předběžných otázek.

Soudní dvůr nejprve uvedl, že GDPR nezakládá subjektu údajů právo žádat zdržení se protiprávního jednání.¹⁸ Vzhledem k tomuto závěru SDEU již nezodpověděl otázky, zda se lze zdržení jednání domáhat pouze tehdy, pokud se lze do budoucna obávat dalších porušení práv subjektu údajů vyplývajících a zda existující porušení GDPR postačuje jako indikace nebezpečí, že se protiprávní jednání bude opakovat. Zároveň SDEU stanovil, že GDPR nicméně neodporuje tomu, aby subjekt údajů tohoto práva využil, jestliže je mu garantované národním právním řádem.¹⁹

Následně byl SDEU dotázán, zda je možné pod nemotnou újmu podřadit pocity vzniklé v důsledku neoprávněného zpřístupnění osobních údajů třetí straně, jako jsou obava nebo nespokojenost, které jsou vyvolány ztrátou kontroly nad těmito údaji, jejich možným zneužitím nebo poškozením jeho pověsti.²⁰ Na tuto otázku Soudní dvůr odpověděl kladně²¹ a na základě páté otázky dodal, že míra zavinění správce nehraje roli při určení výše nemotné újmy.²²

Nakonec se Soudní dvůr zabýval otázkou, zda při určení výše nemotné újmy, která má být nahrazena, lze jako okolnost vedoucí ke snížení výše nároku zohlednit skutečnost, že subjekt údajů má kromě nároku na náhradu nemotné újmy i nárok na zdržení se jednání. Touto otázkou se soud zabýval i přesto, že GDPR nestanovuje právo na zdržení se protiprávního jednání, a odpověděl na ni tak, že není možné právo na náhradu újmy

¹⁶ Bod 24 anotovaného rozhodnutí.

¹⁷ Bod 27 anotovaného rozhodnutí.

¹⁸ Bod 43 anotovaného rozhodnutí.

¹⁹ Bod 46 anotovaného rozhodnutí.

²⁰ Bod 53 anotovaného rozhodnutí.

²¹ Bod 64 anotovaného rozhodnutí.

²² Bod 73 anotovaného rozhodnutí.

snížit nebo nahradit uplatněním práva na zdržení se jednání, které mohlo být přiznané podle vnitrostátního práva.²³

Autorka: KA

PSEUDONYMIZOVANÉ ÚDAJE JSOU V KAŽDÉM PŘÍPADĚ OSOBNÍ ÚDAJE. AKORÁT, ŽE VŮBEC.

Soud: Soudní dvůr Evropské unie

Věc: C-413/23 P

Datum: 4. 9. 2025

Dostupnost: curia.europa.eu

Počátek případu lze datovat do roku 2017, kdy byl řešen hrozící úpadek španělské banky Banco Popular Español, SA. V té době Jednotný výbor pro řešení krizí („Single Resolution Board“ dále jen „SRB“) rozhodl, že v rámci jednotného mechanismu pro řešení krizí a Jednotného fondu pro řešení krizí a mění nařízení (EU) č. 1093/2010 (Úř. věst. 2014, L 225, s. 1) (dále jen „nařízení SRMR“)²⁴ vyzve společnost Deloitte²⁵ aby vypracovala ocenění rozdílného zacházení podle čl. 20 odst. 16 až 18 nařízení SRMR za účelem určení, zda by se akcionářům a věřitelům dostalo lepšího zacházení, pokud by Banco Popular vstoupila do běžného úpadkového řízení (dále jen jako „ocenění 3“).²⁶ V této souvislosti SRB oslovil dotčené akcionáře a věřitele a rozeslal jim link, který jim umožňoval přístup k online formuláři. Ve formuláři se pak strany měly vyjádřit k předběžnému rozhodnutí a nedůvěrnému znění tzv. ocenění 3.²⁷ Dále SRB požádal společnost nezávislého hodnotitele, společnost Deloitte, aby posoudila relevantní připomínky týkající se ocenění 3. V této souvislosti SRB poskytla Deloitte dokument obsahující od-

²³ Body 82 a 83 anotovaného rozhodnutí.

²⁴ Bod 10 anotovaného rozhodnutí.

²⁵ Bod 13 anotovaného rozhodnutí.

²⁶ Bod 13 anotovaného rozhodnutí.

²⁷ Body 17-21 anotovaného rozhodnutí.

povědi tázaných subjektů a vyzvala společnost k hodnocení a přezkoumání toho, zda je ocenění banky ve světle těchto připomínek nadále platné.²⁸

SRB získala 23822 připomínek,²⁹ z nichž každá měla jedinečný alfanumerický kód o 33 číslicích,³⁰ které předložilo 2855 účastníků řízení.³¹ Tyto data SRB roztrídila podle jejich relevance a tématu a na ty které musí analyzovat SRB a ty, které musí analyzovat Deloitte.³² Nakonec bylo společnosti Deloitte předáno 1104 připomínek, které byly sdílené v pseudonymizované formě (obsahovaly alfanumerický kód) skrze zabezpečený virtuální datový server. SRB byl jediným, kdo mohl prostřednictvím tohoto kódu spojit připomínky s konkrétními uživateli a identifikovat tak autora jednotlivých připomínek.³³

Někteří akcionáři a věřitelé s tímto předáním informací nesouhlasili a podali stížnost podle nařízení 2018/1725 k Evropskému inspektorovi ochrany údajů (EIOÚ).³⁴ Věřitelé a akcionáři namítali, že je SRB neinformoval o tom, že údaje shromážděné prostřednictvím odpovědí na otázky ve formuláři budou předány třetím osobám.³⁵ Tuto skutečnost pak vnímali jako rozporuplnou s se zněním prohlášení o ochraně osobních údajů.

EIOÚ dospěl k závěru, že údaje předané společnosti Deloitte byly pseudonymizované, a tedy šlo o osobní údaje.³⁶ Uvedl, že údaje nebyly anonymní, protože SRB si stále zachovával možnost znovu identifikovat jednotlivé osoby. Deloitte tak byl „příjemcem“ osobních údajů. Jelikož SRB ve svém prohlášení o ochraně soukromí Deloitte neuvedl, EDPS konstatoval

²⁸ Bod 21 anotovaného rozhodnutí.

²⁹ Bod 24 anotovaného rozhodnutí.

³⁰ Bod 23 anotovaného rozhodnutí.

³¹ Bod 24 anotovaného rozhodnutí.

³² Bod 25-26 anotovaného rozhodnutí.

³³ Body 27-28 anotovaného rozhodnutí.

³⁴ Bod 29 anotovaného rozhodnutí.

³⁵ Bod 30 anotovaného rozhodnutí.

³⁶ Rozhodnutí EIOÚ ze dne 24. listopadu 2020 přijaté v návaznosti na žádost o přezkum rozhodnutí EIOÚ ze dne 24. června 2020 podanou Jednotným výborem pro řešení krizí (SRB), které se týkalo pěti stížností podaných několika stěžovateli (věci 2019–947, 2019–998, 2019–999, 2019–1000 a 2019–1122).

porušení informační povinnosti. Nicméně SRB toto rozhodnutí napadl u Tribunálu a byl úspěšný.³⁷ Tribunál rozhodnutí EIOÚ zrušil.³⁸

Tři klíčové otázky, které pak řešil CJEU jsou:

Kdy jsou pseudonymizovaná data považována za osobní údaje?

Jaké povinnosti poskytovat informace o případném předání dat třetí straně existují již v době sbírání dat?

Jsou osobní názory (subjektivní i objektivní informace) a stanoviska jednotlivců osobními údaji?

Soud dospěl k tomu, že oproti EIOÚ, pseudonymizované údaje nemusí být v každém případě a ve vztahu ke každé osobě považovány za osobní údaje pro účely použití nařízení 2018/1725.³⁹ V tom se rozhodnutí výrazně liší od rozhodnutí tribunálu, který v roce 2023 došel k závěru, že se nejednalo o pseudonymizované údaje (zpracovatel osobních údajů tedy neměl notifikační povinnost vůči dotčeným osobám).⁴⁰ Pokud je riziko identifikace osob zanedbatelné (např. z důvodu, že správce dat nasadil takové nástroje, které účinně zabrání jiným osobám než správci identifikovat subjekt údajů takovým způsobem, že pro ně není nebo již přestal být subjekt identifikovatelný) může to znamenat, že data jsou anonymní.⁴¹ Nicméně pokud organizace předají údaje, které jsou z jejich pohledu osobní, jiné organizaci, musí o tom i nadále informovat ve svých zásadách ochrany soukromí – i když jsou tyto údaje u příjemce anonymní. Povaha dat vůči subjektu poskytující osobní údaje se tedy vyhodnocuje k momentu sběru dat, jelikož „informační povinnost stanovená v čl. 15 odst. 1 písm. d) nařízení 2018/1725 je součástí právního vztahu mezi subjektem údajů a správcem, a z tohoto důvodu jsou jejím předmětem informace související s tímto subjektem, tak jak byly předány tomuto správci, tedy před jakýmkoli případným předáním třetí straně.“⁴² Pokud tedy SRB bylo schopné z dotazníků

³⁷ Rozsudek Tribunálu Evropské unie ze dne 26. dubna 2023, SRB v. EIOÚ (T-557/20).

³⁸ Body 35-38 anotovaného rozhodnutí.

³⁹ Bod 84-86, 88 anotovaného rozhodnutí.

⁴⁰ Bod 115 anotovaného rozhodnutí.

⁴¹ Bod 84-86, 88 anotovaného rozhodnutí.

⁴² Bod 110 anotovaného rozhodnutí.

identifikovat odpovědi jednotlivých věřitelů a akcionářů, mělo je i obeznámit s tím, že jejich data budou předána třetí straně.⁴³ Nakonec Soudní dvůr EU také potvrdil, že osobní názory (subjektivní i objektivní informace) a stanoviska jednotlivců, pokud jsou „o“ dané osobě, představují osobní údaje.⁴⁴

Tento rozsudek představuje významný krok k vymezení hranic mezi osobními a neosobními údaji v kontextu pseudonymizace a nabourává současný *status quo*. Rozsudek stanovuje, že ochrana osobních údajů se odvíjí nejen od technických vlastností informací (anonymizovaná/ pseudonymizovaná), ale také od toho, v jakých rukou se data nacházejí a v jakém kontextu byla původně shromážděna. Ze situace, kdy se povaha údajů hodnotila především objektivně, se pak dostáváme do opačného stavu. Pojem osobní údaj je nezbytné nově hodnotit a interpretovat subjektivně ve vztahu k tomu, kdo je zrovna „domnělým“ správcem. Rozsudek tedy přesouvá velkou odpovědnost na stranu zpracovatelů dat, kteří nově musí vlastnit pomyslnou křišťálovou kouli, aby byli schopni odhlédnout na veškerá možná budoucí předání údajů. Zároveň pak rozsudek zdůrazňuje, že i subjektivní a objektivní informace osoby, pokud jsou o ní samé, mohou být vnímány jako osobní údaje. Tento ideový posun ve vnímání osobních údajů není možní vnímat jako pouhé rozhodnutí CJEU, ale spíše jako předzvěst vnímání digitální transformace v EU.

Autorka: AB

2. SOCIÁLNÍ SÍTĚ, SVOBODA PROJEVU, ELEKTRONICKÉ DOKUMENTY A ĽSTATNĚ

ANDROID AUTO A NEZBYTNÝ PŘÍSTUP K PLATFORMĚ PRO TŘETÍ STRANU

Soud: Soudní dvůr Evropské unie
Věc: C-233/23
Datum: 25. 2. 2025
Dostupnost: curia.europa.eu

⁴³ Bod 102-105 anotovaného rozhodnutí.

⁴⁴ Body 49-50 a 54-55 anotovaného rozhodnutí.

V původním sporu společnost Enel X Italia Srl provozující zhruba 60 % dobíjecích stanic v Itálii požadovala od společnosti Google, který provozuje službu Android Auto, přístup k platformě Android Auto. To se pro aplikace běžně dělo na základě interoperabilní „šablony“, v čase žádosti ovšem tato šablona neexistovala pro aplikace využívající Google maps, což měla právě společnost Enel X Italia Srl v plánu se svou aplikací Juicepass, která měla umožňovat například navigaci k nabíjecím stanicím nebo jejich rezervaci. Google proto přístup k ekosystému Android auto odepřel s poukazem na chybějící šablonu. Enel X Italia Srl v takovém chování viděl zneužití dominantního postavení Google a bezdůvodné odepření přístupu podle čl. 102 SFEU. Po sérii národních řízení, ve kterých italské orgány dávaly za pravdu Enel X Italia Srl byla věc předložena SDEU⁴⁵ s předběžnými otázkami navazujícími na judikaturu teorie nutných infrastruktur a rozhodnutí Bronner (C-7/97).⁴⁶

Právní otázky, které předkládající soud se zabývaly zejména kritérii z rozhodnutí ve věci Bronner. SDEU se tak musel vypořádat s tím, zda je nutné pro aplikaci teorie nutných infrastruktur z tohoto rozhodnutí dokládat přesně existenci dominantního postavení a konkrétní vymezování navazujících trhů. Dále zda působení stěžovatele na trhu a jeho relativní růst i po odmítnutí přístupu nemohou znamenat nenaplnění kritéria nezbytnosti z rozhodnutí Bronner. A ve finále také jestli je neexistence nutného výrobku nebo služby pro zajištění přístupu na navazující trh skutečně zneužitím dominantního postavení a daný subjekt je povinen tento výrobek či službu vyvinout, případně i za jakých podmínek.⁴⁷

Soudní dvůr ve svém rozhodnutí výrazně změkčil dosavadní doktrínu z rozhodnutí ve věci Bronner. Konkrétně konstatoval, že pokračující existence potenciálně poškozeného subjektu na trhu neznámá, že odmítnutí přístupu nemělo protisoutěžní účinky. Je totiž možné, že ty vyrovnaly jiné

⁴⁵ Viz zejména body 6-13 anotovaného rozhodnutí.

⁴⁶ Rozhodnutí Soudního dvora Evropské unie (šesté komory) ve věci C-7/97 ze dne 26. listopadu 1998.

⁴⁷ Bod 24 anotovaného rozhodnutí.

tržní vlivy nebo snaha poškozeného subjektu se na trhu dále udržet.⁴⁸ Dále Soudní dvůr judikoval, že dominantní subjekt na trhu je povinen zajistit službu či produkt, který může zpřístupnit následný trh (který lze vymezit jen obecně u dynamicky ve vyvíjejících trzích) ale může za to požadovat opodstatněnou finanční kompenzaci od subjektu, který přístup požaduje.⁴⁹ K největší změně ale došlo u kritéria nezbytnosti. Zde se Soudní dvůr opřel o fakt, že platforma Android auto je od počátku zamýšlená jako platforma otevřená třetím stranám.⁵⁰ Kromě bezpečnostních důvodů nebo technické neproveditelnosti tu tedy není příliš legitimních důvodů k dovolenému odmítnutí přístupu. A to i v případě, že takové odmítnutí přístupu nezpůsobí stoprocentní nemožnost účasti na navazujícím trhu. V kontextu online platform podle Soudního dvora nově tedy stačí pouze fakt, že bez přístupu je vstup na trh ztížen a zahrnuje například vyšší míru nepohodlí pro konečné uživatele.⁵¹ Pokud by Android Auto mělo být pouze pro potřeby společnosti Google, tento snížený práh by se neuplatnil.

V rozhodnutí tedy Soudní dvůr výrazně snížil přísnost kritérií z rozhodnutí Bronner v kontextu digitální ekonomiky a online platform. Snížením prahů pro definici navazujícího trhu i zahrnutím kritéria otevřenosti infrastruktury obnovuje důležitost teorie nutných infrastruktur jako nástroje práva hospodářské soutěže v kontextu digitální ekonomiky.

Autor: ME

ELEKTRONICKÝ PODPIS U E-MAILOVÝCH PŘÍLOH

Soud: Ústavní soud ČR

Věc: IV. ÚS 3261/24

Datum: 18. 6. 2025

Dostupnost: nalus.usoud.cz

⁴⁸ Body 59-61 anotovaného rozhodnutí.

⁴⁹ Body 76 a 81 anotovaného rozhodnutí.

⁵⁰ Body 43-47 anotovaného rozhodnutí.

⁵¹ Bod 52 anotovaného rozhodnutí.

Stěžovatelka, společnost Dopravní Stavby Silnic s.r.o., podala odvolání proti rozsudku obvodního soudu. Odvolání bylo odesláno e-mailem jako příloha v PDF souboru a tato příloha byla opatřena uznávaným elektronickým podpisem (konkrétně zaručeným elektronickým podpisem založeným na kvalifikovaném certifikátu dle § 6 odst. 2 zákona o službách vytvářejících důvěru). Samotný e-mail, ke kterému bylo odvolání přiloženo, však daný elektronický podpis neobsahoval. Díky tomu k odvolání příslušný soud nepřihlédl.

Otázkou tedy bylo, jestli je nutno podepisovat rovněž samotné „tělo“ emailu, či postačí elektronicky podepsat odvolání samé.

V tomto případě Ústavní soud odkazoval na příslušné ustanovení občanského soudního řádu (§ 42 odst. 2 a 3), kde je uvedeno, že pokud je elektronické podání ve věci samé opatřeno uznávaným elektronickým podpisem, není třeba podání doplňovat.⁵² Rovněž odkázal na svou předchozí rozhodovací praxi⁵³ a zdůraznil, že procesní pravidla nelze uplatňovat přehnaně formalisticky.

Ústavní soud na základě daného konstatoval, že samotný e-mail plnil pouze funkci pomyslné „obálky“⁵⁴ a není tak nutné, aby e-mail jako takový, byl podepsán uznávaným elektronickým podpisem (pokud jej obsahuje příloha jako podání ve věci samé). Obvodní soud tedy nesprávně spojoval formu e-mailu s obsahem podání, čímž nesprávně aplikoval formální požadavek (který zákon neukládá).

Na závěr Ústavní soud konstatoval, že došlo k porušení práva na soudní ochranu a stížnosti vyhověl. Dodáváme pak, že i z faktického hlediska by takový požadavek mohl být nereálný, jelikož zpravidla verze emailových klientů, které jsou spouštěny v internetovém prohlížeči díky technologické limitaci neumožňují připojení uznávaného elektronického podpisu k samotnému emailu. Dané umožní například komerční certifikáty, které ale nenaplnují právní a technické požadavky kladené na uznávaný elektronický podpis.

⁵² Bod 17 a násl. odůvodnění.

⁵³ Bod 13 odůvodnění.

⁵⁴ Bod 25 odůvodnění.

Autor: PL

ELEKTRONICKÁ PODÁNÍ BEZ UZNÁVANÉHO ELEKTRONICKÉHO PODPISU

Soud: Nejvyšší správní soud

Věc: 3 As 59/2025-23

Datum: 30. 7. 2025

Dostupnost: vyhledavac.nssoud.cz

Žalobce O. S. podal odpor proti příkazu o uložení pokuty za dopravní přešupek prostřednictvím prostého e-mailu bez uznávaného elektronického podpisu.⁵⁵ E-mail obsahoval pouze přílohu – dokument s vlastnoručním podpisem, převedený do elektronické podoby s doložkou o konverzi provedenou Českou poštou.⁵⁶ Správní orgán se uvedeným podáním dále nezabýval a žalobci doručil příkaz o uložení pokuty.

O. S. se tak domáhal u Městského soudu v Praze žalobou na ochranu proti nečinnosti uložení povinnosti správnímu orgánu vydat meritorní rozhodnutí.⁵⁷ MS žalobu zamítl s tím, že odpor nebyl podán řádně, neboť prostý e-mail bez uznávaného elektronického podpisu nelze považovat za platné podání a správní orgán tak nepochybil, když se takovým podáním nezabýval.⁵⁸ Žalobce (nyní stěžovatel) podal proti tomuto rozsudku kasační stížnost. Podle něj MS v Praze posoudil chybně otázku, zda lze učinit řádné podání předáním výstupu z konverze prostým e-mailem.⁵⁹

V daném případě byla řešena otázka, zda lze podání ve výše popsaném případě považovat za podané řádně, a tedy za podání, které vyvolává právní následky.⁶⁰

⁵⁵ Bod 1 anotovaného rozhodnutí.

⁵⁶ Bod 9 anotovaného rozhodnutí.

⁵⁷ Bod 2 anotovaného rozhodnutí.

⁵⁸ Bod 3 anotovaného rozhodnutí.

⁵⁹ Bod 4 anotovaného rozhodnutí.

⁶⁰ Body 2 a 9-10 anotovaného rozhodnutí.

Pro posouzení předmětné otázky jsou relevantní ustanovení § 37 zákona č. 500/2004 Sb., správní řád (dále „SŘ“) a § 6 zákona č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce (dále „ZoS“).⁶¹ Dle § 37 odst. 2 SŘ musí podání obsahovat identifikaci podatele a jeho podpis. Elektronické podání prostřednictvím e-mailu je třeba opatřit uznávaným elektronickým podpisem (dle § 6 odst. 1 ZoS), není-li do 5 dnů potvrzeno či doplněno způsobem upraveným v § 37 odst. 4 SŘ.

NSS dovodil, že prostý e-mail bez uznávaného elektronického podpisu nepředstavuje řádné podání, není-li následně potvrzen.⁶² Doložka o konverzi s podpisem pracovníka pošty prokazuje jen obsahovou shodu listin, nikoliv, že podání učinil sám stěžovatel.⁶³ Z e-mailu nebylo patrné, kdo je podatelem, a žalovaný tak správně k odporu nepřihlédl. Stěžovatel dále argumentoval změnou znění § 37 správního řádu, podle něj tak nově stačí, aby v elektronickém podání byl podpis (a to jakýkoliv) pouze použit.⁶⁴ Dle NSS ani tato teorie stěžovatele neobstojí, změna textového znění měla vést pouze k odstranění nadbytečnosti slov s ohledem na přijetí ZoS, jak vyplývá z důvodového zprávy.⁶⁵

NSS se ztotožnil se závěry MS v Praze a kasační stížnost zamítl.⁶⁶ Potvrdil tak rozhodnutí MS v Praze, že odpor podaný prostým e-mailem bez uznávaného elektronického podpisu a bez následného potvrzení nevyvolává právní následky. Správní orgán tedy v daném případě nebyl nečinný, neboť řízení bylo pravomocně skončeno.⁶⁷

Autorka: KM

⁶¹ Body 11-13 anotovaného rozhodnutí.

⁶² Body 15-16 anotovaného rozhodnutí.

⁶³ Bod 18 anotovaného rozhodnutí.

⁶⁴ Bod 20 anotovaného rozhodnutí.

⁶⁵ Bod 21 anotovaného rozhodnutí.

⁶⁶ Bod 23 anotovaného rozhodnutí.

⁶⁷ Body 22 a 23 anotovaného rozhodnutí.

ESLP ZDŮRAZNIL OCHRANU SVOBODY PROJEVU PLATFORMY: NEPŘIMĚŘENÉ POKUTY A POVINNÉ HOSTOVÁNÍ OBSAHU V RUSKU

Soud: Evropský soud pro lidská práva
Věc: Google v. Russia (stížnost č. 37027/22)
Datum: 8. 7. 2025
Dostupnost: hudoc.echr.coe.int

Ruský telekomunikační úřad Roskomnadzor⁶⁸ nařídil společnosti Google odstranit videa a zablokovat kanály na YouTube, které měly obsahovat protiprávní obsah.⁶⁹ Šlo o kritiku ruské vlády, příkaz zahrnoval např. kanál opozičníka A. Navalného.⁷⁰ Google odmítl s odkazem na svobodu politického projevu.⁷¹ Ruské soudy mu uložily pokuty ve výši cca 400 mil. EUR.⁷²

Ve druhé části případu šlo o blokaci kanálu televize Tsargrad.⁷³ Ta je na sankčních seznamech EU i USA pro svou podporu ruské anexe Krymu a separatistů na východě Ukrajiny.⁷⁴ Podle ruských soudů sankční seznamy odporují ruskému veřejnému pořádku a platformy na jejich základě nemohou blokovat projev uživatelů. Soud uložil platformě pokutu, která se periodicky zvyšovala bez jakéhokoli horního limitu.⁷⁵ Postup Tsargradu kopírovaly další zablokované kanály.⁷⁶ Ruské soudy jim přiznaly podobné pokuty, které celkově dosáhly výše 16 bilionů USD.⁷⁷ Společnost Google Russia vyhlásila bankrot.⁷⁸

⁶⁸ Bod 5 anotovaného rozhodnutí.

⁶⁹ Bod 6 anotovaného rozhodnutí.

⁷⁰ Bod 10 anotovaného rozhodnutí.

⁷¹ Bod 7 anotovaného rozhodnutí.

⁷² Body 11 a 12 anotovaného rozhodnutí.

⁷³ Bod 17 anotovaného rozhodnutí.

⁷⁴ Bod 15 anotovaného rozhodnutí.

⁷⁵ Bod 18 anotovaného rozhodnutí.

⁷⁶ Bod 33 anotovaného rozhodnutí.

⁷⁷ Bod 35 anotovaného rozhodnutí.

⁷⁸ Bod 36 anotovaného rozhodnutí.

ESLP řešil, zda tyto pokuty porušily svobodu projevu podle čl. 10 Úmluvy a právo na spravedlivý proces podle čl. 6 odst. 1. Připomněl, že právo na svobodu projevu náleží i právníkům osobám.⁷⁹

Uložené pokuty představovaly zásah do tohoto práva.⁸⁰ Nebyl „stanoven zákonem“, protože ruská legislativa byla vágní, nepředvídatelná umožňovala svévolný výklad.⁸¹ Videa nedosahovala intenzity pro nenávistný obsah.⁸² Cílem opatření proto nebyla ochrana veřejnosti, ale umlčení kritiky vlády a vytvoření odstrašujícího příkladu.⁸³ Podobné výtky měl ESLP i v případě blokace kanálu Tsargrad.⁸⁴ Platforma má právo rozhodnout o tom, jaký obsah bude hostovat. Může obsah odstranit, pokud k tomu má legitimní důvod. Rusko vymáhalo hostování obsahu pomocí finančních sankcí a přímo do tohoto práva zasáhlo.⁸⁵ Soud také kritizoval způsob udělení pokut, které nebyly zastropované a dosáhly astronomické výše. Ta byla nepředvídatelná a naprosto disproportionální.⁸⁶

ESLP shledal také porušení čl. 6 odst. 1. Ruské soudy v řízení nerozlišovaly mezi jednotlivými strukturami Googlu (Google LLC, Google Ireland a Google Russia). Pokuty udělené jiným společnostem vymáhaly po Google Russia s odůvodněním, že se jedná o *de facto* právní zastoupení těchto společností v Rusku.⁸⁷ Navíc během řízení pominuly prorogační doložku v užívatelských podmínkách, podle níž měly spory rozhodovat soudy v USA.⁸⁸ Místo odůvodnění pouze stručně sdělily, že by zahraniční soudy nerozhodly spravedlivě.⁸⁹

Autor: JM

⁷⁹ Bod 63 anotovaného rozhodnutí.

⁸⁰ Bod 66 anotovaného rozhodnutí.

⁸¹ Bod 69 anotovaného rozhodnutí.

⁸² Bod 76 anotovaného rozhodnutí.

⁸³ Bod 81 anotovaného rozhodnutí.

⁸⁴ Bod 92 anotovaného rozhodnutí.

⁸⁵ Bod 91 anotovaného rozhodnutí.

⁸⁶ Bod 98 anotovaného rozhodnutí.

⁸⁷ Bod 105 anotovaného rozhodnutí.

⁸⁸ Bod 106 anotovaného rozhodnutí.

⁸⁹ Bod 19 anotovaného rozhodnutí.

PŘEKLADY DŮKAZNÍCH LISTIN PROSTŘEDNICTVÍM AI

Soud: Nejvyšší správní soud

Věc: 5 Azs 95/2025-42

Datum: 11. 9. 2025

Dostupnost: vyhledavac.nssoud.cz

Žadatelka o mezinárodní ochranu (stěžovatelka) z Alžírsko požádala o azyl v České republice.⁹⁰ Stěžovatelka uvedla, že z Alžírsko odešla z osobních důvodů, nikoli kvůli obavám z pronásledování, a že jí v případě návratu nic nehrozí.⁹¹ Ministerstvo vnitra její žádost zamítlo, neboť neshledalo, že by v Alžírsku čelila pronásledování nebo vážné újmě a nejsou tak splněny podmínky pro udělení mezinárodní ochrany.⁹²

Stěžovatelka podala proti rozhodnutí Ministerstva vnitra žalobu ke Krajskému soudu v Brně. Tvrdila, že se ve vlasti obává diskriminace jako rozvedená matka nemanželského dítěte.⁹³ KS v Brně se v rámci dokazování zabýval zprávami o zemi původu, konkrétně o situaci samostatně žijících žen. Překlad zpráv byl proveden překladačem eTranslation.⁹⁴ KS konstatoval, že MV nepochybovalo a že zprávy o zemi původu neprokazují systematické pronásledování žen v obdobném postavení. Navíc stěžovatelka původně tyto obavy vůbec neuváděla.⁹⁵ KS žalobu zamítl, vzhledem ke skutečnosti, že humanitární azyl lze udělit pouze v případech hodných zvláštního zřetele. Stěžovatelka poté podala kasační stížnost k Nejvyššímu správnímu soudu. Namítala nepřezkoumatelnost interpretace důkazních prostředků z důvodu použití strojového překladu umělé inteligence a neobjektivního posouzení situace stěžovatelky.⁹⁶ KS navrhl, aby NSS stížnost odmítl jako nepřija-

⁹⁰ Bod 1 anotovaného rozhodnutí.

⁹¹ Bod 1 anotovaného rozhodnutí.

⁹² Bod 2 anotovaného rozhodnutí.

⁹³ Bod 4 anotovaného rozhodnutí.

⁹⁴ Bod 5 anotovaného rozhodnutí.

⁹⁵ Tamtéž.

⁹⁶ Bod 6 anotovaného rozhodnutí.

telnou, jelikož kasační stížnost nabízí pouze obecný nesouhlas stěžovatelky.⁹⁷

V předmětném případě byly řešeny tyto otázky: Je rozsudek krajského soudu nepřezkoumatelný kvůli použití strojového překladu důkazních listin? Lze situaci stěžovatelky považovat za „případ hodný zvláštního zřetele“ pro udělení humanitárního azylu podle § 14 zákona o azylu?⁹⁸

NSS se v předmětném řízení zabýval především otázkou přijatelnosti, tedy zda stížnost svým významem podstatně přesahuje zájmy stěžovatelky ve smyslu § 104a zákona č. 150/2002 Sb., soudní řád správní. Pro otázky humanitární ochrany jsou relevantní ustanovení § 12, 14 a 14a zákona č. 325/1999 Sb., o azylu.⁹⁹

NSS konstatoval, že použití strojového překladu samo o sobě nečiní rozsudek nepřezkoumatelným. Z rozsudku KS je patrné, co dovodil z dokazování a jak dané skutečnosti posoudil.¹⁰⁰ Stěžovatelka měla možnost se s obsahem listin a jejich překladem seznámit, jednání před KS jí bylo tlumočeno.¹⁰¹ Navíc stěžovatelka žádné námitky proti konkrétním zjištěním z daných důkazních prostředků nevznesla.¹⁰² Přijatelnost kasační stížnosti nemůže založit ani námitka stěžovatelky, že nebude schopna uživit sebe a své dítě, a tedy by jí měl být udělen národní humanitární azyl.¹⁰³ NSS konstatoval, že případné ekonomické problémy stěžovatelky by mohly odůvodnit udělení národního humanitárního azylu, pouze pokud by ji ohrožovaly existenčně a docházelo k nim z azylově relevantních důvodů.¹⁰⁴

NSS tak neshledal pochybení KS v Brně. Dále konstatoval, že význam kasační stížnosti nepřesahuje vlastní zájem stěžovatelky. Z tohoto důvodu tak NSS kasační stížnost odmítl jako nepřijatelnou.¹⁰⁵

⁹⁷ Bod 7 anotovaného rozhodnutí.

⁹⁸ Body 8 a 10 anotovaného rozhodnutí.

⁹⁹ Body 8 a 17 anotovaného rozhodnutí.

¹⁰⁰ Body 12-14 anotovaného rozhodnutí.

¹⁰¹ Bod 15 anotovaného rozhodnutí.

¹⁰² Bod 14 anotovaného rozhodnutí.

¹⁰³ Body 17 a 18 anotovaného rozhodnutí.

¹⁰⁴ Body 21 a 22 anotovaného rozhodnutí.

¹⁰⁵ Bod 23 anotovaného rozhodnutí.

Autorka: KM

HALUCINOVANÉ CITACE V KASAČNÍ STÍŽNOSTI

Soud: Nejvyšší správní soud

Věc: 3 As 34/2025-80

Datum: 15. 10. 2025

Dostupnost: vyhledavac.nssoud.cz

Anotace není zpracována kvůli meritů věci, ale kvůli procesní kuriozitě. Jakkoli se totiž rozhodnutí jako celek dotýká velmi důležité problematiky, kterou je realizace práva na přístup k osobním údajům dle § 28 zákona č. 110/2019 Sb., o zpracování osobních údajů, resp. neposkytnutí postupem dle § 28 odst. 2 tohoto zákona, pozornost rozhodnutí přitáhlo z jiného důvodu. Je totiž zařazeno jako první český záznam ve stále rostoucí databázi *AI Hallucination Cases*.¹⁰⁶

V uvedeném rozsudku se Nejvyšší správní soud (dále jen „NSS“) musel vypořádat s postupem Vrchního státního zastupitelství v Praze (dále jen „VSZ“), které odmítlo na žádost fyzické osoby sdělit informace týkající se zpracování osobních údajů, ke kterým došlo u Policie ČR a kterékoli její organizační složky.¹⁰⁷ Postup VSZ byl napaden správní žalobou u Městského soudu v Praze, které soud vyhověl.¹⁰⁸ VSZ následně podalo kasační stížnost k NSS.¹⁰⁹ NSS se s podanou stížností obsáhle vypořádal, když zdůraznil, že rolí správních soudů není poskytovat komplexní návody, jak postupovat, ale adresovat zákonnost postupu v konkrétním řízení.¹¹⁰ NSS zdůraznil informační asymetrii mezi fyzickou osobou a VSZ, kterou připodobnil k přezkumu rozhodnutí, jejichž obsah závisí na obsahu utajovaných informací, a dovedl, že procesní aktivitu účastníka musí částečně suplovat

¹⁰⁶ Databáze je přístupná na adrese <https://www.damiencharlotin.com/hallucinations/>.

¹⁰⁷ Body 1 a 2 anotovaného rozhodnutí.

¹⁰⁸ Bod 3 anotovaného rozhodnutí.

¹⁰⁹ Bod 4 anotovaného rozhodnutí.

¹¹⁰ Bod 11 anotovaného rozhodnutí.

samotný správní soud.¹¹¹ Soud podpůrně využil závěry z rozhodovací praxe SDEU¹¹² a kasační stížnost odmítl. Uzavřel tak, že VSZ nemůže paušálně odmítnout žádost s odkazem na možnou povahu informace, které se žádost týká,¹¹³ a vyjádřil se k náležitostem vhodného postupu v odpovědi na žádost o informace a k obavám VSZ z možného zneužití práva na přístup k informacím osobami z kriminálního prostředí.¹¹⁴

Z textu rozhodnutí je zřejmé, že NSS neměl v rámci tohoto řízení jednoduchou pozici. Kasační stížnost VSZ označil ze „nepříliš koherentní“¹¹⁵ a konstatoval také, že protistrana podala ke kasační stížnosti „obsáhlé a těžko uchopitelné vyjádření“.¹¹⁶ K tomuto tématu se následně vrátil v rámci vyčíslení nákladů řízení, kdy konstatovat, že „vyjádření žalobce byla velmi těžce uchopitelná, neboť se z valné části mýjela se smyslem vyjádření ke kasační stížnosti. Namísto věcných a konkrétních reakcí [...] vystavěl vlastní, velmi obsáhlou, obecnou a z významné části zcela mimoběžnou argumentaci.“¹¹⁷

Skutečná lahůdka pak přichází na samém konci rozhodnutí. NSS totiž identifikuje hned několik rozhodnutí, ze kterých žalobce (resp. jeho právní zástupce) citoval výňatky, které se v daných rozhodnutích nenacházejí. Jde tak o jednu z forem halucinace¹¹⁸ jazykových modelů, kdy identifikované rozhodnutí sice existuje, ale konkrétní argument či výňatek se v něm nenachází. Tento problém se týkal jak citovaných rozhodnutí NSS, tak i Ústavního soudu.¹¹⁹

V průběhu řízení však došlo i na nejběžnější formu halucinace, kdy citovaný dokument vůbec neexistuje. Právní zástupce tak citoval neexistující rozhodnutí 7 As 172/2019 maje snad na mysli existující 7 Azs 172/2019,

¹¹¹ Bod 26 anotovaného rozhodnutí.

¹¹² Bod 30 anotovaného rozhodnutí.

¹¹³ Bod 33 anotovaného rozhodnutí.

¹¹⁴ Body 36 a 37 anotovaného rozhodnutí.

¹¹⁵ Bod 33 anotovaného rozhodnutí.

¹¹⁶ Bod 5 anotovaného rozhodnutí.

¹¹⁷ Bod 43 anotovaného rozhodnutí.

¹¹⁸ Halucinací se rozumí situace, kdy jazykový model generuje nepravdivé nebo neexistující informace, byť ve velmi přesvědčivé podobě.

¹¹⁹ Bod 43 anotovaného rozhodnutí.

dále 1 As 125/2019 namísto existujícího 1 Afs 125/2019 či II. ÚS 1516/14 popletené s existujícím IV. ÚS 1516/14. Soud lakonicky uvádí, že tato „citovaná“ (a NSS zde opravdu využil uvozovky) rozhodnutí „*dokonce vůbec neexistují*“.¹²⁰ Nezbyvá než obdivovat sebekontrolu soudu, který nepovažoval za nutné, aby byla tato věta ukončena minimálně pěti vykřičníky. Soud pak uzavřel následovně: „*Ať již daná vyjádření psal kdokoliv nebo cokoliv, soud tyto ve svém souhrnu nepovažoval pro danou věc za jakkoliv přínosné, a náklady na jejich vznik proto nemohl posoudit jako důvodně vynaložené.*“¹²¹ Soud měl očividně o původu těchto argumentů jasno. Využití halucinované argumentace pak nemělo za následek neúspěch v řízení – minimálně částečně proto, že NSS upřímně usiloval o pochopení argumentace žalobce¹²² – ale vedlo k nepřiznání části nákladů řízení. Nabízí se otázka, zda se touto cestou otevírá cesta pro případné snížení smluvní odměny právního zástupce, protože ten byl ve sporu sice úspěšný (dosáhl zastupovaným chtěného výsledku), nicméně způsobem ne zcela korektním, což soud zohlednil.

Nezbyvá než doufat, že šlo o exces, kterých bude pomálu. Zároveň je však nutné podotknout, že takovéto přání je z kategorie nesplnitelných. Jakkoli mají soudy za notorietu, že ChatGPT nelze považovat za spolehlivý zdroj informací,¹²³ podobně nežádoucích projevů technologického pokroku bude přibývat. Jako naprosté minimum je nutné vyžadovat, aby právní zástupce využívající jazykového modelu ověřil, že citovaná judikatura existuje i mimo pravděpodobnostně generovaný výstup modelu.

Autor: JH

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>).

¹²⁰ Bod 43 anotovaného rozhodnutí.

¹²¹ Bod 43 anotovaného rozhodnutí.

¹²² Jak je zřejmé z první věty bodu 5 anotovaného rozhodnutí.

¹²³ Srov. Rozsudek Městského soud v Praze ze dne 9. 11. 2023, č. j. 10 A 99/2023-73.

ESSAYS II/2025

CONTENTS

Philomène Minima: The state, truth and freedom: Rethinking the fight against disinformation in the digital age	130
Ondřej Sukač: Will use of (G)AI cause profound change in the legal profession or is it simply a new tool?	145

THE STATE, TRUTH, AND FREEDOM: RETHINKING THE FIGHT AGAINST DISINFORMATION IN THE DIGITAL AGE¹

PHILOMÈNE MINIMA²

DESCRIPTION OF AI USE

During the preparation of this essay, I used ChatGPT (OpenAI, GPT-5 version) as an auxiliary tool throughout the writing process. The software was employed to assist with improving sentence structure, linguistic precision, and overall coherence of the text, as well as for verifying bibliographic references.

However, it was not used to generate the core arguments, analysis, or substantive content of the essay. All conceptual reasoning, examples, interpretations, and final formulations were developed independently by the author. Every AI-assisted output was carefully reviewed, edited, and integrated only where appropriate to maintain full academic integrity and originality. The author bears full responsibility for the accuracy and ethical compliance of the essay

1. INTRODUCTION

The State — understood as a political entity organized under one government — has traditionally been seen as the guardian of social order and the public good. Consequently, many argue that it has both the legitimacy and the duty to combat disinformation, which often aims to manipulate pu-

¹ Esej byla zpracována v semestru autumn 2025 v rámci předmětu MVV1368K Privacy and Personal Data. / The essay was written in the autumn 2025 semester for the course MVV1368K Privacy and Personal Data.

² Philomène Minima is a French law student from Aix-en-Provence University of law, currently studying at Masaryk University in Brno as part of an Erasmus exchange, Contact: philomene.minima@gmail.com

blic opinion or destabilize democracy. Yet, to fight such falsehoods means to regulate speech, raising the crucial question of whether such intervention endangers the very freedom it seeks to protect.

Disinformation refers to deliberately false information spread with the intent to deceive, as opposed to misinformation, which is false but shared without malicious intent. « Disinformation can be spread by State or non-State actors. It can affect a broad range of human rights, undermining responses to public policies or amplifying tensions in times of emergency or armed conflict. » according to the United Nations Secretary-General.³

When a government intervenes to curb disinformation, it enters a delicate territory where the line between protection and censorship can become dangerously thin.

Moreover, in an era where information circulates faster than ever before, the rise of disinformation challenges one of the most fundamental democratic principles: freedom of expression. The digital revolution has transformed the way ideas are shared and consumed, allowing every individual to become both a recipient and a producer of information. Social media platforms, while fostering unprecedented connectivity and public participation, have also become powerful tools for the rapid dissemination of false or misleading content.

As a result, the question is no longer limited to what individuals are allowed to say, but rather to how the deliberate manipulation of information can distort public opinion and weaken the very foundations of democratic life. False narratives can shape electoral outcomes, intensify political polarization, and erode citizens' confidence in democratic institutions and the media. The phenomenon of disinformation thus represents not merely a threat to factual accuracy, but a broader challenge to the integrity of democratic debate and the rule of law itself.

³ United Nations General Assembly (2022), Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms, Report of the Secretary-General, A/77/287, 12 August. Available at: <https://docs.un.org/en/a/77/287>

Thus, to what extent should public authorities intervene to combat the deliberate spread of false information, without jeopardizing freedom of expression and democratic debate?

2. THE STATE'S DUTY TO PROTECT TRUTH AND SOCIAL ORDER

2.1 PRESERVING SOCIAL ORDER AND PUBLIC SAFETY

As early as 1721, British essayist Thomas Gordon wrote that laws protecting free speech constitute “the great bulwark of liberty.”⁴ Yet, this freedom can only flourish within a stable and secure society. And it is the state that has been entrusted with this role.

Indeed, according to the famous French philosopher Jean-Jacques Rousseau, in his book *The Social Contract* written in 1762,⁵ each citizen “puts his person and all his power in common under the supreme direction of the general will.” Citizens therefore rely on the state to ensure their safety and regulate their lives, in return for which they cede some of their freedoms. The State, therefore, exists to preserve the common good and social harmony.

In this sense, the fight against disinformation becomes part of the State's responsibility to protect public order. When false information threatens collective security or undermines trust in institutions, government intervention can be justified as an act of preservation, not repression.

A clear illustration emerged during the COVID-19 pandemic in 2020, when rumours circulated that vaccines contained microchips to track citizens.⁶ Such claims endangered public health and generated widespread panic. France, like many other countries, took measures to counter false he-

⁴ John Trenchard & Thomas Gordon (4 February 1721), *Cato's Letters*, “Of Freedom of Speech: That the same is inseparable from publick liberty,” No. 15, p. 19. Available at: <https://nlncrac.org/earlymodern/radical-whigs-and-natural-rights/documents/cato-letters.html>

⁵ Jean-Jacques Rousseau (1762), *Du contrat social*, Book I, Chapter VI, p. 244. Garnier, Paris. Catalogue: <http://catalogue.bnf.fr/ark:/12148/cb31257379p>

⁶ World Health Organization (23 September 2020), “Managing the COVID-19 Infodemic: Promoting Healthy Behaviours and Mitigating the Harm from Misinformation and Disinformation,” WHO. Available at: <https://iris.who.int/server/api/core/bitstreams/533c8487-eb17-4277-83d7-e46f4c9535e2/content>

alth information through mass official communication campaigns and legal mechanisms compelling online platforms to remove harmful content.

But disinformation also carries significant geopolitical implications. In Africa's Sahel region, for instance, Russian-sponsored media operations have sought to discredit Western partners and manipulate local populations.⁷ In this way, disinformation can be used as a strategic tool to turn public opinion against certain countries or governments, thereby destabilising alliances and fuelling mistrust on the international stage.

Thus the State fulfils its social contract: protecting citizens not only from violence or injustice, but also from manipulation that could destabilize society itself.

2.2 SAFEGUARDING DEMOCRACY AND THE INTEGRITY OF PUBLIC DEBATE

Beyond the issue of public safety, disinformation directly threatens the foundations of democracy. As former U.S. President Barack Obama declared in 2021, online disinformation has become “the single biggest threat to our democracy.”⁸

When citizens are systematically misled, their political consent loses its legitimacy and elections cease to reflect an informed “general will,” to use Rousseau's terms.⁹ In today's digital era, individuals are overwhelmed by a constant flow of information — both true and false — that distorts their perception of reality. Moreover, social media algorithms, which amplify content similar to what users have already engaged with, create

FactCheck.org (3 May 2021), “COVID-19 vaccines don't contain microchips and have readily available ingredient lists”. Available at: <https://www.factcheck.org/2022/05/scicheck-pfizer-ceo-not-referencing-covid-19-vaccines-contrary-to-false-impression-in-posts-about-microchips/>

⁷ Dan Whitman (29 August 2023), “Russian Disinformation in Africa: No door on this barn,” Eurasia Program, Foreign Policy Research Institute. Available at: <https://www.fpri.org/article/2023/08/russian-disinformation-in-africa-no-door-on-this-barn/>

⁸ Barack Obama (21 April 2022), “Disinformation and the Erosion of Democracy,” The Atlantic Council Speech, Stanford University. Available at: <https://www.obama.org/stories/democracy-challenges-2022>

⁹ Jean-Jacques Rousseau (1762), *Du contrat social*, Book I, Chapter VI, p. 244. Garnier, Paris. Catalogue: <https://catalogue.bnf.fr/ark:/12148/cb31257379p>

echo chambers that reinforce pre-existing beliefs and discourage exposure to diverse perspectives.

Modern democracies have therefore sought to regulate the information space to preserve electoral integrity.

In France, the 2018 Law on the Manipulation of Information allows judges to order the removal of demonstrably false content during election periods.¹⁰ The rationale is clear: democratic choice depends on access to reliable information, and the State has a duty to ensure that the public sphere remains transparent in order to preserve democracy.

The past decade has provided striking examples of how unchecked disinformation can distort democratic processes:

During the 2016 U.S. presidential election, Russian disinformation campaigns that were mostly led on social media, spread divisive narratives on Facebook and Twitter, influencing voter behaviour in order to boost Donald Trump campaign over Hillary Clinton. Therefore the Internet Research Agency, described as a troll farm, created thousands of social media accounts that purported to be Americans supporting Trump. Fabricated articles and disinformation from Russian government-controlled media were promoted on social media where they reached millions of users between 2013 and 2017.¹¹

In the Brexit referendum the same year, misleading slogans such as “£350 million a week for the NHS” misinformed the British electorate about the real costs of EU membership.¹²

For Rousseau, a democracy without informed citizens is a contradiction in terms. Without truth, the social contract becomes illusory, since indivi-

¹⁰ Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, Journal officiel de la République française, 23 December 2018. Available at: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/>

¹¹ U.S. Senate Select Committee on Intelligence (2019), Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Vol. 2, p. 3. Available at: <https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-report-volume2.pdf>

¹² UK Parliament, Digital, Culture, Media and Sport Committee (2019), Disinformation and ‘Fake News’, Final Report, pp. 56, 69–71, 18 February. Available at: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf>

duals cannot truly consent to what they do not understand. Thus, the State must act as the guarantor of informational integrity, ensuring that public discourse reflects reality rather than deception.

In this light, government action against disinformation is not censorship but a defence of democracy itself — an effort to preserve both truth and trust, the twin pillars of the social order

3. THE LIMITS AND DANGERS OF STATE INTERVENTION IN FIGHTING DISINFORMATION

3.1 THE RISK OF POLITICAL CONTROL OVER INFORMATION: WHEN FIGHTING DISINFORMATION BECOMES A TOOL OF POWER

While combating disinformation can seem like a defense of truth and democracy, it can also lead to the opposite effect: a form of political control over information. Once the State assumes the authority to determine what is true or false, it inevitably opens the door to manipulation and censorship.

Even in democratic regimes, the fight against disinformation can be politicized. History shows that governments have often used information control to justify policies or maintain legitimacy.

For instance, France and the USA during the Vietnam and Iraq wars, shaped public opinion through selective reporting and fabricated evidence; notably the false claims about “weapons of mass destruction” in 2003.¹³ Similarly, in the former Soviet Union, state-controlled media systematically erased dissenting voices, transforming information into an instrument of domination.¹⁴ Today, even liberal democracies are not immune: under the Trump administration, disinformation research in the United States became a political battleground. In 2025, the National Science Foundation cancelled funding for such research, claiming it no longer aligned with go-

¹³ Chad W. Seagren & David R. Henderson (2018), “Why We Fight: A Study of U.S. Government War-Making Propaganda,” *The Independent Review*, Vol. 23, No. 1, pp. 69–90, see pp. 81, 86. Available at: <https://www.jstor.org/stable/26591800>

¹⁴ Mikhail Agursky (1989), “Soviet Disinformation and Forgeries,” *International Journal on World Peace*, Vol. 6, No. 1, pp. 13–30. Available at: <https://www.jstor.org/stable/20751319>

vernment priorities.¹⁵ This decision was widely seen as an attempt to silence politically inconvenient studies.

This evolution illustrates what Hannah Arendt warned against in *Truth and Politics*: the deliberate blurring of truth and falsehood is a precondition for authoritarianism.¹⁶

In short, when the State fights disinformation by deciding what citizens can or cannot hear, it risks transforming a protective mission into a tool of political domination.

3.2 PHILOSOPHICAL LIMITS: FREEDOM OF EXPRESSION AS THE CORNERSTONE OF DEMOCRACY

Beyond these political risks, the State's control of information also raises deeper philosophical and ethical concerns: when a government assumes the power to determine what is true, it jeopardises the very foundation of democracy. The essence of a free society is not the absence of falsehood, but the existence of open, reasoned debate. And this free exchange of ideas, even and especially when those ideas are wrong, unpopular, or provocative only serves to improve democracy.

As John Stuart Mill wrote in *On Liberty*¹⁷ "The peculiar evil of silencing the expression of an opinion is that it is robbing the human race." To suppress an opinion, even a mistaken one, deprives society of the opportunity to confront, refine, and ultimately strengthen the truth. In this sense, freedom of expression is not merely a right, it is a method of discovering truth and ensuring intellectual progress.

This principle underpins all liberal democracies: citizens must remain free to express their views without fear of censorship, for truth emerges

¹⁵ Sarah Scire (21 April 2025), "National Science Foundation cancels research grants related to misinformation and disinformation," NiemanLAB. Available at: <https://www.niemanlab.org/2025/04/national-science-foundation-cancels-research-grants-related-to-misinformation-and-disinformation>

¹⁶ Hannah Arendt (1967), *Between Past and Future*, Chapter 7 "Truth and Politics," pp. 227–264. Available at: https://german.yale.edu/sites/default/files/arendt.truth_and_politicslying_in_politics.pdf

¹⁷ John Stuart Mill (2001), *On Liberty*, p. 19, Batoche Books, Kitchener. Available at: <https://eet.pixel-online.org/files/etranslation/original/Mill,%20On%20Liberty.pdf>

through confrontation, not control. Limiting this right undermines the democratic process itself.

History offers many examples of individuals who proved that words can be acts of resistance. The Czech playwright and dissident Václav Havel, in *The Power of the Powerless*,¹⁸ denounced the lies of Czechoslovakia's communist regime. His underground writings inspired the Charter 77 movement and ultimately the Velvet Revolution,¹⁹ showing that free expression can awaken entire societies to truth and justice. Literature, too, has long warned against the dangers of state-controlled truth. George Orwell's 1984 depicts a world where the government dictates reality itself by rewriting history and language to eliminate independent thought.²⁰ The message remains timeless: when political power controls information, freedom dies silently.

As the Voltairean maxim famously summarises, "I disapprove of what you say, but I will defend to the death your right to say it."²¹ This ethos, echoed centuries later by John F. Kennedy in 1961 "Without debate, without criticism, no administration and no country can succeed and no republic can survive."²² It reminds us that open discourse is not a luxury, but a necessity for any functioning democracy. Thus, while disinformation is a real threat, the suppression of free speech may prove even more dangerous.

¹⁸ Václav Havel (October 1978), "The Power of the Powerless". Available at: <https://www.nonviolent-conflict.org/wp-content/uploads/1979/01/the-power-of-the-powerless.pdf>

¹⁹ John Keane (1999), *Václav Havel: A Political Tragedy in Six Acts*, London: Bloomsbury.

²⁰ George Orwell (1949), *Nineteen Eighty-Four*.

²¹ Evelyn Beatrice Hall (1906), *The Friends of Voltaire*, London: Smith, Elder & Co., p. 199. Available at: https://dn790006.ca.archive.org/0/items/friendsofvoltair00hallrich/friendsofvoltair00hallrich_bw.pdf

²² John F. Kennedy (27 April 1961), "Address Before the American Newspaper Publishers Association," Waldorf-Astoria Hotel, New York City. Available at: <https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/american-newspaper-publishers-association-19610427>

4. BEYOND STATE ACTION: THE NEED FOR A MULTILATERAL AND BALANCE RESPONSE

4.1 INTERNATIONAL COOPERATION AND THE ROLE OF NON-STATE ACTORS

As historian Yuval Noah Harari reminds us in *21 Lessons for the 21st Century*,²³ the digital age has made truth more fragile than ever. In a world of algorithms and instantaneous sharing, no single government can effectively safeguard factual integrity. Fighting disinformation, therefore, requires a collective vigilance, not merely state intervention.

This idea is at the heart of the United Nations report *A/77/287 on Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms*,²⁴ which stresses that: “Countering the different manifestations of disinformation requires addressing underlying societal tensions, fostering respect for human rights, and supporting a plural civic space and media landscape.” In other words, the fight against disinformation must be rooted in human rights, not in state control. It should involve a network of NGOs, journalists, and international institutions acting as safeguards of pluralism and transparency.

For example, the European Court of Human Rights (Article 10 ECHR)²⁵ recognises that restrictions on freedom of expression can only be justified if they are necessary in a democratic society. Which means proportionate, lawful, and aimed at protecting legitimate interests such as public safety or the rights of others.

²³ Yuval Noah Harari (2018), *21 Lessons for the 21st Century*, Chapter 3 “Liberty: Big Data is watching you.”; Chapter 17 “Post-Truth: Some fake news lasts for ever”. Available at: <https://learn.luiss.it/pluginfile.php/776296/course/overviewfiles/harari-21-lessons-for-the-21st-century.pdf>

²⁴ United Nations General Assembly (2022), *Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms*, Report of the Secretary-General, A/77/287, 12 August. Available at: <https://docs.un.org/en/a/77/287>

²⁵ Council of Europe (1950), *European Convention on Human Rights*, Article 10. Available at: https://www.echr.coe.int/documents/d/echr/convention_ENG

Similarly, the Charter of Fundamental Rights of the European Union (Article 11)²⁶ upholds freedom of expression while permitting its limitation only when required to preserve public order or prevent harm. This balance echoes Rousseau's "social contract:" regulation is legitimate only when it serves the general interest without silencing diversity of thought.

Concrete examples illustrate how a multilateral approach can work. The UN and the EU have both condemned state-sponsored disinformation campaigns notably Russian operations in Africa's Sahel region demonstrating that accountability can emerge from international cooperation rather than unilateral censorship.²⁷ NGOs like Reporters Without Borders²⁸ and Amnesty International²⁹ also play an essential role in monitoring abuses and defending media freedom when governments themselves become sources of disinformation.

4.2 CIVIL SOCIETY AND PRIVATE PLATFORMS: NEW FRONTIERS OF RESPONSIBILITY

While states and international organisations are key actors, civil society and the private sector now occupy a central position in the information ecosystem. Liberal democracies, as the UN report notes, "must come to terms with the fact that in the digital city, citizens and institutions cannot be shielded from propaganda or disinformation without compromising their egalitarian and liberal values."³⁰ The solution, therefore, lies in shared responsibility.

²⁶ European Union (2012), Charter of Fundamental Rights of the European Union, 2012/C 326/02, OJ C 326, 26 October. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:C2012/326/02>

²⁷ United Nations Human Rights Council (1 April 2022), Role of States in countering the negative impact of disinformation on the enjoyment and realization of human rights. Available at: <https://docs.un.org/en/A/HRC/res/49/21>

European Council (18 July 2022), Council Conclusions on Foreign Information Manipulation and Interference (FIMI). Available at: <https://data.consilium.europa.eu/doc/document/ST-11429-2022-INIT/en/pdf>

²⁸ Reporters Sans Frontières (2024), World Press Freedom Index 2024. Paris. Available at: <https://rsf.org/fr>

²⁹ Amnesty International (2024), Annual Report 2023/24: The State of the World's Human Rights. London. Available at: <https://www.amnesty.org.uk/resources/state-worlds-human-rights-2024>

Citizens and independent organisations increasingly take part in the effort to debunk false narratives.

For instance, numerous “fact-checking” initiatives such as Les Décodeurs in France³¹ or PolitiFact in the United States³² have emerged to verify viral claims and expose misleading stories. This participatory vigilance strengthens democratic resilience by empowering individuals rather than relying solely on the State.

Private tech companies also play a decisive role. Platforms like Wikipedia flag unsourced content and encourage community corrections, while Facebook and X (formerly Twitter) have developed partnerships with independent fact-checkers. In 2019, Mark Zuckerberg himself called for stronger public regulation of online speech, acknowledging that few companies have the resources to moderate content responsibly at a global scale.³³

Yet as legal scholar Jacob Mchangama argues³⁴ such regulation must align with international human rights norms, ensuring that platforms do not become “privately outsourced censors of dissent.” Instead of silencing controversial voices, social media governance should focus on transparency, accountability, and human rights compliance.

Ultimately, the fight against disinformation cannot be reduced to state control or algorithmic censorship. It requires a polycentric approach by combining state regulation, civil vigilance, and corporate responsibility. That preserves the freedom of expression essential to democracy while defending societies against manipulation and falsehood. The challenge is not

³⁰ United Nations General Assembly (2022), Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms, Report of the Secretary-General, A/77/287, 12 August. Available at: <https://docs.un.org/en/a/77/287>

³¹ Le Monde, “Les Décodeurs: Vérification et décryptage de l'information.” Available at: <https://www.lemonde.fr/les-decodeurs/>

³² PolitiFact, “Fact-Checking the News,” Poynter Institute. Available at: <https://www.politifact.com/>

³³ Mark Zuckerberg (30 March 2019), “The Internet Needs New Rules: Let’s Start in These Four Areas,” The Washington Post. Available at: <https://www.latimes.com/opinion/op-ed/la-oe-mark-zuckerberg-internet-needs-new-rules-20190330-story.html>

³⁴ Jacob Mchangama (2022), “The New Censorship: Why the War on Disinformation is a Threat to Free Speech,” Foreign Affairs, May/June.

to choose between truth and freedom, but to design institutions capable of protecting both.

5. CONCLUSION

To conclude, disinformation threatens the very foundations of democracy by distorting truth and undermining public trust. Yet, while the State has a duty to protect citizens and ensure informed debate, excessive intervention risks sliding into censorship. As Rousseau and Mill remind us, democracy depends on an informed and free public discourse. The truth emerges through debate, not control.

The fight against disinformation must therefore be collective: governments, civil society, media, and international institutions share the responsibility to protect both truth and liberty. Only a balanced, multilateral approach can preserve this delicate equilibrium.

Ultimately, the strength of a democracy lies not in its ability to control information, but in its faith that open dialogue will let truth prevail.

6. BIBLIOGRAPHY

- [1] United Nations General Assembly (2022), Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms, Report of the Secretary-General, A/77/287, 12 August. Available at: <https://docs.un.org/en/a/77/287>
- [2] John Trenchard & Thomas Gordon (4 February 1721), Cato's Letters, "Of Freedom of Speech: That the same is inseparable from publick liberty," No. 15, p. 19. Available at: <https://nlnrac.org/earlymodern/radical-whigs-and-natural-rights/documents/cato-letters.html>
- [3] Jean-Jacques Rousseau (1762), *Du contrat social*, Book I, Chapter VI, p. 244. Garnier, Paris. Catalogue: <http://catalogue.bnf.fr/ark:/12148/cb31257379p>
- [4] World Health Organization (23 September 2020), "Managing the COVID-19 Infodemic: Promoting Healthy Behaviours and Mitigating the Harm from Misinformation and Disinformation," WHO. Available at: <https://iris.who.int/server/api/core/bitstreams/533c8487-eb17-4277-83d7-e46f4c9535e2/content>
- [5] FactCheck.org (3 May 2021), "COVID-19 vaccines don't contain microchips and have readily available ingredient lists". Available at: <https://www.factcheck.org/2022/05/scicheck-pfizer-ceo-not-referencing-covid-19-vaccines-contrary-to-false-impression-in-posts-about-microchips/>

- [6] Dan Whitman (29 August 2023), “Russian Disinformation in Africa: No door on this barn,” Eurasia Program, Foreign Policy Research Institute. Available at: <https://www.fpri.org/article/2023/08/russian-disinformation-in-africa-no-door-on-this-barn/>
- [7] Barack Obama (21 April 2022), “Disinformation and the Erosion of Democracy,” The Atlantic Council Speech, Stanford University. Available at: <https://www.obama.org/stories/demo-cracy-challenges-2022>
- [8] Jean-Jacques Rousseau (1762), *Du contrat social*, Book I, Chapter VI, p. 244. Garnier, Paris. Catalogue: <https://catalogue.bnf.fr/ark:/12148/cb31257379p>
- [9] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, Journal officiel de la République française, 23 December 2018. Available at: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/>
- [10] U.S. Senate Select Committee on Intelligence (2019), *Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Vol. 2, p. 3. Available at: <https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-report-volume2.pdf>
- [11] UK Parliament, Digital, Culture, Media and Sport Committee (2019), *Disinformation and ‘Fake News’*, Final Report, pp. 56, 69–71, 18 February. Available at: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf>
- [12] Chad W. Seagren & David R. Henderson (2018), “Why We Fight: A Study of U.S. Government War-Making Propaganda,” *The Independent Review*, Vol. 23, No. 1, pp. 69–90, see pp. 81, 86. Available at: <https://www.jstor.org/stable/26591800>
- [13] Mikhail Agursky (1989), “Soviet Disinformation and Forgeries,” *International Journal on World Peace*, Vol. 6, No. 1, pp. 13–30. Available at: <https://www.jstor.org/stable/20751319>
- [14] Sarah Scire (21 April 2025), “National Science Foundation cancels research grants related to misinformation and disinformation,” NiemanLAB. Available at: <https://www.niemanlab.org/2025/04/national-science-foundation-cancels-research-grants-related-to-misinformation-and-disinformation>
- [15] Hannah Arendt (1967), *Between Past and Future*, Chapter 7 “Truth and Politics,” pp. 227–264. Available at: https://german.yale.edu/sites/default/files/arendt.truth_and_politicslying_in_politics.pdf
- [16] John Stuart Mill (2001), *On Liberty*, p. 19, Batoche Books, Kitchener. Available at: <https://eet.pixel-online.org/files/etranslation/original/Mill,%20On%20Liberty.pdf>
- [17] Václav Havel (October 1978), “The Power of the Powerless”. Available at: <https://www.nonviolent-conflict.org/wp-content/uploads/1979/01/the-power-of-the-powerless.pdf>
- [18] John Keane (1999), *Václav Havel: A Political Tragedy in Six Acts*, London: Bloomsbury.
- [19] George Orwell (1949), *Nineteen Eighty-Four*.

- [20] Evelyn Beatrice Hall (1906), *The Friends of Voltaire*, London: Smith, Elder & Co., p. 199. Available at: https://dn790006.ca.archive.org/0/items/friendsofvoltair00hallrich/friendsofvoltair00hallrich_bw.pdf
- [21] John F. Kennedy (27 April 1961), “Address Before the American Newspaper Publishers Association,” Waldorf-Astoria Hotel, New York City. Available at: <https://www.jfklibrary.org/archives/other-resources/john-f-kennedy-speeches/american-newspaper-publishers-association-19610427>
- [22] Yuval Noah Harari (2018), *21 Lessons for the 21st Century*, Chapter 3 “Liberty: Big Data is watching you.”; Chapter 17 “Post-Truth: Some fake news lasts for ever”. Available at: <https://learn.luiss.it/pluginfile.php/776296/course/overviewfiles/harari-21-lessons-for-the-21st-century.pdf>
- [23] United Nations General Assembly (2022), *Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms*, Report of the Secretary-General, A/77/287, 12 August. Available at: <https://docs.un.org/en/a/77/287>
- [24] Council of Europe (1950), *European Convention on Human Rights*, Article 10. Available at: https://www.echr.coe.int/documents/d/echr/convention_ENG
- [25] European Union (2012), *Charter of Fundamental Rights of the European Union*, 2012/C 326/02, OJ C 326, 26 October. Available at: <https://eur-lex.europa.eu/legal-content/EN/TEXT/PDF/?uri=CELEX:C2012/326/02>
- [26] United Nations Human Rights Council (1 April 2022), *Role of States in countering the negative impact of disinformation on the enjoyment and realization of human rights*. Available at: <https://docs.un.org/en/A/HRC/res/49/21>
- [27] European Council (18 July 2022), *Council Conclusions on Foreign Information Manipulation and Interference (FIMI)*. Available at: <https://data.consilium.europa.eu/doc/document/ST-11429-2022-INIT/en/pdf>
- [28] Reporters Sans Frontières (2024), *World Press Freedom Index 2024*. Paris. Available at: <https://rsf.org/fr>
- [29] Amnesty International (2024), *Annual Report 2023/24: The State of the World’s Human Rights*. London. Available at: <https://www.amnesty.org.uk/resources/state-worlds-human-rights-2024>
- [30] United Nations General Assembly (2022), *Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms*, Report of the Secretary-General, A/77/287, 12 August. Available at: <https://docs.un.org/en/a/77/287>
- [31] *Le Monde*, “Les Décodeurs: Vérification et décryptage de l’information.” Available at: <https://www.lemonde.fr/les-decodeurs/>
- [32] PolitiFact, “Fact-Checking the News,” Poynter Institute. Available at: <https://www.politifact.com/>

[33] Mark Zuckerberg (30 March 2019), “The Internet Needs New Rules: Let’s Start in These Four Areas,” The Washington Post. Available at: <https://www.latimes.com/opinion/op-ed/la-oe-mark-zuckerberg-internet-needs-new-rules-20190330-story.html>

[34] Jacob Mchangama (2022), “The New Censorship: Why the War on Disinformation is a Threat to Free Speech,” Foreign Affairs, May/June.

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>).

WILL USE OF (G)AI CAUSE PROFOUND CHANGE IN THE LEGAL PROFESSION OR IS IT SIMPLY A NEW TOOL?¹

ONDŘEJ SUKAČ²

DESCRIPTION OF AI USE

I declare that for the essay “Will use of (G)AI cause profound change in the legal profession or is it simply a new tool?”, I have used ChatGPT to help with research, English phrasing, translations, and to get short summaries and comparisons of different ideas. All thoughts and the final text were reviewed and edited by me according to my own understanding and judgment.³

1. INTRODUCTION

Generative AI (G(AI)) is changing many jobs, including the legal profession. Unlike older tools like legal databases or document templates, G(AI) can write, research, and predict outcomes in ways we have not seen before. This essay looks at how G(AI) will change how law firms make money, affect jobs for lawyers, and give clients new tools to help themselves. Some people think G(AI) is just another tool to make work faster, but it could al-

¹ Esej byla zpracována v podzimním semestru 2025 v rámci předmětu MVV57917K Regulating Disruptive Technologies. / The essay was written in the autumn 2025 semester for the course MVV57917K Regulating Disruptive Technologies.

² Ondřej Sukač is a student at the Faculty of Law, Masaryk University. Contact e-mail: 529356@mail.muni.cz

³ Summarize key arguments in recent academic literature on how generative AI may transform the legal profession [prompt] List potential positive and negative impacts of AI adoption on law firms' financial structures [follow-up prompt] Explain how AI tools might influence clients' ability to represent themselves in legal disputes [follow-up prompt]. In: ChatGPT 4.0 [cited 1. 12. 2024]. Prompt link: [unavailable]

so change how lawyers and clients work together and improve access to legal help.

2. EVOLUTION OF TECHNOLOGY IN LEGAL PRACTICE

Technology has always helped lawyers work faster and smarter. Now, generative AI takes things further by writing legal drafts, researching faster, and even predicting case outcomes. Unlike older tools like legal databases or document templates, AI can create new content, making it helpful for complex tasks like contract writing or summarising cases. However, it also raises concerns about mistakes and ethical use. While AI saves time, lawyers still need to check its work to avoid problems⁴.

3. FINANCIAL AND STRUCTURAL IMPACTS

Generative AI is set to change how law firms operate financially and structurally. One major shift is the reduction in costs. AI can handle repetitive tasks like document review, contract drafting, and legal research faster than humans, saving money on staff hours. This may lead to fewer billable hours, challenging the traditional hourly billing model and pushing firms toward flat fees or subscription-based pricing. Smaller law firms could benefit greatly, as AI tools allow them to compete with larger firms by offering similar services at lower cost.⁵

Another change is the investment in AI tools. Law firms will need to spend money on acquiring, maintaining, and training staff to use AI systems. These costs could be high upfront, but the long-term savings and efficiency gains may outweigh them. Larger firms may have the resources to

⁴ WHITE, Stu. *How AI is reshaping the future of legal practice* [online]. Law Society, 20.11.2024 [cit. 1.12.2024]. Available at: <https://www.lawsociety.org.uk/topics/ai-and-lawtech/partner-content/how-ai-is-reshaping-the-future-of-legal-practice>

⁵ COOKE, Emma, Elyse BARG, Melissa LEE, Gaurav DEWANI, Jacob JACKSON, Migara RODRIGO, Marcus ROXBURGH, Kassandra SALVADOR, Ingrid SOMMER a Tom STOKELD. *AI in Law & the Legal Profession* [online]. LSE Law, březn 2024, s. 13 [cit. 1.12.2024]. Available at: <https://www.lse.ac.uk/law/Assets/Documents/news/AI-in-Law-the-Legal-Profession-Industry-Insights-Report.pdf>

adopt AI quickly, creating a gap between firms that can afford these technologies and those that cannot.⁶

Additionally, AI could reshape internal structures. Firms may rely less on junior lawyers for routine tasks, leading to fewer entry-level jobs. Instead, firms might hire more legal tech specialists and data analysts to manage AI systems. This could change the traditional law firm pyramid, with fewer associates and more specialised roles.

Overall, while AI brings financial savings and efficiency, it also forces law firms to rethink their business models and staffing structures.

4. EMPLOYMENT AND JOB TRANSFORMATION

Generative AI is changing how legal jobs work. Many routine tasks that lawyers and paralegals used to do, like researching cases, reviewing contracts, or drafting simple documents, can now be done by AI much faster. This means fewer people may be needed for these types of jobs, which could lead to job losses, especially for junior lawyers and paralegals⁷.

However, AI is also creating new roles. Law firms and legal departments are now hiring specialists who can manage AI systems, check their accuracy, and ensure they follow legal rules. Roles like legal tech advisors, data privacy officers, and AI ethics consultants are becoming more important. Lawyers who understand how to work with AI will have an advantage over those who do not.⁸

AI is also changing what lawyers focus on in their work. Instead of spending hours on repetitive tasks, lawyers can focus on more complex and stra-

⁶ COOKE, Emma, Elyse BARG, Melissa LEE, Gaurav DEWANI, Jacob JACKSON, Migara RODRIGO, Marcus ROXBURGH, Kassandra SALVADOR, Ingrid SOMMER a Tom STOKELD. AI in Law & the Legal Profession [online]. LSE Law, březn 2024, s. 10 [cit. 1.12.2024]. Available at: <https://www.lse.ac.uk/law/Assets/Documents/news/AI-in-Law-the-Legal-Profession-Industry-Insights-Report.pdf>

⁷ WHITE, Stu. *How AI is reshaping the future of legal practice* [online]. Law Society, 20.11.2024 [cit. 1.12.2024]. Available at: <https://www.lawsociety.org.uk/topics/ai-and-lawtech/partner-content/how-ai-is-reshaping-the-future-of-legal-practice>

⁸ Redefining legal business - the end of the billable hour? [online]. Wolters Kluwer, 24.10.2024 [cit. 1.12.2024]. Available at: <https://www.wolterskluwer.com/en/expert-insights/ai-impact-on-legal-business-models>

tegic work, like gaining new clients, talking about deals, or solving legal problems. This shift can make the legal profession more rewarding and creative, but it also means lawyers need to develop new skills, like understanding technology and data analysis.

Overall, while AI may reduce some traditional legal jobs, it also opens doors to new opportunities and helps lawyers focus on higher-value tasks. The challenge will be adapting to these changes and learning the skills needed to work with AI⁹.

5. CLIENT BEHAVIOUR AND SELF-REPRESENTATION

Generative AI is changing how clients interact with lawyers and handle their legal issues. With AI tools, people can draft contracts, prepare legal forms, and even get advice on their rights without needing a lawyer. For example, AI-powered chatbots can help someone create a will or respond to a landlord dispute. This is making legal help cheaper and more accessible, especially for people who cannot afford a lawyer.

Because of this, some clients might choose to represent themselves in court or legal matters, relying on AI tools for guidance. However, this can be risky. AI can make mistakes or misunderstand complex situations.¹⁰

Complex situations, leading to incorrect or incomplete advice. Lawyers may still be needed to review the AI's work and handle complicated issues¹¹.

For lawyers, this means a shift in their role. Instead of doing basic tasks, they might focus more on advising clients who use AI, fixing mistakes, or handling cases where AI falls short. Some law firms may also create AI-

⁹ PWC. *PwC 2024 Global AI Jobs Barometer* [online]. 21.5.2024 [cit. 1.12.2024]. Available at: <https://www.pwc.com/gx/en/issues/artificial-intelligence/job-barometer.html>

¹⁰ Risks of Litigants in Person (LiPs) Using AI and ChatGPT for Self-Representation [online]. Pearcelegal, 21.5.2024 [cit. 1.12.2024]. Available at: <https://pearcelegal.co.uk/blog/using-ai-and-chatgpt-for-self-representation>

¹¹ EDELMAN, David C. a Mark ABRAHAM. *Customer Experience in the Age of AI* [online]. Harvard Business Review, 2022-03 [cit. 2024-12-01]. Available at: <https://hbr.org/2022/03/customer-experience-in-the-age-of-ai>

based services to attract clients who want affordable, tech-friendly solutions.

While AI empowers clients, it raises concerns about accountability. If an AI tool gives bad advice, who is responsible? Lawyers and regulators will need to address these issues to protect clients and ensure fair outcomes¹².

In summary, AI is giving clients more control over their legal needs but also creating new risks. Lawyers must adapt to work alongside AI and provide value where machines cannot.

6. ETHICAL AND REGULATORY CONSIDERATIONS

Generative AI in legal work raises important ethical and regulatory questions. One key issue is bias. AI systems learn from data, and if the data contains biases, the AI can repeat or even amplify them. For example, an AI tool might suggest unfair outcomes in discrimination cases if the training data reflects biased decisions. This puts lawyers and regulators under pressure to ensure that AI tools are fair and reliable.

Accountability is another big concern. If AI makes a mistake, like drafting a flawed contract or providing wrong advice, who is responsible? Is it the lawyer using the tool, the company that created the AI, or the client relying on it? Current laws don't fully address these situations, creating uncertainty for both lawyers and clients¹³.

To address these challenges, new rules and standards are being developed. Governments and legal organisations are working on regulations to ensure that AI tools are transparent, accurate, and used ethically. For example, some jurisdictions require AI tools to be tested for fairness and reliability before use.¹⁴ Lawyers also need to follow ethical rules when using AI. They must review the AI's output carefully and make sure it

¹² *AI Accountability: Who's Responsible When AI Goes Wrong?* [online]. Emerge Digital, 11.8.2023 [cit. 1.12.2024]. Available at: <https://emerge.digital/resources/ai-accountability-whos-responsible-when-ai-goes-wrong/>

¹³ WALSH, Colleen. *How to think about AI* [online]. Harvard Law School, 27.6.2023 [cit. 1.12.2024]. Available at: <https://hls.harvard.edu/today/how-to-think-about-ai/>

¹⁴ EUROPEAN COMMISSION. *AI Act* [online]. Digital Strategy [cit. 1.12.2024]. Available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

aligns with legal standards. This means AI cannot replace human judgment but must be treated as a tool under lawyers' control¹⁵.

7. BUT... INTEGRATION OVER REVOLUTION

While Generative AI is bringing changes to the legal field, it appears more as an advanced tool integrating into existing workflows than a complete revolution. Many tasks that AI handles, like contract review or legal research, were already being done with traditional software, albeit more slowly and with more human effort. AI simply speeds up these processes and makes them more efficient.

Additionally, lawyers' core roles, like offering legal advice, representing clients in court, or making complex decisions, still require human judgment, empathy, and expertise that AI cannot replicate. These tasks involve a nuanced understanding of laws, ethics, and human behaviour, which AI is not equipped to handle.¹⁶

Some also argue that AI's impact will be limited by its accessibility and adoption. Smaller firms or lawyers in regions with fewer resources may not have the tools or infrastructure to fully embrace AI. While larger firms might lead the way, it could take years for AI to be fully integrated across all sectors of the legal profession.¹⁷

¹⁵ NORVELL, Meghan. *Common ethical dilemmas for lawyers using artificial intelligence* [online]. National Jurist, 8.10.2024 [cit. 1.12.2024]. Available at: <https://nationaljurist.com/smartlawyer/professional-development/common-ethical-dilemmas-for-lawyers-using-artificial-intelligence/>

¹⁶ INTERNATIONAL BAR ASSOCIATION. *The Future is Now: Artificial Intelligence and the Legal Profession* [online]. London: IBA, září 2024, s. 11 [cit. 1.12.2024]. Available at: <https://www.ibanet.org/document?id=The-future-is-now-AI-and-the-legal-profession-report>

¹⁷ BROOKS, Chay, Cristian GHERHES a Tim VORLEY. *Artificial intelligence in the legal sector: pressures and challenges of transformation*. Cambridge Journal of Regions Economy and Society [online]. Prosinec 2019, s. 5 [cit. 1.12.2024]. Available at: https://www.researchgate.net/publication/338163462_Artificial_intelligence_in_the_legal_sector_pressures_and_challenges_of_transformation

Lastly, AI cannot entirely replace the relationship between clients and lawyers. Trust, communication, and personalised service are still central to many legal services, especially in sensitive matters¹⁸.

8. THE FUTURE OF LEGAL EDUCATION

As Generative AI becomes a bigger part of the legal field, legal education will need to adapt. Future lawyers will need to learn how to use AI tools effectively. This means law schools will have to teach students not only about the law, but also about technology, data analysis, and AI tools that are now part of legal practice. Understanding how to use AI for legal research, document drafting, and case predictions will be crucial for new lawyers.

In addition to technical skills, law students will need to focus on areas where AI cannot replace human judgment, such as ethical decision-making, client relationships, and strategic thinking. AI can handle routine tasks, but it cannot understand human emotions or provide the personal touch that clients expect from their lawyers¹⁹.

Some law schools are already integrating AI-focused courses into their curriculum, teaching students how to use legal tech and consider its ethical implications.²⁰ The challenge will be ensuring that legal education remains balanced, with a focus on both technology and the human aspects of law.

Ultimately, lawyers who are comfortable using AI and understand its limitations will have an advantage in the job market. The future of legal edu-

¹⁸ How is generative artificial intelligence changing the legal profession? [online]. Economics Observatory [cit. 1.12.2024]. Available at: <https://www.economicsobservatory.com/how-is-generative-artificial-intelligence-changing-the-legal-profession>

¹⁹ PRAKASH, Aswathy G. a Vishnu NAIR. Integrating Generative AI into Legal Education: From Casebooks to Code, Opportunities and Challenges. *Law, Technology and Humans* [online]. 2024, roč. 6, s. 64 [cit. 1.12.2024]. DOI: 10.5204/lthj.3640. Available at: https://www.researchgate.net/publication/386174047_Integrating_Generative_AI_into_Legal_Education_From_Casebooks_to_Code_Opportunities_and_Challenges_NA

²⁰ MURRAY, Seb. Law Schools Integrate Artificial Intelligence into Curricula [online]. LLM GUIDE, 29.8.2024 [cit. 1.12.2024]. Available at: <https://llm-guide.com/articles/law-schools-integrate-artificial-intelligence-into-curricula>

cation will likely include a mix of traditional legal theory and modern technological skills.

9. CONCLUSION

Generative AI is reshaping the legal profession, offering opportunities for efficiency and cost savings, while also posing challenges to jobs, ethical standards, and legal education. AI can perform repetitive tasks quickly, but its ability to handle complex legal issues, make ethical decisions, or build client relationships remains limited. While some jobs may be replaced, new roles are emerging in tech management and AI ethics, and lawyers will still be needed for tasks that require human judgment.

AI also gives clients more control over their legal matters, offering cheaper and more accessible tools, but raises concerns about accountability and quality. The legal profession must balance innovation with caution, ensuring AI tools are used ethically and responsibly.

Looking ahead, legal education will need to prepare students for this new reality by teaching both technology and traditional legal skills. The future of the legal profession will likely be a blend of human expertise and advanced technology, enhancing efficiency while preserving essential human elements.

10. BIBLIOGRAPHY

- [1] WHITE, Stu. *How AI is reshaping the future of legal practice* [online]. Law Society, 20.11.2024 [cit. 1.12.2024]. Available at: <https://www.lawsociety.org.uk/topics/ai-and-law-tech/partner-content/how-ai-is-reshaping-the-future-of-legal-practice>
- [2] KHANOLKAR, Swapnish. *A Cost-Benefit Analysis of AI for Law* [online]. Gitselect, 25.1.2024 [cit. 1.12.2024]. Available at: <https://www.gitselect.com/post/a-cost-benefit-analysis-of-ai-for-law>
- [3] PWC. *PwC 2024 Global AI Jobs Barometer* [online]. 21.5.2024 [cit. 1.12.2024]. Available at: <https://www.pwc.com/gx/en/issues/artificial-intelligence/job-barometer.html>
- [4] EDELMAN, David C. a Mark ABRAHAM. *Customer Experience in the Age of AI* [online]. Harvard Business Review, March 2022 [cit. 2024-12-01]. Available at: <https://hbr.org/2022/03/customer-experience-in-the-age-of-ai>

- [5] *AI Accountability: Who's Responsible When AI Goes Wrong?* [online]. Emerge Digital, 11.8.2023 [cit. 1.12.2024]. Available at: <https://emerge.digital/resources/ai-accountability-whos-responsible-when-ai-goes-wrong/>
- [6] WALSH, Colleen. *How to think about AI* [online]. Harvard Law School, 27.6.2023 [cit. 1.12.2024]. Available at: <https://hls.harvard.edu/today/how-to-think-about-ai/>
- [7] NORVELL, Meghan. *Common ethical dilemmas for lawyers using artificial intelligence* [online]. National Jurist, 8.10.2024 [cit. 1.12.2024]. Available at: <https://nationaljurist.com/smartlawyer/professional-development/common-ethical-dilemmas-for-lawyers-using-artificial-intelligence/>
- [8] How is generative artificial intelligence changing the legal profession? [online]. Economics Observatory [cit. 1.12.2024]. Available at: <https://www.economicsobservatory.com/how-is-generative-artificial-intelligence-changing-the-legal-profession>
- [9] PRAKASH, Aswathy G. a Vishnu NAIR. Integrating Generative AI into Legal Education: From Casebooks to Code, Opportunities and Challenges. *Law, Technology and Humans* [online]. 2024, vol. 6 [cit. 1.12.2024]. DOI: 10.5204/lthj.3640. Available at: https://www.researchgate.net/publication/386174047_Integrating_Generative_AI_into_Legal_Education_From_Casebooks_to_Code_Opportunities_and_Challenges_NA
- [10] COOKE, Emma, Elyse BARG, Melissa LEE, Gaurav DEWANI, Jacob JACKSON, Migara RODRIGO, Marcus ROXBURGH, Kassandra SALVADOR, Ingrid SOMMER a Tom STOKELD. AI in Law & the Legal Profession [online]. LSE Law, March 2024 [cit. 1.12.2024]. Available at: <https://www.lse.ac.uk/law/Assets/Documents/news/AI-in-Law-the-Legal-Profession-Industry-Insights-Report.pdf>
- [11] Redefining legal business - the end of the billable hour? [online]. Wolters Kluwer, 24.10.2024 [cit. 1.12.2024]. Available at: <https://www.wolterskluwer.com/en/expert-insights/ai-impact-on-legal-business-models>
- [12] Risks of Litigants in Person (LiPs) Using AI and ChatGPT for Self-Representation [online]. Pearcelegal, 21.5.2024 [cit. 1.12.2024]. Available at: <https://pearcelegal.co.uk/blog/using-ai-and-chatgpt-for-self-representation>
- [13] EUROPEAN COMMISSION. AI Act [online]. Digital Strategy [cit. 1.12.2024]. Available at: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>
- [14] INTERNATIONAL BAR ASSOCIATION. The Future is Now: Artificial Intelligence and the Legal Profession [online]. London: IBA, September 2024 [cit. 1.12.2024]. Available at: <https://www.ibanet.org/document?id=The-future-is+now-AI-and-the-legal-profession-report>
- [15] BROOKS, Chay, Cristian GHERHES a Tim VORLEY. Artificial intelligence in the legal sector: pressures and challenges of transformation. *Cambridge Journal of Regions Economy and Society* [online]. December 2019 [cit. 1.12.2024]. Available at: https://www.researchgate.net/publication/338163462_Artificial_intelligence_in_the_legal_sector_pressures_and_challenges_of_transformation

[16] MURRAY, Seb. Law Schools Integrate Artificial Intelligence into Curricula [online]. LLM GUIDE, 29.8.2024 [cit. 1.12.2024]. Available at: <https://llm-guide.com/articles/law-schools-integrate-artificial-intelligence-into-curricula>

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>).

RECENZE ZÁVĚREČNÝCH PRACÍ II/2025

OBSAH SEKCE

Kristýna Akil: SPRINGINSFELD, P.: <i>Pověřenec pro ochranu osobních údajů v praxi územních samosprávných celků</i>	156
Ondřej Böhm: MARTÍNEK, J.: <i>Algoritmická moderace obsahu internetových platform</i>	159
Martin Erlebach: FIEBEROVÁ, V.: <i>Přístup k údajům pro prověřené výzkumné pracovníky dle Aktu o digitálních službách</i>	162
Martin Erlebach: MATUŠOVÁ, B.: <i>Subjektivní odpovědnost za protiprávní zpracování osobních údajů</i>	166
František Kasl: SZABÓ, M.: <i>Svoboda projevu na internetových platformách</i>	170
Tina Mizerová: GROMAN, L.: <i>Právní aspekty užití technologie deepfake ve filmu</i>	174
Damián Palašta: BAUMANN, R.: <i>Ochrana modelu strojového učení právem duševního vlastnictví</i>	178
Damián Palašta: ŽVÁČEK, A.: <i>Autorskoprávní aspekty tracingu</i>	182

SPRINGINSFELD, P.: POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ V PRAXI ÚZEMNÍCH SAMOSPRÁVNÝCH CELKŮ

KRISTÝNA AKIL¹

SPRINGINSFELD, P.: Pověřenec pro ochranu osobních údajů v praxi územních samosprávných celků. 2025, bakalářská práce, Masarykova univerzita, Právnická fakulta, 47 s.

ANOTACE

Tato bakalářská práce se zabývá postavením pověřence pro ochranu osobních údajů v obcích České republiky. V obecné části rozebírá právní rámec dle GDPR a národní legislativy, včetně metodických doporučení. Ve zvláštní části pomocí dotazníkového šetření zkoumá, jak obce tuto funkci v praxi zajišťují a do jaké míry naplňují normativní a metodologické požadavky. Práce identifikuje nejčastější nedostatky a formuluje konkrétní doporučení pro obce, metodické orgány i zákonodárce.

KLÍČOVÁ SLOVA

Pověřenec pro ochranu osobních údajů, GDPR, obce, empirický výzkum, soulad s pravidly

ABSTRACT

This bachelor thesis examines the position of the Data Protection Officer in municipalities of the Czech Republic. The general part analyses the legal framework under the GDPR and national legislation, including methodological guidelines.

¹ Mgr. Kristýna Akil je doktorandkou Ústavu práva a technologií na Právnické fakultě Masarykovy univerzity. Kontakt: Kristyna.Akil@law.muni.cz.

The special part uses a questionnaire survey to explore how municipalities ensure this function in practice and to what extent they meet normative and methodological requirements. The thesis identifies the most common shortcomings and formulates specific recommendations for municipalities, methodological bodies, and legislators.

KEYWORDS

Data Protection Officer, Municipalities, Empirical Research, Compliance

Plná verze práce je dostupná z: <https://is.muni.cz/th/y3ue9/>

V práci se autor věnuje oblasti ochrany osobních údajů v rámci veřejné správy, což samo o sobě zcela originálním tématem není, nicméně existují zde stále oblasti, kterým dává smysl se věnovat. Zaměření se na roli pověřence pro ochranu osobních údajů a zhodnocení dobré praxe po několika letech účinnosti GDPR je originálním a potenciálně přínosným tématem, které má silný přesah do praxe.

Cíl práce představit roli pověřence v právním řádu a následně provést dotazníkové šetření a vyhodnotit poznatky z něj považuji bezpochyby za naplněný.

Bakalářskou práci považuji za velmi zdařilou, a to zejména díky zvláštní části práce. V obecné části se autor pečlivě věnuje analýze právní úpravy, nicméně mám k ní dvě výhrady. První je lehce nadbytečná část věnující se „historickému“ kontextu role pověřence. Druhou je zjevně popisný přehled povinností pověřence, který autor uchopil přesně podle jednotlivých článků GDPR a v podstatě je přepsal, což nepůsobí pro čtenáře dobře. Vyjma těchto dvou připomínek nicméně považuji obecnou část práce za pečlivě, přehledně a srozumitelně zpracovanou.

Ve zvláštní části autor představuje dotazník, který vytvořil, a odpovědi, které získal. Zvláštní část považuji za obzvláště dobře zpracovanou a díky obdrženým odpovědím místy i humornou, což vůbec není na škodu. Autor provedl opravdu svědomitou analýzu odpovědí, v níž dokázal důsledně popsat nejen limity metodologie, ale také vždy vysvětlil důvody, které mohly

vést k určitým odpovědím, a propojoval odpovědi s reálným stavem, který se v nich odráží. Zvláštní část přináší uceleně zpracované a zajímavé výsledky, z nichž autor dobře formuluje své závěry.

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>).

MARTÍNEK, J.: ALGORITMICKÁ MODERACE OBSAHU INTERNETOVÝCH PLATFORM

ONDŘEJ BÖHM¹

MARTÍNEK, J.: Algoritmická moderace obsahu internetových platform. 2025, Masarykova univerzita, Právnická fakulta, 80 s.

ANOTACE

Internetové platformy poskytují prostor ohromnému množství uživatelů, jejich regulace státem je ale poměrně problematická. Diplomová práce rozebírá problematiku moderace obsahu na platformách a její vztah ke svobodě projevu uživatelů i platformy samotné, s ohledem na rozdíly v EU a USA. Dále představuje klíčové koncepty regulace a odpovědnosti platform, včetně vztahu mezi regulací a cenzurou. Zvláštní část se věnuje moderaci na platformách Mety, včetně podrobnější analýzy regulace nenávistného projevu a souvisejících rozhodnutí odvolacího orgánu Oversight Board.

KLÍČOVÁ SLOVA

svoboda projevu, soukromá cenzura, moderace obsahu, internet, odpovědnost ISP, sociální sítě, akt o digitálních službách, Oversight Board

ABSTRACT

Internet platforms provide space for a huge number of users, but their regulation by the state is quite problematic. The thesis examines the content moderation on platforms and its relationship to the freedom of expression for both users and platforms, considering differences in the EU and the US. It also introduces key

¹ Mgr. Ondřej Böhm je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontakt: 242398@mail.muni.cz

concepts of platform regulation and liability, including the relationship between regulation and censorship. A special section focuses on Meta's moderation, with a more detailed analysis of hate speech regulation and related decisions of the Oversight Board.

KEYWORDS

Freedom of Expression, Private Censorship, Content Moderation, Internet, ISP Liability, Social Networks, Digital Services Act, Oversight Board

Plný text práce je dostupný z: <https://is.muni.cz/th/ej255/>

Téma diplomové práce lze bezpochyby považovat za zcela aktuální, nejen v souvislosti s národními implementacemi DSA, ale také v kontextu dlouhodobě rostoucího množství obsahu na sociálních sítích a v kontextu současné geopolitické situace, která nabízí nejen podnět k šíření nezákonného obsahu online. Současně je také třeba poznamenat, že se navzdory uvedenému nejedná o téma, které by bylo v českém právním prostředí příliš propírané, jde tedy o téma přínosné. Autor zároveň na mnoha místech správně adresoval složitost celé problematiky, zejména pokud jde o uplatňování veřejné moci prostřednictvím provozovatelů sociálních sítí, kteří jsou však stále osobami soukromého práva poskytujícími komerční službu. Nelze u nich proto zcela odmyslet práva, která jsou s touto povahou spojená, např. svoboda projevu nebo právo na podnikání. Autor si je této skutečnosti velmi dobře vědom a v obecné části vhodně nastiňuje vzájemné souvislosti těchto práv a povinností, které vyplývají např. z compliance s DSA. Už vzhledem k uvedenému tedy vnímám téma jako poměrně náročné a zároveň autorem dobře zvládnuté.

Pokud jde o splnění cílů a zadání práce, zde mám určité výhrady. Slovy autora je cílem práce "představit systém algoritmické moderace obsahu na platformách a ukázat možnosti jeho regulace ze strany státu a dalších relevantních subjektů." Takto formulovaný cíl mi připadá poměrně bezvýznamný v kontextu toho, co práce ve výsledku dělá. Navíc autor neuvádí, proč cíl formuloval právě takto a není z něj dostatečně jednoznačné, co má

práce sdělovat. To je ostatně vidět i na skutečnosti, že samotné algoritnické moderaci se text věnuje pouze místy, a to v obecné části, kde ji velmi stručně představuje, poté na několika málo místech, kde říká, že je tento způsob moderace dominantní, a poté v závěru, kde opakuje uvedené. Těžiště textu, tak jak ho já čtu, spočívá spíše ve vyrovnávání zájmů mezi platformou, uživatelem a veřejnou mocí, a dále v analýze procesních aspektů stížností proti automatizované moderaci. Pokud autor zváží další publikaci díla, doporučuji cíle přehodnotit a upravit v kontextu toho, co je jejím skutečným těžištěm, a v čem práce zároveň dost vyniká. Rovněž mi z textu není zcela jasný smysl porovnávání svobody projevu v ČR a USA. Ano, tyto režimy jsou odlišné, ale proč si autor zvolil právě tyto? Proč se v první řadě vůbec uchýlil ke komparaci? Společnosti provozující platformy jsou sice usídleny v USA, ale chtějí-li provozovat své služby v EU, poté se místní regulaci nevyhnou a úvahy o režimu v USA se tak jeví nadbytečnými. Spatřuje v tom autor nějaký širší smysl, kterému pouze schází vyústění, nebo je to proto, že se o tom dobře píše? Tím neříkám, že to smysl a priori nemá, pouze se domnívám, že nebylo dostatečně prezentováno, co tím autor sleduje a zda to podporuje nějaký jeho argument.

Přestože je obecná část práce místy poněkud stručná, zejména pokud jde o algoritnickou moderaci, autor prokázal velmi dobrou orientaci a odbornou znalost problematiky, a to zejména analýzou rozhodovací praxe soudů a dále ve zvláštní části analýzou činnosti OB, z níž autor činí velmi zajímavé a originální závěry použitelné v praxi - inspirace pro ODS a vedení dialogu platformy s regulátorem, které má navíc řádně argumentačně podložené. Přestože tedy mám určité výhrady vůči obecné části, celek funguje jako ucelený odborný text. Zvláštní část bych se poté nebál označit za samonosnou.

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>).

FIEBEROVÁ, V.: PŘÍSTUP K ÚDAJŮM PRO PROVĚŘENÉ VÝZKUMNÉ PRACOVNÍKY DLE AKTU O DIGITÁLNÍCH SLUŽBÁCH

MARTIN ERLEBACH¹

FIEBEROVÁ, V.: Přístup k údajům pro prověřené výzkumné pracovníky dle Aktu o digitálních službách. 2025, závěrečná práce v programu LLM, Masarykova univerzita, Právnická fakulta, 114 s.

ANOTACE

Závěrečná práce se zabývá přístupem k údajům podle nařízení DSA. Jejím cílem je zhodnotit stávající právní úpravu sdílení údajů digitálních platforem na evropské a národní úrovni. V práci je nejprve vymezen stav sdílení dat před přijetím nařízení DSA a následně jsou rozebrány některé relevantní aspekty tohoto nařízení. Stěžejní částí práce je analýza a kritické zhodnocení úpravy sdílení údajů dle čl. 40 DSA a návrhu aktu v přenesené pravomoci. V závěrečné části je posouzena implementační úprava ve vybraných členských státech a rovněž aktuální řízení vedená Evropskou komisí pro porušení čl. 40 nařízení DSA.

KLÍČOVÁ SLOVA

Nařízení o digitálních službách, prověřený výzkumný pracovník, přístup k údajům, velmi velké online platformy, velmi velké online vyhledávače, systémová rizika

¹ Mgr. Martin Erlebach je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontakt: Martin.Erlebach@law.muni.cz

ABSTRACT

The thesis examines data access under the DSA regulation. The objective of this thesis is to evaluate the legal framework for data access at both European and national levels. First, it defines the state of data sharing before the adoption of the DSA and discusses key aspects of the Regulation. The core section analyses and critically evaluates data sharing rules under Article 40 and proposal for a delegated regulation on data access. The final part assesses implementation in selected Member States and ongoing European Commission proceedings for breaches of Article 40.

KEYWORDS

Digital Services Act, Vetted Researcher, Data Access, Very Large Online Platform, Very Large Online Search Engine, Systemic Risks

Plná verze práce je dostupná z: <https://is.muni.cz/th/k8oda/?info>

Autorka si jako téma práce zvolila hloubkovou analýzu čl. 40 nařízení o digitálních službách (DSA) a na tento článek navázaných řízení vedených Evropskou komisí. Konkrétně se tedy jedná o přístup k údajům velkých online platform a vyhledávačů pro výzkumníky. Jedná se o velmi aktuální téma, jelikož jeho součástí je i v době odevzdání práce připravovaný akt v přenesené působnosti Evropské komise, který má čl. 40 upřesňovat. Téma celkově hodnotím jako náročné, zejména kvůli nutnosti pracovat téměř výhradě se zahraničními zdroji a rychle se měnícím chápáním tohoto nového nařízení mezi odborníky. Problematika samotná by mohla lehce sklouznout pouze k popisu, ale zároveň nabízí široký prostor pro projevení vlastních myšlenek, složitost samotného pojetí práce je do značné míře na autorce samotné. Téma, které autorka zvolila, nabízí taktéž velký potenciál pro praktické využití, pokud jsou do něj dostatečně promítnuty originální myšlenky autorky při interpretaci jednotlivých ustanovení.

Cíle práce jsou bohužel v práci samotné formulovány příliš obecně. Přestože čtenáři rychle dojde, že cílem práce je provést kritickou analýzu

čl. 40 DSA, implementace tohoto článku v ČR a Irsku i zhodnotit probíhající řízení proti velmi velkým online platformám a vyhledávačům podle čl. 40, artikulované cíle práce v anotaci a na konci úvodu práce toto dle mého dostatečně nereflektují. Na těchto místech můžeme najít, že cílem práce je „*zhodnotit stávající právní úpravu, a to jak na evropské, tak na národní úrovni v rámci implementačních předpisů. Zaměřuje se především na analýzu jednotlivých kroků vedoucích ke zpřístupnění dat v rámci privilegovaného přístupu, včetně posouzení návrhu aktu v přenesené pravomoci, a na zmapování aktuálních procesů vymáhání povinnosti přístupu k údajům ze strany Evropské komise*“ v úvodu a „*zhodnotit stávající právní úpravu sdílení údajů digitálních platform na evropské a národní úrovni*“ v anotaci. Z takových formulací nemusí nutně vyplývat, co je skutečným (výše popsáním) cílem práce. Jedná se zřejmě ale jen o formulační problém, který je překonatelný lehkou orientací v kontextu práce. Pokud tedy za cíl považujeme hloubkovou analýzu způsobů přístupu k údajům pro výzkumníky podle DSA, což dle mého autorka implikuje, je možné konstatovat, že práce cíl splnila.

Práce je členěna do 6 kapitolu, úvodu a závěru. Většina textu se pak soustředí v kapitole č. 4, což je pochopitelné vzhledem k jejímu zaměření na stěžejní bod práce, tedy přístup prověřených výzkumníků k údajům velmi velkých online platform a vyhledávačů.

Celkově má práce analytický charakter, a tak může působit na první pohled velmi popisně. To ale není pravda, autorka zručně do textu vplétá vlastní názory a výklady, které jsou vždy zřetelně odlišitelné od textu a ve stěžejních kapitolách č. 4 a 5 je dokonce vhodně shrnuje na konci každé z nich v samostatné podkapitole. Jako příklad těchto autorčiných myšlenek je možné uvést identifikovanou nejasnost u postupu po tom, co výzkumník i po možnosti opravy nenaplní podmínky pro udělení statusu prověřeného výzkumníka ze strany 44 nebo identifikovanou provázanost mezi výsledky výzkumu provedeného na základě zpřístupněných údajů a jejich následné nutné zohlednění při zvážování systémových rizik ze strany velmi velké online platformy nebo vyhledávače na straně 68.

I v popisných částech ovšem autorka ukazuje svůj hluboký vhled a ukázkovou orientaci v problematice, když při popisu jednotlivých ustanovení

obsažených v čl. 40 DSA reflektuje i navržená znění těchto ustanovení, která se do finální verze nařízení nedostala, občas i přímo s odkazem na konkrétní pozměňovací návrhy. V práci je tak zřejmá profesionální angažovanost autorky v tomto tématu během jejího stávajícího působení na Ministerstvu průmyslu a obchodu. Jako poslední si pak dovoluji vypíchnout, že na straně 48 autorka upozorňuje na interpretační problém vzniklý různým zněním DSA a jako pomocný jazyk pak dokonce využívá i němčinu. Tento interpretační problém pak následně vhodně rozřeší dále v textu. Pozornosti čtenáře také nesmí uniknout ani kapitola 6, která nabízí vhled do národní právní úpravy týkající se čl. 40 DSA v České republice a v Severním Irsku. Zejména v podkapitole zabývající se implementací DSA v ČR jsou obsaženy cenné informace a autorčina vlastní kritika problematického přijímání aktů v přenesené působnosti, které mají DSA upřesnit až po uplynutí implementační lhůty a následného překryvu či dokonce nadbytečné právní úpravy, které kvůli tomu vzniká. Oceňuji také vhodné metodologické zdůvodnění výběru těchto dvou národních úprav ukazujících, že nedošlo pouze k arbitrárnímu výběru. Přestože bych kapitolu nutně nenazval komparací, jde rozhodně o cenný vhled, který prozatím v české akademické obci pro toto téma chyběl.

V poslední kapitole, která rozebírá probíhající řízení proti velkým online platformám a vyhledávačům pak zejména oceňuji, že autorka dokázala identifikovat tendenci těchto subjektů nechtít sdílet údaje s výzkumníky a její závěr, že pokud je již nyní problematický přístup pro neproověřené výzkumníky, přístup pro ty prověřené by mohl být ještě mnohonásobně složitější. Celkově je práce velmi zdařilá a jen těžko se na ní hledají věci k vytknutí. Pokud bych měl být skutečně vybíravý, líbilo by se mi aby autorka navrhla či rozvedla řešení pro některé problémy identifikované v rámci této práce, případně navrhla ucelenější úvahy *de lege ferenda* či doporučení pro národního koordinátora, ale to by už šlo nad vytyčené zaměření práce.

MATUŠOVÁ, B.: SUBJEKTIVNÍ ODPOVĚDNOST ZA PROTIPRÁVNÍ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

MARTIN ERLEBACH¹

MATUŠOVÁ, B.: *Subjektivní odpovědnost za protiprávní zpracování osobních údajů. 2025, diplomová práce, Masarykova univerzita, Právnická fakulta, 74 s.*

ANOTACE

Tato diplomová práce se zabývá odpovědností za protiprávní zpracování osobních údajů, zejména sporem mezi českou teorií správního trestání a judikaturou Soudního dvora Evropské unie. Zatímco česká praxe dlouhodobě vycházela z objektivní odpovědnosti, SDEU ustálil požadavek zavinění jako podmínku pro uložení sankce. Práce analyzuje vývoj rozhodovací praxe Úřadu pro ochranu osobních údajů, sleduje přechod k subjektivní odpovědnosti a hodnotí dopady této změny na české správní trestání v oblasti ochrany osobních údajů.

KLÍČOVÁ SLOVA

GDPR, ochrana osobních údajů, odpovědnost, osobní údaje, protiprávní zpracování, správní trestání, Úřad pro ochranu osobních údajů

ABSTRACT

This thesis examines liability for unlawful processing of personal data, focusing on the conflict between Czech administrative penal theory and the case law of the Court of Justice of the European Union. While Czech practice has long been based on strict (objective) liability, the CJEU has established the culpability

¹ Mgr. Martin Erlebach je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontakt: Martin.Erlebach@law.muni.cz

requirement as a condition for imposing sanctions. The thesis analyses the development of the decision-making practice of the Office for Personal Data Protection, tracks the transition to subjective liability, and assesses the impact of this shift on Czech administrative sanctioning in the field of personal data protection.

KEYWORDS

Personal Data Protection, Liability, Personal Data, Unlawful Processing, Administrative Sanctioning, The Office for Personal Data Protection

Plná verze práce je dostupná z: <https://is.muni.cz/th/hp2df>

Autorka zvolila pro svou práci dobře vymezené téma, které je velmi aktuální vzhledem k relativně nedávnému posunu v judikatuře SDEU. Ostatně na to sama autorka vhodně v práci poukazuje. Téma je úzce zaměřeno na rozhodovací praxi SDEU a ÚOOÚ, proto vyžadovalo ze strany autorky větší množství kreativity při získávání informací nutných pro zodpovězení zvolené výzkumné otázky. Celkově hodnotím téma práce jako středně až velmi náročné. Většina této náročnosti je přitom tvořena nedostatkem volně dostupných informací a nutností jejich získávání skrze zákon o svobodném přístupu k informacím. Přitom takový postup u tohoto typu práce není obvyklý.

Práce „...analyzuje vývoj rozhodovací praxe Úřadu pro ochranu osobních údajů, sleduje přechod k subjektivní odpovědnosti a hodnotí dopady této změny na české správní trestání v oblasti ochrany osobních údajů.“ Alespoň takto autorka formuluje cíl práce v její anotaci. Dále pak v textu specifikuje také výzkumnou otázku, která zní: „...jakým způsobem lze při trestání porušení povinností dle GDPR sladit požadavky judikatury SDEU s pravidly stanovenými českou úpravou správního trestání.“ Tento cíl autorka naplňuje a na výzkumnou otázku v rámci práce odpovídá vhodně a uceleně. Na tomto místě bych také chtěl vyzdvihnout, že autorka takto jasně formulovala své cíle a výzkumnou otázku a následně se jich držela až do konce práce. Takto dobře naformulovaný výzkum není u prací tohoto typu běžný.

Práce je rozdělena do 5 kapitol, úvodu a závěru. V rámci tohoto členění autorka vhodně postupuje od obecnějších konceptů odpovědnosti ve správním právu přes koncepty subjektivní a objektivní odpovědnosti až po rozbor konkrétních rozhodnutí SDEU a rozhodovací praxe ÚOOÚ. Kapitoly na sebe tematicky navazují a provází čtenáře vhodně prezentovanou problematikou až k závěru. Hlavní jádro práce a její největší přínos je situován zejména v poslední kapitole před závěrem, kde autorka kriticky hodnotí rozhodovací praxi ÚOOÚ. Práce je celkově poměrně popisná a zhruba polovina se jí zabývá obecně koncepty objektivní a subjektivní odpovědnosti. Za zvláštní považuji dvě instance popisů fungování odpovědnosti čerpané z oblasti občanského práva a trestního práva. Přestože vztah správního trestání a trestního práva je zřejmý, přijde mi méně vhodné, aby byla koherence práce snižována těmito přílišnými odbočkami mimo oblast správního práva. Zejména vezmu-li v potaz, že jde o místa práce, kde autorka používá jedny z mála akademických zdrojů, což je obecně jeden z mála neduhů práce. Ocenil bych výrazně více zdrojů z akademického prostředí i k částem o správním právu. Jde ale spíš o mou preferenci než nutnost. a jsou využity na podporu popisu odpovědnosti v právních odvětvích, která nejsou předmětem práce.

V práci bych ocenil transparentnější postup při formulování metodologie výzkumu. Autorka, zejména v závěru, pracuje s „vybranými“ rozhodnutími ÚOOÚ a není zřejmé, jak tato rozhodnutí vybírala, nebo jak přesně hodnotila soulad rozhodovací praxe ÚOOÚ s judikaturou SDEU. Přestože z textu je poté možné dovodit, jak hodnocení zhruba probíhalo, ocenil bych alespoň drobnou metodologickou kapitolu vysvětlující důvody za zvolenými postupy jakož i důvody výběru daných rozhodnutí ÚOOÚ.

Přes tyto problémy musím ocenit závěry, ke kterým autorka v práci dochází. Poukázání na pouze formální soulad s judikaturou SDEU v rozhodovací praxi ÚOOÚ je na místě a skvělým závěrem práce. Autorka tento kritický závěr na můj vkus formuluje možná až příliš zdrženlivě, ale to není něco, co bych chtěl kritizovat.

Je tedy možné shrnout, že jde o obsahově zdařilý text, i když z větší části popisný. Ocenil bych sice větší množství autorčiných originálních

vstupů, ale to by naopak ubralo na jinak velmi úzkém zaměření práce. Kromě méně průhledné metodologie a několika málo drobných odboček od tématu zmíněných výše, je na práci těžké najít po obsahové stránce něco ke kritice.

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>).

SZABÓ, M: SVOBODA PROJEVU NA INTERNETOVÝCH PLATFORMÁCH

FRANTIŠEK KASL¹

Szabó, M: Svoboda projevu na internetových platformách. 2025, diplomová práce, Masarykova univerzita, Právnická fakulta, 128 s.

ANOTACE

Diplomová práce se zabývá svobodou projevu na online platformách v kontextu Nařízení o digitálních službách (DSA) a souvisejících pravomocí koordinátorů digitálních služeb (DSCs). Cílem práce je zhodnotit, jak mohou tyto národní instituce přispět k ochraně svobody projevu online. Obecná část práce popisuje nařízení DSA a relevantní kompetence DSCs. Zvláštní část se zaměřuje na praktické využití a institucionální nastavení národních úřadů. Práce zároveň prezentuje roli DSCs při ochraně svobody projevu na případových studiích Irska, Německa a Rumunska. Z nich pak vyvozuje doporučení.

KLÍČOVÁ SLOVA

Svoboda projevu; internetové platformy; systémová rizika; DSA; akt o digitálních službách; koordinátoři digitálních služeb; DSC; moderace obsahu

ABSTRACT

The thesis deals with freedom of speech on internet platforms in the context of the Digital Services Act (DSA) and the related powers of Digital Service Coordinators (DSCs). The aim of the thesis is to assess how coordinators contribute to the protection of freedom of expression online. The general part of the thesis

¹ JUDr. Ing. František Kasl, Ph.D. je odborným asistentem na Ústavu práva a technologií na Masarykově univerzitě v Brně. Kontakt: frantisek.kasl@muni.cz

describes the DSA regulation and the relevant competences of the DSCs. The specific part focuses on the practical competences and institutional settings. The thesis also presents the role of DSCs through case studies of Ireland, Germany and Romania.

KEYWORDS

Freedom of Expression; Online Platforms; Systemic Risks; Digital Services Act; Digital Service Coordinators; Content Moderation

Plná verze práce je dostupná z: <https://is.muni.cz/th/gptts/>

Autor si zvolil téma vysoce aktuální a do značné míry náročné s ohledem na novost předmětné právní úpravy a dynamický vývoj jejího výkladu a aplikace v praxi. Toto následně přiměřeně reflektoval zahrnutím tří případových studií, skrze které autor dobře zacílil diskuzi na nejvýznamnější rysy řešené problematiky.

Za cíl si autor v úvodu práce stanovil zhodnotit, jakou roli hrají koordinátoři zřízení národními státy podle regulace DSA při ochraně svobody projevu na internetu, z čehož formuloval výzkumnou otázku "Jakým způsobem mohou národní koordinátoři svoje kompetence efektivně využít k tomu, aby chránili, či naopak omezovali, svobodu projevu online?" Práce je zdařile strukturovaná tak, že čtenáři poskytuje podrobné pojednání směřující k tomuto cíli a v závěru autor poskytuje nejen dobře argumentovanou odpověď na výzkumnou otázku,² ale též výstižně shrnuje stěžejní části textu a poskytuje tak přehledné "manažerské shrnutí".³

Autor prokazuje značnou akademickou vyspělost a schopnost důsledné práce s dostupnými zdroji, reflexi širšího kontextu, výstižných shrnutí komplexní právní úpravy i dobře argumentovaných postojů a komentářů. Na s. 20 výstižně odlišuje rizika spojená s nečinností národních koordinátorů a naopak rizika spojená s jejich neefektivní činností a formuluje paradigmat, která se v práci následně znatelně odrážejí.

² Viz s. 104 závěrečné práce.

³ Viz s. 100-103 závěrečné práce.

V kapitole 2 je autorem poskytnut robustní teoretický základ právního pojetí svobody projevu, který má velmi solidní zpracování a poukazuje na důslednou rešerši zdrojů i autorovu orientaci v širší problematice. Zde i v následujících kapitolách autor čerpá ze širokého okruhu související odborné literatury, u které opakovaně prokazuje schopnost její reflexe při zpracování vlastního odborného textu. V práci je v poznámce pod čarou č. 50⁴ nadto poukázáno na související autorovu odbornou publikační činnost v časopise Právník.

V kapitole 3 je představena předmětná úprava koordinátorů digitálních služeb (DSC) v nařízení o digitálních službách (DSA). Velmi oceňuji, že autor disciplinovaně a transparentně soustředí svou pozornost na instituty související s tématem práce a nezaplňuje tedy práci nadbytečnou "vatou". V této části bych pak vyzdvihl autorovu polemiku a logickou argumentaci vlastních pohledů v podkapitole 3.2.2, zvláště ohledně institutu důvěryhodných oznamovatelů.

Kapitola 4 je zaměřena na výlučné kompetence národních koordinátorů. I tato část je zpracována na vysoké úrovni, je však na místě upozornit, že autor v podkapitolách 4.1.1 a 4.1.2 nepřesně pojednává o udělení statusu důvěryhodného oznamovatele a prověřeného výzkumného pracovníka jako o certifikaci. V podkapitole 4.2 je představen a dobře okomentován příklad irského DSC. Autor zde zahrnul i srovnání s nedostatky vymáhání povinností dle GDPR irským dozorovým úřadem a zdárně propojuje tento exkurz se svým zhodnocením předpokladů účinnosti fungování irského DSC. Dále autor v práci poskytuje dobrý rozbor nedávného vývoje dynamiky interakce velkých platforem a politické reprezentace, přičemž vystihuje i geopolitický rozměr americko-evropských vztahů, který dokládá i překvapivě nízká sankce udělená Komisí společnosti Meta v dubnu 2025 za porušení DMA v souvislosti s modelem pay or ok. V podkapitole 4.2.3 autor poskytuje dobré zhodnocení předpokladů pro naplnění role DSC. Výstižná je taktéž poznámka autora o možném vlivu politiky na aktivity Komise.⁵

⁴ Viz s. 27 závěrečné práce.

⁵ Viz s. 70 závěrečné práce.

Kapitola 5 se věnuje kompetencím, které národní koordinátoři sdílejí s Komisí, tedy problematice velmi velkých online platform (VLOPs). I zde autor zvolil vhodné případové studie nedávných prezidentských voleb v Rumunsku a parlamentních voleb v Německu. Práce obsahuje střídme a vyvážené zhodnocení komplexní otázky povinností společnosti TikTok ve vztahu k rumunským volbám s důslednou rešerší zdrojů, které jsou řádně reflektovány v argumentaci autora. Na dobré úrovni je také pojednání o kodexech chování dle čl. 45 DSA a komentář o jejich ne zcela dobrovolné povaze pro VLOPs.⁶ Zdařilé je i pojednání o krizových stavech včetně výstižných komentářů a zhodnocení autorem, které vedou mmj. k zajímavým úvahám o hrozbě politického vlivu na postoj Sboru k vyhlášení krizového stavu.⁷

Kapitola 6 je diskuzní kapitolou ohledně budoucího vývoje a doporučení autora a obsahuje především validní apel na kvalitu expertízy obsazení DSC na s. 95-96, ale též dobré zhodnocení geopolitických vlivů na aplikaci nařízení i rizik přílišného paternalismu Komise.⁸

V závěru práce je důsledně reflektována výzkumná otázka zvolená v úvodu práce a formulován výsledný postoj autora. Současně je zde již výše zmíněné "manažerské shrnutí" hlavních bodů z předchozích částí práce.

Celý text je přes svůj značný rozsah úzce provázán s řešenou problematikou a autor celkově poskytuje velmi čtivé a informačně bohaté pojednání, které dle mého názoru obohacuje odborný diskurz značně nad rámec požadavků na diplomovou práci a zaslouží si pozornost širšího odborného publika.

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>).

⁶ Viz s. 85-86 závěrečné práce.

⁷ Viz s. 93 závěrečné práce.

⁸ Viz s. 98-99 závěrečné práce.

GROMAN, L.: PRÁVNÍ ASPEKTY UŽITÍ TECHNOLOGIE DEEPPFAKE VE FILMU

TINA MIZEROVÁ¹

GROMAN, L.: Právní aspekty užití technologie deepfake ve filmu. 2025, diplomová práce, Masarykova univerzita, Právnická fakulta, 92 s.

ANOTACE

Diplomová práce zkoumá ochranu osobnosti při užití technologie deepfake ve filmu. Po klasifikaci možných užití v kinematografii se věnuje zejm. nekon-senzuálnímu umístění herce či slavné osobnosti do filmového nebo televizního snímku. Pozornost je soustředěna na zásah do ochrany podoby člověka, důstojnosti i jeho majetkových zájmů. Rozebrány jsou okolnosti, které mohou pod-miňovat ochranu, a to jak týkající se snímku, tak i osoby. Na typizovaných příkladech pořadí demonstruje střet protichůdných zájmů herce a tvůrce. Okrajově představí i smluvní užití jakožto vhodnou cestu pro aplikaci deepfake.

KLÍČOVÁ SLOVA

Deepfake, umělá inteligence, film, umění, ochrana osobnosti, podoba člověka, důstojnost, majetkový zájem, karikatura

ABSTRACT

The thesis examines the protection of personality in the use of deepfake technology in film. After a classification of possible uses in cinema, it focuses on the non-consensual placement of an actor or a celebrity in a movie or TV show. Attention is paid to the interference with the protection of the image, dignity and

¹ Mgr. et Mgr. Tina Mizerová je doktorandkou na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontakt: tina.mizerova@mail.muni.cz

property interests. The circumstances that may condition protection are discussed, both in relation to the show and the person. Using typified examples of programmes, it demonstrates the competition of conflicting interests of the actor and the creator. It will also marginally introduce the contractual use as a suitable method for the application of deepfake.

KEYWORDS

Artificial Intelligence, Movie, Art, Personality Rights, Image, Dignity, Property Interest, Satire

Plná verze práce je dostupná z: <https://is.muni.cz/th/s8gwe>

Autor se v práci zabýval problematikou využití deepfake technologie ve filmu v kontextu práva na ochranu osobnosti dotčených herců a hereček. Téma je rozhodně zajímavé a originální, náročnost spočívá především v tom, že autor aplikuje závěry stávající legislativy a judikatury v kontextu technologie, o níž soudy ještě nerozhodovaly. Zvolené téma tak kromě právní analýzy po autorovi vyžadovalo seznámení se s problematikou využití deepfake technologie ve filmu a spojení této technologie s východisky stávající legislativy a judikatury. Zároveň jde o téma v českém právním prostředí dosud nezpracované, což obecně zvyšuje relevanci a přínos práce autora.

Autor se měl v práci zabývat využitím technologií deepfake ve filmu a s tímto tématem související zákonnou úpravou, zejména se zaměřením na právní úpravu ochrany osobnosti. V úvodní části práce autor deklaruje, že se bude zabývat výhradně právem na ochranu osobnosti, a to zejména v kontextu využití deepfake v rámci filmu či videa bez souhlasu vyobrazeného herce, okrajově se zabývá vyobrazením na základě smlouvy a kvůli rozsáhlosti tématu z diplomové práce vylučuje situace, kdy je herec vyobrazen po své smrti. Zadáání práce a provedenému zúžení jejího záběru odpovídá i autorem v úvodu položená výzkumná otázka: "Za jakých okolností dochází k zásahu do subjektivních práv osoby, která je ztvárněna v zábavním snímku za užití technologie deepfake, a to konkrétně do jejího osobnostního práva a majetkových zájmů, a jaké jsou limity právní ochrany takové

osoby.” Přestože v rámci práce autor na tuto otázku neodpovídá explicitně, celkově ale v rámci práce na tuto v úvodu položenou otázku odpovídá a zadání práce tak lze považovat za splněné.

Po úvodu, ve kterém autor vymezil, čemu se v práci bude věnovat, následuje první část práce, v níž autor představuje deepfakes, jejich použití ve filmovém průmyslu a zabývá se i dvěma souvisejícími tématy, které ale leží mimo pozornost představené práce: deepfake pornografií a ztvárněním zesnulého herce. Autor v této části pracuje s relevantními zdroji a z textu jde vidět, že dané problematice rozumí (obecně je propojení autorovy znalosti možností využití deepfake ve filmu s relevantní právní úpravou nejsilnější stránkou práce). V této části práce mi trochu chybělo podrobnější představení deepfake, včetně například dostupné legální definice v čl. 3 odst. 60 aktu o umělé inteligenci, neboť část, v níž se autor věnoval představení fenoménu deepfake a technologie byla na poměry práce, která se zabývá právními aspekty využití této technologie dost obecná.

Následuje druhá část, v níž se autor aplikuje právní úpravu ochrany osobnostních práv na různé případy využití deepfake ve filmu či jiných audiovizuálních produktech (reality shows nebo tvorbě fanoušků). Právní analýza jednotlivých se prolíná celou kapitolou, je velmi kvalitně provedená a autor s relevantní právní literaturou i judikaturou.

Problematická je ale struktura této části. Po úvodu věnujícímu se základnímu výkladu ohledně ochrany osobnosti přechází autor k aplikaci těchto poznatků na použití deepfake ve filmu, satirických pořadech, reality shows a kontroverzních filmech, následně opět přeskakuje k právnímu výkladu o nižší ochraně osobnostních práv osob veřejného zájmu, aby po dvou podkapitolách zase přeskočil ke konkrétním případům. Práci by prospělo, kdyby se autor nejprve představil východiska právní úpravy a až poté je aplikoval na konkrétní případy. Podle zadání práce měl autor provést případové studie. V práci ale autor spíše aplikuje poznatky na vybrané související případy. To ukazuje na další nedostatek práce, a to chybějící metodologickou část, v níž by autor lépe popsal, jak bude v práci postupovat a proč vybral zrovna tyto případy z praxe. Taková kapitola by přispěla k lepší přehlednosti a srozumitelnosti práce.

Část práce věnovanou právnímu výkladu pak uzavírá podkapitola věnující se užití deepfake technologie pro vyobrazení herce na základě uzavřené smlouvy, kde se autor zabývá především odlišnostmi situací, kdy je herec prostřednictvím deepfake vyobrazen na základě smlouvy oproti situacím vyobrazení bez smlouvy a některé limity využití tohoto nástroje. Obecně tak jde o kvalitní právní analýzu, jejíž kvalitu ale snižuje struktura výkladu, kterou autor zvolil. Vzhledem k hodnocení poznamenávám, že v kategorii prospěl tato práce určitě patří k těm povedenějším.

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>).

BAUMANN, R.: OCHRANA MODELU STROJOVÉHO UČENÍ PRÁVEM DUŠEVNÍHO VLASTNICTVÍ

DAMIÁN PALAŠTA¹

BAUMANN, R.: Ochrana modelu strojového učení právem duševního vlastnictví. 2025, závěrečná práce v programu LL.M. v právu informačních a komunikačních technologií, Masarykova univerzita, Právnická fakulta, 119 s.

ANOTACE

Závěrečná práce sa zaoberá problematikou ochrany modelov strojového učenia podľa práva duševného vlastníctva EÚ. Systematicky analyzuje a kriticky hodnotí, do akej miery je možné chrániť jednotlivé komponenty modelu, ako sú zdrojový kód, architektúra, tréningové dáta a autonómne generované parametre. Ťažisko spočíva v aplikácii troch pilierov ochrany, a to autorského práva, databázového práva sui generis a patentového práva, s cieľom posúdiť, či existujúci právny rámec adekvátne chráni investície do tejto kľúčovej technológie.

KLÍČOVÁ SLOVA

Strojové učenie, umelá inteligencia, právo duševného vlastníctví, model strojového učenia, autorské právo, ochrana databáz, patentové právo, trénovateľné parametre

ABSTRACT

This thesis addresses the protection of machine learning models under EU intellectual property law. It systematically analyzes and critically evaluates the ex-

¹ Mgr. Damián Palašta je doktorandem na Ústavu práva a technológií Právnické fakulty Masarykovy univerzity. Kontakt: 554257@mail.muni.cz

tent to which individual model components, such as source code, architecture, training data, and autonomously generated parameters, can be protected. The focus lies on applying the three pillars of protection – copyright, sui generis database rights, and patent law – to assess whether the existing legal framework adequately protects investments in this key technology.

KEYWORDS

Machine Learning, Artificial Intelligence, Intellectual Property Law, Machine Learning Model, Copyright Law, Database Protection, Patent Law, Trainable parameters

Plná verze práce je dostupná z: <https://is.muni.cz/th/i0dio>

Z hľadiska náročnosti výberu možno jednoznačne povedať, že predkladaná kvalifikačná práca sa dotýka vysoko aktuálnej a náročnej problematiky – a to regulácie práva duševného vlastníctva vo vzťahu k modelom umelej inteligencie, prípadne k umelej inteligencii ako takej, vrátane jej premenných a parametrov. Tému osobne považujem za veľmi náročnú, o to viac, že umelá inteligencia predstavuje určitú formu paradigmatickej zmeny aj vo sfére aplikácie právnych inštitútov. Súčasnú judikatúru nemožno opomenúť, aj keď sama o sebe nedáva všetky odpovede - skôr naznačuje, a to napriek jej súčasnému vývoju. Autor sa do problematiky pustil „naplno“ a ne snažil sa ju zjednodušovať – spracovanie je komplexné. Zvolil tri prístupy: po prvé autorskoprávnu ochranu, ktorá je tradične relatívne najviac skúmaná a kde existuje množstvo odbornej literatúry; po druhé ochranu databáz, ktorá je už menej explorovaná; a napokon patentové riešenia pre ochranu AI, ktoré sú z hľadiska aplikácie ešte náročnejšie. Práca si vyžiadala intenzívnu prácu s odbornou literatúrou, predovšetkým zahraničnou, a je zjavné, že autor musel naraz zvládať technické, právne aj koncepčné výzvy. Niektoré poznámky sa ešte budú týkať formy a konceptu, no už teraz možno povedať, že práca dosahuje veľmi vysokú úroveň.

Možno povedať, že autor si stanovil za cieľ preskúmať problém, ako je možné chrániť modely strojového učenia podľa práva duševného vlastníctva.

tva Európskej únie. Cieľom bolo systematicky analyzovať a kriticky zhodnotiť, do akej miery je možné chrániť jednotlivé komponenty modelu – zdrojový kód, architektúru, tréningové dáta a autonómne generované parametre. Ťažisko práce spočívalo v aplikácii troch pilierov ochrany: autorského práva, databázového práva *sui generis* a patentového práva, s cieľom posúdiť, či existujúci právny rámec dokáže adekvátne chrániť investície do tejto kľúčovej technológie.

Čo sa týka poslednej otázky – či právny rámec investície skutočne adekvátne chráni – to je otázka možno aj mimo čistej právnej dogmatiky. Ale vo všeobecnosti mám za to, že autorovi sa podarilo ciele naplniť. Prvá časť práce (kapitoly 1–4) je viac súhrnná, mapuje a vysvetľuje súčasný stav, čo je vzhľadom na povahu novej technológie úplne správne. Druhá časť (kapitoly 5–8) predstavuje jadro práce, kde sú položené a analyzované samotné otázky právnej ochrany.

V kapitole 5 sa autor venuje autorskoprávnej ochrane softvéru a modelov strojového učenia. Kapitola 6 rozvíja autorskoprávny pohľad na tréňované modely, konceptne pomenované ako „Software 2.0“. Kapitola 7 sa obracia na právnu povahu dátových komponentov systémov umelej inteligencie a možnosti ich ochrany databázovým právom. Kapitola 8 napokon skúma patentovú ochranu modelov strojového učenia. Autor v týchto častiach dospel k viacerým záverom, a to, že najperspektívnejšia je ochrana prostredníctvom autorského práva pre zdrojový kód, aj keď jej limity sú zrejmé. Ochrana tréningových súborov resp. dát, je podľa autora prakticky nedosiahnuteľná, pretože tieto komponenty nie sú výsledkom tvorivej činnosti, ale sú skôr súčasťou procesov. Databázová ochrana má svoje špecifické podmienky – systematické usporiadanie a podstatnú investíciu – ktoré sú v kontexte umelej inteligencie problematické. Patentová ochrana je síce konceptne možná, no vo väčšine prípadov narazí na limity nepatentovateľnosti algoritmov a matematických metód.

Z hľadiska celku možno povedať, že skúmať takúto širokú paletu vzťahov práva duševného vlastníctva na tému umelej inteligencie je veľmi ambiciózny cieľ. Napriek tomu, autor naplno využil dostupnú literatúru, analyzoval judikatúru a vytvoril vlastné kritické hodnotenie. Ciele, ktoré si

stanovil, boli splnené – a to v miere, ktorá je primeraná náročnosti a novosti skúmanej témy.

Práca má potenciál aj pre ďalšie smerovanie – ak by autor uvažoval napríklad o doktorandskom štúdiu. Zvolený prístup je veľmi široký, čo prináša výhodu komplexnosti, ale aj nevýhodu v tom, že nie je možné vždy kriticky rozvinúť každú otázku do hĺbky. Autor si vybral tri spektrá práva duševného vlastníctva – autorské, databázové a patentové právo. To je ambiciózne a hodnotné, ale zároveň sa tým práca miestami rozptyľuje. Ak by šlo o praktickú aplikáciu, dalo by sa rozšíriť aj na obchodné tajomstvo, ktoré hrá v tejto oblasti veľkú rolu, no autor vedome zostal v rámci tradičných pilierov ochrany.

Prvé kapitoly (2–3) sú úvodom do umelej inteligencie a strojového učenia. Považujem to za dôležité a správne, pretože práca je právnická, a tak je potrebné vysvetliť, čo je vlastne technickým základom celej témy. Takýto úvod má analógiu aj v súdnej praxi – napríklad v USA je bežné, že súd (resp. žalobca) si najskôr vysvetlí technológiu a až potom aplikuje právne normy. V tomto duchu má práca veľmi dobrý základ.

Od kapitoly 5 vyššie sa práca stáva jadrom autorskoprávna ochrana softvéru (kap. 5), autorskoprávny pohľad na trénované modely (kap. 6), právna povaha dátových komponentov - databázy (kap. 7) a napokon patentová ochrana (kap. 8). Každá z týchto kapitol by pokojne mohla byť samostatnou kvalifikačnou prácou – a to je dôkaz, že téma je nesmierne široká. Text je pritom vždy podopretý literatúrou, prevažne zahraničnou, čo je veľké pozitívum.

Autor neprináša nové vedecké teórie, ale robí syntézy a na ich základe formuluje vlastné závery. V niektorých častiach možno cítiť skratky alebo zjednodušenia, no vo väčšine prípadov sú presvedčivé a dávajú zmysel. Oceňujem najmä kritické zamyslenia v kapitolách 6–8, kde sa autor nespolieha len na zdroje, ale aj sám hodnotí, čo považujem za známku kvality.

ŽVÁČEK, A.: AUTORSKOPRÁVNÍ ASPEKTY TRACINGU

DAMIÁN PALAŠTA¹

ŽVÁČEK, A.: Autorskoprávní aspekty tracingu. 2025, diplomová práce, Masarykova univerzita, Právnická fakulta, 114 s.

ANOTACE

Práce se zabývá autorskoprávními aspekty tracingu, tj. netradiční způsob odvozené tvorby. Tracing, dílo ním vytvořené a tím zasažená práva autora jsou analyzována v autorském právu ve světle relevantní judikatury Soudního dvora Evropské unie a českého Nejvyššího soudu. Učiněné poznatky jsou komparovány s případy zabývajícími se tracingem ze Spojených států amerických a Japonska. Dále je zkoumána aplikovatelnost výjimek a omezení pro tracing. Výsledkem práce je pragmatická subsumpce tracingu do českého autorského zákona, společně s návrhem, jak tracing právně regulovat.

KLÍČOVÁ SLOVA

Autorské právo, tracing, autorské dílo, odvozené dílo, autorskoprávní individualita, obecný fond, výtvarné dílo, choreografie

ABSTRACT

Thesis deals with copyright aspects of tracing, i.e., a non-traditional method of derivative creation. Tracing, the work created by it and the author's rights affected by it are analysed in copyright law, considering relevant case law of the Court of Justice of the European Union and the Czech Supreme Court. The fin-

¹ Mgr. Damián Palašta je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontakt: 554257@mail.muni.cz

dings are compared with cases of tracing from the United States and Japan. Next is examined the applicability of exceptions and limitations to tracing. The result is a pragmatic subsumption of tracing into Czech copyright law, together with a proposal on how to legally regulate tracing.

KEYWORDS

Copyright, Author's Work, Derivative Work, Individuality of Author's Work, Public Domain, Artistic Work, Choreography

Plná verze práce je dostupná z: <https://is.muni.cz/th/r71x2>

Môžem s väčšou istotou konštatovať, že autor si zvolil tému mimoriadne aktuálnu a právne náročnú, ktorú spracováva na vysoko nadpriemernej úrovni, s analytickými úvahami presahujúcimi štandardné požiadavky kladené na diplomovú prácu. Problematika tracingu z pohľadu autorského práva pritom nadobúda čoraz väčší význam aj v rámci Európskej únie, Českej a Slovenskej republiky, a to aj s prihliadnutím na vývoj v Japonsku alebo Spojených štátoch, kde už majú litigáciu, či už tracing stricto alebo largo sensu. Absencia judikatúry/rozsudkov, ktorá by v rámci EÚ túto otázku priamo riešila, núti akademickú obec opierať sa najmä o rozhodnutia v iných oblastiach autorského práva – čo samo o sebe hovorí o aktuálnosti zvolenej témy.

Z vyššie popísaných dôvodov si diplomová práca kladie za cieľ odpovedať na výskumnú otázku: „Jak kvalifikovat tracing pohledem českého autorského práva?“, pričom reflektuje relevantnú judikatúru Súdneho dvora Európskej únie a vnútroštátnych súdov, spolu s tuzemskou i zahraničnou odbornou monografiou a komentárovou literatúrou.

Možno povedať, že autor nielenže odpovedá na položenú výskumnú otázku, ale ju v niektorých pasážach aj presahuje. Osobitnú pozornosť si zasluhuje komparácia českého, japonského a amerického prístupu k autorskoprávnej regulácii tracingu, ktorá je spracovaná na vysokej teoretickej úrovni.

Možno konštatovať, že autor stanovený cieľ práce nielenže splnil, ale niektoré jeho úvahy rámec pôvodného zadania aj prekročili – a to nielen v teoretickej rovine, ale aj v časti *de lege ferenda*. Za najhodnotnejšiu považujem kapitolu 6.1 - Zákonná licence pro tracing, a to najmä pre jej potenciálny dopad na právnu prax a zvýšenie predvídateľnosti v tejto dynamicky sa vyvíjajúcej oblasti.

Ostatné kapitoly sú spracované na nadpriemernej odbornej úrovni, a to tak po obsahovej, ako aj analytickej stránke.

Prácu považujem za nadštandardnú a jednoznačne ju odporúčam na ďalšie odborné publikovanie – či už vo forme článku, monografie alebo ako východisko pre ďalší výskum. Bola by škoda, keby zapadla bez širšej odbornej reflexie.

Práca je výborne vystavaná. Autor postupuje systematicky od komparácie vybraných zahraničných autorskoprávných úprav, cez analýzu fenoménu tracingu, až po aplikáciu v podobe kazuistiky. Vhodne zvolený informačný aparát – práca s tabuľkami, grafmi a vizuálnymi prvkami – dopomáha čitateľovi k pochopeniu témy a autorových úvah, ktoré sú formulované na viac než primeranej úrovni.

Čitateľnosť práce je vysoká, s výnimkou niekoľkých miest, ktoré by si zaslúžili precizáciu. Napríklad tvrdenie na strane 36:

”Je nutné podotknout, že nikoli každý případ tracingu je nakonec odhalen a dovolím si tvrdit, že většina případů, kdy dojde k odhalení tracingu, neskončí před soudem, ale dojde k mimosoudnímu vyrovnání. Toto tvrzení je založené na faktu, že soudy musí řešit tyto případy ad hoc, neboť z výše uvedených důvodů se jednotlivé případy mohou lišit, a proto stejný výsledek není zaručen. Dále se domnívám, že i dokazování tracingu bude nákladné, a proto může některé autory od podání žaloby odradit.”

Toto tvrdenie by si zaslúžilo oporu v údajoch alebo aspoň analogickú paralelu – napríklad cez porovnanie so stavom sporov alebo cez zmienku relevantnej sekundárnej literatúry (napr. Husovec a jeho práca na tému DSA a IP litigácie, príp. empirické poznatky z oblasti litigácie Google).

Na strane 39 autor uvádza, že ”Dokonce se domnívám, že rozmnoženina (neúplná napodobenina) musí vzniknout v průběhu tracingu vždy, avšak sa-

ma o sobě není konečným výsledkem (novým dílem)”. V tejto súvislosti by som odporúčal presnejšie rozpracovať, čo znamená pojem „rozmnožovanie“ v autorskoprávnom zmysle, najmä vo vzťahu k § 2 ods. 6 českého autorského zákona, ktorý sa týka tzv. obecného fondu. Nie je celkom zrejmé, či by rozmnoženie časti diela, ktorá patrí do verejnej domény, mohlo byť ešte považované za rozmnožovanie chráneného diela – najmä v prípadoch, keď je možné dokázať, že ide o čerpanie výlučne z týchto prvkov. Formulácia by mohla byť doplnená o úvahu, či je relevantné hovoriť o rozmnožovaní diela aj v prípade, keď je využitý iba „obecný fond“, resp. keď nie je možné preukázať zásah do príslušného diela. Viď aj spomínaný rozsudok – Najvyššieho súdu zo dňa 24. 3. 2021, sp. zn. 27 Cdo 2023/2019 („mít Filipa“ – najmä body 34–35 rozsudku).

Na strane 42 autor uvádza, že „extenzívnym výkladom by bolo možné hovoriť o inspirácii ako o prevzatí časti pôvodného diela, ktorá obsahuje prvky z obecného fondu, ako napríklad myšlienku.“ V tejto súvislosti považujem za nevyhnutné zdôrazniť, že myšlienky ako také nepodliehajú autorskoprávnej ochrane, keďže ochrana sa podľa právnej doktríny vzťahuje výlučne na ich konkrétne vyjadrenie. Prvky z tzv. obecného fondu – vrátane samotných ideí, princípov či štýlov – nie sú predmetom ochrany podľa českého autorského zákona. V tejto pasáži by preto bolo vhodné doplniť jasné kvalifikačné kritérium, podľa ktorého možno rozlíšiť, kedy ide ešte o legitímnu inšpiráciu a kedy už o zásah do autorsky chráneného diela. Z pohľadu praktickej aplikácie práva je vhodné vedieť, od akého momentu možno aplikovať autorské právo a na základe akého testu (napr. substantial similarity).

V tomto ohľade možno jednoznačne konštatovať, že študent preukázal výbornú znalosť a orientáciu v danej problematike, a to nielen v rovine českej právnej úpravy, ale aj v kontexte zahraničných prístupov a aktuálnej judikatúry. Téma je spracovaná systematicky, odborne a s vysokou mierou samostatnosti, čo sa prejavuje nielen v schopnosti syntetizovať náročné informácie, ale aj v ich uchopení a interpretácii. Autor zvládol problematiku s nadštandardnou analytickou hĺbkou, pričom výsledkom je ucelený odborný text, ktorý má potenciál presiahnuť rámec diplomovej práce a ob-

stáť aj ako odborný článok či podklad pre širšiu akademickú diskusiu. Za zvlášť hodnotné považujem spracovanie kapitoly de lege ferenda (6), ktorá svedčí o kontakte s praxou – či už explicitne alebo v uvažovaní o dopadoch riešení na aplikačnú rovinu.

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>).

LEISER, M.: DARK PATTERNS, DECEPTIVE DESIGN, AND THE LAW. AI'S HIDDEN INFLUENCE ON OUR DIGITAL EXPERIENCE

KRISTÝNA AKIL¹

LEISER, M.: Dark patterns, deceptive design, and the law: AI's hidden influence on our digital experience. Oxford: Hart Publishing, 2025, 363 s. ISBN 978-1-50998-711-5.

1. ÚVOD

Dark patterns představují praktiky, které spočívají v úpravě designu takovým způsobem, který narušuje autonomní rozhodovací proces uživatele. Může se jednat jak o úpravu webového rozhraní nebo cookie lišty, tak o nastavení systému v zařízeních, které jsou součástí internetu věcí. Dark patterns jsou dlouholetým fenoménem, který fascinuje mnoho akademiků, a pozornost jim je věnována také z pohledu legislativy. Výslovně byly poprvé zmíněny v nařízení o digitálních službách, které nabylo účinnosti v roce 2024. Nicméně na dark patterns lze aplikovat i starší evropské legislativní akty, zejména směrnici o nekalých obchodních praktikách.

Klamavý design, jak v úvodu vyjasňuje sám autor, je širší pojem než dark patterns – zahrnuje praktiky, které zneužívají zranitelnosti uživatelů, skryté poplatky nebo komplexní úpravy samotné architektury systému,² včetně praktik využívající umělou inteligenci. Autor ve svém pojetí do klamavého designu řadí také personalizaci, kterou označuje za manipulativní.

¹ Mgr. Kristýna Akil je doktorandkou na Ústavu práva a technologií, Právnické fakulty Masarykovy univerzity, a právničkou na Pracovišti pověřence pro ochranu osobních údajů na Rektorátu Masarykovy univerzity. Kontaktní e-mail: kristyna.akil@law.muni.cz.

² LEISER, M. Dark patterns, deceptive design, and the law: AI's hidden influence on our digital experience. Oxford: Hart Publishing, 2025, s. xvii.

Kniha je výsledkem dlouholetého úsilí Leisera přispět ke srozumitelnosti dark patterns a jeho snahy vyjasnit aplikovatelnost jednotlivých evropských regulací.³ Vzhledem ke svojí komplexnosti je kniha bezpochyby nepominutelným přínosem v oboru. Autor v první polovině knihy komplexně shrnuje dosavadní poznatky v oblasti dark patterns a ve druhé části analyzuje dark patterns a personalizaci z pohledu regulace umělé inteligence. Důraz na umělou inteligenci významně přispívá k aktuálnosti závěrů a podtrhuje přínos této knihy.

Kniha je formálně rozdělena do tří částí, nicméně není jim věnován stejný prostor a jako jádro knihy by se daly považovat pouze první dvě části. V první části nazvané Dark, Darker, and Darkest Patterns se autor zabývá nejen dark patterns, ale také jinými klamavými designy a jejich vymezení. Současně tyto praktiky analyzuje z perspektivy evropských legislativních aktů. Ve druhé části Manipulation Beneath the Interface se autor zaměřuje na tři hlavní oblasti – uživatelské rozhraní, umělou inteligenci a koncept zranitelnosti. Význam umělé inteligence rozebírá zejména z pohledu aktu o umělé inteligenci, čímž pokrývá celý balíček nejnovější evropské digitální legislativy. Třetí, nejmenší část tvoří závěr knihy, kde se autor věnuje nástinu možných směrů, které by mohly přispět ke zlepšení regulace manipulativního designu.

Autor v knize popisuje širokou škálu praktik, od primitivních až po komplexní. Radí mezi ně přizpůsobení profilového obrázku chatbota, skryté poplatky, časové měřiče, personalizované reklamy, řazení obsahu na webové stránce a spoustu dalších. V průběhu knihy všechny tyto praktiky označuje za manipulativní a zároveň je řadí do množiny praktik, které označuje jako „klamavý design.“ Leiser se zabývá také tím, jaké újmy mohou takové praktiky způsobit, nicméně napříč knihou se odkazuje právě na pojem „manipulativní praktiky,“ který nijak nevymezuje a není zřejmé, zda autor veškeré formy těchto praktik považuje za klamavé a manipulativní. Přidává se tak ke stoupajícímu trendu označování

³ Srov. Např. LEISER, M., Caruana, M. Dark Patterns: Light to be found in Europe's Consumer Protection Regime. *Journal of European Consumer and Market Law*, 2021, roč. 10, č. 6.

praktik za „manipulativní“ bez jakéhokoli právního ukotvení.⁴ Pro zjednodušení jsou v této recenzi tyto pojmy používány tak, jak jsou používány v knize.

2. TEMNÝ, KLAMAVÝ A MANIPULATIVNÍ

V první části knihy autor nejprve představuje několik drobných případových studií, na nichž zjednodušeně ilustruje, jaké typy praktik společnosti využívají v digitálním prostředí k ovlivnění rozhodování uživatelů, a do jaké hloubky mohou společnosti v těchto praktikách zajít. Jednou z nich je případ dospívající Jessicy, u níž algoritmus vyhodnotí problém s psaním a interpretací textu a následně jí jsou prezentovány personalizované obchodní podmínky v komplikované podobě, aby byla zvýšena šance, že jim Jessica bude obtížně rozumět a bez dalšího je přijme. Jako další příklad autor uvádí příběh dívky, která sdílela na sociální síti parte svého dědečka a v den, kdy uplynul rok od jeho úmrtí, dívka na webové stránce komunikuje s chatbotem. Algoritmus zvolí pro chatbota profilový obrázek starého pána s brýlemi, aby v dívce podvědomě vyvolal vzpomínky na dědečka, se kterým si dle interakcí na sociálních sítích byla zjevně blízká, a aby byla tak při pohledu na obrázek staršího pána byla zranitelnější. Vzhledem k tomu, že případy nejsou ocitovány, a vzhledem k povaze uvedených příkladů lze předpokládat, že jsou smyšlené. Ačkoli nepodceňuji technologické možnosti dnešní doby, autor se zjevně snažil do těchto příkladů vnést co nejvíce detailů a šokovat natolik, až vytvořil situace, které nepůsobí příliš důvěryhodně a realisticky. Případy personalizace a manipulativních praktik je často těžké prokázat a stejně tak je těžké dokázat jejich skutečnou újmu. Přesto však existuje několik reálných případů,⁵ které autor mohl využít jako věrohodnější důkaz pro obhajobu svého tématu.

⁴ Vhodně s tímto pojmem pracuje např. SUSSEY, Daniel; ROESSLER, Beate a NISSENBAUM, Helen. Technology, autonomy, and manipulation. *Internet Policy Review*, 2019, roč. 8, č. 2.

⁵ Např. případ Gambling app: European Commission, *Behavioural study on unfair commercial practices in the digital environment. Dark patterns and manipulative personalisation: final report*, 2022, s. 91. Dostupné z: <https://op.europa.eu/en/publication-detail/-/publication/606365bc-d58b-11ec-a95f-01aa75ed71a1/language-en>.

Autor se v první části knihy věnuje obecnému úvodu do problematiky a popisuje strukturu celé knihy. Už na tomto místě tedy struktura knihy působí zmateně, neboť samostatný úvod se nachází i před první částí a není zřejmé, proč byly vytvořeny úvody dva. Prvních několik stran navíc působí, že autor chce především vzdát hold vlastním dosavadním publikacím a že se mimo jiné snaží zavděčit Harrymu Brignullovi.

Dále v této části uvádí výčet dostupných taxonomií a klasifikací dark patterns, které již vytvořili jiní autoři, čímž vytváří dobrý přehled dosavadního poznání. U každé z těchto systematizací navíc stručně hodnotí jejich přínos pro stav poznání, ačkoli je jinak vzájemně nesrovnává.⁶

Jednotlivé dark patterns mohou spotřebitelům působit újmu v různých podobách – svým primárním působením na autonomii jednotlivce sekundárně zasahují jak do ekonomické, tak kognitivní nebo psychologické sféry. Tyto účinky Leiser pokrývá ve stručném shrnutí, v němž nastiňuje možné negativní následky. Dále Leiser analyzuje dosavadní legislativu dopadající na dark patterns – konkrétně se věnuje směrnici o nekalých obchodních praktikách, nařízení o digitálních službách, nařízení o digitálních trzích, nařízení o datech, ePrivacy směrnici a GDPR. Autor přehledně vyjasňuje vztah mezi jednotlivými evropskými akty dopadajícími na dark patterns a navzájem příslušná ustanovení srovnává. Zároveň analyzuje, na které praktiky dopadají jednotlivá nařízení a směrnice a jakým způsobem je případně jejich aplikovatelnost omezena. Leiser například dochází k závěru, že článek 25 nařízení o digitálních službách dopadá pouze na malou množinu dark patterns, neboť velké množství je již obsaženo ve směrnici o nekalých obchodních praktikách – aniž by to v době tvorby této směrnice bylo jejím záměrem. Přehled jednotlivých právních úprav dark patterns je důležitým krokem k vyjasnění jejich regulace a zároveň odrazovým můstkem a nezbytným základem pro jakékoli další případné zkoumání regulace dark patterns. V tomto ohledu lze autorovi vytknout pouze zakomponování Fe-

⁶ LEISER, M. *Dark patterns, deceptive design, and the law: AI's hidden influence on our digital experience*, s. 25-34.

deral Trade Commission Act, který je z veškeré mimoevropské právní úpravy vybrán jako jediný a bez jakéhokoli objasnění.

3. SOFISTIKOVANÁ MANIPULACE

Ve druhé části knihy s názvem *Manipulation beneath interface* se autor věnuje personalizaci a manipulativním praktikám využívajícím umělou inteligenci. Tyto praktiky autor považuje za komplexnější a vysvětluje jejich fungování nejen na úrovni uživatelského rozhraní, ale již v procesu jejich implementace – tedy v samotné architektuře daného systému.

Leiser na úvod vymezuje uživatelské rozhraní a architekturu systému. Poté stručně analyzuje personalizaci od sběru dat a profilování až po potenciální psychologickou újmu. Personalizace představuje jednu ze sofistikovaných praktik, kterou společnosti mohou využít za účelem větší angažovanosti ze strany spotřebitele. Personalizaci se autor věnuje pouze krátce a sám ji označuje jako jeden z *dark patterns*, kterými se zabývá již v první části knihy. Hlavním přínosem druhé části knihy je pojednání o aplikaci aktu o umělé inteligenci. Autor nejprve opět uvádí smyšlené *case studies*, na kterých prezentuje, jak může být umělá inteligence využívána k manipulaci spotřebitelů. Dále se zaměřuje na rozbor článku 5 odst. 1 písm. a).

Autor dále navazuje konceptem zranitelnosti, který tentokrát analyzuje v kontextu článku 5 odst. 1 písm. b) aktu o umělé inteligenci. Zároveň do své analýzy ale prolíná i článek 5 odst. 1 písm. a) a tato dvě ustanovení navzájem srovnává. Zde opět kniha působí silně nestrukturovaně. Leiser se zabývá konceptem zranitelnosti, kterému již věnoval prostor v první části knihy. Toto rozdělení by se částečně dalo pochopit vzhledem k zaměření se na úpravu umělé inteligence. Nicméně zdvojení témat se v knize objevuje často a rozbor článku 5 se navíc prolíná dvěma kapitolami knihy, což činí knihu pro čtenáře nepředvídatelnou a zároveň matoucí, neboť autor na každém místě opakuje i svá předchozí tvrzení.

Závěrečnou třetí část knihy Leiser věnuje pohledům do budoucna – tedy možným oblastem, které by mohly přispět buď k regulaci manipulativních praktik. Poukazuje zejména na roli spotřebitelského práva a práva

na ochranu osobních údajů. Pozornost autor upíná také k řešením na technické úrovni, např. fair patterns.⁷ Dochází k závěru, že je potřeba upřednostňovat práva uživatelů a jejich autonomii a že zlepšení situace tkví ve strukturálních změnách, jako je zvýšení efektivity vymáhání. Spíše než o hloubkovou analýzu se tedy jedná o stručný nástin možných cest, které mohou sloužit jako inspirace pro další výzkum nebo regulatorní úvahy.

4. ZÁVĚR

Kniha představuje komplexní pojetí problematiky dark patterns a klamavých designů. Autor dbá na vymezení jednotlivých typů manipulativních praktik a důsledně se věnuje analýze veškeré evropské legislativy, která se na zmiňované praktiky aplikuje. Autor navíc legislativní akty vzájemně srovnává a vymezuje jejich limity. Zároveň se ve druhé polovině knihy zaměřuje na umělou inteligenci, která má nezpochybnitelně velký vliv na vývoj těchto praktik a v budoucnu bude pravděpodobně čím dál více relevantní.

Ačkoli je kniha psaná čtivým a srozumitelným způsobem, její čtení místy ztěžuje struktura, kterou autor pro knihu zvolil. Praktiky rozčlenil na ty, které nevyužívají umělou inteligenci, a na personalizaci využívající umělou inteligenci. Tím sice podtrhl její význam, nicméně také způsobil, že na několika místech vede autor čtenáře k zamyšlení, jak daná problematika zapadá do základního rámce a autorových východisek. Lepšímu ukotvení v tématu by také pomohlo důsledné citování zdrojů a používání příkladů z praxe.

I přes uvedenou kritiku nicméně kniha slouží jako hutný zdroj informací k problematice klamavého designu, vyjasňuje základní termíny a fungování praktik a svojí hloubkou přesahuje pouhou základní literaturu k dark patterns.

⁷ De JONGE, Tim; SCHRAFFENBERGER, Hanna; GEELS, Jorrit; HOEPMAN, Jaap-Henk; SIMON, Marie-Sophie; BORGESIU, Frederik Zuiderveen. *If Deceptive Patterns are the problem, are Fair Patterns the solution?* In Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency (FAccT '25). Association for Computing Machinery, 2025, New York, 3131–3137.

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>).

<https://doi.org/10.5817/RPT2025-2-5>

ZÁZNAMY UDÁLOSTÍ: STANOVENÍ DOBY UCHOVÁNÍ A IMPLEMENTACE KOMPLEXNÍCH POŽADAVKŮ V ORGANIZACI¹

JAKUB SAUER,² STANISLAV ŠPAČEK,³ PATRIK FRÁŇA,⁴ DENISA
DRAPPANOVÁ⁵ A JAKUB HARAŠTA⁶

ABSTRAKT

Security Information and Event Management (SIEM) jsou standardní součástí infrastruktury řady organizací. Jde o nástroje sloužící k monitoringu provozu systémů a sítí, korelaci událostí a uchovávání těchto údajů pro jejich pozdější využití. Jde o způsob, jakým je možné shromažďovat a konsolidovat záznamy události a další relevantní informace z různých zdrojů. V principu SIEM umožňuje pružnější reakci na kybernetické události a incidenty, ale přispívá také k efektivnější správě provozovaných systémů a sítí.

¹ Vznik publikace byl podpořen projektem specifického výzkumu Právo a technologie XIII (MUNI/A/1739/2024, Denisa Drappanová) a projektem Grantové agentury MU Forensic Support for Building Trust in Smart Software Ecosystems (MUNI/G/1142/2022, Jakub Harašta). Názory uvedené v příspěvku nevyjadřují oficiální postoj organizací, ke kterým jsou jednotliví autoři afiliováni.

² Mgr. Jakub Sauer je IT specialista působící na Ústavu výpočetní techniky Masarykovy univerzity. Kontaktní e-mail: sauer@ics.muni.cz

³ RNDr. Stanislav Špaček, Ph. D. je výzkumným a vývojovým pracovníkem na Ústavu výpočetní techniky Masarykovy univerzity. Kontaktní e-mail: spaceks@ics.muni.cz.

⁴ Mgr. Patrik Fráňa je referentem Národního úřadu pro kybernetickou a informační bezpečnost. Kontaktní e-mail: PatrikFrana@seznam.cz.

⁵ Mgr. Denisa Drappanová je doktorandkou Ústavu práva a technologií Právnické fakulty Masarykovy univerzity v programu Právo informačních a komunikačních technologií. Kontaktní e-mail: 493922@mail.muni.cz.

⁶ JUDr. Mgr. Jakub Harašta, Ph. D. je odborným asistentem Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontaktní e-mail: harasta@muni.cz.

SIEM může organizace implementovat mimo jiné za účelem vyhovění legislativním požadavkům, které na organizaci mohou dopadat (např. povinnost monitorovat a vyhodnocovat kybernetické bezpečnostní incidenty). S tím je spojeno mnoho problematických aspektů, které mohou být obtížně identifikovatelné, a to jak IT odborníky pracujícími s uvedenými nástroji, tak právními experty, kteří si nemusí vždy nutně uvědomit složitost technologického řešení.

Článek je zaměřen na výklad a implementaci legislativních požadavků, které dopadají na SIEM způsobem umožňujícím SIEM využít s minimalizací právního rizika plynoucího z nedostatečné implementace. Cílem tohoto textu je (1) vymezit požadavky plynoucí z překrývajících se právních předpisů v oblasti kybernetické bezpečnosti, ochrany osobních údajů a elektronických komunikací, (2) identifikovat místa, kde se překrývají nebo jsou v konfliktu, a (3) navrhnout postupy k zajištění souladu SIEM s právními požadavky.

KLÍČOVÁ SLOVA

Uchování dat; záznamy bezpečnostních událostí; SIEM; compliance

ABSTRACT

Security Information and Event Management (SIEM) is a standard part of the infrastructure of many organizations. These are tools used to monitor the operation of systems and networks, to correlate events, and to store this data for later use. It is a way to collect and consolidate event logs and other relevant information from various sources. In essence, SIEM enables a more flexible response to cyber events and incidents, while also contributing to more efficient management of operated systems and networks.

Organizations may implement SIEM, among other reasons, to comply with applicable legislative requirements (e.g., the obligation to monitor and evaluate cybersecurity incidents). This involves many problematic aspects that can be difficult to identify, both for IT professionals working with these tools and for legal experts, who may not always be aware of the complexity of the technological solution.

The text focuses on interpreting and implementing legislative requirements that affect SIEM, enabling its use while minimizing the legal risk arising from in-

sufficient implementation. The aim is to (1) define the requirements arising from overlapping legislation in the areas of cybersecurity, personal data protection, and electronic communications, (2) identify areas where they overlap or are in conflict, and (3) propose procedures to ensure SIEM compliance with legal requirements.

KEYWORDS

Retention of data; Security Records, SIEM; Compliance

1. ÚVOD

Článek se zabývá problematikou uchovávání a správy bezpečnostních informací a událostí v organizaci. Jde o problematiku důležitou a komplexní nejenom z technického, ale i z právního pohledu.⁷

Text se věnuje dvěma souvisejícím výzkumným otázkám: Jaké jsou požadavky právních předpisů na stanovení doby uchování a zabezpečení záznamů událostí zpracovávaných logovacím nástrojem? Jaké jsou technické možnosti implementace právních požadavků na uchovávání údajů?

Ze záběru je zřejmé, že předložený text není a nemá být přehledem legislativy dopadajícím na problematiku. V zásadě jde o komplexní *compliance* zadání identifikující nejenom dopadající právní požadavky, ale navrhuje také jejich promítnutí do technické vrstvy.

Příspěvek je strukturován následovně: po úvodu následuje první kapitola věnující se vymezení problematiky SIEM (Security Information and Event Management). Druhá kapitola mapuje právní pravidla dopadající na problematiku zpracování událostí v SIEM. Třetí kapitola identifikuje procesy k adresování právních požadavků. Čtvrtá kapitola se pak věnuje technické implementaci identifikovaných požadavků vč. automatizace. Pátá kapitola představuje závěr textu.

⁷ Srov. MENGES, Florian, Tobias LATZO, Manfred VIELBERTH, Sabine SOBOLA, Henrich C. POHLS, Benjamin TAUBMANN, Johannes KOSTLER, Alexander PUCHTA, Felix FREILING, Hans P. REISER a Günther PERNU. Towards GDPR-compliant data processing in modern SIEM systems, *Computers & Security*, 2021, sv. 103, 102165.

2. POVAHA A ROLE SIEM

Termín Security Information and Event Management (dále také jen „SIEM“) označuje komplexní systém pro správu bezpečnostních informací a událostí v organizaci. Jeho účelem je shromažďovat kyberbezpečnostně-relevantní data z kybernetického prostředí organizace a podpořit nebo automatizovat jejich analýzu a vyhodnocení v reálném čase.⁸ Konkrétně si lze pod tímto pojmem představit širokou škálu informací – síťový provoz, události z mezilehlých síťových prvků, serverů, služeb, i z koncových zaměstnaneckých stanic. Zjednodušeně řečeno, SIEM je systém, který shromažďuje informace ze zařízení zapojených v síti organizace a tato data filtruje, agreguje, koreluje⁹, a vyhodnocuje. V případě, že v monitorovaných datech odhalí kyberbezpečnostní událost, nebo i jen anomálii, pak buď sám provede automatizovanou reakci, nebo alespoň vygeneruje upozornění pro kyberbezpečnostní operátory. Zastřešujícím cílem všech funkcí SIEM je zajištění dostatečné úrovně kybernetické bezpečnosti v organizaci.¹⁰

Přes značné pokroky v oblasti umělé inteligence¹¹ je v centru prevence a reakce na kyberbezpečnostní incidenty stále nezbytný expertní lidský operátor. SIEM je nástrojem, který má operátorovi v zajišťování kybernetické bezpečnosti asistovat a sejmout z něj zátěž v případech, kdy je to možné. Zejména tedy slouží jako jednotný centrální systém pro přístup ke kyberbezpečnostně relevantním datům. Kde původně musel operátor data

⁸ Viz GONZÁLEZ-GRANADILLO, Gustavo, GONZÁLEZ-ZARZOSA, SUSANA and DIAZ Rodrigo. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*. [online]. 2021, roč. 21, č. 14, [cit. 20. 9. 2025], s. 2. Viz také BHATT, Sandeep, MANADHATA, Pratyusa K. a ZOMLOT, Loai. The Operational Role of Security Information and Event Management Systems. *IEEE Security & Privacy*. [online]. 2014, roč. 12, č. 5, [cit. 20. 9. 2025], s. 35-37.

⁹ Tzn. data sjednocuje a shrnuje z mnoha zdrojů do jednoho přehledného celku (agreguje) a hledá mezi nimi souvislosti a vztahy (koreluje).

¹⁰ VELÁSQUEZ, Juan, Miguel, Lopez, MONTERRUBIO, Sergio, Mauricio, Martínez, CRESPO, Luis, Enrique, Sánchez and ROSADO, David, Garcia. Systematic review of SIEM technology: SIEM-SC birth. *International Journal of Information Security*. [online]. 2023, roč. 22, [cit. 20. 9. 2025], s. 692-693.

¹¹ ALI, Sijjad; WANG, Jia a LEUNG, Victor Chung Ming. AI-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms- A comprehensive review. *Information Fusion*. [online]. 2025, svazek 118, [cit. 20. 9. 2025], s. 3-4, 10-17.

vztahující se k jednomu incidentu manuálně dohledávat až na úrovni logů jednotlivých služeb, v SIEM najde vše na jednom místě. S tím souvisí i pokročilé možnosti agregace bezpečnostních dat pocházejících z různých míst v síti do upozornění (tzv. *alertů*) vyšší úrovně, což by při lokální bezpečnostní analýze dat nebylo možné. SIEM je tak schopen použít komplexnější procesy pro identifikaci podezřelého chování v síti. V neposlední řadě pak umí SIEM automatizovat reakce na některé dobře známé a popsané útoky a řešit je v semiautonomním režimu pod dohledem operátora. Vzhledem k množství kyberbezpečnostně-relevantních dat, která vygeneruje i síť menší organizace poskytující dnes běžné služby, je SIEM kritickým kyberbezpečnostním nástrojem.¹²

Základní funkcí SIEM je shromažďování kyberbezpečnostně-relevantních dat. Na úplnosti a korektnosti těchto dat totiž stojí všechny další operace, které SIEM provádí. Monitorování by mělo pokrývat primárně všechna důležitá zařízení a služby organizace, ale i ostatní prvky, zejména mezilehlá síťová zařízení.¹³ Pod toto monitorování by měly spadat také koncové zaměstnanecké nebo uživatelské stanice. Systémem shromažďovaná data tak budou nutně zahrnovat informace o zaměstnancích, klientech, i jiných osobách, které interagovaly s infrastrukturou organizace (např. navštívily její webové stránky). Je zde tedy nutné balancovat potřebu organizace na zajištění kybernetické bezpečnosti, a zájmy osob, jichž se organizací zpracovávaná data týkají. Zásadními oblastmi, které je z pohledu práva při provozu SIEM nutné adresovat, jsou z našeho pohledu zejména retence kyberbezpečnostně-relevantních dat a řízení přístupu k nim.¹⁴

Za účelem sjednocení výše popsaných kyberbezpečnostně-relevantních dat se kterými SIEM pracuje bude pro účely tohoto článku používán pojem záznam událostí. Pod záznamem událostí si lze představit informace o udá-

¹² SASHWIN, K; NITHIKA, K S; PRIYADHARSHINI, S; MADUVANT, S P a SARANYA. Analysis, Trends, and Utilization of Security Information and Event Management (SIEM) in Critical Infrastructures. 2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS). [online]. 2024, [cit. 20. 9. 2025], s. 1980-1983.

¹³ *Ibid.*, s. 1980-1981.

¹⁴ LIU, Che-Wei; HUANG, Peng a LUCAS, Henry C. Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal of Management Information Systems*. [online]. 2019, roč. 37, č. 3, [cit. 20. 9. 2025], s. 761-762.

lostech¹⁵ komunikačního systému nebo technického zařízení. Typicky záznamy událostí představují informace o tom, co, kdy, kde, jak a kým bylo v systému provedeno (např. přihlášení, změny konfigurace, přístup k datům, selhání systémů apod.). Záznamy událostí mohou sloužit pro účely auditu, detekce bezpečnostních incidentů, ladění systémů a zajištění souladu s právními předpisy. V souvislosti se záznamem událostí je nutné vymezit také jejich zpracování, neboť v návaznosti na to právní předpisy formulují požadavky na zabezpečení dostupnosti, důvěrnosti a integrity, či stanovení doby uchování.

Zpracování poté představuje operace nebo soubor operací, který je prováděn pomocí či bez pomoci automatizovaných postupů.¹⁶ Tyto postupy mohou být např. shromáždění, uložení nebo odstranění.¹⁷ Zpracování je přitom s ohledem na požadavky právních předpisů naprosto zásadním konceptem. Samotná informace o záznamu události (například čas, délka hovoru) nemá takovou vypovídající hodnotu pro jeho zabezpečení, či nastavení doby zpracování. Pokud je ale záznam zasazený do kontextu zpracování, je možné zjistit jeho účel a také například identifikovat rizika, před kterými je potřeba zpracování záznamu událostí zabezpečit.¹⁸ Zároveň mohou informace o zpracování záznamu událostí sloužit pro ověření, zdali dochází k dosažení stanoveného účelu pro zpracování.¹⁹

¹⁵ MAISNER, Martin. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015, s. 99-101.

¹⁶ V mnoha ohledech se tato definice kryje s pojmem zpracování ve smyslu článku 4 odst. 2 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES.

¹⁷ NONNEMANN, František; ČERVENÝ, Vlastimil a VÍTEK, Dominik. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. 2. vydání. Praha: Wolters Kluwer, 2025, s. 32.

¹⁸ Např. narušení dostupnosti zpracování záznamu událostí v důsledku zaplavení serverovny.

¹⁹ NONNEMANN, František; ČERVENÝ, Vlastimil a VÍTEK, Dominik. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. 2. vydání. Praha: Wolters Kluwer, 2025, s. 132-133.

3. ZPRACOVÁNÍ ZÁZNAMŮ UDÁLOSTÍ V PROSTŘEDÍ SIEM

3.1 VYMEZENÍ RELEVANTNÍCH PRÁVNÍCH PŘEDPISŮ

Jak je uvedeno výše, zpracování záznamů událostí v prostředí SIEM může zahrnovat velmi citlivé informace o samotné organizaci i o dotčených fyzických osobách. Narušení jejich dostupnosti, důvěrnosti anebo integrity by mohlo způsobit významnou škodu organizaci, dotčeným osobám a v případě některých služeb také státu. Tento závěr lze dovodit například z § 4 odst. 1 písm. a) zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „ZoKB“).

Zákonodárce se rozhodl regulovat jejich zpracování především skrze dále uvedené právní předpisy, jejichž požadavky tento příspěvek zpracovává. Z důvodu, že součástí záznamů událostí mohou být osobních údaje je na místě také upozornit na nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „nařízení GDPR“). V poslední řadě v tomto příspěvku zohledňujeme zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (dále jen „ZEK“). Tato kapitola dále shrnuje relevantní požadavky uvedených předpisů s ohledem na zpracování dat v rámci SIEM a celkový účel tohoto textu. Byť v praxi není běžné, že by na každý jeden záznam událostí dopadaly všechny uvedené právní předpisy, je cílem této práce představit i takové situace, ke kterým by mohlo teoreticky dojít. Je však namístě uvést, že článek neuvádí vyčerpávající výčet legislativy, která na zpracování záznamů událostí spadá. Další, v tomto článku nerozebírané, požadavky lze nalézt například v prováděcím nařízení Komise (EU) 2024/2690, které funguje jako obdoba prováděcích předpisů ZoKB pro vybrané regulované služby.²⁰

3.2 ZOKB

V době přípravy tohoto textu již byl schválen ZoKB, který nabyl účinnosti 1. 11. 2025. ZoKB rozděluje povinné osoby do 2 režimů povinností, které

²⁰ Viz § 18 ZoKB.

popisuje v prováděcích předpisech. Těmito jsou aktuálně vyhláška č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností (dále také jen “VNR”) a vyhláška č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále také jen “VVR”).

Primárním rozdílem v otázce zaznamenávání událostí mezi původní a novou legislativou je rozdíl v době uchování záznamů událostí. Nová legislativa totiž požaduje podle § 22 odst. 5 písm. c) minimálně 18 měsíců s tím, že tato povinnost se vztahuje na poskytovatele služeb v režimu vyšších povinností.

§ 23 VVR požaduje po povinných osobách uchovávání bezpečnostních událostí technických aktiv (technických nebo programových prostředků) pro účely zkoumání bezpečnostních incidentů a případné spolupráce s relevantními orgány. Pokud je povinná osoba identifikována jako poskytovatel regulovaných služeb v režimu vyšších povinností, má povinnost zaznamenávat události detekované za pomoci nástroje pro detekci v rámci komunikační sítě, na síťovém perimetru a v technických aktivech. Náležitosti záznamu těchto událostí podle ZoKB a prováděcích předpisů zachycuje Tabulka 1.

Náležitosti záznamu událostí ve vyšším režimu povinností	Datum a čas; typ činnosti; dotčené technické aktivum; účet původce; zařízení původce; úspěšnost činnosti.
Události, které se zaznamenávají ve vyšším režimu	Přihlášení; provedení a neúspěšné pokusy o provedení privilegovaných činností; manipulace a neúspěšné pokusy o manipulaci s uživatelskými účty, oprávněními a přístupovými právy; pokusy o provedení činností, které nebyly dokončeny z důvodu nedostatečných přístupových práv nebo oprávnění; zahájení a ukončení

	činností technických aktiv; kritická a chybová hlášení generovaná technickými aktivy; přístupy a neúspěšné pokusy o přístupy k záznamům událostí; manipulace a neúspěšné pokusy o manipulaci se záznamy událostí; změny a neúspěšné pokusy o změny nastavení nástrojů pro zaznamenávání událostí a další činnosti uživateľů, které mohou mít vliv na bezpečnost regulované služby.
Záznamy událostí v režimu nižších povinností	V souladu s § 9 VNR, požaduje zaznamenávat události zejména na serverech a koncových stanicích, přičemž o událostech požaduje zaznamenávat informace (datum; čas; typ činnosti; ...), nepředepisuje však minimální dobu uchování záznamů událostí, ani typové události, které mají být zaznamenávány. V tomto ohledu může režim vyšších povinností zároveň sloužit jako inspirace pro důkladné řešení zaznamenávání událostí i pro osoby, které spadají pouze do režimu nižších povinností.

Tabulka 1: Náležitosti záznamu událostí podle ZoKB a prováděcích předpisů

3.3 NAŘÍZENÍ GDPR

Nařízení GDPR se zabývá ochranou osobních údajů. Jak již bylo uvedeno výše, osobní údaje jsou často součástí zpracování záznamů událostí. Podle nařízení GDPR jsou osobními údaji veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“). Identifikovatelnou fyzickou osobou pak je podle článku 4 odst. 1 nařízení GDPR fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, identifikační číslo, lokační údaje, síťový iden-

tifikátor²¹⁾ nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

Středobodem ochrany osobních údajů je jejich zpracování.²²⁾

Zpracování osobních údajů musí probíhat na základě titulů, které jsou uvedeny v čl. 6 nařízení GDPR. Pro účely zpracování záznamů událostí lze uvažovat zejména o následujících titulech pro zpracování:

1. Plnění právní povinnosti (čl. 6 odst. 1 písm. c) nařízení GDPR);

Tento titul je aplikovatelný, pokud zpracování vyplývá z povinností stanovených právními předpisy. V kontextu zákona o kybernetické bezpečnosti (ZoKB) a prováděcích vyhlášek jde zejména o:

- § 13 ZoKB v povinnosti poskytovatele regulované služby zavádět a provádět bezpečnostní opatření v rozsahu stanoveném vyhláškami.
- § 15 ZoKB v povinnosti hlásit kybernetické bezpečnostní incidenty.
- VNR a VVR obsahují detailní požadavky na detekci, zaznamenávání a uchovávání bezpečnostních a provozních událostí (např. § 9 VNR ukládá uchovávat záznamy po dobu stanovenou na základě bezpečnostních potřeb).

2. Oprávněný zájem (čl. 6 odst. 1 písm. f) nařízení GDPR);

Oprávněný zájem lze použít, pokud správce prokáže, že jeho zájem na zpracování převažuje nad právy subjektů údajů, typicky skrz balanční test. Musí tedy existovat oprávněný zájem sledovaný správcem (např. zajištění kybernetické bezpečnosti, prevence incidentů, ochrana majetku), pro jehož naplnění je nezbytné zpracování, protože jej není možno dosáhnout jinak. Zároveň pak musí

²¹⁾ V kontextu tohoto článku se dále může jednat například o IP adresu, přihlašovací údaje účtů, čas a způsob přihlášení uživatele, použitý prohlížeč nebo zařízení apod.

²²⁾ Zpracováním osobních údajů je podle nařízení GDPR jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení, dle článku 4 odst. 2 nařízení GDPR.

platit, že práva subjektů údajů na nezpracování nepřevažují nad oprávněným zájmem správce.

Oprávněný zájem by se v praxi mohl objevit například při uchovávání logů pro účely interního vyšetřování bezpečnostních incidentů nebo monitoring přístupů do systémů za účelem prevence zneužití (pokud nejde o realizaci zákonné povinnosti).

Každé zpracování poté musí být evidováno na základě alespoň jednoho titulu²³ zpracování osobních údajů. Jakkoli se titul a účel v rámci zpracování často oddělují (jde totiž o dva odlišné koncepty), pro identifikaci titulu je vhodné vést účel v patrnosti. Stanovený účel totiž může pomoci při ověření, zdali je zpracování záznamů událostí přiměřené a nezbytné, tedy zda by nešlo dosáhnout stanoveného účelu s menším rozsahem zpracovávaných osobních údajů. Jde o jedny ze základních zásad obsažených v článku 5 GDPR.

Nad rámec shora uvedených titulů teoreticky připadá v úvahu ještě souhlas se zpracováním²⁴. V případě souhlasu je však prakticky problematické, že musí být oddělitelný. Jinými slovy v případě, že je využitý jako titul pro zpracování a subjekt údajů jej odmítne dát, musí mu být služba, ke které se váže zpracování, poskytnuta na základě jiného právního titulu pro zpracování osobních údajů. Zároveň souhlas nelze, v důsledku nerovného vztahu, vyžadovat po zaměstnancích organizace. Souhlas je také kdykoli odvolatelný. V praxi je tak jeho využití v kontextu SIEM natolik problematické, až je možné uzavřít konstatováním jeho nevhodnosti.

V souvislosti se zpracováním osobních údajů je pak také důležité zmínit zvláštní kategorii osobních údajů. Osobní údaje zvláštní kategorie jsou údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě

²³ KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher a DRECHSLER, Laura (ed.). *The EU general data protection regulation (GDPR): a commentary*. Oxford: Oxford University Press, 2020, s. 321 – 344.

²⁴ URŠIČ VRABEC, Helena. *Data subject rights under the GDPR: with a commentary through the lens of the data-driven economy*. Oxford: Oxford University Press, 2021, s. 70 – 71.

nebo sexuální orientaci fyzické osoby.²⁵ V některých případech hrozí, že tyto osobní údaje budou součástí zpracování záznamů událostí.

V případě zpracovávání osobních údajů zvláštní kategorie²⁶ je potřeba jednak naplňovat právní titul, ale také je nutné splňovat některý z dodatečných právních titulů stanovených článkem 9 nařízení GDPR.²⁷ Pokud tyto podmínky nejsou splněny, je zpracování osobních údajů zvláštní kategorie zakázáno.

Je třeba mít na paměti základní principy GDPR, tedy zásady přiměřenosti, minimalizace zásahu, zákonnosti a vymezení účelů zpracování. Proto má ke zpracování docházet jen tam, kde je to účelné a na tak dlouho jak je to potřebné k naplnění stanoveného účelu. Nelze tak stanovit jednotnou dobu, ale je potřeba vždy posuzovat zpracování s ohledem na jeho účel.

3.4 ZEK

ZEK pracuje s provozními a lokalizačními údaji, vůči kterým mají provozovatelé veřejné komunikační sítě nebo poskytovatelé veřejné dostupné služby elektronických komunikací zákonné povinnosti uchovávat je po dobu stanovenou tímto zákonem. V souvislosti s uchováváním událostí se s provozními a lokalizačními údaji pojí dva typy povinností. První z nich jsou obecné, které vyplývají z § 90 ZEK a § 91 ZEK.²⁸ Obecné povinnosti stanovují, že je možné provozní údaje a lokalizační údaje uchovávat po dobu provozu. Poté je potřeba tyto údaje odstranit anebo anonymizovat, pokud nedojde k využití výjimek uvedených v § 90 ZEK.²⁹ V případě zpracovávání lokalizačních údajů, které nejsou provozními údaji, mohou být údaje vztahující se k uživateli nebo účastníku zpracovávány pouze v roz-

²⁵ KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher a DRECHSLER, Laura (ed.). *The EU general data protection regulation (GDPR): a commentary*. Oxford: Oxford University Press, 2020, s. 365 – 385.

²⁶ Například údaje v záznamech zdravotního vyšetření nebo informace o návštěvě webových stránek pro pacienty s atypickou vážnou nemocí.

²⁷ Tím může být například zpracování, které je nutné pro splnění povinností a uplatnění práv v pracovním a sociálním právu, pokud to dovoluje právo Unie nebo státu a jsou zajištěny potřebné záruky.

²⁸ CHUDOMELOVÁ, Zuzana. *Zákon o elektronických komunikacích: komentář*. 2. vydání. Komentáře Wolters Kluwer. Praha: Wolters Kluwer, 2025, s. 390 – 396.

sahu a trvání nezbytném pro poskytování služeb s přidanou hodnotou, a to za předpokladu odvolatelného souhlasu.³⁰ Speciální kategorie je spojena s povinnostmi uchovávat záznamy událostí po dobu 6 měsíců dle § 97 ZEK.³¹ Tato speciální kategorie se váže na ty typy záznamů událostí, které jsou vymezeny ve vyhlášce č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů. U těchto záznamů je povinnost zaznamenávat především:

- Datum a čas komunikace,
- komunikující stanice,
- dobu spojení,
- množství přenesených dat,
- identifikátory účastníků.

Pro účely splnění této povinnosti se údaje o času musejí uchovávat v místním čase. Pakliže daný místní čas neodpovídá času v České republice, musí být údaje o čase uváděny s označením časového pásma. Provozní a lokalizační údaje požadované vyhláškou (výše uvedená druhá kategorie) zároveň musí být dle § 4 této vyhlášky po uplynutí šestiměsíční doby zlikvidovány.

Poskytovatel veřejně dostupné služby elektronických komunikací nebo osoba zajišťující veřejnou komunikační síť musí zároveň zajistit bezpečnost a integritu veřejných komunikačních sítí a služeb elektronických komunikací dle § 98 ZEK.³² I při plnění této povinnosti může dojít k potřebě zpra-

²⁹ Výjimky pro provozní údaje jsou obsaženy v § 90 odst. 3 – 6 ZEK: Odst. 3 – Povinnost uchování provozních údajů poskytnutých účastníkovi či uživateli dokud nebude rozhodnuto o sporu dle § 129 odst. 3 ZEK nebo uplynutí doby pro právní napadení vyúčtování ceny či uplynutí doby možného vymáhání úhrady; Odst. 4 – Možnost zpracovávat provozní údaje nezbytné pro vyúčtování ceny do konce doby, během níž může být úhrada vymáhána; Odst. 5 – Možnost předávání dat mezi provozovateli a poskytovateli pro účely vzájemného vyúčtování nebo pro účely identifikace zneužívání sítě a služeb elektronických komunikací; Odst. 6 – Podnikatel poskytující veřejně dostupnou službu elektronických komunikací může, za předpokladu odvolatelného souhlasu, zpracovávat osobní údaje pro poskytování služeb s přidanou hodnotou či pro marketing, a to v nezbytném rozsahu a po nezbytně nutnou dobu.

³⁰ Pokud uživatel či účastník souhlas neučiní, musí se údaje anonymizovat.

³¹ CHUDOMELOVÁ, Zuzana. *Zákon o elektronických komunikacích: komentář*. 2. vydání. Komentáře Wolters Kluwer. Praha: Wolters Kluwer, 2025, s. 406 - 413.

³² *Ibid.*, s. 423 – 432.

covávat záznamy událostí. V tomto ohledu není právním předpisem stanovena doba uchování záznamu událostí.

3.5 SANKCE ZA NEDODRŽENÍ PRÁVNÍCH POVINNOSTÍ

V důsledku nesprávných parametrů zpracování mohou organizaci uniknout citlivá data, případně může dojít k jejich smazání nebo neplánované změně. V návaznosti na nedostatečné zabezpečení totiž může dojít k reputační škodě nebo snížení provozuschopnosti. Navíc však – což je u organizací s nízkým bezpečnostním povědomím hlavním motivačním faktorem – také může dojít k udělení sankce ze strany dozorujícího správního orgánu. Ilustrativně vybrané příklady sankcí jsou uvedeny v Tabulce 2.

Právní předpis	Maximální sankce	Cílové subjekty	Příklad porušení
ZKB14 § 25 odst. 14 písm. a)	5 mil. Kč	Správce informačního nebo komunikačního systému kritické informační infrastruktury, Správce významného informačního systému	Nezavedení nebo neprovedení bezpečnostních opatření (řízení přístupů), nenahlášení incidentu (např. únik údajů)
ZoKB § 59 odst. 1 a odst. 4 písm. a)	250 mil. Kč / 2 % obrátu	Poskytovatel regulované služby v režimu vyšších povinností	Nezavedení nebo neprovedení bezpečnostních opatření (řízení přístupů), nenahlášení incidentu (např. únik údajů)
ZoKB § 59 odst. 2 a odst. 4	175 mil. Kč / 1,4 % obrátu	Poskytovatel regulované služby v režimu nižších po-	Nezavedení nebo neprovedení bezpečnostních opatření (řízení

písm. b)		vinností	přístupů), nenahlášení incidentu (např. únik údajů)
ZEK § 118 odst. 14 písm. j) a odst. 26 písm. b)	15 mil. Kč / 5 % obratu	Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací	Ohrožení důvěrnosti zpráv a s nimi spojených provozních a lokalizačních údajů (§ 89 odst. 1 nebo § 91 odst. 2, 3 nebo 4)
ZEK § 118 odst. 14 písm. c) a odst. 26 písm. c)	50 mil. Kč / 10 % obratu	Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací	Neuchování či nepředání provozních a lokalizačních údajů, nelikvidování po uplynutí doby, ... (§ 97 odst. 3)
ZEK § 118 odst. 16 a odst. 26 písm. b)	15 mil. Kč / 5 % obratu	Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací	Nesplnění některé z povinností při zabezpečení ochrany údajů (§ 88a odst. 1 nebo 2)
GDPR článek 83 odst. 4 písm. a)	10 mil. EUR / 2 % obratu	Všechny organizace zpracovávající osobní údaje	Nezavedení pseudonymizace nebo jiných opatření (čl. 32)
GDPR článek 83 odst. 5 písm. a)	20 mil. EUR / 4 % obratu	Všechny organizace zpracovávající osobní údaje	Porušení zásad zpracování osobních údajů (čl. 5)

Tabulka 2: Příklady sankcí za porušení platné legislativy

4. PROCESY SMĚŘUJÍCÍ K NAPLNĚNÍ PRÁVNÍCH POŽADAVKŮ

4.1 NASTAVENÍ DOBY PRO ZPRACOVÁNÍ ZÁZNAMŮ UDÁLOSTÍ

V praxi je možné, že se na konkrétní záznamy událostí bude vztahovat více právních předpisů³³, kdy každý z těchto právních předpisů bude vyžadovat jinou dobu pro jejich uchování. Tento problém si lze představit při aplikaci pravidel plynoucích ze ZEK a ZoKB. Údaje uchovávané podle obou předpisů se budou často obsahově překrývat. ZEK stanoví na jednu stranu povinnost obecné údaje ihned smazat nebo anonymizovat, na stranu druhou uchovávat speciální kategorii údajů po dobu 6 měsíců, zatímco ZoKB, respektive VVR, povinnost uchovávat záznamy událostí alespoň po dobu 18 měsíců. Na první pohled tak dochází ke střetu dvou právních předpisů.

V úvahu připadá aplikace derogačních pravidel (pravidlo právní síly, pravidlo času a pravidlo speciality). Pakliže by k aplikaci derogačních pravidel došlo, pravděpodobně by na základě použití pravidla právní síly byl uplatněn ZEK před pravidly plynoucími z prováděcích předpisů ZoKB. Druhou teoretickou možností je derogační pravidla neuplatnit vůbec a ponechat souběžné působení obou právních předpisů, a to na základě rozdílného účelu právních norem. Účelem ustanovení v ZEK je, v případě § 91, zajištění přenosu zprávy sítí elektronických komunikací (a případně účtování služby) nebo, v případě § 97 ZEK, vyšetřování trestné činnosti a zpravodajská činnost. ZoKB oproti tomu cílí na zajištění kybernetické bezpečnosti pro zajištění řádného poskytování regulovaných služeb. Současné uplatnění pravidel obou předpisů není vyloučeno ani povahou zpracovávaných dat³⁴ a v případě využívání těchto dat v souladu s titulem, na základě kterého jsou zpracovávána, ani nedojde k negativnímu dopadu na subjekt údajů.

Důsledkem uplatnění derogačních pravidel by bylo smazání všech údajů vyžadovaných ZEK v případě, kdy vyprší právní titul, který ZEK poskytuje. V takovém případě by byly zbývající uchovávané údaje dle ZoKB s vysokou

³³ NONNEMANN, František; ČERVENÝ, Vlastimil a VÍTEK, Dominik. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. 2. vydání. Praha: Wolters Kluwer, 2025, s. 193-195.

³⁴ Zejména z toho důvodu, že zpracovávaná data mohou být fyzicky či logicky oddělena.

pravděpodobností nevyužitelné. Oproti tomu uplatnění druhého přístupu zachovává smysl a účel všech předpisů a navíc jej lze vyřešit také po stránce technologické implementace. Z tohoto důvodu byla v textu rozpracována právě tato druhá varianta včetně popisu možné implementace v organizaci. V tomto případě k oprávnění uchovávat záznam událostí postačí, aby jeho uchování svědčila alespoň jedna lhůta daná právním předpisem anebo stanovena organizací v souladu s tímto právním předpisem. Zároveň není nezbytné (a ani účelné, např. s přihlédnutím k nákladům na uchovávání), aby byly uchovávané záznamy událostí duplikovány na více místech. Postačí jejich zaznamenání na jednom místě a evidence jednotlivých oprávnění zpracovávat záznam událostí bude vedena jako příznak záznamu událostí. Po uplynutí rozhodné doby vztahující se k právním předpisům či interním potřebám bude nezbytné, aby byl příznak ze záznamu událostí odstraněn manuálně nebo na základě automatické expirace (mohou však zůstat příznaky plynoucí z jiného právního předpisu). Pakliže je záznam naprosto bez příznaků, musí se smazat anebo musí být anonymizován.³⁵ Do úvahy připadá také zavedení určité *grace period*, tedy přechodného období, během kterého se administrátor musí rozhodnout, jak dál se záznamem událostí naloží.

Většina záznamů událostí obsahuje osobní údaje. Vzhledem k tomu, že nařízení GDPR samo o sobě nestanovuje lhůtu pro uchování záznamu událostí, ale buďto odkazuje na plnění dalších zákonných povinností (plnění zákonných povinností) anebo vyžaduje posouzení pro daný případ zpracování (oprávněný zájem), může být na všechna zpracování záznamů událostí nahlíženo jako by obsahovala osobní údaje. Tento přístup je účelný z hlediska alokace zdrojů (klasifikace může být personálně, časově či finančně náročná) a také z určité procesní opatrnosti. Pokud jsou záznamy událostí zpracovávány za účelem plnění zákonných povinností, lze automaticky nastavit uchování těchto záznamů v souladu s požadavky relevantního právního předpisu.

³⁵ Jiným řešením může být uchovávání různých datasetů pro různé potřeby. V těchto datasetech by byly obsaženy pouze údaje vyžadované např. ZEK, které by byly po nastání rozhodné skutečnosti smazány, zatímco dataset ZoKB by byl naprosto nedotčen.

V souvislosti s osobními údaji je nezbytné dbát na to, aby byly plněny povinnosti správce vůči subjektům údajů. Správce má především povinnost subjekty údajů vhodným způsobem informovat³⁶ o tom, že jsou jejich osobní údaje zpracovávány. Tato informační povinnost musí být naplněna přiměřeně povaze a okolnostem daného zpracování – to znamená, že subjekty musí obdržet jasné, srozumitelné a úplné informace o účelu zpracování, právním základu, době uchování údajů, případných příjemcích a také o svých právech dle kapitoly III nařízení GDPR.³⁷

Součástí odpovědného zpracování je rovněž povinnost zabezpečit osobní údaje přiměřeným způsobem v souladu s článkem 32 nařízení GDPR.³⁸ To zahrnuje přijetí technických a organizačních opatření, která zohledňují aktuální stav techniky, povahu, rozsah, kontext účely zpracování, jakož i rizika pro práva a svobody fyzických osob. V tomto ohledu je často zmiňována anonymizace, která představuje způsob zpracování osobních údajů, při kterém dojde k takové úpravě dat, jež znemožní zpětnou identifikaci fyzických osob, kterých se původně týkala.³⁹ Po provedení anonymizace přestávají být tyto údaje považovány za osobní a nevztahuje se na ně nařízení GDPR.

Navzdory častému přesvědčení, že odstraněním přímých identifikátorů lze data učinit anonymními, judikatura Soudního dvora EU ukazuje, že skutečná anonymizace je v praxi velmi obtížně dosažitelná. Soudní dvůr EU zdůraznil,⁴⁰ že pseudonymizace sama o sobě neznamená anonymizaci – pokud existují prostředky, o nichž lze rozumně předpokládat, že by mohly vést k opětovné identifikaci osob, jak je tomu při propojení s jinými databázi či při technologickém rozvoji, údaje zůstávají osobními a nadále se

³⁶ Toto informování může být vyřešeno například oznámením na webových stránkách organizace.

³⁷ URŠIČ VRABEC, Helena. *Data subject rights under the GDPR: with a commentary through the lens of the data-driven economy*. Oxford: Oxford University Press, 2021, s. 69-70.

³⁸ KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher a DRECHSLER, Laura (ed.). *The EU general data protection regulation (GDPR): a commentary*. Oxford: Oxford University Press, 2020, s. 630 – 639.

³⁹ Viz rec. 26 nařízení GDPR.

⁴⁰ Rozsudek SDEU (prvního senátu) ze dne 4. 11. 2025 ve věci C-413/23 P, EDPS v SRB (Notion de données à caractère personnel), body 71–75, 80–86.

na ně vztahuje GDPR. Pouhé technické oddělení doplňujících informací (např. klíčů k přiřazení) proto nestačí. Tento výklad je v souladu i s pokyny EDPB 01/2025. Z tohoto důvodu je namístě zacházet i s údaji považovanými za anonymizované tak, jako by šlo o vysoce pseudonymizované osobní údaje, které stále podléhají pravidlům GDPR. Pro tyto účely je vhodné v organizaci postupovat jednotně a v koordinaci s pověřencem pro ochranu osobních údajů.

Zároveň je potřeba zkoumat, zdali určité zpracování záznamů událostí nepředstavuje při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování, vysoké riziko pro práva a svobody fyzických osob. Pokud je vysoké riziko identifikováno, je potřeba, aby organizace zpracovala *Data Protection Impact Assessment* (dále také jen “DPIA”) podle článků 35 a 36 nařízení GDPR.⁴¹ DPIA je potřeba provést v případech:

1. systematického a rozsáhlého vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;
2. rozsáhlého zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nařízení GDPR nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10 nařízení GDPR; nebo
3. rozsáhlé systematické monitorování veřejně přístupných prostorů.

V případě podezření na povinnost zpracování DPIA je namístě zavést pravidelnou kontrolu změn, v důsledku kterých by mohlo být nakonec nutné DPIA provést. Zároveň by osoby (oddělení, organizační složky) měly spolupracovat s pověřencem pro ochranu osobních údajů organizace, případně s jinou osobou odpovědnou za zajištění souladu s nařízením GDPR.

⁴¹ KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher a DRECHSLER, Laura (ed.). *The EU general data protection regulation (GDPR): a commentary*. Oxford: Oxford University Press, 2020, s. 665 – 697.

Také je důležité mít stanovenou obecnou dobu pro uchování záznamů událostí i pro záznamy událostí, u kterých právní předpisy nestanoví konkrétní dobu pro zpracování anebo u kterých doba již uplynula a je účelné a možné je uchovávat dále. Stanovení obecné doby mitiguje právní riziko spojené s nesprávnou klasifikací (například když údaje nebudou označeny za osobní, ač se o osobní údaje jedná) a zároveň bezpečnostní riziko spojené s nepřiměřeným uchováváním záznamů.⁴²

4.2 VYBRANÉ OTÁZKY K ZABEZPEČENÍ ZÁZNAMŮ UDÁLOSTÍ

V souvislosti s uchováváním záznamů je potřeba řídit přístup ke zpracování a zabezpečit zpracování záznamů událostí. Požadavky směřující k zajištění kybernetické bezpečnosti lze nalézt implicitně nebo explicitně v § 88–91, 97, 98 ZEK, dále ZoKB v rámci VVR a VNR a také v článku 32 nařízení GDPR.

Nehledě na legislativu, která se na dané zpracování a uchovávání záznamů událostí aplikuje, je vhodné vycházet z pravidel uvedených ve VVR – a to z toho důvodu, že dává nejdůtější popis pro zavedení opatření s ohledem na zabezpečení dostupnosti, důvěrnosti a integrity zpracovávaných dat a informací.⁴³ Základním kamenem pro řešení bezpečnosti je ve VVR řízení rizik, od kterého by se mělo odvíjet zavádění dalších bezpečnostních opatření v oblastech ve vyhlášce uvedených.⁴⁴ Tato bezpečnostní opatření ve většině případů představují obecné požadavky, jejichž cílem je nechat k jejich realizaci co největší prostor pro přizpůsobení individuálním podmínkám organizace.⁴⁵

Detailnější rozpis bezpečnostních opatření přesahuje rámec tohoto článku. Proto je nezbytné projít jednotlivé právní předpisy, případně se po-

⁴² Může se jednat například o zastaralé šifrování uchovávaných údajů, a jejich stále narůstající objem, který musí být spravován.

⁴³ JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. Šesté, doplněné a upravené elektronické vydání. Praha: Centrum kybernetické bezpečnosti, z.ú., 2025, s. 109.

⁴⁴ Pro naplnění opatření je vhodné vytvořit a srozumitelně komunikovat interní metodiku s jasně stanovenými pravidly, odpovědnostmi, nástroji a kontrolními postupy.

⁴⁵ Např. § 14 VVR řízení přístupu na základě rolí. Jak je vidět, zákonodárce nechal konkrétní realizaci (typy rolí, jejich oprávnění apod.) na organizaci.

radit s odpovědnými osobami v rámci organizace. V souvislosti se zpracováváním záznamů událostí byly v rámci VVR identifikovány jako relevantní především ustanovení § 7 (řízení aktiv), § 13 (řízení přístupů), (§ 15 řízení kontinuity), § 16 (audit), § 19 (požadavky na autentizaci a autorizaci), § 22 (záznamy událostí), § 25 (požadavky na kryptografii), § 26 (testování obnovy) a příloha č. 2 (likvidace dat).⁴⁶

Součástí zabezpečení zpracování záznamů událostí je také hodnocení rizik. Obecně se doporučuje před implementací zbývajících opatření provést hodnocení rizik a realizovat další opatření v souvislosti s ošetřováním jednotlivých rizik, viz § 8 VVR a článek 32 nařízení GDPR. Vyjma toho, že je tento přístup přímo vyžadován ZoKB, umožňuje zároveň efektivnější implementaci opatření i alokaci dostupných zdrojů.

Pro konkretizaci lze zároveň využít různé bezpečnostní standardy např. National Institute of Standards and Technology. *NIST Special Publication 800-92: Guide to Computer Security Log Management*,⁴⁷ který uvádí konkrétní povinnosti spojené se zabezpečením záznamu událostí.

4.3 KONTROLA SOULADU S PRÁVNÍMI POŽADAVKY

Obecně platí, že na počátku je oprávnění ke zpracování záznamů událostí a obsažených osobních údajů (užitečnost jejich uchovávání) nejsilnější a s postupem doby se tato vlastnost oslabuje a začíná převažovat potřeba jejich odstranění či anonymizace.⁴⁸ Pro případ pochybení nebo změny okolností je vhodné mít nastavený proces kontroly nastavených pravidel pro zpracování záznamů událostí (automatizovanou/manuální). Kontrola nemusí probíhat na úrovni jednotlivých záznamů událostí, ale na úrovni typových zpracování. Pokud dochází ke zpracování záznamů událostí – např. přihlášení informačního systému – může kontrola probíhat na úrovni

⁴⁶ POLČÁK, Radim; LOUTOCKÝ, Pavel; KASL, František; MÍŠEK, Jakub; HOSTAŠ, Petr et al. *Právo informačních technologií*. 2. vydání. Praha: Wolters Kluwer, 2024, s. 825-829.

⁴⁷ KENT, Karen a SOUPPAYA, Murugiah. NIST SP 800-92. Guide to Computer Security Log Management. In: COMPUTER SECURITY RESOURCE CENTER NIST [online]. 2006. [cit. 20. 9. 2025]. Dostupné z: <https://csrc.nist.gov/pubs/sp/800/92/final>

⁴⁸ Podobný argument v jiném kontextu přináší i SARTOR, Giovanni. The right to be forgotten: balancing interests in the flux of time. *International Journal of Law and Information Technology*, 2016, roč. 24, č. 1, s. 72-98.

ověření aktuálnosti nastavených pravidel pro daný typ zpracování, nikoli pro každý zvlášť. Záleží ovšem na rizikosti daného zpracování záznamů událostí a kapacitách organizace.

Kontrola by měla zahrnovat minimálně následující položky:

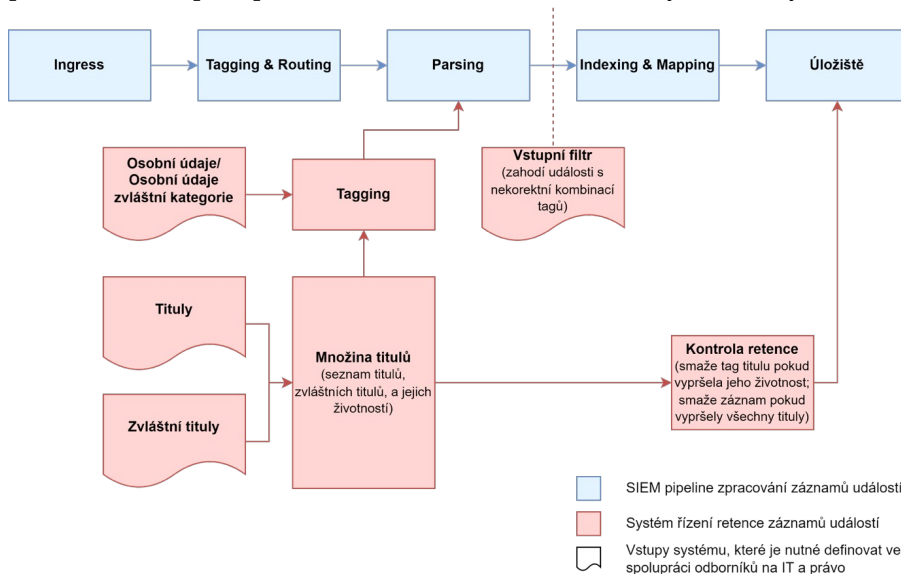
- Zda je splněn alespoň jeden z právních titulů a dodržené podmínky zpracování
- Zda jsou záznamy událostí stále dostupné a pokud hrozí riziko nečitelnosti převést události na jiná média nebo do jiných formátů
- Zda jsou zvolená pravidla zabezpečení skutečně dodržována
- Zda je obsah záznamů událostí správný a korektní

5. TECHNICKÁ IMPLEMENTACE/AUTOMATIZACE IDENTIFIKOVANÝCH POŽADAVKŮ

Tato kapitola je věnována způsobu, kterým je možné implementovat opatření na aktuální SIEM již nasazené v organizacích tak, aby byly v souladu s diskutovanou legislativou. Řízení přístupů je technicky snadno realizovatelné; aktuální SIEM nabízí široké možnosti nastavení zabezpečení přístupů až na úroveň jednotlivých uživatelů a záznamů událostí. Korektní nastavení přístupů tedy závisí více na procesech organizace a jejich dodržování než technické implementaci. Řízení retence záznamů událostí je z pohledu implementace zajímavější problém, který bude podrobněji adresován. Žádný nám známý SIEM toto řízení nativně nepodporuje, lze jej ale implementovat externě běžícím systémem při využití existujících funkcí API SIEM.

Princip navrhovaného systému pro řízení retence záznamů událostí v SIEM vychází z předpokladu, že pro zpracování každého záznamu události je třeba jeden nebo více konkrétních právních titulů, jak je určuje např. nařízení GDPR. Tyto právní tituly je nutné určit již při vstupu záznamu události do SIEM a uchovávat je u něj po celou dobu zpracování. Zároveň je nutné počítat s tím, že právní tituly pro zpracování mají typicky omezenou životnost, danou některým z relevantních předpisů (např. ZoKB, ZEK). Po celou dobu přítomnosti záznamu události v SIEM je tedy nutné sledovat,

kteřé právní tituly pro zpracování již pominuly a v případě expirace všech právních titulů pro zpracování daného záznamu tento vyřadit ze systému.



Obrázek 1: Schéma pipeline pro zpracování záznamů událostí se zapojením navrhovaného systému pro řízení retence

Před pojednáním o návrhu implementace systému pro řízení retence je třeba stručně popsat co se rozumí pod termínem pipeline pro zpracování záznamů událostí. Obecně řečeno, jde o řetězec modulů nebo funkcí v rámci SIEM, které postupně mění typicky nestrukturovaný záznam události na vstupu na strukturovaný a otypovaný záznam, použitelný pro analytické funkce uživatelské vrstvy SIEM. Příklad takové pipeline je zobrazen na schématu na Obrázku 1 (modrá barva). Prvním modulem, do něhož záznam události v SIEM zpravidla vchází, je *Ingress*. Zde je dešifrován a je ověřena jeho autenticita. Druhým modulem je *Tagging & Routing*. Zde jsou záznamu události přiřazeny interní značky (tagy), pomocí nichž je směrován do příslušných větví pipeline. V jedné pipeline tak může být zpracováváno více druhů záznamů událostí, které vyžadují rozdílné metody zpracování. Třetím modulem je *Parsing*. Zde dochází k extrakci informací ze záznamu události. Modul transformuje záznamy událostí, mnohdy ve formě prostého

textu, do podoby strukturovaných dat, která je poté možné automatizovaně zpracovávat. Čtvrtým modulem je *Indexing & Mapping*, kde je pro každou položku nyní strukturovaného záznamu události určen nejvhodnější typ, např. IP adresa, textový řetězec, nebo časová známka, a záznamy událostí jsou optimalizovány pro vyhledávání. Teprve poté je záznam události uložen na centrálním SIEM úložišti a mohou k němu přistupovat uživatelé systému.

Návrh implementace algoritmu pro řízení retence událostí je znázorněn na Obrázku 1 (červená barva). Pro přehlednost je potřeba prvně uvést, jak systém ovlivní průchod záznamu události SIEM pipeline a poté, jak lze jednotlivé moduly systému implementovat. Konec kapitoly je věnován výhodám i nevýhodám systému, a otevřeným otázkám, které je nutné před nasazením systému vyřešit, zejména s ohledem na pokročilejší automatizaci.

Zpracování záznamů událostí v SIEM pipeline ovlivní systém poprvé v modulu *Parsing*, do které zasahuje modulem *Tagging*. Modul je posunutý nad úroveň *Tagging & Routing* modulu v pipeline z toho důvodu, že až v *Parsing* modulu dochází k extrakci všech relevantních informací ze záznamu události. Typicky teprve zde je možné nejspolehlivěji odlišit osobní údaje zvláštní kategorie a určit příslušné právní tituly zpracování. Na základě výše uvedených informací lze očekávat, že naprostá většina zpracovávaných záznamů bude spadat do údajů regulovaných nařízení GDPR. *Tagging* modul tedy nejprve označí každý záznam události procházející pipeline buď jako osobní údaj, nebo osobní údaje zvláštní kategorie. Poté modul přiřadí záznamu události jeden nebo více tagů odpovídajících výběru z množiny všech možných právních titulů pro zpracování. Z modulu odchází záznam události obohacen o všechny informace, které jsou nezbytné k vyhodnocení oprávněnosti zpracování a k určení délky retence.

Záznam události následně musí projít modulem *Vstupní filtr*. Tento filtr zahazuje záznamy událostí bez tagů, nebo s nevyhovující kombinací tagů, aby nedošlo ke zpracovávání záznamů událostí, pro které nebyl naplněn odpovídající titul. Např. filtr zahodí všechny záznamy, u nichž není žádný tag titulu, nebo záznamy obsahující osobní údaje zvláštní kategorie, kterým

není přidělen zvláštní právní titul. Filtr zajišťuje, že záznamy událostí, u nichž by hrozilo nedostatečně odůvodněné zpracování, jsou zahozeny ihned, jak je nedostatečnost odhalena.

V poslední fázi pipeline zpracování záznamů událostí jsou záznamy událostí uloženy na SIEM úložiště. Na tomto úložišti jsou záznamy spravovány modulem *Kontrola retence*. *Kontrola retence* periodicky, například jednou denně, prochází všechny záznamy událostí na úložišti. Řídí se následující logikou:

1. Pokud se u záznamu událostí nachází tag právního titulu, jehož životnost vypršela, smaž daný tag.
2. Pokud záznam událostí obsahuje osobní údaje zvláštní kategorie a zároveň nemá tag zvláštního právního titulu, smaž daný záznam.
3. Pokud záznam událostí nemá žádný tag titulu, smaž daný záznam.

Na úložišti by se tak neměly nacházet neodůvodněně zpracovávané záznamy událostí déle, než je nastavená perioda běhu modulu.

Moduly námi navrhovaného systému pro řízení retence lze implementovat částečně s využitím existujících funkcí SIEM, částečně jako vlastní kód. Modul *Tagging* je postavený na funkci SIEM, která umožňuje přidat každé události libovolné tagy. Tato funkce již při zpracovávání záznamů událostí obvykle bývá využita, a to pro směřování záznamů událostí do různých větví pipeline. Kategorie osobních údajů a tituly pro zpracování lze tedy uvádět přímo do konfigurace SIEM. *Vstupní filtr* je rovněž implementovatelný na úrovni SIEM, jako další modul včleněný do pipeline pro zpracování záznamů událostí. Poslední modul systému, *Kontrola retence*, přesahuje obvyklé možnosti SIEM a nejspíš bude muset být provozován externě. V principu jde ale o jednoduchý algoritmus, implementovatelný periodicky spouštěným skriptem, který volá příslušné SIEM funkce (přečti záznam, smaž položku, smaž záznam) přes jeho API. Pro modul postačí např. kombinace Python skriptu spravovaného v plánovači Temporal.⁴⁹

Kromě zajištění souladu retence dat v SIEM s legislativou platnou v České republice, má navrhovaný model následující výhody:

⁴⁹ Temporal. Webové sídlo. Dostupné z: <https://temporal.io/> [cit. 20. 9. 2025].

1. Škálovatelnost – všechny vstupy (kategorie osobních údajů, tituly, pravidla vstupního filtru) je možné jednoduše rozšiřovat a reagovat tak na změny v legislativě.
2. Granularita – retenci je možné nastavovat a kontrolovat až na úroveň jednotlivých záznamů událostí. Aktuálně je běžná různá retence pouze na úrovni kategorií záznamů událostí.
3. Snadný auditing – u každého záznamu události v SIEM je jasné stanoveno, z jakých titulů je zpracováván.

Na druhou stranu, zásadní nevýhodou systému je závislost na statické manuální konfiguraci, a to zejména u identifikace osobních údajů zvláštní kategorie. V současnosti je možné použít nastavení pipeline, kde například záznamy událostí z obecných webových serverů instituce budou staticky kategorizovány jako osobní údaje, zatímco záznamy z podмноžiny webových serverů poskytujících zdravotní služby, budou preventivně kategorizovány jako osobní údaje zvláštní kategorie. Takové statické nastavení je těžkopádné a náchylné k omylu, ale bohužel aktuálně neexistují nástroje, které by kategorizaci alespoň částečně automatizovaly.

S výše zmíněnou závislostí na statické konfiguraci závisí i otevřené otázky, které je třeba před nasazením systému vyřešit. Zejména jak lépe automatizovat:

1. Plnění množiny titulů – aktuálně řešení spoléhá na periodické kontroly právních předpisů, identifikaci účelů pro zpracování, a manuální přepis do tagů.
2. Stanovení pravidel pro vstupní filtr – primárním pramenem jsou pravidla obsažena v nařízení GDPR pro kategorie osobních dat a tituly pro zpracování.
3. Rozlišení osobních údajů zvláštní kategorie – kategorii lze nyní pouze odhadnout na základě typu zařízení a služeb, ze kterých jsou záznamy sbírané, a analýzy informačního obsahu vzorku záznamů událostí.

U otevřených otázek je plná automatizace převodu právních předpisů do praxe jen stěží uskutečnitelná, protože prostředí, na něž se tyto předpisy vztahují, je příliš proměnlivé. V tom případě je třeba alespoň definovat pro-

cesy pro provádění a kontrolu převodu daných pravidel ve spolupráci odborníků na právo a informační technologie.

6. ZÁVĚR

Tento článek představil problematiku uchovávání a správy bezpečnostních informací a událostí v organizaci z pohledu požadavků kladených legislativou a navrhuje právní i technické řešení souběžné aplikace více legislativních požadavků na konkrétní údaje. V rámci toho došlo k odpovědi na dvě stanovené výzkumné otázky:

Jaké jsou požadavky právních předpisů na stanovení doby uchování a zabezpečení záznamů událostí zpracovávaných logovacím nástrojem? Nakládání se zpracovávanými daty je v různých předpisech řešeno různě, avšak na základě povahy ukládaných údajů a odlišných účelů legislativy mohou být tyto požadavky aplikovány souběžně. Některé povinnosti jsou vymezeny konkrétně (ZEK), minimální dobou (ZoKB) nebo jsou ponechány na posouzení organizace (oprávněný zájem dle nařízení GDPR). Nastavení pravidel přístupu k takovýmto datům je primárně v režii dotčené organizace.

Jaké jsou technické možnosti implementace právních požadavků na uchovávání údajů? Technické provedení navrženého právního řešení je založeno na tagování (štítkování) jednotlivých záznamů podle účelu jejich zpracování v kombinaci s ověřováním aktuality jednotlivých tagů a nastavením pravidel pro případ, že tagy již aktuální nebudou, neboť účely zpracování vyprší. Navržené řešení se neobejde bez lidského zásahu, co se týče klasifikace zpracovávaných údajů, identifikace titulů pro zpracování a nastavení doby uchování. Po uskutečnění těchto kroků však dokáže fungovat automatizovaně a zároveň nabízí praktické vlastnosti v podobě škálovatelnosti, uzpůsobení granularity a jednoduché auditovatelnosti.

7. SEZNAM POUŽITÝCH ZDROJŮ

- [1] ALI, Sijjad; WANG, Jia a LEUNG, Victor Chung Ming. AI-driven fusion with cybersecurity: Exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms- A comprehensive review. *Information Fusion*. [online]. 2025, roč. 118, s. 1-45. [cit. 20. 9. 2025]. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S1566253524007000>
- [2] BHATT, Sandeep; MANADHATA, Pratyusa K. a ZOMLOT, Loai. The Operational Role of Security Information and Event Management Systems. *IEEE Security & Privacy*. [online]. 2014, roč. 12, č. 5, s. 35-41. [cit. 20. 9. 2025]. Dostupné z: <https://ieeexplore.ieee.org/document/6924640>
- [3] CHUDOMELOVÁ, Zuzana. *Zákon o elektronických komunikacích: komentář*. 2. vydání. Komentáře Wolters Kluwer. Praha: Wolters Kluwer, 2025, 661 s. ISBN 978-80-286-0151-5.
- [4] GONZÁLEZ-GRANADILLO, Gustavo, GONZÁLEZ-ZARZOSA, Susana and DIAZ Rodrigo. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors*. [online]. 2021, roč. 21, č. 14, s. 1-38. [cit. 20. 9. 2025]. Dostupné z: <https://www.mdpi.com/1424-8220/21/14/4759>
- [5] JIRÁSEK, Petr; NOVÁK, Ludík a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. Šesté, doplněné a upravené elektronické vydání. Praha: Centrum kybernetické bezpečnosti, z.ú., 2025, 396 s. ISBN 978-80-53054-00-3.
- [6] KENT, Karen a SOUPPAYA, Murugiah. NIST SP 800-92 Guide to Computer Security Log Management In: COMPUTER SECURITY RESOURCE CENTER NIST [online]. 2006. [cit. 20. 9. 2025]. Dostupné z: <https://csrc.nist.gov/pubs/sp/800/92/final>
- [7] KUNER, Christopher; BYGRAVE, Lee A.; DOCKSEY, Christopher a DRECHSLER, Laura (ed.). *The EU general data protection regulation (GDPR): a commentary*. Oxford: Oxford University Press, 2020, 1393 s. ISBN 978-0-19-882649-1.
- [8] LIU, Che-Wei; HUANG, Peng a LUCAS, Henry C. Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions. *Journal of Management Information Systems*. [online]. 2019, roč. 37, č. 3, s. 758 - 787. [cit. 20. 9. 2025]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2850178
- [9] MAISNER, Martin. *Zákon o kybernetické bezpečnosti: komentář*. Komentáře Wolters Kluwer. Praha: Wolters Kluwer, 2015, 219 s. ISBN 978-80-7478-817-8.
- [10] MENGES, Florian, Tobias LATZO, Manfred VIELBERTH, Sabine SOBOLA, Henrich C. POHLS, Benjamin TAUBMANN, Johannes KOSTLER, Alexander PUCHTA, Felix FREILING, Hans P. REISER a Günther PERNUL. Towards GDPR-compliant data processing in modern SIEM systems, *Computers & Security*, 2021, sv. 103, 102165.
- [11] NONNEMANN, František; ÈERVENÝ, Vlastimil a VÍTEK, Dominik. *Kybernetický bezpečnostní incident 3D: IT, právo a compliance*. 2. vydání. Právní monografie. Praha: Wolters Kluwer, 2025, 258 s. ISBN 978-80-286-0331-1.

- [12] POLČÁK, Radim; LOUTOCKÝ, Pavel; KASL, František; MÍŠEK, Jakub; HOSTAŠ, Petr et al. *Právo informačních technologií*. 2. vydání. Právní monografie. Praha: Wolters Kluwer, 2024, 955 s. ISBN 978-80-286-0059-4.
- [13] Rozsudek SDEU (prvního senátu) ze dne 4. 11. 2025 ve věci C-413/23 P, Evropský inspektor ochrany údajů v. SRB (Notion de données à caractère personnel), ECLI:EU:C:2025:645.
- [14] SARTOR, Giovanni. The right to be forgotten: balancing interests in the flux of time. *International Journal of Law and Information Technology*, 2016, roč. 24, č. 1, s. 72-98. ISSN: 0967-0769
- [15] SASHWIN, K; NITHIKA, K S; PRIYADHARSHINI, S; MADUVANT, S P a SARANYA. Analysis, Trends, and Utilization of Security Information and Event Management (SIEM) in Critical Infrastructures. *2024 10th International Conference on Advanced Computing and Communication Systems (ICACCS)*. [online]. 2024, s. 1980-1984. [cit. 20. 9. 2025]. Dostupné z: <https://ieeexplore.ieee.org/document/10717237>
- [16] *Temporal*. Webové sídlo. Dostupné z: <https://temporal.io/> [cit. 20. 9. 2025].
- [17] URŠIÈ VRABEC, Helena. *Data subject rights under the GDPR: with a commentary through the lens of the data-driven economy*. Oxford: Oxford University Press, 2021, 268 s. ISBN 978-0-19-886842-2.
- [18] VELÁSQUEZ, Juan, Miguel, Lopez; MONTERRUBIO, Sergio, Mauricio, Martínez; CRESPO, Luis, Enrique, Sánchez a ROSADO, David, Garcia. Systematic review of SIEM technology: SIEM-SC birth. *International Journal of Information Security*. [online]. 2023, roč. 22, s. 691-711. [cit. 20. 9. 2025]. Dostupné z: <https://link.springer.com/article/10.1007/s10207-022-00657-9>

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>).

INSTRUCTIONS FOR AUTHORS

The Review of Law and Technology is a peer-reviewed scientific journal for technological areas of law and jurisprudence.

Since 1st January 2015 the journal is listed in the List of non-impact peer-reviewed journals published in the Czech Republic and since 24th June 2015 in ERIH PLUS database.

Contributions submitted for the Topic and Discussion sections are anonymously peer-reviewed by at least two independent reviewers and the final decision on publication is in the sole discretion of the editorial board. Review process takes approximately one month. The submissions are not subject to language proofreading.

Contributions shall be submitted through our web-based system available at <https://journals.muni.cz/revue>

RECOMMENDED EXTENT OF THE CONTRIBUTIONS:

Discussion:	15 – 30 standard pages
Annotation:	2 – 10 standard pages
Essays:	5 – 10 standard pages
Thesis review:	2 – 5 standard pages
Book review:	2 – 5 standard pages
Topic:	30 – 50 standard pages
(including spaces, footnotes and bibliography)	

CITATIONS FORMAT

Citations shall be in accordance with the ISO 690:2022 citation standard.

Referencing examples are available in interpretations of the aforementioned citation standard (e. g. at <https://www.citace.com/CSN-ISO-690>).

Individual sources are referenced in the text by upper index. The actual citation of the source is then contained in a footnote.

Authors must transparently state the use of AI generative tools in the creation of the text.

DEADLINES FOR CONTRIBUTIONS SUBMISSIONS

For the summer issue: 28th February

For the winter issue: 31st August

The Review of Law and Technology is a gold open access journal.

The journal and contributions are available on the journal website at www.journals.muni.cz/revue under the terms of public license Creative Commons Attribution-ShareAlike 4.0 International (Available at: <http://creativecommons.org/licenses/by-sa/4.0/legalcode>).

Contributions are included into respective electronic legal information systems operated by Wolters Kluwer ČR, a. s. (ASPI), Nakladatelství C. H. BECK, s. r. o. (beck-online.cz) and ATLAS consulting spol. s r. o. (CODEXIS).

Detailed information about the publication process, structure and format of the contributions, the review process and copyright are available in the “For authors” section at <https://journals.muni.cz/revue/about/submissions>. Further information is available upon request addressed to editorial staff (contact e-mail: revue@law.muni.cz).

REVIEW OF LAW AND TECHNOLOGY

VOLUME 16 | YEAR 2025 | NUMBER 32

DISCUSSION

Georgia Hejduková: Malware as a work of authorship: Analysis of protection and its limits in European law	3
Tomáš Lechner: Legal aspects of data format requirements	21
Adam Žváček: Tracing from the perspective of copyright law	49

ANNOTATION

K. Akil, A. Blechová, M. Erlebach, Š. Chvojka, J. Harašta, P. Loutocký, J. Martínek, K. Mlčáková, O. Woznica: Overview of the Current Case Law II/2025	107
---	-----

ESSAYS

P. Minima, O. Sukač: Essays II/2025	129
--	-----

THESIS REVIEW

K. Akil, O. Böhm, M. Erlebach, T. Mizerová, D. Palašta, F. Kasl: Thesis Review II/2025	155
---	-----

BOOK REVIEW

Kristýna Akil: LEISER, M.: Dark patterns, deceptive design, and the law: AI's hidden influence on our digital experience	187
---	-----

TOPIC

Jakub Sauer, Stanislav Špaček, Patrik Fráňa, Denisa Drappanová, Jakub Harašta: Event records: Determining retention periods and implementing complex requirements within the organization	195
--	-----

Review of Law and Technology

Peer-reviewed scientific journal for technological areas of law and jurisprudence, listed in the List of non-impact peer-reviewed journals published in the Czech Republic and ERIH PLUS database.

Only the contributions submitted for the Discussion and Topic sections are peer-reviewed.

Published bi-annually. This issue was published on 31st December 2025.

ISSN 1804-5383 (Print), ISSN 1805-2797 (Online), Ev. nr. MK ČR E 19707

Published by: Masaryk University, Žerotínovo nám. 9, 601 77 Brno, Czech Republic, ID-Nr. 00216224

Editor-in-chief and contact person: JUDr. Ing. František Kasl, Ph.D., Institute of Law and Technology, Faculty of Law, Masaryk University, Veveří 70, 611 80 Brno, Czech Republic, tel: +420 549 49 5545, contact e-mail: frantisek.kasl@muni.cz | revue@law.muni.cz | <https://journals.muni.cz/revue>

Deputy editor-in-chief: Jakub Stojan

Editorial Staff: JUDr. Mgr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek, Ph.D.

Editor: Mgr. Martin Erlebach, Adéla Dočkalová, Martin Plášek

Editorial Board: prof. JUDr. Radim Polčák, Ph.D. (honorary chairman), JUDr. Zuzana Adamová, Ph.D., prof. JUDr. Michael Bogdan, B.A., LL.M., jur. dr. (Lund), JUDr. Marie Brejchová, LL.M., JUDr. Jiří Čermák, prof. JUDr. Bc. Tomáš Gřivna, Ph.D., prof. JUDr. Josef Kotásek, Ph.D., JUDr. Bc. Zdeněk Kučera, Ph.D., Mgr. Ing. Zbyněk Loeb, LL.M., JUDr. Ján Matejka, Ph.D., prof. RNDr. Václav Matyáš, M.Sc., Ph.D., doc. JUDr. Matěj Myška, Ph.D., Mgr. Antonín Panák, LL.M., Mgr. Bc. Adam Ptašník, Ph.D., JUDr. Danuše Spáčilová, JUDr. Eduard Szattler, Ph.D., JUDr. Tomáš Ščerba, Ph.D.

Layout: Mgr. Martin Loučka, doc. JUDr. Matěj Myška, Ph.D.

Print: POINT CZ, s.r.o., Milady Horákové 20, 602 00 Brno

The publication of this issue of the Review of Law and Technology was funded by the project „Právo a technologie XIII“, MUNI/A/1739/2024.

Journal © Masaryk University, 2025

děkuje svým partnerům za podporu v roce 2025



Wolters Kluwer

ZÁKONY **PRO**
LIDI

ROWAN®
LEGAL

Diskuze

Georgia Hejduková: **Malware jako autorské dílo: Analýza ochrany a jejích limitů v evropském právu**

Tomáš Lechner: **Právní aspekty požadavků na datové formáty**

Adam Žváček: **Tracing pohledem autorského práva**

Anotace

K. Akil, A. Blechová, M. Erlebach, Š. Chvojka, J. Harašta, P. Loutocký, J. Martínek, K. Mlčáková, O. Woznica: **Přehled aktuální judikatury II/2025**

Essays

P. Minima, O. Sukač: **Essays II/2025**

Recenze závěrečných prací

K. Akil, O. Böhm, M. Erlebach, T. Mizerová, D. Palašta, F. Kasl: **Recenze závěrečných prací I/2025**

Recenze

Kristýna Akil: **LEISER, M.: Dark patterns, deceptive design, and the law: AI's hidden influence on our digital experience**

Téma

Jakub Sauer, Stanislav Špaček, Patrik Fráňa, Denisa Drappanová, Jakub Harašta: **Záznamy události: Stanovení doby uchování a implementace komplexních požadavků na organizaci**

MUNI
PRESS

