

33

REVUE PRO PRÁVO A TECHNOLOGIE

Ústav práva a technologií Právnické fakulty Masarykovy univerzity

ROČNÍK 17 / ROK 2026 / ČÍSLO 33

REVUE.LAW.MUNI.CZ

České právo a informační technologie 2026

pořádá Ústav práva a technologií Právnické fakulty Masarykovy Univerzity
cyber.law.muni.cz

Konference bude rozdělena na plenární panelovou diskusi a jednání v sedmi odborných sekcích.

Pořadatel konference vyzývá zájemce o aktivní účast, aby hlásili své příspěvky do některé z odborných sekcí. Rozšířený abstrakt v rozsahu 1–2 stran obsahující strukturu příspěvku, výzkumnou otázku a zásadní myšlenky, které budou v prezentaci představeny, posílejte do **31. 7. 2026** na adresu **cpit@law.muni.cz**. O přijetí příspěvku k prezentaci bude rozhodnuto do 15. 8. 2026.

Písemná vyhotovení příspěvků jsou vítána k posouzení pro případnou publikaci v recenzovaném časopise **Revue pro právo a technologie**.

[Další informace na webu cpit.law.muni.cz](https://cpit.law.muni.cz)

Předběžný program konference

Čtvrtek 10. září 2026

12:00–13:00 Registrace

13:00–14:30 Plenární panelová diskuze

Lětzebuerg Urquell: aktuální judikatura SDEU v oblasti práva informačních technologií

Diskutující: Jan Passer, Andrea Moravčíková

Moderuje: Radim Polčák

14:30–15:00 Coffee break

15:00–16:30 Paralelní odborné sekce

Kyberkriminalita a elektronické důkazy (Václav Stupka)

Duševní vlastnictví online (Matěj Myška)

Právo a umělá inteligence (Andrej Křištofík)

16:30–17:00 Coffee break

17:00–18:30 Odborná sekce a minipanel

Ochrana osobních údajů a soukromí (Jakub Míšek)

Akt o umělé inteligenci a prováděcí legislativa v ČR (Andrej Křištofík) - minipanel s vstupem ČTÚ

19:00–23:00 Konferenční večere SONO

Pátek 11. září 2026

9:00–10:30 Paralelní odborné sekce

Kybernetická bezpečnost a obrana (Jakub Vostoupal)

Dopady umělé inteligence na ochranu spotřebitele (Jakub Harašta)

Digitalizace veřejné správy a soudnictví (Pavel Loutocký)

10:30–11:00 Coffee break

11:00–12:30 Plenární panelová diskuze

Právní rámec digitální ekonomiky: digitální služby v aplikační praxi

Diskutující: Tomáš Ondrejka, TBD

Moderuje: František Kasl

REVUE PRO PRÁVO A TECHNOLOGIE

ROČNÍK 17 | ROK 2026 | ČÍSLO 33

DISKUZE

Eva Fialová, Veronika Příbáš Žolnerčíková, Ján Matejka, Tereza Novotná: Právní limity využití dat pro trénink a provoz systémů umělé inteligence 3

Jan Martínek: Jak spravedlivě regulovat algoritmickou moderaci? Vyvažování projevu uživatelů a platformy v rozhodovací praxi Oversight Board 39

ANOTACE

Jan Martínek: Domestic partnership of Campos & Munoz: Kdo odpovídá za vyhalucinované precedenty?.. 85

A. Blechová, M. Erlebach, J. Harašta, A. Karpjáková, P. Loutocký, T. Mizerová, K. Mlčáková, M.

Plášek: Přehled aktuální judikatury I/2026..... 93

ESSAYS

Adéla Mertová: Life in the datasphere: The new always-online self..... 115

RECENZE ZÁVĚREČNÝCH PRACÍ

M. Erlebach, I. Holcová, A. Jareš, F. Kasl, P. Loutocký, O. Málek, M. Mesarčík, J. Míšek:

Recenze závěrečných prací I/2026 127

RECENZE

Ondřej Böhm: YEUNG, K., RANCHORDÁS, S.: An introduction to law and regulation: Text and materials 173

Martin Erlebach: VAN CLEYNENBREUGEL, P., GROZDANOVSKI, L. (eds). The Standards of Fairness in Digital Law: The Normative Foundations of the Data, Data Governance, Digital Services, Digital Markets and Artificial Intelligence Acts 185

Jan Martínek: CASAROSA, Federica, PSYCHOGIOPOULOU, Evangelia (eds.): Social Media, Fundamental Rights and Courts: A European Perspective 195

TÉMA

Zdeněk Fiala, Pavel Mates, Marek Pačmag: Aktuální otázky postihování deepfakes 201

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 30. 6. 2026.

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: Mgr. 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 Grivna, 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 Ptašík, 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

Časopis © Masarykova univerzita, 2026

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/RPT2026-1-1>

PRÁVNÍ LIMITY VYUŽITÍ DAT PRO TRÉNINK A PROVOZ SYSTÉMŮ UMĚLÉ INTELIGENCE¹

EVA FIALOVÁ, VERONIKA PŘÍBAŇ ŽOLNERČÍKOVÁ, JÁN MATEJKA,²
TEREZA NOVOTNÁ³

ABSTRAKT

Článek analyzuje právní limity využití dat pro trénink a provoz systémů umělé inteligence v českém a unijním právu. Soustředí se především na dva nosné okruhy: autorskoprávní režim využití chráněného obsahu, včetně výjimek pro text and data mining, a zpracování osobních údajů podle GDPR. V autorskoprávní části článek zkoumá, zda a za jakých podmínek představuje trénink modelu užití díla, jaký význam mají TDM výjimky, výhrada práv a otázka perzistence či memorování tréninkových dat. V části věnované ochraně osobních údajů článek hodnotí právní základy zpracování, test slučitelnosti účelů a dopady memorování modelu na postavení subjektů údajů. Stručně se věnuje též dalším právům třetích osob jako doplňkovým limitům. Cílem článku je vymezit hlavní interpretační problémy a nabídnout jejich systematické právní zhodnocení.

¹ Příspěvek vznikl za podpory projektu Technologické agentury ČR č. TQ12000040 s názvem Prospěšný multiagentní AI avatar v malé demokratické společnosti.

² Autoři působí na Ústavu státu a práva AV ČR, v. v. i., kontaktní e-mail: eva.fialova@ilaw.cas.cz, matejka@ilaw.cas.cz, veronika.zolnercikova@ilaw.cas.cz.

³ Autorka působí na Ústavu práva a technologií Právnické fakulty MU, kontaktní email: tereza.novotna@law.muni.cz

KLÍČOVÁ SLOVA

Umělá inteligence; akt o umělé inteligenci; tréninková data; text and data mining; GDPR; syntetická data; test slučitelnosti; ochranná známka; obchodní tajemství

ABSTRACT

The article analyses the legal limits on the use of data for the training and operation of artificial intelligence systems under Czech and European Union law. It focuses primarily on two core areas: the copyright regime governing the use of protected content, including the text and data mining exceptions, and the processing of personal data under the GDPR. In the copyright section, the article examines whether and under what conditions AI training constitutes use of a work, and what significance should be attributed to the TDM exceptions, rights reservations, and the persistence or memorisation of training data. In the data protection section, the article assesses the legal bases for processing, the compatibility test for further processing, and the implications of model memorisation for the position of data subjects. It also briefly addresses other third-party rights as supplementary legal constraints. The aim of the article is to identify the principal interpretative issues and to provide their systematic legal assessment.

KEY WORDS

Artificial intelligence; Artificial Intelligence Act; training data; text and data mining; GDPR; synthetic data; compatibility test; trademark; trade secret

1. ÚVOD

Umělá inteligence pro své fungování nezbytně potřebuje data, a to jak ve fázi vývoje (zejména formou tréninkových datasetů), tak i při samotném provozu systému. Kromě technických charakteristik, jako je typ, kvalita, rozsah nebo aktuálnost dat, hraje zásadní roli i jejich právní režim, zejména rozsah povolených způsobů jejich užití. Poskytovatelé systémů umělé inte-

ligence,⁴ jejichž legální definice je obsažena v aktu o umělé inteligenci (dále též „AIA“),⁵ jsou vázáni při vývoji a nasazení těchto systémů nejen technickými požadavky, ale také omezeními plynoucími z právních předpisů – zejména autorského práva, práv na ochranu osobních údajů a dalších souvisejících oblastí.

Povinnosti zajistit soulad s právními předpisy se přitom netýkají pouze subjektů, kteří výslovně spadají pod regulaci vysoce rizikových systémů podle aktu o umělé inteligenci, ale všech aktérů, kteří pracují s daty v rámci vývoje nebo provozu AI systémů.⁶ Již ve fázi návrhu systému je nezbytné věnovat pozornost právnímu režimu dat, která mají být použita. U systémů schopných autonomního učení totiž může docházet ke stírání hranice mezi daty a samotným algoritmem: data jsou transformována do modelových instrukcí, které určují chování systému.⁷ Z právního hlediska je proto nutné zohlednit zamýšlený účel využití systému již při výběru vstupních dat – například zda bude AI nasazena komerčně, nebo výlučně pro výzkumné účely, či zda má přístup k externím zdrojům, jako je internet.

Současný právní rámec v oblasti využívání dat pro AI systémy je roztržštěný, ne vždy konzistentní a často zaostává za dynamikou technologického vývoje. Český právní řád se musí vypořádat nejen s transpozicí a aplikací evropských předpisů, ale také s praktickými otázkami, které se objevují při nasazování konkrétních AI modelů – ať už jde o jazykové modely, systémy rozpoznávání obrazu, nebo prediktivní analytiku. Článek si klade otázku, za jakých podmínek je podle českého a unijního práva pří-

⁴ Poskytovateli umělé inteligence myslíme subjekty, které se podílí na vytváření systému umělé inteligence nebo obecných modelů umělé inteligence a uvádí je na trh nebo do provozu pod svým jménem nebo ochranou známkou. Celá právní definice je k dispozici v čl. 3 odst. 3 Aktu o umělé inteligenci.

⁵ Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci).

⁶ Systém umělé inteligence je považován za vysoce rizikový, pokud splňuje alespoň jedno z kritérií v čl. 6 Aktu o umělé inteligenci.

⁷ Komentář k § 1, Radim Polčák. POLČÁK, Radim et al. *Autorský zákon. Praktický komentář s judikaturou*. Praha: Leges, 2020, s. 58.

pustné využívat data pro trénink a provoz systémů umělé inteligence, pokud tato data zahrnují autorskoprávně chráněný obsah nebo osobní údaje. Pozornost je soustředěna především na dva nosné právní režimy – autorské právo a ochranu osobních údajů. Další práva třetích osob, zejména ochranné známky, obchodní tajemství a pravidla opakovaného využití informací veřejného sektoru, článek sleduje pouze jako doplňkové hraniční limity, které mohou ovlivnit zákonnost tréninku nebo nasazení modelu. Cílem článku není podat úplný přehled všech právních režimů vztahujících se k datům, ale identifikovat ty limity, které mají pro poskytovatele a uživatele AI systémů největší praktický význam a současně vyvolávají nejvýraznější interpretační nejistotu.

Metodologicky článek kombinuje právní analýzu vybraných ustanovení relevantních právních předpisů (autorský zákon, GDPR,⁸ akt o umělé inteligenci) s výkladovou praxí evropských orgánů a judikaturou Soudního dvora Evropské unie (dále jen „SDEU“). Zvláštní důraz je kladen na praktické aplikace a modelové situace, které mohou poskytovatelé AI systémů v České republice reálně řešit – například zjišťování oprávnění užít chráněné dílo, legální způsoby anonymizace osobních údajů v datasetech, nebo správné vymezení účelu vědeckého výzkumu z hlediska výjimek a omezení. Cílem je poskytnout čtenářům přehled relevantních právních limitů i orientační rámec, jak s daty pro AI v souladu se zákonem nakládat.

První část článku („Autorské právo a AI“) se věnuje problematice autorského díla a otázce, zda zpracování takového díla AI systémem představuje užití ve smyslu autorského zákona. Dále analyzuje podmínky uplatnění výjimek pro rozmnožování díla pro účely automatizované analýzy textů nebo dat neboli anglicky *text and data mining* (dále jen „TDM“) a upozorňuje na možnost autorů výslovně omezit užití jejich děl prostřednictvím technických prostředků. Závěr kapitoly se věnuje právnímu režimu tzv. syntetických dat.

⁸ 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 (obecné nařízení o ochraně osobních údajů).

Druhá část článku („Ochrana osobních údajů v AI datasetech“) se zabývá právním rámcem využití datových souborů obsahujících osobní údaje. Kromě základních principů zpracování podle nařízení GDPR poukazuje také na povinnost zohlednit pravidla aktu o umělé inteligenci a výkladové stanovisko Evropského sboru pro ochranu osobních údajů (č. 28/2024),⁹ které se zabývá vztahem obou předpisů. Kapitola dále vymezuje možné právní tituly zpracování osobních údajů, podmínky jejich legitimacy, tříkový test oprávněného zájmu a test slučitelnosti účelů zpracování.

Třetí část článku se stručně věnuje dalším právům třetích osob, zejména ochranným známkám, obchodnímu tajemství a režimu veřejných dat, a vymezuje jejich roli jako doplňkových limitů zákonnosti tréninku a nasazení AI systémů. Závěrečná část shrnuje dílčí právní závěry formulované v předchozích kapitolách.

2. AUTORSKÉ PRÁVO A AI

Z definice autorského díla podle § 2 odst. 1 zákona č. 121/2000 Sb., autorského zákona (dále též „AZ“) vyplývají tři kumulativně znaky: (1) tvůrčí činnost, (2) jedinečnost a (3) objektivní vnímatelnost. Tvůrčí činnost neboli kreativita se projevuje prostřednictvím rozhodnutí učiněných na základě tvůrčí svobody autora neboli rozhodnutími, kterými autor dílu vtiskl svůj osobní dotek.¹⁰ Autorské dílo musí být individuálním projevem osobnosti autora.¹¹ Tato podmínka odlišuje chráněná díla od pouhých kopií.¹²

Na způsobilosti být chráněno autorským právem neubírá dílu jeho rozsah. SDEU přiznal autorskoprávní ochranu i výňatku 11 slov, který svým výběrem, uspořádáním a kombinací umožňuje autorovi, aby vyjádřil svého

⁹ Evropský sbor pro ochranu osobních údajů. Stanovisko 28/2024 k určitým aspektům ochrany údajů v souvislosti se zpracováním osobních údajů v kontextu modelů umělé inteligence. [online] 2024 [cit. 15. 07 2025]. Dostupné z: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_cs

¹⁰ Rozsudek SDEU ze dne 1. prosince 2011, věc C-145/10 (*Painer*).

¹¹ Rozsudek Nejvyššího soudu České republiky ze dne 24. června 2015, sp. zn. 30 Cdo 360/2015.

¹² Rozsudek SDEU ze dne 12. září 2019, věc C-683/17 (*Cofemel*).

tvůrčího ducha originálním způsobem a aby dosáhl výsledku, který představuje duševní výtvar. Samotná slova však chráněna nejsou.¹³

Za dílo autorský zákon považuje také počítačový program, který je původní v tom smyslu, že je výsledkem autorovy vlastní duševní činnosti.

Kromě děl, která autorský zákon z ochrany vyjímá, nejsou za autorské dílo považovány mimo jiné principy, metody, matematické a obdobné vzorce, statistické grafy a další výstupy vypočtené v § 2 odst. 6 AZ. Zákon tak chrání monopolizaci myšlenek, principů a teorií.

Před trénováním umělé inteligence je potřeba vyhodnotit autorskoprávní charakter děl určených k trénování umělé inteligence a provozu AI. Povahu díla nelze posuzovat podle jeho estetické hodnoty či rozsahu. Posouzení, zda se jedná o autorské dílo, či nikoliv je právní otázkou. Soud by v konkrétním případě zkoumal, zda jsou naplněny všechny výše uvedené znaky díla.¹⁴

Specifickou ochranu mají podle autorského zákona databáze. Databáze mají povahu souborného díla, pokud jsou způsobem výběru nebo uspořádáním obsahu autorovým vlastním duševním výtvořem (§ 2 odst. 2 AZ). Taková databáze je pak chráněna jako autorské dílo. Specifickou ochranu databází obsahuje § 88 až 94 AZ.

Počítačový program a databáze jsou úzce propojeny. Databáze může být součástí samotného počítačového programu nebo jeho výstupem.¹⁵

2.1 NAPLNĚNÍ ZNAKŮ UŽITÍ AUTORSKÉHO DÍLA PŘI ZPRACOVÁNÍ DAT UMĚLOU INTELIGENCÍ

Užitím díla se rozumí jakákoli forma zpřístupnění, rozmnožení nebo komerčního využití autorského díla. Mezi užití díla patří mimo jiné rozmnožování díla, rozšiřování originálu nebo rozmnoženiny díla nebo sdělování díla veřejnosti. § 12 odst. 4 AZ je demonstrativním výčtem způsobů užití, který může být rozšiřován. Rozšiřující výklad pojmu „užití díla“ po-

¹³ Rozsudek SDEU ze dne 16. července 2009, věc C-5/08 (*Infopaq*).

¹⁴ Usnesení Nejvyššího soudu ze dne 26. srpna 2009, sp. zn. 5 Tdo 815/2009.

¹⁵ JANSÁ, Lukáš; OTEVŘEL, Petr; ŠTEVKO, Martin. *Softwarové právo*. Computer Press, 2018, s. 49 – 50.

dává SDEU v některých rozsudcích. Rozmnožování díla může mít podobu převzetí dvou vteřin zvukového záznamu,¹⁶ nebo přenesení díla na jiný materiál.¹⁷ Analogicky k rozsudku *Art & Allposters*¹⁸ můžeme tvrdit, že převedení díla do jiného formátu je jeho rozmnožení v autorskoprávním smyslu.

V souvislosti s rozvojem umělé inteligence a strojového učení se do popředí odborné diskuse dostává otázka, jaký je vztah mezi tréninkem umělé inteligence na datech a autorským právem. Může proces trénování na datech pocházejících z autorských děl představovat právně relevantní užití díla ve smyslu autorského práva? Ve vědeckém diskurzu je sporné, zda využití chráněných děl pro účely strojového učení je autorským právem chráněno jako užití díla, ke kterému je oprávněn primárně jeho autor. Podle Borghiho a Karapapy mění masová digitalizace chráněný obsah na data pro algoritmy.¹⁹ Díla jsou použita pro trénování ve formě dat. Rosanna Ducato a Alain Strowel²⁰ tvrdí, že výrazové prvky díla nejsou při zpracování umělou inteligencí využívány a také, že neexistuje publikum, které by dílo užívalo. Dílo v podobě dat slouží jen jako vstup pro trénování, pro hledání vzorů a souvztažností.²¹ Autorské dílo je zde redukováno na sadu dat, které neslouží k estetické recepci (*work as works*), ale k výpočtům (*work as data*). Trénování je analytické zpracování, nikoli užití díla jako takového.²²

Výše uvedený přístup vychází z principu, že autorské právo chrání formu vyjádření, nikoliv samotné myšlenky, fakta nebo algoritmy. Z tohoto pohledu je strojové učení analytickým užitím díla, které není užitím ve smyslu zákona, protože nezasahuje do chráněné podoby výrazu. Tento prin-

¹⁶ Rozsudek SDEU ze dne 29. července 2019, věc C-476/17 (*Pelham*).

¹⁷ Rozsudek SDEU ze dne 22. ledna 2015, věc C-419/13 (*Art & Allposters*).

¹⁸ Ibid.

¹⁹ BORGHI, Maurizio; KARAPAPA, Stavroula. Non-display Uses of Copyright Works: Google Books and Beyond, *Queen Mary Journal of Intellectual Property*, 2011, Vol. 2 No. 1.

²⁰ DUCATO, Rossana; STROWEL, Alain, M. Ensuring Text and Data Mining: Remaining Issues with the EU Copyright Exceptions and Possible Ways Out. *European Intellectual Property Review*. 2021, Vol. 43, No. 5, s. 334.

²¹ Ibid.

²² SENTLEBEN, Martin. Win-win: How to Remove Copyright Obstacles to AI Training While Ensuring Author Remuneration (and Why the European AI Act Fails to Do the Magic). [online] 2024 [cit. 15. 07 2025], s. 15. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4964460

cip bývá nazýván dichotomií výrazu a myšlenky nebo skutečnosti (*idea/expression* nebo *fact/expression dichotomy*).²³

Senftleben tvrdí, že otázku výše zmíněného rozlišování vyřešil alespoň v evropském právu akt o umělé inteligenci, který tuto distinkci nečiní a ukládá všem poskytovatelům AI systémů povinnost k ochraně dat.²⁴ Akt výslovně odkazuje na právní úpravu TDM zakotvenou v čl. 3 a 4 ve směrnici 2019/790 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu (dále jen „DSMD“). Poskytovatelé obecných modelů mají povinnost zavést politiku pro dodržování právních předpisů Unie v oblasti autorského práva, a zejména pro určení a dodržování výhrady práv vyjádřené podle čl. 4 odst. 3 směrnice (EU) 2019/790, a to i prostřednictvím nejmodernějších technologií (čl. 53 odst. 1 písm. c) AIA). Pokud byla práva výslovně a vhodným způsobem vyhrazena, musí poskytovatelé obecných modelů získat od nositelů práv licenci (bod 105 odůvodnění AIA).

2.2 TEXT AND DATA MINING A POVAHA ROZMNOŽENINY

V této podkapitole se podrobně zabýváme TDM výjimkami neboli výjimkami z práva na rozmnožování autorského díla pro účely automatizovaného vytěžování textů a možnostmi, které přináší poskytovatelům umělé inteligence. TDM výjimky mají základ v již zmíněném čl. 3 a 4 DSMD. Tyto výjimky se vztahují i na databáze chráněné *sui generis*. První výjimka se týká TDM pro účely vědy a výzkumu, druhá se pak vztahuje na TDM pro obecné účely.

Trénování modelů umělé inteligence je z technického hlediska proces statistické optimalizace. Model není vybaven soustavou předem napsaných pravidel, ale učí se z velkého množství dat postupnou úpravou svých para-

²³ Např. MARGONI, Thomas; KRETSCHMER, Martin. A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology. *GRUR International*. Oxford University Press, 2022, roč. 71, č. 8. s. 689. DOI: 10.1093/grur-int/ikac054.

²⁴ SENFTLEBEN, Martin. Win-win: How to Remove Copyright Obstacles to AI Training While Ensuring Author Remuneration (and Why the European AI Act Fails to Do the Magic). Op. cit.

metrů tak, aby minimalizoval chybu predikce.²⁵ U současných systémů, zejména jazykových a difuzních, je základem zpravidla architektura transformeru, která převádí vstupy na tokeny nebo jiné numerické reprezentace.²⁶ Pro právní analýzu je vhodné rozlišovat základní fáze tréninku, kterými jsou sběr a jejich předzpracování, samotný trénink na tréninkových datech, optimalizace parametrů a testování.²⁷ Na tuto fázi může navázat fine-tuning, tedy další trénink již předem natrénovaného modelu na užším data-setu za účelem jeho přizpůsobení konkrétnímu úkolu, doméně nebo stylu.²⁸

Pro právní posouzení je klíčový pojem memorování. Ne každé naučení statistických vzorů znamená, že model uchovává konkrétní data, avšak výzkum ukazuje, že modely mohou za určitých podmínek reprodukovat i velmi specifické části trénovacích dat.²⁹ Riziko memorování roste zejména tehdy, jedná-li se o velký model, nebo o určitý datový formát.³⁰

Z hlediska práva jsou významné i techniky machine unlearning, neboli strojové odučení, jejichž cílem je oslabit nebo odstranit účinek konkrétních trénovacích dat bez úplného přetrénování celého modelu.³¹

Do českého práva byly výjimky transponovány ustanovením § 39c a § 39d AZ. Podle § 39c odst. 1 AZ do práva autorského nezasahuje ten, kdo zhotoví rozmnoženinu díla za účelem automatizované analýzy textů nebo dat v digitální podobě. Druhý odstavec umožňuje autorovi výslovnou výhradu vhodným způsobem (tzv. *TDM-opt-out*). Pokud bylo dílo zveřejněno na internetu, má být výhrada učiněna strojově čitelnými prostředky.

²⁵ What is model training? IBM. [online] [cit. 15. 03. 2026]. Dostupné z: <https://www.ibm.com/think/topics/model-training>

²⁶ What is a transformer model? IBM. [online] [cit. 15. 03. 2026]. Dostupné z: <https://www.ibm.com/think/topics/transformer-model>

²⁷ What is model training? Op. cit.

²⁸ BOMMASANI, Rishi et al. On the Opportunities and Risks of Foundation Models. [online] 2021 [cit. 15. 06. 2025]. s. 85 Dostupné z: <https://arxiv.org/abs/2108.07258>

²⁹ Např. COOPER, Feder A.; GRIMMELMANN, James. The Files Are in the Computer: On Copyright, Memorization, and Generative AI. [online] 2025 [cit. 15. 03. 2025]. Dostupné z: <https://arxiv.org/abs/2404.12590>

³⁰ WEI, Jiaheng et al., Memorization in Deep Learning: A Survey. [online] 2025 [cit. 15. 03. 2025]. Dostupné z: <https://dl.acm.org/doi/10.1145/3769076>

³¹ NGUYEN, Thanh Tam. et al. A Survey of Machine Unlearning. [online] 2025 [cit. 15. 03. 2025]. Dostupné z: <https://dl.acm.org/doi/10.1145/3749987>

Ustanovení § 39d AZ se vztahuje na TDM prováděný pro účely vědeckého výzkumu vysokými školami nebo výzkumnými organizacemi definovanými v AZ a institucemi kulturního dědictví. Kromě institucí uvedených v zákoně nelze výjimku podle tohoto ustanovení využít jinými subjekty, které často provádí výzkum, např. soukromými společnostmi, klinikami, i když by toto využití bylo pouze pro účely výzkumu. Podle Zemského soudu v Hamburku, který řešil TDM pro trénování umělé inteligence by pojem vědecký výzkum neměl být vykládán příliš úzce tak, že by zahrnoval pouze pracovní kroky přímo související se získáváním znalostí. Stačí, aby daný pracovní krok směřoval k pozdějšímu získání znalostí.³²

Bez ohledu na to, zda je výjimka pro TDM využita pro obecné nebo výzkumné účely, následné užití chráněného obsahu (např. zpřístupnění veřejnosti) již nespadá pod výjimku TDM.³³ Pokud byl generativní AI model natrénován v souladu se zákonnou výjimkou pro TDM, ale později výstupem modelu dojde k rozmnožení nebo zpřístupnění chráněného obsahu třetích stran, takové užití již není chráněno touto výjimkou a může představovat porušení autorského práva.

Tyagi tvrdí, že výlučné zaměření na TDM jako podmínku zákonnosti tréninku AI je příliš úzké, a neodráží rychle se vyvíjející potřeby digitální ekonomiky.³⁴ Tyagi se přiklání k revidování taxativních výjimek pro oprávněné užití autorských děl, která podle ní neodpovídají flexibilitě, co technologický vývoj potřebuje.³⁵ Naproti tomu Margoni a Kretschmer považují výjimku pro TDM za dostatečně širokou, neboť zahrnuje známé metody analýzy dat. Podle těchto autorů bude definice TDM uplatnitelná i v budoucnu.³⁶

³² Rozsudek Zemského soudu v Hamburku ze dne 27. září 2024, No. 310 O 227/23 (*Kneschke v. LAION*) [online] [cit. 15. 03. 2026] Dostupné z: <https://www.landesrecht-hamburg.de/bsha/document/NJRE001588058>

³³ Např. ROSATI, Eleonora. No step-free copyright exceptions: The role of the three-step in defining permitted uses of protected content (including TDM for AI-training purposes). *University Faculty of Law Legal Studies Research Paper Series*. 2023, s. 16.

³⁴ TYAGI, Kalpana. Copyright, text & data mining and the innovation dimension of generative AI. *Journal of Intellectual Property Law & Practice*. 2024, s. 16.

³⁵ Ibid. s. 17.

³⁶ MARGONI, Thomas; KRETSCHMER, Martin. A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology. Op. cit., s. 687.

Tyagi se při kritice uzavřeného systému výjimek odvolává na americkou *fair use*.³⁷ Tato doktrína umožňuje užití autorských děl bez předchozího souhlasu autora nebo jiného nositele práv. I když má *fair use* svoje pravidla, nejedná se o uzavřený výčet výjimek, ale spíš o test přípustnosti užití.³⁸ Také evropské, a tím i české právo, zná tzv. třístupňový test přípustnosti, resp. přiměřenosti užití chráněných děl. Tento test se neuplatní samostatně, ale spolu se zákonnou výjimkou užití autorského díla. Pro výjimku TDM je tedy kromě § 39c a § 39d AZ třeba zohlednit i tento třístupňový test. V autorském zákoně je tento test zakotven v § 29 odst. 1 AZ. Výjimky a omezení práva autorského lze uplatnit pouze:

- 1) ve zvláštních případech stanovených zákonem, a
- 2) pouze tehdy, pokud takové užití díla není v rozporu s běžným způsobem užití díla, a
- 3) nejsou jím nepřiměřeně dotčeny oprávněné zájmy autora.

SDEU zdůrazňuje, že třístupňový test musí soudy provést pokaždé, když posuzují existenci výjimek a omezení autorského práva.³⁹ Nezbytnost provedení testu přiměřenosti v konkrétním případě uvádí i Nejvyšší soud.⁴⁰ Pro posouzení rozporu s obvyklým užitím díla, jímž by byly nepřiměřeně dotčeny oprávněné zájmy autora, není sama o sobě významná skutečnost, zda v důsledku užití díla došlo k přímému nebo nepřímému hospodářskému prospěchu, kupříkladu zisku z licencování systému umělé inteligence.

Výjimka pro TDM zahrnuje jen získání a rozmnožování díla, nikoliv jeho následné použití. Pro obecné využití TDM platí, že ten, kdo dílo pro účely TDM užije, je naopak zhotovenou rozmnoženinu oprávněn uchovat pouze po dobu nezbytnou pro účely této automatizované analýzy textů nebo dat. Mezi odbornou veřejností se vede debata o tom, zda memorování tréninkových dat vylučuje využití výjimky. Podle britského rozsudku ve věci Get-

³⁷ TYAGI, Kalpana. Copyright, text & data mining and the innovation dimension of generative AI. op. cit. s. 17.

³⁸ Fair use je zakotveno v § 107 Copyright Act (1976) a dotvářen judikaturou.

³⁹ ROSATI, Eleonora. No step-free copyright exceptions: The role of the three-step in defining permitted uses of protected content (including TDM for AI-training purposes). *University Faculty of Law Legal Studies Research Paper Series*. 2023, s. 20.

⁴⁰ Rozsudek Nejvyššího soudu ze dne 28. července 2023, sp.zn. 23 Cdo 2178/2022.

ty Images v Stability AI samotný model žádná autorská díla neukládá. Parametry modelu (*model weights*) jsou pouze výsledkem vzorců a znaků, které se model postupně naučil během trénovacího procesu. Soud neshledal, že by model byl tzv. *infringing copy* podle britského práva.⁴¹ Naopak německý soud ve věci GEMA v OpenAI uvedl, že pokud model memoruje autorská díla (konkrétně texty písní), které může na základě promptu vyvolat, nemůže se odvolávat na TDM.⁴²

Naopak pro využití TDM pro účely výzkumu je instituce zhotovenou rozmnoženinu povinna uložit s vhodnou úrovní zabezpečení a může ji uchovávat pro účely vědeckého výzkumu, včetně ověření výsledků výzkumu.

Čl. 4 odst. 1 DSMD uvádí, že obecná výjimka pro TDM je mimo jiné výjimkou z práv a jejich omezení uvedených v čl. 2 směrnice 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti (dále jen: „InfoSoc“), podle kterého členské státy stanoví autorům a držitelům autorských práv výlučné právo udělit svolení nebo zakázat přímé nebo nepřímé, dočasné nebo trvalé rozmnožování jakýmikoliv prostředky a v jakékoliv formě, vcelku nebo po částech mimo jiné pro autory v případě jejich děl. Omezením tohoto práva je právo pořídit za určitých okolností dočasnou rozmnoženinu. Čl. 5 odst. 1 InfoSoc uvádí, jaké jsou podmínky pro pořízení dočasné rozmnoženiny. Jsou jimi dočasné úkony rozmnožení, které jsou krátkodobé nebo příležitostné. Zároveň musí rozmnožení tvořit nedílnou a podstatnou část technologického procesu a jejich výhradním účelem musí být přenos v rámci sítě mezi třetími stranami uskutečněný zprostředkovatelem nebo oprávněné užití díla nebo jiného předmětu ochrany. Další podmínkou je, že nesmí mít žádný samostatný hospodářský význam.

⁴¹ Rozsudek Royal Courts of Justice ze dne 4. listopadu 2025, case No: IL-2023-000007 (Getty Images v Stability AI Ltd). [online] [cit. 15. 03. 2026]. Dostupné z: <https://www.judiciary.uk/wp-content/uploads/2025/11/Getty-Images-v-Stability-AI.pdf>

⁴² Rozsudek LG München I ze dne 11. listopadu 2025, No. 42 O 14139/24 (GEMA v OpenAI). [online] [cit. 15. 03. 2026]. Dostupné z: <https://www.gesetze-bayern.de/Content/Document/Y-300-Z-GRURRS-B-2025-N-30204>

Čl. 4 odst. 1 DSMD lze sice vykládat tím způsobem, že kromě omezení práva na rozmnožování zavádí další výjimku vedle výjimek uvedených v InfoSoc směrnici. Bod odůvodnění 9 InfoSoc uvádí, že omezení autorského práva uvedené v čl. 5 odst. 1 InfoSoc se uplatní. To znamená, že pokud dojde k výhradě z TDM, má nadále ten, kdo má v úmyslu dílo využít, možnost využít výjimku pro dočasnou rozmnoženinu podle čl. 5 odst. 1 InfoSoc. Dále i při uplatnění výjimky z TDM pro obecné účely je možné uchovávat rozmnoženinu pouze po dobu nezbytnou pro účely vytěžování textů a dat, tedy nikoliv trvale, nýbrž pouze dočasně po nezbytnou dobu.

Pojem dočasná rozmnoženina vyložil SDEU v rozsudcích *Infopaq* a *Infopaq II*.⁴³ Aby nebylo dočasné rozmnožení díla protiprávní, musí být splněno současně pět podmínek, a to

- 1) dočasnost – rozmnoženina musí být přechodná nebo nahodilá;
- 2) pomíjivost – rozmnoženina musí být krátkodobá a musí být automaticky bez lidského zásahu odstraněna, jakmile splní svůj technologický účel, automatické technologické procesy, které vyžadují takové rozmnožení a samy jej automaticky smažou;
- 3) neoddělitelná součást technologického procesu – pořízení rozmnoženiny musí proběhnout výhradně v rámci technologického procesu, bez něž by tento proces nemohl správně fungovat, rozmnožení musí být nepostradatelné pro fungování daného procesu;
- 4) účelem je umožnit oprávněné užití – jediným cílem pořízení rozmnoženiny je umožnit legální užití díla, buď na základě souhlasu nositele práv, nebo na základě zákonné výjimky;
- 5) bez samostatného hospodářského významu – pořízení rozmnoženiny nesmí vytvářet zvláštní zisk oddělitelný od běžného užití a nesmí vést ke změně díla, ekonomický význam se posuzuje relativně, tj. tato podmínka je splněna, pokud provedení těchto úkonů neumožňuje dosáhnout dodatečného prospěchu překračujícího prospěch vyplývající z oprávněného užití díla a pokud dočasné úkony rozmnožení nevedou k pozměnění díla.

⁴³ Usnesení SDEU ze dne 17. ledna 2012, věc C-302/10 (*Infopaq II*).

Pokud autor učiní výhradu proti využití svého díla k trénování AI systémů a jejich využití za provozu AI, nebude se moct poskytovatel systému zpravidla spolehnout na výjimku uvedenou v čl. 5 odst. 1 InfoSoc.

Pokud by však někdo chtěl využít autorská díla pro AI mimo rámec obecné TDM výjimky a příslušné smluvní licence na základě čl. 5 odst. 1 InfoSoc, muselo by být rozmnožení pouze přechodné nebo nahodilé. To však omezuje využitelnost této výjimky, protože trénink zahrnuje memorování určitého množství tréninkového materiálu.⁴⁴

Tradiční výjimka z rozmnožovacího práva podle InfoSoc navíc vyžaduje, aby byly rozmnoženiny automaticky odstraněny, jakmile splní svůj technologický účel. V praxi se však data často používají i pro následné testování modelů, což nesplňuje tuto podmínku.⁴⁵

Podle InfoSoc výjimky musí být účelem pořízení rozmnoženiny umožnění oprávněného užití, nikoliv být hlavním užitím samotným. U tréninku a provozu umělé inteligence je však cílem právě samotné využití rozmnoženin pro vytvoření modelu.

Nakonec InfoSoc výjimka platí pouze tehdy, pokud rozmnoženiny nemají samostatný hospodářský význam. U tréninku umělé inteligence je tomu naopak – rozmnoženiny zpravidla vedou ke vzniku komerčně využitelných modelů, a tedy mají značný ekonomický význam.

Obecná TDM výjimka i výjimka pro dočasnou rozmnoženinu podle čl. 5 odst. 1 InfoSoc neumožňuje ukládání trvalých rozmnoženin autorských děl. Trvalé rozmnoženiny však podle Margoniho a Kretschmera mají dvě podstatné funkce.⁴⁶ První z funkcí je uchovávání toho, z čeho byla data abstrahována. Jde o paměť AI modelu. Model navíc v některých případech obsahuje vysoce abstraktní reprezentace dat. V jiných případech může ale model obsahovat i části původních dat, včetně fragmentů chráněných děl

⁴⁴ COOPER, Feder, A.; GRIMMELMANN, James. The Files are in the Computer: Copyright, Memorization, and Generative AI. 2024, s. 15. Op. cit.

⁴⁵ Např. ZHANG, Andy K.; KLYMAN, Kevin; MAI, Yifan; LEVINE, Yoav; ZHANG, Yian; BOMMASANI, Rishi; LIANG, Percy. Language model developers should report train-test overlap. [online] [cit. 10. 08. 2025] 2024. Dostupné z: <https://arxiv.org/abs/2410.08385>

⁴⁶ MARGONI, Thomas; KRETSCHMER, Martin. A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology. Op. cit. s. 693.

nebo databází. Ani v jednom případě nelze data ve formátu původních děl použít.⁴⁷ Druhou z funkcí je ověření správnosti a spolehlivosti výstupu. Bez uložení děl, na kterých byl model trénován nebo je využil ke generování odpovědi, není toto ověření možné.⁴⁸ Naopak vědecké instituce mohou podle TDM výjimky pro vědecké účely rozmnoženinu uchovávat pro účely vědeckého výzkumu, včetně ověření výsledků výzkumu. Podmínkou takového uchování je samozřejmě vhodné zabezpečení rozmnoženin.

2.3 VÝHRADA AUTORA PROTI VYUŽITÍ TDM PRO OBECNÉ ÚČELY

Podle § 39c AZ může autor učinit výslovnou výhradu z využití svého díla pro TDM pro obecné účely. Výhradu může učinit strojově čitelnými prostředky. Strojově čitelná výhrada by měla být možná podle rozsudku hamburského soudu ve věci *Kneschke v. LAION* provedena i vyjádřením učiněným v přirozeném jazyce.⁴⁹

Ačkoliv by poskytovatelé generativních modelů měli respektovat tzv. TDM výhrady ze strany autorů, v praxi neexistuje jednotný způsob, jak tyto výhrady zveřejňovat, ani jak je technicky provádět. Tento problém analyzuje Paul Keller a Zuzanna Warso ve své zprávě pro Nadaci Open Future.⁵⁰ Upozorňují, že stále chybí obecně uznávané standardy nebo technické protokoly pro vyjádření takových výhrad. Pokud již nějaké protokoly existují, vztahují se obvykle jen na webové stránky – nikoliv na samotná autorská díla. Z toho důvodu je jejich použití v rukou provozovatelů těchto stránek, nikoliv samotných autorů nebo držitelů autorských práv.⁵¹

Držitelé práv zároveň upozorňují, že je velmi obtížné jasně odlišit výhrady určené pro generativní AI modely od těch, které se vztahují k jinému užití TDM. Není také zřejmé, zda má být výhrada vztažena ke konkrétnímu

⁴⁷ Ibid.

⁴⁸ Ibid., s 694.

⁴⁹ Rozsudek Zemského soudu v Hamburku ze dne 27. září 2024, No. 310 O 227/23 (*Kneschke v. LAION*).

⁵⁰ KELLER, Paul; WARSO, Zuzanna. Defining best practices for opting out of ML training. Open Future policy brief. [online] 2023 [cit. 10. 08. 2025] Dostupné z: <https://openfuture.eu/publication/defining-best-practices-for-opting-out-of-ml-training/>

⁵¹ Ibid., s. 8.

dílu jako celku, nebo ke každé jeho verzi či kopii zvlášť. Autoři zprávy rovněž upozorňují na riziko zneužití tohoto nástroje – například pokud výhradu uplatní osoba, která k tomu nemá zákonné oprávnění, případně pokud tak učiní úmyslně ve zlé víře. Výhrady se navíc mohou vztahovat i na díla, která již nejsou chráněna autorským právem, nebo na ta, jejichž užití je zcela volné.⁵²

Dalším problematickým bodem je, pokud strojově čitelná výhrada automaticky znemožní užití díla i vědecké instituci nebo instituci kulturního dědictví, které mají nezávisle na výjimce právo pro zákonem dané účely autorská díla využívat.

Výkon práva na výhradu naráží v praxi na další zásadní problém související se zvyklostí zveřejňování děl na internetu. Mechanismus vyjádření výhrady je závislý na prostředí, v němž je dílo zveřejněno. Podle § 39c odst. 2 AZ musí být vyjádřena vhodným způsobem, což v online prostředí typicky znamená realizaci prostřednictvím metadat nebo technických protokolů. Tyto nástroje však nejsou pod kontrolou samotného autora, nýbrž provozovatelů platform, kde je obsah zveřejňován, typicky online platformem či digitálních knihoven.

V důsledku toho autor často nemá faktickou možnost učinit výhradu vůči subjektům shromažďujícím data pro účely trénování a vytváření odpovědí za pomoci umělé inteligence. Pokud platforma neumožňuje technické označení výhrady, je výkon práva autora výrazně oslaben, ne-li znemožněn. Navíc, jak již bylo výše uvedeno, neexistuje harmonizovaný nebo závazný standard pro formu vyjádření výhrady napříč digitálními platformami, což vytváří právní nejistotu. Tím dochází k disproporcii mezi formálním oprávněním autora a jeho faktickými možnostmi svou vůli ohledně nepřístupnosti díla pro strojové učení účinně projevit.

Pokud je dílo poskytováno pod některým typem veřejné licence a je učiněna výhrada z výjimky pro TDM, musí být respektována licence, pod kterou je dílo poskytováno. Naopak, pokud výhrada učiněna není a uplatní se výjimka pro TDM, veřejná licence se na takové autorské dílo vztahovat ne-

⁵² Ibid. s. 13.

bude, neboť zákonná výjimka z užití autorského díla nad touto licencí převáží.⁵³

2.4 ZÁKONNÝ PŘÍSTUP

Ačkoliv to §§ 39c a 39d AZ výslovně nezmiňují, k dílům, která jsou použita pro TDM je potřeba mít zákonný přístup. Tuto podmínku uvádí u obecné TDM výjimky i výjimky pro vědecké účely DSMD, např. na základě předplatného publikací nebo licencí na otevřený přístup u vědeckých institucí (bod 10 odůvodnění DSMD). Margoni upozorňuje na to, že zákonný přístup se nerovná zákonný zdroj. Zákonný přístup se vztahuje na toho, kdo za účelem TDM ke zdroji přistupuje. Zákonný přístup nevypovídá o povaze díla a jeho zveřejnění. Osoba využívající výjimku může mít tak zákonný přístup k nezákonnému zdroji.⁵⁴ Vědecká instituce může mít zákonný přístup do databáze vědeckých děl, ve kterých mohou být zařazena díla bez příslušené licence. Přestože je dílo zveřejněno v rozporu s právem, může ho vědecká instituce legálně využít. Tento výklad však není v souladu s judikaturou SDEU, který pro uplatnění zákonné výjimky z rozmnožování podle čl. 5 InfoSoc vyžaduje, aby byl zdroj oprávněný, tj. aby byl sdílen, nebo byl užit jiným způsobem v souladu s právem.⁵⁵

Pokud by se učinilo rovnítko mezi zákonným přístupem a zákonným zdrojem, musela by osoba, která TDM výjimku využívá, zkoumat oprávněnost užití každého díla, což by bylo nepřiměřené a ukládalo by to navíc povinnost zdroj po identifikaci jeho neoprávněného užití z databáze tréninkových dat vymazat a již natrénovaný systém umělé inteligence přetrénovat. Na druhou stranu, jak upozorňuje Margoni, pokud zákonný přístup vykládáme tak, že vše, co je dostupné volně na internetu, tedy nechráněno

⁵³ SZKALEJ, Kacper; SENFTLEBEN, Martin. Generative AI and Creative Commons Licences The Application of Share Alike Obligations to Trained Models, Curated Datasets and AI Output. *JIPITEC - Journal of Intellectual Property, Information Technology and E-Commerce Law*. 2024, roč. 15, č. 3, s. 325.

⁵⁴ MARGONI, Thomas. TDM and generative AI: Lawful access and opt-outs. [online] 2024, [cit. 15. 06. 2025], s. 12. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5036164

⁵⁵ Rozsudek SDEU ze dne 10. dubna 2014, věc C-435/12 (*ACI Adam*), rozsudek SDEU ze dne 5. března 2025, věc C-463/12 (*Copydan*).

paywallem nebo jinými technickými prostředky, může být využito pro trénování umělé inteligence v rámci TDM výjimky, což je ostatně výklad zákonného přístupu, který uvádí sama DSMD v bodu 14 odůvodnění, mohou být takto díla pro trénování užita. Podle Margoniho lze u vědeckých institucí v takovém případě zvážit test přiměřenosti mezi veřejným zájmem na výzkumu a ochranou autorských práv, u obecné TDM výjimky, kde modely může testovat kdokoli pro jakýkoliv účel, by mělo být znění ustanovení čl. 4 DSMD odlišné. Zákonodárce měl podle Margoniho místo podmínky zákonného přístupu zvolit podmínku zákonného zdroje.⁵⁶ Na internetu volně dostupná díla jsou i díla uložená na tzv. pirátských platformách. Pirátské platformy definuje Ondřejová a kol. jako „*služby informační společnosti [....] které svým uživatelům umožňují nahrávat audiovizuální a obdobné digitální soubory, jež jsou jiným uživatelům veřejně dostupné k přehrávání či stahování, přičemž hlavním účelem těchto platforem je provádět nebo usnadňovat pirátství v oblasti autorských práv, tj. provádět nebo usnadňovat neoprávněné užití děl nebo jiných předmětů ochrany.*“⁵⁷ Vedle pirátských platforem se na internetu se vyskytují i další webové stránky, na něž jejich provozovatelé nahrávají autorská díla bez toho, aniž by měli právo dílo takovým způsobem užít.

Čl. 4 DSMD měl obsahovat podmínku ve smyslu rozsudku SDEU GS Media,⁵⁸ kdy by osoba využívající TDM výjimku mohla volně dostupné dílo využít k trénování systému umělé inteligence a jejímu provozu, tedy u odkazů na autorská díla, která nebyla zveřejněná za účelem dosažení zisku a osoba, která je využila, nevěděla nebo nemohla vědět o protiprávní povaze zveřejnění. V případě, když by díla byla zveřejněná za účelem dosažení zisku, by se vědomost presumovala.

⁵⁶ MARGONI, Thomas. *Saving research: Lawful access to unlawful sources under Art. 3 CDSM Directive?* Kluwer Copyright Blog [online] 2023 [cit. 15. 06. 2025]. Dostupné z: <https://legal-blogs.wolterskluwer.com/copyright-blog/saving-research-lawful-access-to-unlawful-sources-under-art-3-cdsm-directive/>

⁵⁷ ONDŘEJOVÁ, Dana; ŘIČÁNEK, Matěj; NEPUŠTIL, David, Pirátské platformy pro sdílení obsahu online z pohledu práva proti nekalé soutěži, *Právník*, 2025, č. 1, s. 47.

⁵⁸ Rozsudek SDEU ze dne 8. září 2016, věc C-160/15 (GS Media).

2.5 SYNTETICKÁ DATA

Na některé nedostatky TDM může být odpovědí použití syntetických dat, která si vytvoří poskytovatel AI sám a která nejsou chráněná autorským právem jiného. Nicméně i syntetická data jsou tvořena AI systémy, které na počátku musely být trénovány na reálných datech. Není tedy vyloučeno, že výstupy systému budou shodné nebo velmi podobné dílu, na kterém byl trénován původní systém.⁵⁹ Pokud trénovací data – byť syntetická – zachovávají strukturu, či charakteristické prvky původního díla, může jít o užití díla v autorskoprávním smyslu.

Používání dat generovaných umělou inteligencí pro další trénování modelů může vést k degeneraci modelu, známé také jako *model collapse* nebo *data contamination*.⁶⁰ Pokud AI systém trénujeme na výstupech jiného nebo téhož AI systému namísto na původních, lidských nebo reálných datech, dochází k postupnému snižování kvality modelu. Tyto výstupy generované z modelu již vytrénovaného na výstupech umělé inteligence často postrádají nuance, originalitu a faktickou přesnost, čímž model přejímá a reprodukuje své vlastní zjednodušené či zkreslené reprezentace světa. AI systém se stává méně schopným reagovat na komplexitu reálných dat.

V souvislosti se syntetickými daty je třeba poznamenat, že v současnosti většina právních řádů nepřiznává autorské právo k výstupu vytvořenému umělou inteligencí.⁶¹ Pokud by však došlo ke změně a výstupy umělé inteligence by požívaly právní ochrany autorským právem nebo právem souvi-

⁵⁹ KRISTENSEN, Gareth; DUNNING, Angela; SHEN, Gaia; BUCKLAND, Prudence; KEUSTERMANS, Jan-Frederik; ANCIAUX, Alix. Training AI models on Synthetic Data: No silver bullet for IP infringement risk in the context of training AI systems (Part 2 of 4). *Cleary AI and Technology Insights*. [online] 2023 [cit. 11. 08. 2025]. Dostupné z: <https://www.clearyiptechinsights.com/2023/12/training-ai-models-on-synthetic-data-no-silver-bullet-for-ip-infringement-risk-in-the-context-of-training-ai-systems-part-2-of-4/>

⁶⁰ BURDEN, John; CHIODO, Maurice; RUSE-KHAN, Henning Grosse; MARKSCHIES, Lisa; MÜLLER, Dennis; Ó HÉIGEARTAIGH, Seán; PODSZUN, Rupprecht; ZECH, Herbert. Model Collapse and the Right to Uncontaminated Human-Generated Data. [online] 2025 [cit. 11. 08. 2025] Dostupné z: <https://jolt.law.harvard.edu/digest/model-collapse-and-the-right-to-uncontaminated-human-generated-data>

⁶¹ Více např. FIALOVÁ, Eva. Umělá inteligence a otázky autorského práva, in: ZOUFALÝ, Vladimír. XXXI. Karlovarské právní dny. Praha: Leges, 2024. 401 s. ISBN 978-80-7502-7351.

sejícím s právem autorským, použití takových dat k trénování jiných AI modelů by výhody využití syntetických dat omezilo.

Z provedené analýzy plyne, že právní posouzení tréninku AI nelze redukovat na otázku, zda model „kopíruje“ původní dílo v tradičním smyslu. Rozhodující je, v jaké fázi a v jaké podobě dochází k rozmnožování chráněného obsahu, zda jsou splněny podmínky TDM výjimek a zda technické vlastnosti modelu, zejména memorování a možnost reprodukce konkrétních částí tréninkových dat, nevedou k překročení mezí zákonné licence. Právě zde se ukazuje, že technologické rozlišení mezi tréninkem, fine-tuningem, inferencí a perzistencí dat není jen technickým popisem, ale především předpokladem přesného právního závěru.

3. OCHRANA OSOBNÍCH ÚDAJŮ V TRÉNINKOVÝCH DATASETECH UMĚLÉ INTELIGENCE

Pokud se v tréninkových datech a datech zpracovávaných AI při jejím provozu vyskytnou osobní údaje,⁶² je třeba s nimi zacházet v souladu s GDPR. GDPR zakotvuje v čl. 5 odst. 1 sedm základních zásad, které představují obecný rámec zákonného a legitimního zpracování osobních údajů. Právě v kontextu těchto zásad je nezbytné rozlišovat tři vrstvy práce s daty v systémech umělé inteligence: (a) tréninkové datasety, (b) samotný parametrizovaný model a (c) jednotlivé výstupy. Tréninková data typicky představují klasickou „informaci o identifikované nebo identifikovatelné fyzické osobě“ ve smyslu čl. 4 odst. 1 GDPR, pokud obsahují osobní údaje. Tyto zásady pak plní funkci interpretačního vodítka pro výklad povinností správců a zpracovatelů.

Jednou ze zásad je zásada zákonnosti, korektnosti a transparentnosti, která vyžaduje, aby bylo zpracování prováděno na základě jednoho

⁶² Konkrétní výstupy modelu mohou takové údaje znovu reprodukovat nebo nově generovat, například v podobě textu či obrazu vztahujícího se ke konkrétní osobě. Naproti tomu samotný velký jazykový model není paměťovou strukturou, v níž by byly jednotlivé záznamy uchovány adresně obdobně jako v databázi; jde o soubor parametrů zachycujících statistické vztahy v tréninkových datech. To má význam pro posouzení, kdy lze hovořit o tom, že je zpracovávána „informace o“ konkrétním subjektu údajů – a tedy zda, a v jakém rozsahu, se GDPR vztahuje také na samotný model, nikoli pouze na tréninková data a výstupy.

z právních titulů podle čl. 6 GDPR. Zásada omezení účelu stanoví, že osobní údaje musí být shromažďovány pouze pro konkrétně vymezené, výslovně formulované a legitimní účely, přičemž jakékoli následné zpracování musí být s těmito účely slučitelné. Tato zásada tak vylučuje extenzivní interpretaci původních účelů zpracování či jejich dodatečnou změnu bez právního základu.

Zde je vhodné poznamenat, že se smíšenými daty, tedy s daty obsahujícími jak osobní, tak neosobní údaje musí být podle čl. 2 odst. 2 nařízení 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii nakládáno podle GDPR. Stejný princip platí i v případě dat obsahujících zvláštní kategorie údajů a běžné údaje (např. biometrické charakteristiky). Tyto daty je nutné podle SDEU zpracovávat podle pravidel pro zvláštní kategorie údajů.⁶³

3.1 OSOBNÍ ÚDAJE A TRÉNOVÁNÍ GENERATIVNÍCH AI SYSTÉMŮ

Trénování systémů umělé inteligence přináší v kontextu ochrany osobních údajů řadu netriviálních právních výzev.⁶⁴ Tyto problémy se týkají jak fáze sběru a předzpracování dat, tak samotného trénovacího procesu a jeho dopadů na práva subjektů údajů. Některá pravidla pro trénování systémů umělé inteligence obsahuje čl. 10 AIA, nicméně toto ustanovení se vztahuje výlučně na AI systémy označené za vysoce rizikové a zaobírá se převážně správou dat, aniž by poskytovalo nový základ pro zpracování osobních údajů (bod 63 odůvodnění AIA).

Z tohoto důvodu vypracoval Evropský sbor pro ochranu osobních údajů (dále jen: „EDPB“) stanovisko ke zpracování osobních údajů v kontextu modelů umělé inteligence.⁶⁵ Stanovisko sice uvádí, že poskytovatel systémů umělé inteligence musí dodržovat zákonnost zpracování podle čl. 6 odst. 1

⁶³ Rozsudek SDEU ze dne 4. července 2023, věc C-252/21 (*Meta proti Bundeskartellamt*).

⁶⁴ Např. HACKER, Philipp. legal framework for ai training data from first principles to the artificial intelligence act. *Law, Innovation and Technology*, 2021, Vol. 13, No. 2, s. 276.

⁶⁵ Evropský sbor pro ochranu osobních údajů. Stanovisko 28/2024 k určitým aspektům ochrany údajů v souvislosti se zpracováním osobních údajů v kontextu modelů umělé inteligence. [online] 2024 [cit. 15. 04. 2025]. Dostupné z: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_cs

GDPR, který obsahuje právní tituly zpracování. Zaměřuje se ale však pouze na titul zpracování pod písmem f), tedy zpracování na základě titulu spočívajícího v oprávněném zájmu. Toto stanovisko bylo vydáno na základě žádosti irského dozorového úřadu, který tento titul zpracování výslovně deklaroval ve svých otázkách. Uvedené reflektuje i současnou praxi, kde je oprávněný zájem zpravidla nejčastějším titulem, na základě, kterého poskytovatelé systémy umělé inteligence trénují.

Aby mohl být oprávněný zájem použit jako právní titul, musí být podroben tzv. tříkrokovému testu, který se skládá z identifikace konkrétního zájmu, zhodnocení nezbytnosti zpracování pro dosažení tohoto zájmu, a provedení testu vyváženosti, zda zájem správce nepřeváží nad právy a svobodami subjektů údajů.⁶⁶

V rámci prvního kroku je nutné, aby oprávněný zájem byl zákonný, přesně definovaný, reálný a nespekulativní. V oblasti AI může jít například o vývoj konverzačního modelu nebo o zajištění bezpečnosti informačních systémů. Ve druhém kroku musí být doloženo, že zpracování je skutečně nezbytné, tedy že existuje přímý vztah mezi účelem a prostředky a že neexistuje jiný, méně invazivní způsob, jak cíle dosáhnout. Správce musí také prokázat, že rozsah zpracovaných údajů odpovídá zásadě minimalizace. Zásada minimalizace dat v prostředí AI neznamena pouze omezení počtu položek v datasetu, ale i omezení rozsahu atributů, délky uchování, granularity dat a jejich dalšího sekundárního využití. V praxi to vyžaduje, aby správce již ve fázi tvorby datasetu rozlišoval, které kategorie údajů jsou pro daný model skutečně nezbytné, které lze pseudonymizovat nebo agregovat a které je třeba z tréninkového souboru zcela vyloučit.⁶⁷

Třetí krok, tedy test vyváženosti, vyžaduje posouzení konkrétních rizik dopadu zpracování na subjekty údajů. Důležité je přihlídnout ke kontextu zpracování, druhu údajů, vztahu správce a subjektu údajů a také k tomu, zda může subjekt oprávněně očekávat takové zpracování. EDPB zdůrazňuje,

⁶⁶ Ibid., s. 19.

⁶⁷ U fine-tuningu a dalších forem sekundárního tréninku je pak nutné minimalizaci posuzovat znovu, nikoli jen převzít závěry učiněné při původním sběru dat.

že složitost AI modelů může tato očekávání narušit. Poskytnutí jasných informací o zpracování je tak klíčovým prvkem v posuzování legitimacy.

Stanovisko rovněž připomíná, že v případech, kdy by zájmy subjektů údajů mohly převážet, může správce přistoupit k zavedení zmírňujících opatření – například omezení přístupu k údajům, technická opatření nebo omezení účelu. Tato opatření ale nenahrazují povinnosti plynoucí přímo z GDPR. Jejich vhodnost musí být vždy zvažována případ od případu s ohledem na konkrétní model, jeho použití a potenciální dopady na osoby, jejichž údaje byly použity, včetně např. možných dopadů do soukromí s ohledem na citlivost dotčených údajů.⁶⁸ Stanovisko EDPB zároveň konstatuje, že některé generativní (AI) modely jsou přímo navrženy tak, aby poskytovaly osobní údaje o jednotlivcích, jejichž data byla použita k trénování, případně aby tato data jinak zpřístupňovaly. EDPB pro tyto případy dovozuje, že tyto modely ze své podstaty (a typicky i nutně) obsahují informace o identifikované či identifikovatelné fyzické osobě, a proto představují zpracování osobních údajů. Nelze je tedy považovat za anonymní. Osobní údaje tak mohou dle názoru EDPB zůstat v parametrech modelu „absorbované“ jako matematické reprezentace: i když se liší od původních tréninkových záznamů, mohou nadále nést původní informaci, která může být z modelu nakonec získána či odvozena, přímo nebo nepřímo.

Takto formulovaný závěr lze podle našeho názoru považovat za správný, otázkou však je, zda jej lze bez dalšího zobecnit na všechny generativní modely. V existujícím diskurzu se objevují i kritické názory,⁶⁹ podle kterých tyto modely nezpracovávají kopie poskytnutých osobních údajů (dat), ale k jejich „produkci“ dochází až následně na základě zadání specifického promptu, který pak vede ke generování těchto výtvorů. Modely tak pracují pouze s určitým matematicky parametrizovaným popisem pravdě-

⁶⁸ K tomu více viz MATEJKA, Ján; MATOCHOVÁ, Soňa; PROKEŠ, Josef. Analysis of Biometric Data Under the General Data Protection Regulation. *Acta Informatica Pragensia*, Vol. 8, No. 2, 2019, případně též KANICH, Ondřej; MATEJKA, Ján; FIALOVÁ, Eva et al. Technological, legal, and sociological summary of biometric technology usage. *ScienceOpen Research*. 2022. DOI: 10.14293/S2199-1006.1.SOR.2022.0002.v1

⁶⁹ DHAMELIYA, Savan. US Court allows claims against text-to-image AI Companies [online] 2024 [cit. 06.07.2025]. Dostupné z: <https://iprmentlaw.com/2024/08/25/us-court-allows-claims-against-text-to-image-ai-companies-sarah-anderson-v-stability-ai/>

podobnostních vztahů v datech. Samotné výstupy modelu proto nelze chápat jako informaci „o“ konkrétní osobě ve stejném smyslu jako záznam v databázi. Takovou interpretaci zaujaly i některé dozorové úřady (DPA) ochrany osobních údajů, a to německý a dánský.⁷⁰ Tyto úřady dovozují, že samotný model neobsahuje osobní údaje – ty se v něm objevují až jako výstup na základě konkrétního promptu a generovaného výsledku.

Shora uvedená argumentace EDPB je přesvědčivá a z pohledu principů ochrany osobních údajů i argumentačně správná, nicméně s ohledem na fungování generativních (LLM) modelů ji lze označit za problematickou, resp. vyžadující bližší vhled do architektury těchto modelů. Tyto modely jsou založeny na neuronových sítích, přičemž jednotlivé parametry se často počítají ve stovkách miliard.⁷¹ Tyto parametry vznikají technickou optimalizací během procesu tréninku, kdy se model učí rozpoznávat statistické korelace mezi symboly. Primárním cílem není ukládat jednotlivá data, ale nacházet statistické vzorce.⁷² Generativní model (LLM) tak neobsahuje komplexní paměťové struktury (jak je tomu např. u databáze), ale pouhé pravděpodobnostní aproximace, jejímž cílem je predikovat následující výskyt slov. Ačkoli za určitých podmínek může LLM vygenerovat výstup, který se podobá reálným údajům (jako projev statistické funkce),⁷³ jde spíše

⁷⁰ LOKKE, Moerel; STORM, Martijn. Do LLMs “store” personal data? This is asking the wrong question. [online] 2024 IAPP [cit. 06.07.2025]. Dostupné z: https://iapp.org/news/a/dollms-store-personal-data-this-is-asking-the-wrong-question?utm_source=chatgpt.com

⁷¹ Např. model Open AI u aktuální verze (GPT 5.2) počet těchto parametrů nezveřejňuje, u některých LLM modelů je velikost uvedena přímo v primárních materiálech (např. GPT-3 jako 175 mld. parametrů; GPT-2 jako 1,5 mld. parametrů), zatímco u otevřených modelů bývá parametrická velikost standardně deklarována (např. Llama 405 mld., Gemma 27 mld.). K problematice parametrů více viz např. catherinebreslin.medium.com/what-is-a-parameter-3d4b7736c81d

⁷² Tyto parametry jsou výsledkem aproximace funkce, která maximalizuje pravděpodobnost výskytu sekvencí – avšak bez explicitního uchovávání původních vstupů. To je zásadně odlišné např. od databáze, kde se informace ukládá přímo a adresně. K tomu více viz např. HARTLEY, John. et al. Neural networks memorise personal information from one sample. In: *Scientific Reports* [online]. 2023, roč. 13, č. 1, s. 1 [cit. 06.07.2025]. DOI: 10.1038/s41598-023-48034-3

⁷³ SMITH, Victoria. et al. Identifying and Mitigating Privacy Risks Stemming from Language Models: A Survey. In: [online]. 2024, s. 3 [cit. 06.07.2025]. DOI: 10.48550/arXiv.2310.01424

o výjimku než pravidlo. Následný výskyt osobního údaje je pak závislý na typu promptu, rozsahu kontextu i samotné architektuře modelu.

Stanovisko EDPB je ve smyslu svých závěrů správné, neboť osobní údaje jsou těmito modely zpracovávány (a následně také generovány) jako vedlejší projev poskytované jazykové, resp. pravděpodobnostní funkce. Problémem tohoto stanoviska tak zůstává pouze určitá generalizace a absence technického rozlišení mezi paměťovým uchováváním údajů (jak je tomu u databáze) a strojovým učením vzorců (LLM).⁷⁴

3.2 TEST SLUČITELNOSTI JAKO PODMÍNKA TRÉNOVÁNÍ A DALŠÍHO PROVOZU AI SYSTÉMŮ

Za účelem posouzení, zda je zamýšlené následné zpracování osobních údajů slučitelné s původním účelem jejich shromáždění, je správce povinen provést tzv. test slučitelnosti ve smyslu čl. 6 odst. 4 GDPR. Tento test představuje systematické zhodnocení okolností zpracování, jehož cílem je zjistit, zda může správce provést nové zpracovatelské operace.

V rámci testu slučitelnosti musí správce zohlednit zejména tyto faktory: (i) míru souvislosti mezi účelem původního sběru údajů a účelem zamýšleného dalšího zpracování; (ii) kontext, v němž byly osobní údaje původně získány, a to se zvláštním důrazem na vztah mezi subjektem údajů a správcem; (iii) povahu dotčených údajů, zejména zda se jedná o zvláštní kategorie osobních údajů podle čl. 9 GDPR nebo o údaje týkající se trestních odsouzení a trestných činů ve smyslu čl. 10 GDPR; (iv) možné dopady dalšího zpracování na práva a svobody subjektů údajů; a (v) přítomnost vhodných

⁷⁴ Obdobná (avšak z pohledu regulace jiná) je úvaha o odvozeninách autorských děl, kde modely generativní umělé inteligence neobsahují přímé kopie chráněných autorských děl. Jde o statisticky odvozené z agregovaných korelací, nikoli o kopie samotných děl nebo jejich částí. Model proto neuchováva obsah děl jako takový, ale pouze abstraktní vztahy v datech. K reprodukci chráněného díla tedy nedochází existencí modelu jako takového, ale až v okamžiku konkrétního výstupu, který je možné zpětně identifikovat jako rozmnoženinu existujícího díla. Samotný model je proto z autorskoprávního hlediska neutrální technickou entitou – analogicky jako tiskárna nevytváří rozmnoženinu, že existuje, ale až v okamžiku tisku, a jen tehdy, pokud výstup představuje rozmnoženinu chráněného obsahu. K tomu více viz HOAG, Mark. Why AI Training Should Fall Outside Copyright's Domain: A Legal Analysis., [online] 2025 [cit. 06.07.2025]. s. 4. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5291815

záruk, jako je např. pseudonymizace, šifrování či jiné prostředky zmírňující zásah do soukromí.

Test slučitelnosti je možné provést pouze u zpracování prováděné týmě správcem, tj. posuzuje se slučitelnost mezi účely zpracování prováděné jedním správcem. Správce by tak mohl, pokud sekundární zpracování tímto testem úspěšně projde, znovu využít osobní údaje získané za jiným účelem k testování systému umělé inteligence. Naproti tomu předání těchto údajů jinému správci nemůže být hodnoceno testem slučitelnosti.

3.3 VÝKON PRÁVA NA VÝMAZ

Samostatnou otázkou je výkon práva na výmaz podle čl. 17 GDPR v případě parametrizovaných modelů. Je-li osobní údaj obsažen nikoli již v původním datasetu, ale v parametrech modelu nebo ve schopnosti modelu určitý údaj reprodukovat, naráží praktická realizace výmazu na technické limity. Model totiž zpravidla neuchovává jednotlivý údaj jako oddělitelnou položku, nýbrž jako součást distribuované reprezentace rozprostřené napříč velkým množstvím parametrů. Vliv konkrétního tréninkového záznamu se navíc v modelu typicky překrývá s vlivem jiných, legitimně ponechávaných dat, takže odstranění jedné informace může současně zasáhnout i znalosti, které mají být zachovány.

Tento problém je v novější technické literatuře označován jako retain-forget entanglement. Praktický výmaz dále komplikuje skutečnost, že předtrénování a následný fine-tuning probíhají jako stochastické a distribuované procesy. Bez detailní evidence tréninkových kroků, checkpointů a dalších technických záznamů proto zpravidla nelze přesně rekonstruovat stav modelu, který by odpovídal hypotetickému tréninku bez dotčených dat. Z právního hlediska proto nelze vystačit s pouhým odstraněním původního záznamu z datasetu, ale je třeba posoudit, zda model nadále umožňuje dotčený údaj rekonstruovat, generovat nebo inferenčně odvozovat. Právě zde nabývají významu techniky machine unlearning, omezení inferenčních schopností modelu, práce s checkpointy a průběžné testování reprodukovatelnosti osobních údajů. Současně je však třeba dodat, že u velkých jazykových modelů bývá post-hoc unlearning zpravidla pouze aproximativní.

Nejvyšší míru jistoty poskytuje až opětovné přetrénování, případně deterministický replay tréninku bez zapomenutých dat, jsou-li pro něj splněny technické předpoklady.⁷⁵

3.4 ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PRO ÚČELY VĚDY A VÝZKUMU

GDPR upravuje zpracování osobních údajů pro účely vědeckého výzkumu nikoli jako obecnou blanketní výjimku, ale jako zvláštní režim, který za splnění stanovených podmínek připouští dílčí odchylky od některých obecných pravidel zpracování. Podmínkou tohoto režimu je přijetí vhodných záruk pro práva a svobody subjektů údajů a zavedení odpovídajících technických a organizačních opatření. Tento režim přitom není obecně vázán na určitou právní formu správce. Rozhodující je účel zpracování a splnění materiálních podmínek stanovených právem ochrany osobních údajů.⁷⁶

Za podmínek čl. 89 odst. 1 GDPR se další zpracování osobních údajů pro účely vědeckého výzkumu nepovažuje za neslučitelné s původními účely zpracování a osobní údaje mohou být uchovávány po delší dobu, vyžaduje-li to tento účel. Totéž platí i pro zvláštní kategorie osobních údajů, avšak pouze tehdy, je-li vedle splnění požadavků čl. 89 odst. 1 GDPR dán také právní základ podle čl. 6 GDPR a některá z podmínek podle čl. 9 odst. 2 GDPR, zejména písm. j). V českém právu jsou konkrétní ochranná opatření rozvedena v § 16 zákona č. 110/2019 Sb., o zpracování osobních údajů.

Z uvedeného neplatí, že by zpracování osobních údajů při trénování AI systémů pro účely vědeckého výzkumu bylo podle GDPR automaticky přípustné. Přesnější je závěr, že takové zpracování může být právně přípustné, jsou-li v konkrétním případě splněny požadavky na zákonnost, účelové vy-

⁷⁵ CHENG, Jingpu et al. Machine Unlearning under Retain-Forget Entanglement. Dostupné z: <https://doi.org/10.48550/arXiv.2603.26569>

⁷⁶ K tomu více viz např. PASERI, Ludovica. Defining Scientific Research Within the EU's Politics of Data: The Impact on Personalized Smart Medicine. In: CASAROSA, F.; GENNARI, F.; ROSSI, A. (eds) *Enabling and Safeguarding Personalized Medicine. Data Science, Machine Intelligence, and Law*, 2025, vol 7. Springer. Dostupné z: https://doi.org/10.1007/978-3-031-99709-9_2

mezení, minimalizaci, proporcionalitu a vhodné záruky.⁷⁷ Na rozdíl od výjimky TDM pro výzkumné účely, která je omezena na určité typy institucí, výjimky pro vědecký výzkum nejsou omezeny osobou správce, a zpracování tedy může realizovat jakákoli organizace či podnikatelský subjekt.

4. OCHRANA DALŠÍCH PRÁV TŘETÍCH STRAN

Dosavadní diskurs o tréninkových datech se primárně soustředí na ochranu autorských práv a osobních údajů. Tento přístup vychází z logiky platného práva i z praktického významu těchto režimů – autorské právo chrání původce tvůrčího obsahu, zatímco právo na ochranu osobních údajů chrání jednotlivce před zneužitím informací o jejich identitě či chování. Při důkladnější analýze je však zřejmé, že právní režim tréninkových datasetů může být dotčen i dalšími právními instituty, jejichž porušení může mít pro poskytovatele AI systémů zásadní důsledky. Mezi tato další práva třetích osob patří především ochranné známky, obchodní tajemství a práva na informace, zejména z veřejného sektoru.

V obecné rovině platí, že AI modely, zejména generativního typu, pracují s rozsáhlým množstvím vstupních dat, která zahrnují nejen oprávněná zveřejněná data (zpravidla texty a obrázky), ale i strukturované databáze, interní dokumenty a případně i citlivé nebo komerčně hodnotné informace. V této fázi, kdy AI pouze „čte“ a „analyzuje“ vstupy, může dojít k neúmyslnému přijetí informací chráněných jako obchodní tajemství, k zaznamenání ochranných známek nebo k využití neveřejných dat z veřejné správy. Takové užití může z pohledu některých právních režimů vést k soudním sporům⁷⁸ a může představovat neoprávněné nakládání s chráněným prvkem, a to i přesto, že nebylo motivováno úmyslem škodit či konkurovat.

⁷⁷ Současné je třeba odlišovat tento datový režim (data governance) od autorskoprávní výjimky pro vytěžování textů a dat (TDM) pro účely vědeckého výzkumu, která je podle čl. 3 směrnice DSMD konstruována institucionálně pro výzkumné organizace a instituce kulturního dědictví.

⁷⁸ GROZDANOVSKI, Ljupcho. My AI, my code, my secret – Trade secrecy, informational transparency and meaningful litigant participation under the European Union's AI Liability Directive Proposal, *Computer Law & Security Review*, Roč. 56, 2025, 106117. Dostupné z: <https://doi.org/10.1016/j.clsr.2025.106117>.

Relevantní právní rizika přitom vyvstávají zejména v okamžiku, kdy je výstup modelu zpřístupněn uživateli, například pokud AI nástroj vygeneruje návrh produktu obsahující označení podobné registrované ochranné známce, nebo pokud zneužije interní informaci získanou z trénovacích dat pro konkurenční rozhodování.⁷⁹

Zatímco ochranné známky a obchodní tajemství jsou právně chráněny v obchodním kontextu a jejich porušení typicky dopadá na hospodářskou soutěž, práva na informace se týkají specifického režimu přístupu k veřejným datům. AI systémy přitom mohou využívat i informace pocházející z veřejného sektoru.⁸⁰ I v těchto případech je však třeba rozlišovat mezi volně přístupnými informacemi a informacemi, jejichž zpřístupnění je vázáno na konkrétní účel či licenci.⁸¹

Zahrnutí těchto dalších právních režimů do právní analýzy tréninkových dat je důležité i z pohledu principu due diligence.⁸² Nezohlednění právních překážek plynoucích z ochranné známky, obchodního tajemství nebo z licenčního režimu veřejných dat může vést nejen k porušení zákona, ale i k reputačnímu poškození a ztrátě důvěry veřejnosti v AI systémy.

Pro efektivní právní posouzení tréninkových datasetů je tedy nezbytné, aby byla vzata do úvahy práva, která mohou podstatným způsobem ovlivnit legálnost trénovacího procesu i následného využití modelu, a to zcela bez ohledu na to, zda jsou tradičně spojována s právní problematikou AI. Tato širší perspektiva právní odpovědnosti je rovněž v souladu s požadavky evropského regulačního rámce na důvěryhodnost a odpovědnost při vývoji a provozu systémů umělé inteligence.

⁷⁹ V těchto případech už nejde o čistě „interní“ zpracování dat, ale o situaci, kdy může být naplněn skutkový stav porušení práv třetích stran podle občanského, obchodního či veřejného práva.

⁸⁰ Zpravidla půjde o informace z registrů, úředních záznamů nebo otevřených databází (např. Registr smluv, Centrální registr oznámení, aj.)

⁸¹ K tomu srov. např. Směrnice Evropského parlamentu a Rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru.

⁸² Tj. povinnosti poskytovatelů AI systémů předem identifikovat, vyhodnotit a minimalizovat právní a etická rizika spojená s použitím dat – včetně rizika porušení práv třetích osob (např. autorských práv, ochranných známek, osobních údajů či obchodního tajemství). Tento přístup odpovídá požadavku na proaktivní a odpovědné nakládání s daty, jak jej stanoví např. čl. 10 a 53 AIA.

Jedním z práv třetích stran tohoto typu jsou ochranné známky, které představují chráněná označení, jejichž výskyt v tréninkových datech AI systémů vyvolává otázky související se zákonem č. 441/2003 Sb., o ochranných známkách (dále jen „ZOS“), jakož i s právem Evropské unie, konkrétně s nařízením (EU) 2017/1001 o ochranné známce EU. Obecně platí, že ochranná známka poskytuje jejímu majiteli výlučné právo označení používat v obchodním styku k odlišení jeho výrobků nebo služeb od ostatních. Využití ochranné známky ve fázi tréninku AI samo o sobě nemusí být „užitím v obchodním styku“, nicméně výstup modelu,⁸³ který ochrannou známku reprodukuje, už toto kritérium naplnit může.⁸⁴

Pokud jazykový model například generuje reklamní sdělení, v němž se objeví chráněné označení (např. „iPhone“ v popisu konkurenčního produktu), může jít o zásah do práv majitele známky, zejména pokud je použití způsobilé způsobit klamání veřejnosti, narušit rozlišovací způsobilost značky nebo její pověst (§ 10 ZOS; čl. 9 odst. 2 písm. c) nařízení (EU) 2017/1001) o ochranné známce.

V tomto kontextu je nutné rozlišovat mezi tzv. vyčerpáním práv (§ 11 ZOS) a zákonnými výjimkami, jako je užití v souladu s poctivými zvyklostmi v obchodním styku (§ 10 odst. 3 písm. b) ZOS). Nicméně samotné trénování AI systému na datech obsahujících ochranné známky nelze považovat samo o sobě za užití v obchodním styku,⁸⁵ pokud k němu nedojde ve spojení s konkrétní nabídkou zboží nebo služby.

Dalším rizikem při využití tréninkových dat je možné porušení obchodního tajemství podle § 504 občanského zákoníku (zákon č. 89/2012 Sb.) a zákona č. 286/2018 Sb., o ochraně obchodního tajemství, kterým byla transponována směrnice (EU) 2016/943. Obchodní tajemství představuje konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních

⁸³ Např. generovaný text, obrázek nebo značka.

⁸⁴ K tomu více viz BONADIO, Enrico; ROHATGI, Akshita, Trademarks and Artificial Intelligence: Some Preliminary Considerations, *European Intellectual Property Review*, [online] 2024, No. 11[cit. 06.07.2025]. Dostupné z: <https://ssrn.com/abstract=5364772> nebo <http://dx.doi.org/10.2139/ssrn.5364772>

⁸⁵ Viz např. rozsudek SDEU ze dne 23. března 2010, věc C-236/08 až C-238/08 (*Google France v. Louis Vuitton*), v němž bylo uvedeno, že klíčové pro zásah do práv je to, zda užití ochranné známky ovlivňuje její základní funkce, především funkci rozlišovací.

kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení. Neoprávněné získání, užití nebo zveřejnění takových informací může vést k občanskoprávní odpovědnosti nebo dokonce k trestnímu postihu.

Trénink AI systémů na datech, která obsahují interní dokumenty podniků, analytické modely, návrhy produktů, neveřejné smlouvy nebo nepublikované výzkumné výsledky, může představovat zásah do obchodního tajemství, pokud k jejich získání nedošlo oprávněným způsobem (např. smluvním poskytnutím).

Zvláštní pozornost si zaslouží využívání dat pocházejících z veřejné správy. Směrnice (EU) 2019/1024 o otevřených datech a opakovaném využívání informací veřejného sektoru (Open Data Directive) zavedla jednotný rámec, který umožňuje opakované využití veřejných informací včetně trénování AI systémů. V českém právu je tato problematika upravena zákonem č. 106/1999 Sb., o svobodném přístupu k informacím. Tyto předpisy umožňují přístup a opětovné využití veřejných dat, avšak stanovují rovněž výjimky.⁸⁶ Přestože by se mohlo zdát, že data z veřejných registrů jsou vhodným zdrojem pro trénování AI, platí zde zásada zákonného účelu a omezení rozsahu užití. Databáze veřejné správy nejsou automaticky bez právních omezení – např. katastr nemovitostí obsahuje osobní údaje, a jejich užití AI nástrojem by podléhalo režimu GDPR.

Další práva třetích osob nepředstavují samostatné těžiště právní regulace AI, ale doplňkové korektivy, které mohou v konkrétních případech rozhodnout o zákonnosti tréninku nebo nasazení systému.

5. ZÁVĚR

Vývoj a provoz systémů umělé inteligence je zásadně podmíněn dostupností kvalitních a právně využitelných dat. Tento článek ukázal, že právní limity užití tréninkových dat vycházejí především z oblasti autorského práva a ochrany osobních údajů. Vzhledem k dynamice vývoje AI systémů a aktuálně fragmentované právní úpravě se poskytovatelé těchto systémů často pohybují v prostředí právní nejistoty. V praxi je tak nezbytné uplatnit pre-

⁸⁶ Např. ochranu osobních údajů, obchodních tajemství a práv k duševnímu vlastnictví.

ventivní přístup a vyhodnocovat právní charakter dat již při jejich získávání a předzpracování.

Z hlediska autorského práva je nutno především zohlednit, zda data použita pro trénink obsahují chráněná autorská díla nebo databáze, případně zda jsou taková díla předmětem výhrady dle § 39c AZ. Výjimky pro TDM sice představují relevantní nástroj pro legální využití chráněných děl, avšak jejich uplatnění je podmíněno splněním striktních zákonných podmínek – včetně zákonného přístupu ke zdrojům a respektování výslovných výhrad. Právní rámec zatím neřeší dostatečně technickou proveditelnost těchto výhrad ani jejich interoperabilitu napříč platformami.

Ve vztahu k osobním údajům je klíčové správně zvolit právní titul zpracování. Nejčastěji půjde o oprávněný zájem, jehož použití musí být odůvodněno na základě tříkrokového testu. Při opakovaném nebo následném zpracování je třeba provést test slučitelnosti. GDPR sice umožňuje výjimky pro vědecký výzkum, ale i zde musí být zavedena vhodná technická a organizační opatření, zejména při zpracování zvláštních kategorií údajů.

Kromě autorského práva a ochrany osobních údajů je třeba při právním posuzování tréninkových dat věnovat pozornost i dalším právům třetích stran. Významná právní rizika mohou vzniknout v případě neoprávněného využití ochranných známek, obchodního tajemství nebo informací pocházejících z veřejného sektoru. Samotný výskyt registrovaných označení v trénovacích datasetech zpravidla nebude postačovat k závěru o zásahu do práv z ochranné známky; relevantní riziko vzniká zejména tehdy, pokud je označení reprodukováno nebo použito ve výstupu modelu v obchodním styku způsobem způsobilým vyvolat záměnu, oslabit rozlišovací způsobilost známky nebo poškodit její pověst. Stejně tak může neoprávněné využití interních dokumentů či analytických modelů představovat zásah do obchodního tajemství, a to i bez úmyslu konkurovat. Systémy AI mohou také zpracovávat data získaná z veřejné správy, jejichž použití je podmíněno specifickým účelem nebo licencí. Pro poskytovatele AI je proto nezbytné při tvorbě a používání tréninkových datasetů důsledně vyhodnocovat i tato rizika a zavést procesy právní due diligence, které zohlední nejen tradiční, ale i méně zjevné právní překážky. Vedle těchto majetkových práv nelze

opomenout ani klasická osobnostní práva fyzických osob podle občanského zákoníku, zejména právo na podobu, čest, důstojnost a soukromí. Rizika se zde neprojevují ani tak ve fázi tréninku, jako spíše na úrovni konkrétních výstupů generativních systémů.⁸⁷ V těchto případech může mít dotčená osoba k dispozici prostředky ochrany osobnosti (negativní nároky, odstranění závadného obsahu, náhradu nemajetkové újmy), a to i v případech, kdy autorské právo nebo GDPR neposkytují jednoznačnou ochranu.

Na základě provedené analýzy lze formulovat několik dílčích závěrů. Za prvé, zákonnost využití dat pro trénink a provoz AI systémů nelze odvozovat z jediného univerzálního právního režimu. Rozhodující je povaha dotčených dat a konkrétní fáze životního cyklu modelu. Za druhé, v oblasti autorského práva zůstává klíčovým limitem rozsah TDM výjimek, zejména ve vztahu k výhradě práv, zákonnému přístupu a otázce, zda model uchovává nebo reprodukuje chráněný obsah v právně relevantní podobě. Za třetí, v oblasti ochrany osobních údajů je třeba rozlišovat mezi tréninkovým datasetem, parametrizovaným modelem a konkrétním výstupem, neboť každá z těchto rovin může vyvolávat odlišné právní důsledky, zejména z hlediska právního základu zpracování, minimalizace dat a výkonu práv subjektu údajů. Za čtvrté, další práva třetích osob nepředstavují samostatné těžiště právní regulace AI, ale působí jako významné korektivy, které mohou v konkrétních případech rozhodnout o zákonnosti tréninku nebo nasazení systému.

6. SEZNAM POUŽITÝCH ZDROJŮ

[1] BOMMASANI, Rishi et al. On the Opportunities and Risks of Foundation Models. [online] 2021 [cit. 15. 06. 2025]. Dostupné z: <https://arxiv.org/abs/2108.07258>

[2] BONADIO, Enrico; ROHATGI, Akshita, Trademarks and Artificial Intelligence: Some Preliminary Considerations, *European Intellectual Property Review*. [online] 2024, No. 11. [cit. 06.07.2025]. Dostupné z: <https://ssrn.com/abstract=5364772> or <http://dx.doi.org/10.2139/ssrn.5364772>

[3] BORGHI, Maurizio; KARAPAPA, Stavroula. Non-display Uses of Copyright Works: Google Books and Beyond. *Queen Mary Journal of Intellectual Property*, 2011, Vol. 2, No. 1.

⁸⁷ Např. při vytváření deepfake obsahu, stylové imitaci výtvarné tvorby nebo generování textů, které jsou účelově přiřítány určité osobě a zasahují do její pověsti.

- [4] BURDEN, John; CHIODO, Maurice; RUSE-KHAN, Henning Grosse; MARKSCHIES, Lisa; MÜLLER, Dennis; Ó HÉIGEARTAIGH, Seán; PODSZUN, Rupprecht; ZECH, Herbert. Model Collapse and the Right to Uncontaminated Human-Generated Data. [online] 2025 [cit. 11. 08. 2025]. Dostupné z: <https://jolt.law.harvard.edu/digest/model-collapse-and-the-right-to-uncontaminated-human-generated-data>
- [5] COOPER, Feder A.; GRIMMELMANN, James. The Files are in the Computer: Copyright, Memorization, and Generative AI. [online] 2024 [cit. 15. 03. 2025]. Dostupné z: <https://arxiv.org/abs/2404.12590> [<https://arxiv.org/abs/2404.12590>]
- [6] DHAMELIYA, Savan. US Court allows claims against text-to-image AI Companies [online] 2024 [cit. 06.07.2025]. Dostupné z: <https://iprmentlaw.com/2024/08/25/us-court-allows-claims-against-text-to-image-ai-companies-sarah-anderson-v-stability-ai/>
- [7] DUCATO, Rossana; STROWEL, Alain M. Ensuring Text and Data Mining: Remaining Issues with the EU Copyright Exceptions and Possible Ways Out. *European Intellectual Property Review*, 2021, Vol. 43, No. 5, s. 334.
- [8] EVROPSKÝ sbor pro ochranu osobních údajů. Stanovisko 28/2024 k určitým aspektům ochrany údajů v souvislosti se zpracováním osobních údajů v kontextu modelů umělé inteligence. [online] 2024 [cit. 15. 04. 2025]. Dostupné z: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_cs
- [9] FIALOVÁ, Eva. Umělá inteligence a otázky autorského práva. In: ZOUFALÝ, Vladimír (ed.). XXXI. *Karlovarské právnícké dny*. Praha: Leges, 2024. 401 s. ISBN 978-80-7502-735-1.
- [10] GROZDANOVSKI, Ljupcho. My AI, my code, my secret – Trade secrecy, informational transparency and meaningful litigant participation under the European Union's AI Liability Directive Proposal. *Computer Law & Security Review*, Roč. 56, 2025, 106117. Dostupné z: <https://doi.org/10.1016/j.clsr.2025.106117>.
- [11] HACKER, Philipp. Legal framework for AI training data from first principles to the artificial intelligence act. *Law, Innovation and Technology*, 2021, Vol. 13, No. 2.
- [12] HOAG, Mark. Why AI Training Should Fall Outside Copyright's Domain: A Legal Analysis. [online] 2025 [cit. 06. 07. 2025]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5291815
- [13] CHALOUPKOVÁ, Helena; HOLÝ, Petr. *Autorský zákon. Komentář*. 6. vydání. Praha: C. H. Beck, 2023.
- [14] CHENG, Jingpu et al. Machine Unlearning under Retain-Forget Entanglement. Dostupné z: <https://doi.org/10.48550/arXiv.2603.26569>
- [15] JANSÁ, Lukáš; OTEVŘEL, Petr; ŠTEVKO, Martin. *Softwarové právo*. Computer Press, 2018.
- [16] KANICH, Ondřej; MATEJKA, Ján; FIALOVÁ, Eva et al. Technological, legal, and sociological summary of biometric technology usage. *ScienceOpen Research*, 2022. DOI: 10.14293/S2199-1006.1.SOR.2022.0002.v1

- [17] KELLER, Paul; WARSO, Zuzanna. Defining best practices for opting out of ML training. *Open Future policy brief*. [online] 2023 [cit. 10. 08. 2025]. Dostupné z: <https://openfuture.eu/publication/defining-best-practices-for-opting-out-of-ml-training/>
- [18] KRISTENSEN, Gareth; DUNNING, Angela; SHEN, Gaia; BUCKLAND, Prudence; KE-USTERMANS, Jan-Frederik; ANCIAUX, Alix. Training AI models on Synthetic Data: No silver bullet for IP infringement risk in the context of training AI systems (Part 2 of 4). *Cleary AI and Technology Insights*. [online] 2023 [cit. 11. 08. 2025]. Dostupné z: <https://www.clearyiptechinsights.com/2023/12/training-ai-models-on-synthetic-data-no-silver-bullet-for-ip-infringement-risk-in-the-context-of-training-ai-systems-part-2-of-4/>
- [19] LOKKE, Moerel; STORM, Martijn. Do LLMs “store” personal data? This is asking the wrong question. 2024 [online] *IAPP* [06.07.2025]. Dostupné z: https://iapp.org/news/a/do-llms-store-personal-data-this-is-asking-the-wrong-question?utm_source=chatgpt.com
- [20] MARGONI, Thomas. Saving research: Lawful access to unlawful sources under Art. 3 CD-SM Directive? *Kluwer Copyright Blog* [online] 2023 [cit. 15. 06. 2025]. Dostupné z: <https://legallblogs.wolterskluwer.com/copyright-blog/saving-research-lawful-access-to-unlawful-sources-under-art-3-cdsm-directive/>
- [21] MARGONI, Thomas. TDM and generative AI: Lawful access and opt-outs. [online] 2024 [cit. 15. 06. 2025]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5036164 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5036164)
- [22] MARGONI, Thomas; KRETSCHMER, Martin. A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology. *GRUR International*, 2022, roč. 71, č. 8, s. 687–694.
- [23] MATEJKA, Ján; MATOCHOVÁ, Soňa; PROKEŠ, Josef. Analysis of Biometric Data Under the General Data Protection Regulation. *Acta Informatica Pragensia*, 2019, Vol. 8, No. 2.
- [24] 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 (obecné nařízení o ochraně osobních údajů).
- [25] Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci).
- [26] NGUYEN, Thanh Tam. et al. *A Survey of Machine Unlearning*. [online] 2025 [cit. 15. 06. 2025]. Dostupné z: <https://dl.acm.org/doi/10.1145/3749987>
- [27] ONDREJOVÁ, Dana; ŘIČÁNEK, Matěj; NEPUŠTIL, David. Pirátské platformy pro sdílení obsahu online z pohledu práva proti nekalé soutěži. *Právník*, 2025, č. 1.
- [28] PASERI, Ludovica. Defining Scientific Research Within the EU’s Politics of Data: The Impact on Personalized Smart Medicine. In: CASAROSA, F.; GENNARI, F.; ROSSI, A. (eds) *Enabling and Safeguarding Personalized Medicine. Data Science, Machine Intelligence, and Law*, 2025, vol 7. Springer. Dostupné z: https://doi.org/10.1007/978-3-031-99709-9_2

- [29] POLČÁK, Radim et al. *Autorský zákon. Praktický komentář s judikaturou*. Praha: Leges, 2020.
- [30] ROSATI, Eleonora. No step-free copyright exceptions: The role of the three-step in defining permitted uses of protected content (including TDM for AI-training purposes). *University Faculty of Law Legal Studies Research Paper Series*, 2023.
- [31] Rozsudek LG München I ze dne 11. listopadu 2025, No. 42 O 14139/24 (GEMA v OpenAI). [/iapp.org/news/a/do-llms-store-personal-data-this-is-asking-the-wrong-question?utm_source=chatgpt.com](https://iapp.org/news/a/do-llms-store-personal-data-this-is-asking-the-wrong-question?utm_source=chatgpt.com) Dostupné z: <https://www.gesetze-bayern.de/Content/Document/Y-300-Z-GRURRS-B-2025-N-30204>
- [32] SENFTLEBEN, Martin. Win-win: How to Remove Copyright Obstacles to AI Training While Ensuring Author Remuneration (and Why the European AI Act Fails to Do the Magic). [online] 2024 [cit. 15. 07. 2025]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4964460
- [33] Směrnice Evropského parlamentu a Rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru.
- [34] SMITH, Victoria. et al. Identifying and Mitigating Privacy Risks Stemming from Language Models: A Survey. 2024, s. 3 DOI: 10.48550/arXiv.2310.01424
- [35] SZKALEJ, Kacper; SENFTLEBEN, Martin. Generative AI and Creative Commons Licences: The Application of Share Alike Obligations to Trained Models, Curated Datasets and AI Output. *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2024, roč. 15, č. 3.
- [36] TYAGI, Kalpana. Copyright, text & data mining and the innovation dimension of generative AI. *Journal of Intellectual Property Law & Practice*, 2024.
- [37] WEI, Jiaheng et al., Memorization in Deep Learning: A Survey. [online] 2025 [cit. 15. 03. 2025]. Dostupné z: <https://dl.acm.org/doi/10.1145/3769076>
- [38] ZHANG, Andy K.; KLYMAN, Kevin; MAI, Yifan; LEVINE, Yoav; ZHANG, Yian; BOMMA-SANI, Rishi; LIANG, Percy. Language model developers should report train-test overlap. [online] 2024 [cit. 10. 08. 2025]. Dostupné z: <https://arxiv.org/abs/2410.08385>(<https://arxiv.org/abs/2410.08385>)

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/RPT2026-1-2>

JAK SPRAVEDLIVĚ REGULOVAT ALGORITMICKOU MODERACI? VYVAŽOVÁNÍ PROJEVU UŽIVATELŮ A PLATFORMY V ROZHODOVACÍ PRAXI OVERSIGHT BOARD¹

JAN MARTÍNEK²

ABSTRAKT

Internetové platformy poskytují prostor ohromnému množství uživatelů, jejich regulace státem je ale poměrně problematická. Článek 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 platforem, včetně vztahu mezi regulací a cenzurou. Zvláštní část se věnuje moderaci na platformách Mety, včetně podrobnější analýzy regulace nenávislného projevu a souvisejících rozhodnutí odvolacího orgánu Oversight Board.

KLÍČOVÁ SLOVA

Svoboda projevu; soukromá cenzura; moderace obsahu; internet; sociální sítě; nařízení o digitálních službách; Oversight Board

¹ Tento článek vznikl na základě diplomové práce autora na téma *Algoritmická moderace internetových platforem*, která byla obhájena v roce 2025 na Právnické fakultě Masarykovy univerzity. Článek z této diplomové práce obsahově vychází.

² Mgr. Jan Martínek je doktorandem Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontaktní email: 508778@muni.cz; ORCID: 0009-0008-3151-2259.

ABSTRACT

Internet platforms provide space for a huge number of users, but their regulation by the state is quite problematic. The article 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 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.

KEY WORDS

Freedom of Expression; Private Censorship; Content Moderation; Internet; Social Media; Digital Services Act; Oversight Board

1. ÚVOD

Mladí lidé tráví na svých telefonech v průměru až čtyři hodiny denně. Většinu času zabírají sociální sítě.³ Je to logické, trend používání těchto platform je na vzestupu a platformy samotné se snaží udržet pozornost uživatelů po co nejdelší dobu- Zvládnou jim tak zobrazit co největší množství reklam, ze kterých jim plyne zisk.⁴

Klíč k ekonomickému úspěchu těchto společností vězí v profilování uživatelů a následném moderování obsahu. Platformy shromažďují obrovské množství dat o jednotlivých uživateli, kterým následně zvládnou přizpůsobit obsah na míru tak, aby jejich pozornost udržely po co nejdelší dobu. Čím více uživatelů (a jejich dat) platforma má, tím přesnější výsledky

³ Viz BLAHOŠOVÁ, Jana, LEBEDÍKOVÁ, Michaela, TANCOS, Martin, PLHÁK, Jaromír, ŠMAHEL, David, ELAVSKY, Steriani, TKACZYK, Michal, SOTOLÁŘ, Ondřej. *Jak čeští adolescenti používají své mobily? Analýza dat z chytrých telefonů* [online]. Brno: Masarykova univerzita, 2023 [cit. 19. 2. 2025]. https://irtis.muni.cz/media/3524142/wp4_report-jak-cesti-adolescenti-pouzivaji-sve-mobily.pdf

⁴ Tento model známý také jako „attention economy“ popisuje např. KIM, Ah Sang. Social Media Algorithms: Why You See What You See. *Georgetown Law Technology Review*. 2017, roč. 1, č. 2, s. 147-149.

může poskytovat (tzv. *network effect*).⁵ Tím se stává pro inzerenty atraktivnější a může dosáhnout lepšího postavení na trhu.⁶

Platformy sledují jak aktivní, tak pasivní chování uživatelů (např. přeskakování určitého typu obsahu) a tato data dále vyhodnocují.⁷ Profilovací algoritmy stojí za komerčním úspěchem platform, proto si je platformy střeží jako obchodní tajemství. Z pohledu uživatele se jedná o neprůhledné algoritmy (*opaque*),⁸ nejsou totiž k dispozici k nahlédnutí a případné analýze jejich fungování. Jistý vhléd umožňují analýzy některých patentů.⁹ Z těch vyplývá mimořádná schopnost vytvořit ze zdánlivě nesouvisejících dat ucelený obraz o chování uživatele. Platforma může cílit na uživatele podle reakcí na události nebo podle vyhledávání či využívat GPS lokaci ke stanovení jejich denní rutiny.¹⁰

Na profilaci úzce navazuje moderace obsahu. Jejím prostřednictvím platforma vybírá, jaký konkrétní obsah danému uživateli zobrazí. Budoucnost moderace stojí na algoritmech schopných učit se, tedy na umělé inteligenci. Oproti fyzickým moderátorům jsou totiž mnohem rychlejší a levnější. Na druhou stranu často blokují neopodstatněně. Nezohledňují např. výjimky pro satiru nebo uměleckou tvůrčí činnost, protože nemusí být schopny je rozpoznat.¹¹ Algoritmy také mohou poškozovat menšiny,¹² často totiž dostatečně nezvládají porovnávat kontext daného obsahu nebo

⁵ Viz MCINTOSH, Daniel. We Need to Talk about Data: How Digital Monopolies Arise and Why They Have Power and Influence. *Journal of Technology Law & Policy*. 2019, roč. 23, č. 2, s. 191-195.

⁶ V této souvislosti se mluví o „datových monopolech“. K problematice blíže viz MCINTOSH. *We Need to Talk about Data: How Digital Monopolies Arise and Why They Have Power and Influence*.

⁷ Viz AMARIKWA, Melany. Social Media Platforms' Reckoning: The Harmful Impact of TikTok's Algorithm on People of Color. *Richmond Journal of Law & Technology*. 2023, roč. 29, č. 3, s. 76.

⁸ Viz AMARIKWA. *Social Media Platforms' Reckoning: The Harmful Impact of TikTok's Algorithm on People of Color*, s. 123.

⁹ Viz POLČÁK, Radim. Zákaz cenzury jako zásah do svobody podnikání a svobody projevu internetových platform. In: Šimíček, Vojtěch. (ed.). *Právo svobodně podnikat*. Praha: Leges, 2023, s. 98-99.

¹⁰ Viz JOLER, Vladan, PETROVSKI, Andrej. Human Data Banks and Algorithmic Labour [online]. *labs.rs*, 20. 8. 2016 [cit. 19. 2. 2025]. <https://labs.rs/en/facebook-algorithmic-factory-human-data-banks-and-algorithmic-labour/>

postavení autora, jako v případě “ochrany” queer osob před šikanou na Tik-Toku.¹³ Algoritmická moderace přináší i další rizika spojená s amplifikací agresivního či nenávistného obsahu. Uživatelé mají totiž daleko větší tendenci reagovat na extrémní názory, které následně algoritmy vyhodnotí jako zajímavé a šíří je mezi další uživatele.¹⁴

Základní otázkou textu je, zda a jak lze moderaci obsahu na internetových platformách regulovat. Jde o složitý problém, kdy státy (veřejná moc) musí zároveň vyvažovat ochranu svobodného projevu uživatelů i platforem samotných. Většina velkých platforem navíc vznikla v americkém právním prostředí, které garantuje projevu daleko širší rozsah. Svůj komerční model založily na tomto pojetí, a proto se evropským požadavkům přizpůsobují spíše neochotně. Ačkoli můžeme tvrdit, že pokud chtějí platformy podnikat v Evropě, musí se přizpůsobit místnímu systému, je podstatné pochopit důvody, proč k této situaci vůbec došlo. Z tohoto právního systému vychází také přezkumný orgán Oversight Board, s jehož rozhodnutími budu dále pracovat. Proto do textu zahrnuji též přehled vývoje pojetí svobodného projevu platforem ve Spojených státech. Cílem textu je ukázat problémy vzájemného vztahu uživatele, platformy a státu v oblasti moderace obsahu a demonstrovat je na konkrétní analýze fungování částečně autonomního přezkumného orgánu Oversight Board. Závěrem podávám návrhy, jak jeho zkušenosti využít v nově vznikajícím evropském systému, např. v rozhodovací praxi orgánů pro mimosoudní řešení sporů.

2. LZE PLATFORMY REGULOVAT?

Internetové platformy disponují velkou škálou nástrojů, které mohou být pro demokratickou společnost rizikové. S jejich pomocí lze ovlivňovat

¹¹ Viz DUTKIEWICZ, Lidia. Artificial Intelligence and Media. In: *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*. Cambridge: Cambridge University Press, 2025, s. 294.

¹² Viz AMARIKWA. *Social Media Platforms' Reckoning: The Harmful Impact of TikTok's Algorithm on People of Color*, s. 73.

¹³ Tamtéž, s. 131.

¹⁴ K tomu blíže např. RATHJE, Steve. et al. People Think That Social Media Platforms Do (but Should Not) Amplify Divisive Content. *Perspectives on Psychological Science*. 2024, roč. 19, č. 5, s. 781-795.

chování uživatelů, potažmo veřejné mínění.¹⁵ Objevuje se tedy logická snaha států je nějakým způsobem regulovat. Na druhou stranu jsou i platformy soukromým subjektem, kterému stát garantuje svobodný projev. Dochází proto k paradoxní situaci: uživatelé upozorňují, že moderace (zejména mazání příspěvků) omezuje jejich svobodu projevu; naproti tomu platformy ji chápou jako vlastní svobodný projev, do kterého by jim stát neměl zasahovat. Při nástupu nové Trumpovy administrativy v USA v lednu 2025 začaly oba názory ještě více rezonovat, např. díky prohlášení CEO Mety Marka Zuckerberga o „zrušení cenzury“ na svých sítích právě s odkazem na svobodu projevu.¹⁶

Situace je pro platformy také podstatně odlišná na dvou velkých západních trzích, tedy v USA a v EU. Většina velkých platform z USA pochází a jejich komerční model stojí právě na široké svobodě projevu, která jim umožňuje rozsáhlou moderaci obsahu. Pokud chceme pochopit důvody, proč přistupují platformy k evropským pravidlům spíše neochotně, je potřeba krátce představit právě prostředí, ze kterého vzešly.

V USA zastává svoboda projevu výsostnou pozici. Doktrína ji chápe jako tzv. preferovanou svobodu, která je nezbytná k fungování demokratického systému vůbec.¹⁷ Její vnímání je založeno na představě „svobodného trhu myšlenek“, ze kterých má každý možnost utvořit si vlastní názor. Jediným kritériem pro potírání svobody projevu by měla být skutečnost, zda „byl projev učiněn za takových okolností a je takové povahy, že by mohl způsobit zjevné a bezprostřední nebezpečí“ (Schenck v. U. S. z roku 1919).¹⁸ Evropské (resp. české) pojetí naopak ovlivnil koncept bránící se demokracie. Ten rea-

¹⁵ Jako k tomu došlo např. u rumunských prezidentských voleb v roce 2024. K tomu více SOLEA, Anda Iulia. How a little-known far-right candidate manipulated TikTok to rise to the top in the Romanian election [online]. *University of Portsmouth*, 29. 11. 2024 [cit. 19. 2. 2025]. <https://www.port.ac.uk/news-events-and-blogs/blogs/academic-expertise/how-a-little-known-far-right-candidate-manipulated-tiktok-to-rise-to-the-top-in-the-romanian-election>

¹⁶ Viz BOOTH, Robert. Meta to get rid of factcheckers and recommend more political content [online]. *The Guardian*, 7. 1. 2024 [cit. 19. 2. 2025]. <https://www.theguardian.com/technology/2025/jan/07/meta-facebook-instagram-threads-mark-zuckerberg-remove-fact-checkers-recommend-political-content>

¹⁷ Viz VLČKOVÁ, Veronika. Svoboda projevu v USA. *Právník*. 2004, roč. 143, č. 3, s. 267.

¹⁸ Tamtéž, s. 265.

guje na zneužívání demokratických svobod totalitními režimy 20. století a stanovuje možnost některá základní práva omezit z důvodu ochrany demokratického zřízení.¹⁹ Svobodu projevu lze omezit pouze zákonem, z nezbytných důvodů²⁰ a za účelem dosažení legitimního cíle.²¹ Jedná se „pouze“ o jednu ze složek lidské důstojnosti,²² podléhá tedy poměrování s dalšími právy a nemá oproti nim žádné výsadní postavení.

Ochrana svobodného projevu se vztahuje také na právnické osoby a komerční projev, což dovodil ESLP skrze označení oprávněného subjektu jako „každého“.²³ Stát tedy musí chránit také projev internetové platformy. A to i v případě, že jde „jen o zisk“²⁴ a nevyjadřuje žádný konkrétní světonázor, jako to dělají např. veganská fóra nebo blogy politických stran. V kontextu využívání platformy proto nemůžeme zapomínat kromě projevu uživatele také na projev platformy jako takové. Platformy využívají různé prostředky, kterými vybírají obsah pro konkrétního uživatele, nebo obsah jinak modelují.

V takových případech se nabízí analogie s výběrem článků v tištěných médiích, tzv. *editorial choice*. Tato paralela ale úplně neodpovídá realitě, s ohledem na podstatné rozdíly obou typů subjektů. V souladu se svým posláním „hlídacího psa demokracie“ mají média jinou míru odpovědnosti než běžná osoba. V Evropě je vždy potřeba poměřovat střet s dalšími dotčenými právy, přesto mají média velkou míru volnosti. ESLP judikoval např. možnost odvysílání rozhovoru, ve kterém se host kladně vyjadřuje o (zakázaném) užívání marihuany²⁵ nebo publikace článků obsahujících infor-

¹⁹ Viz VÝBORNÝ, Štěpán. Koncept bránící se demokracie v judikatuře Ústavního soudu ČR. *Časopis pro právní vědu a praxi*. 2012, roč. 20, č. 2, s. 157.

²⁰ Dle čl. 17 odst. 4 Listiny základních práv a svobod.

²¹ Viz nálezn Ústavního soudu ze dne 8. 2. 2000, sp. zn. I. ÚS 156/99.

²² Viz HART, Jan. Svoboda projevu v USA a v Evropě. *Právní rozhledy*. 2002, roč. 10, č. 1, s. 30.

²³ Viz *Cascado Coca proti Španělsku*, rozhodnutí Evropského soudu pro lidská práva ze dne 24. 2. 1994 č. stížnosti 15450/89.

²⁴ Viz POLČÁK. *Zákaz cenzury jako zásah do svobody podnikání a svobody projevu internetových platform*, s. 98-99.

²⁵ Viz *Ringier Axel Spiegel proti Slovensku*, rozhodnutí Evropského soudu pro lidská práva ze dne 23. 9. 2021, č. stížnosti 26826/16.

mace o drastických praktikách lovců tuleňů ve střetu s jejich právem na ochranu osobnosti.²⁶ Míra odpovědnosti však zdaleka nedosahuje odpovědnosti provozovatele tzv. pasivního hostingu, médiím nenáleží tak široký bezpečný přístav, jsou v podstatě zavázána vždy, pokud se jim nepodaří liberovat.

Z pohledu platformy je velmi výhodná pozice, kdy na jednu stranu disponuje širokou svobodou projevu (jako tradiční média s právem na editorial choice), ale zároveň za obsah neodpovídá a snaží se přenést maximum odpovědnosti na uživatele. Platformy argumentují tím, že jen poskytují prostor obsahu, který však aktivně nespravují. Již několikrát jsme ale byli svědky toho, že zasahovaly do postupů automatické moderace za účelem zviditelnění některého typu obsahu. Např. u žebříčku nejpobulárnějších příspěvků (tzv. TrendingTopics), které zaměstnanci Facebooku aktivně vybírali, ačkoli měly být generovány na základě objektivních kritérií (jako je počet reakcí),²⁷ nebo v případě sestavování feedu a upřednostňování příspěvků vybraných uživatelů (např. Elona Muska po jeho převzetí Twitteru, později přejmenovaného na X).²⁸

Obyvatelé ČR stále více čtou internetové mutace klasických novin (informace o veřejném dění zde čerpá až 65 % obyvatel), sociální sítě jsou rovněž na vzestupu (z těch vychází až 35 % populace).²⁹ Zákony jsou ale stavěny a přizpůsobeny pro regulaci „starých médií“, které stát může kontrolovat pomocí registračního nebo licenčního principu,³⁰ příp. klást nároky na skladbu vysílaných pořadů.³¹ Kvůli požadavku na restriktivní výklad

²⁶ Viz *Bladet Tromsø a Stensaas proti Norsku*, rozhodnutí Evropského soudu pro lidská práva ze dne 20. 5. 1999, č. stížnosti 21980/93.

²⁷ Viz KOLTAY, András. The Private Censorship of Internet Gatekeepers. *University of Louisville Law Review*. 2021, roč. 59, č. 255, s. 298.

²⁸ Viz KARI, Paul. Elon Musk reportedly forced Twitter algorithm to boost his tweets after Super Bowl flop [online]. *The Guardian*, 15. 2. 2023 [cit. 19. 2. 2025]. <https://www.theguardian.com/technology/2023/feb/15/elon-musk-changes-twitter-algorithm-super-bowl-slump-report>

²⁹ Viz NMS Market Research. *Kde si Češi hledají informace? Vedou internetová média. Sociální sítě využívá třetina lidí v Česku* [online]. Tisková zpráva ze dne 5. 11. 2024 [cit. 19. 2. 2025]. <https://nms.global/cz/kde-si-cesi-hledaji-informace-vedou-internetova-media-socialni-site-vyuziva-tretina-lidi-v-cesku/>

však tyto možnosti nejdou automaticky rozšířit i na internetová média.³² Stát jim sice může vytvořit speciální režim,³³ s ohledem na jejich potenciální větší dosah a vyšší riziko zásahu do práv dalších osob, musí ho však dostatečně odůvodnit a upravit zákonem.³⁴

V USA je součástí svobody projevu také právo něco vynechat nebo neuvést.³⁵ Proto neobstála povinnost novin zveřejnit odpověď politických kandidátů na článek, který o nich otiskly.³⁶ Soudy také rozhodly, že noviny mají právo některé skvěle prodávané knihy z komerčních důvodů vynechat ze seznamu bestsellerů.³⁷ V USA jde o vyjádření subjektivního názoru platformy,³⁸ která se tedy může sama rozhodnout, co uživatelům ukáže.³⁹ Tato složka se silně projevuje u internetových vyhledávačů a v Evropě se dostává do střetu se zneužitím dominantního postavení. Stejně jako u všech vyhledávačů se uživatel po zadání dotazu zobrazí velká škála výsledků, každý vyhledávač pak pomocí algoritmů stanovuje jejich pořadí. V případě Go-

³⁰ Oba principy jsou upravuje zákon č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání a o změně dalších zákonů, v aktuálním znění. Spočívají v kontrole nad vysíláním, kterou provádí Rada pro rozhlasové a televizní vysílání. Licence (§ 12 an.) slouží pro nová vysílání, registrace (§ 27 an.) pro převzatá vysílání. Blíže viz CHALOUPKOVÁ, Helena, HOLÝ, Petr, URBÁNEK, Jiří. *Mediální právo*. Praha: C. H. Beck, 2018, s. 92-96 a 118-119.

³¹ Viz BARTOŇ, Michal. *Svoboda projevu a její meze v právu ČR*. Praha: Linde, 2002, s. 40-42.

³² Viz *Times Newspapers Ltd proti Spojenému království*, rozhodnutí Evropského soudu pro lidská práva ze dne 10. 3. 2009, č. stížností 3002/03 a 23676/03.

³³ Viz *Pravoye Delo a Shtekel proti Ukrajině*, rozhodnutí Evropského soudu pro lidská práva ze dne 5. 5. 2011, č. stížnosti 33014/05.

³⁴ Viz TYMOFEYEVA, Alla. Svoboda projevu právnických osob na internetu z pohledu Evropského soudu pro lidská práva. *Právník*. 2022, roč. 161, č. 2, s. 140-155.

³⁵ Viz VOLOKH, Eugene, FALK, Donald M. Google First Amendment for Search Engine Search Results. *Journal of Law, Economics & Policy*. 2012, roč. 8, č. 4, s. 883-899. <https://www2.law.ucla.edu/Volokh/searchengine.pdf>

³⁶ Viz *Miami Herald Publishing Co. v. Tornillo*, rozsudek Nejvyššího soudu USA ze dne 25. 6. 1974, č. 73-797. USA.

³⁷ Viz *Blatty v. New York Times Co.*, rozhodnutí Nejvyššího soudu státu Kalifornie ze dne 29. 12. 1986. USA.

³⁸ Viz *Search King, Inc. v. Google Technology, Inc.*, rozhodnutí Obvodního soudu pro Západní obvod Oklahomy ze dne 27. 5. 2003, č. CIV-02-1457-M. USA.

³⁹ Viz *Langdon v. Google, Inc.*, rozhodnutí Obvodního soudu pro Delaware ze dne 20. 2. 2007, č. 06-319-JJF. USA.

ogle Search (Shopping)⁴⁰ upřednostnil vyhledávač v pořadí výsledků vlastní službu nad jinými. Evropská komise shledala porušení zákazu zneužití dominantního postavení a vyměřila rekordní pokutu ve výši 2,42 mil. EUR.⁴¹

Platformy proto v našem prostředí regulovat lze. Stát má pozitivní závazek chránit práva uživatelů a demokratické procesy, k čemuž je regulace platform vhodným nástrojem. Analogická pravidla pro „stará média“ nepočítala s tak ohromným množstvím obsahu a „neprůhlednými“ moderačními procesy, nová regulace je tak nezbytná. Zpravidla však bude narážet na ústavní limity svobodného projevu nebo svobodného podnikání samotných platform, které jsou soukromými subjekty. Státy musí tento střet vyvažovat. Je totiž rozdíl, pokud přímo vyžaduje blokaci konkrétního obsahu nebo pouze stanoví obecná pravidla, která už platformy samy promítnou do svých smluvních podmínek. O takové vyvažování se státy snaží při tvorbě regulace, jak ukazuje následující kapitola.

3. PRÁVNÍ RÁMEC PRO REGULACI PLATFORM

Internetové platformy disponují velkou škálou nástrojů, kterými mohou ovlivňovat chování uživatelů, potažmo veřejné mínění. Stojí tak v postavení *definiční autority*: přestože nejsou subjektem nadaným veřejnou mocí, mohou na základě své vůle ovlivňovat fungování daného uměle vytvořeného prostředí a nastavovat v něm pravidla chování.⁴² Pokud chce stát splnit svůj pozitivní závazek ochrany lidských práv, tedy aktivně dohlížet na jejich dodržování a respektování, musí také aktivně vést diskusi se sociálními sítěmi a zavést systém, na základě kterého bude možné zaručit jejich dodržování.

3.1 ODPOVĚDNOST ZA PUBLIKOVANÝ OBSAH

V situaci, kdy uživatel na platformě uveřejní závadný obsah (např. video porušující autorská práva), smí oprávněný subjekt (tedy autor) logicky žá-

⁴⁰ Viz *Google Search (Shopping)*, rozhodnutí Evropské komise ze dne 27. 6. 2017, sp. zn. 39740.

⁴¹ Viz bod 754 rozhodnutí Evropské komise ze dne 27. 6. 2017, sp. zn. 39740.

⁴² Viz POLČÁK, Radim. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018, s. 12.

dat jeho odstranění. Otázkou však je, do jaké míry za nahrání odpovídá platforma, která umožnila přístup širší skupině svých uživatelů, a do jaké míry samotný uživatel, který na ni daný obsah neoprávněně nahrál. Obecně má platforma zakročovací a prevenční povinnost dle §§ 2900 a 2901 o. z.,⁴³ avšak její důsledné uplatňování by platformy nutilo k detailní kontrole a v podstatě by je vyřadilo z provozu. SDEU⁴⁵ navíc takový přístup vyhodnotil jako zásah do svobody podnikání.⁴⁶ Evropský zákonodárce proto zvolil cestu snížené odpovědnosti platform, která však zaručí možnost efektivně vymáhat práva poškozených. Ti se nemusí domáhat odstranění obsahu složitě po konkrétních uživateli, nýbrž přímo po platformě. Nejedná se o nový model, podobné názory se objevily již v 70. letech v judikatuře Nejvyššího soudu USA.⁴⁷

Odpovědnost je založena na dvou podmínkách - (1) porušení povinnosti dané platformy (jako je právě zakročovací a prevenční povinnost) a (2) prolomení institutu bezpečného přístavu.⁴⁸ V rámci bezpečného přístavu nemá platforma povinnost aktivně vyhledávat závadný obsah, ale na upozornění ho musí odstranit (systém *notice and take-down*),⁴⁹ resp. zabránit jeho opětovnému zveřejnění (*stay down*).⁵⁰ Právo tedy předpokládá, že platforma o závadném obsahu neví, dokud jí o něm někdo “neřekne”. Z toho důvodu musí zřídit mechanismy pro nahlašování.⁵¹ O bezpečný přístav rovněž při-

⁴³ Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

⁴⁴ Viz HUSOVEC, Martin. *Zodpovednosť na internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014, s. 77-78.

⁴⁵ Soudní dvůr Evropské unie.

⁴⁶ Viz *SABAM proti Netlog NV*, rozsudek Soudního dvora EU ze dne 16. 2. 2012 ve věci C-360/10.

⁴⁷ Srov. s kauzou *Betamax, Sony Corp. of America v. Universal City Studios, Inc.*, rozhodnutí Nejvyššího soudu USA ze dne 17. 1. 1984, č. 81-1687. USA. Blíže viz POLČÁK. *Právo informačních technologií*, s. 69.

⁴⁸ Viz MYŠKA, Matěj, KOUKAL, Pavel, VLACHOVÁ, Zuzana, WOZNICA, Ondřej. *Liability of Hosting ISPs: the Czech Perspective*. In: Szostek, Dariusz, Załucki, Mariusz. (eds). *Internet and New Technologies Law*. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 2021, s. 400.

⁴⁹ Viz čl. 8 nařízení o digitálních službách (DSA). Čl. 7 navíc upravuje možnost dobrovolného vyšetřování z vlastního podnětu ze strany platformy, aniž by při tom byla automaticky zbavena bezpečného přístavu.

chází, pokud s obsahem aktivně pracuje.⁵² Další požadavky pak stanovuje judikatura vrcholných evropských soudů, roli pro stanovení odpovědnosti hrají především kontext dané situace, možnost odpovědnosti samotných uživatelů, opatření přijatá platformou a přiměřenost sankce ze strany státu.⁵³

Americkou obdobou evropského systému je tzv. princip dobrého samaritána. Ten platformám zajišťuje velmi široké pole působnosti, platformy odpovídají jen za nelegální obsah, k němuž „přispěly“.⁵⁴ Pokud jednají v dobré víře, neodpovídají ani za protiprávní obsah, o jehož existenci věděly. Tomu odpovídá poměrně bohatá judikatura i v extrémních případech jako je podněcování teroristických útoků⁵⁵ nebo poskytování sexuálních služeb nezletilými.^{56 57} Princip dobrého samaritána navíc zahrnuje také moderaci, jejíž ochrana je rovněž velmi široká a v podstatě neomezená, pokud se děje v dobré víře.⁵⁸

⁵⁰ Někteří autoři popisují systém notice and take-down jako zastaralý a představují další možnosti zakročení. Pro souhrnné označení těchto postupů se používá pojem notice and action. K tomu blíže např. HANYCH, Monika, PIVODA, Marek. Facebook, Twitter a YouTube jako garanti svobodného projevu? Kritika současného systému notice-and-takedown. *Revue pro právo a technologie*. 2017, roč. 8, č. 16.

⁵¹ Čl. 16 DSA.

⁵² Srov. *L'Oréal SA a další vs. eBay International AG*, rozsudek Soudního dvora EU ze dne 12. 7. 2011 ve věci C-324/09.

⁵³ *Viz Delfi AS proti Estonsku*, rozsudek Velkého senátu Evropského soudu pro lidská práva ze dne 16. 6. 2015, č. stížnosti 64569/09.

⁵⁴ *Viz BERBEC, Adriana. To What Extent Can Online Service Providers Adopt Voluntary Content Moderation Measures without Losing Their Immunity Shields? A Comparative Analysis of Online Service Providers' Liabilities in the European Union and the United States. Journal of Intellectual Property, Information Technology and Electronic Commerce Law*. 2024, č. 1, roč. 15, s. 23.

⁵⁵ Srov. *Force v. Facebook, Inc.*, rozhodnutí Obvodního soudu pro Druhý obvod ze dne 31. 7. 2019, č. 18-397. USA.

⁵⁶ *Viz Doe No 1 v. Backpage.com, LLC*, rozhodnutí Obvodního soudu pro První obvod ze dne 14. 3. 2016, č. 15-1724. USA.

⁵⁷ *Viz BERBEC. To What Extent Can Online Service Providers Adopt Voluntary Content Moderation Measures without Losing Their Immunity Shields? A Comparative Analysis of Online Service Providers' Liabilities in the European Union and the United States*, s. 29.

⁵⁸ *Viz McCABE, Brigid. A First Amendment Right to Censor: Social Media Regulation and Freedom of Speech in the NetChoice Cases. Columbia Undergraduate Law Review*. 2024, č. 3, roč. 20, s. 35.

3.2 REGULACE NEBO CENZURA?

Regulace obsahu, který mohou platformy sdílet, je však z pohledu státu dvojsečnou zbraní. Na jednu stranu musí stát zajistit dostatečnou svobodu projevu uživatelům a stanovit tak podmínky, za kterých mohou obsah publikovat. Na druhou stranu musí tuto svobodu zajistit také samotné platformě. Pokud by reguloval příliš, může se dostávat až k hranici cenzury, kterou Listina⁵⁹ specificky zakazuje (čl. 17 odst. 3).

Cenzurou je ve smyslu Listiny předběžný zásah státu (výkonné moci), jehož cílem je zabránit publikaci nežádoucího obsahu.⁶⁰ Vzhledem k historické zkušenosti s totalitními režimy je stát pod poměrně silným dozorem ze strany soudní moci a veřejnosti,⁶¹ ovšem není jediným subjektem schopným omezovat publikaci obsahu. V současné odborné literatuře se objevuje termín soukromé „cenzury“ (private censorship), kdy „cenzuru“ neprovádí stát ve vrchnostenském postavení, ale soukromý subjekt. Ten tak typicky činí z vlastní iniciativy, např. za účelem dosažení nějakého obchodního cíle nebo zaručení určitého názorového směřování platformy. Přestože důsledky pro běžného uživatele mohou být velmi podobné, nejde o cenzuru jako takovou (právě proto, že ji neprovádí stát), nýbrž o jakýsi její derivát. V textu ji proto uvádím v uvozovkách.

Na pomezí mezi klasickou cenzurou a soukromou „cenzurou“ pak stojí případy, kdy regulaci sice provádí soukromý subjekt, ale z vůle státu. Takové případy jsou vzhledem k pozitivnímu závazku státu garantovat svobodu projevu poměrně problematické. Stát se v tomto ohledu může uchýlit k tzv. podružné cenзуře nebo k zastřenému zavedení cenzury.

Podružná cenzura se podle Hanych a Pivody projevuje tak, že stát nastavuje pravidla pro cenzurování a následně vyžaduje jejich vykonávání po

⁵⁹ Listina základních práv a svobod. Usnesení č. 2/1993 Sb. Usnesení předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky, ve znění pozdějších předpisů.

⁶⁰ Viz WAGNEROVÁ, Eliška. Čl. 17 (Svobodný projev a právo na informace). In: Wagnerová, Eliška, Šimíček, Vojtěch, Langášek, Tomáš, Pospíšil, Ivo a kol. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer, 2012, s. 433-434.

⁶¹ Viz HANYCH, PIVODA. *Facebook, Twitter a YouTube jako garanti svobodného projevu? Kritika současného systému notice-and-takedown*, s. 183.

soukromém subjektu.⁶² Typicky se objevuje u autoritářských režimů, jako je současná Čína. Ta po západních společnostech, které mají zájem působit na jejím území, požaduje (ať už přímo nebo nepřímo) blokování některého typu obsahu. Své výsledky v citlivých otázkách, jako je nezávislost Tchaj-wanu nebo masakr na Náměstí nebeského klidu, upravovaly vyhledávače Google⁶³ a Yahoo!⁶⁴ Blokování informací lze vidět v reálném čase také u čínského AI chatbotu DeepSeek.⁶⁵

Zastřené zavedení cenzury pak podle Poppeové⁶⁶ spočívá v nepřijetí dostatečně jasných pravidel, která by tuto problematiku upravovala. Může jít o situaci, kdy stát nepřijme žádné opatření a dává tak soukromému subjektu v podstatě neomezené možnosti blokovat obsah, ale také o situaci, kdy jsou opatření příliš vágní a platforma tak z důvodu nejistoty nebo nepřímé hrozby blokuje obsah „pro jistotu“. K situaci stojící na hraně zastřené cenzury došlo v České republice při zablokování tzv. dezinformačních webů po vpádu Ruska na Ukrajinu v roce 2022. Weby zablokovala soukromá společnost CZ NIC na základě dopisu Ministerstva vnitra. Vrcholné soudy⁶⁷ však porušení práva na svobodu projevu opakovaně odmítly. Upozorňovaly na povahu dopisu, ve kterém ministerstvo pouze „žádalo“ bez jakékoli hrozby sankcí nebo vynucení blokáce.⁶⁸

Je otázkou, do jaké míry lze pod svobodu projevu podřadit „cenzuru“ z vlastní iniciativy provozovatele platformy. Platforma si může nastavit vlastní pravidla chování v rámci sociální sítě, která následně vymáhá

⁶² Tamtéž, s. 186.

⁶³ Viz KOLTAY. *The Private Censorship of Internet Gatekeepers*, s. 275.

⁶⁴ Blíže viz GOLDSMITH, Jack, WU, Tim. *Kdo řídí Internet? Iluze o světě bez hranic*. Praha: Dokořán, Argo, 2008, s. 23.

⁶⁵ Viz WANG, Vivian. How Does DeepSeek's A.I. Chatbot Navigate China's Censors? Awkwardly [online]. *The New York Times*. 19. 1. 2025 [cit. 19. 2. 2025]. <https://www.nytimes.com/2025/01/29/world/asia/deepseek-china-censorship.html>

⁶⁶ Viz POPPEOVÁ, Marie. Odpovědnost zprostředkovatelů za protiprávní projevy na internetu: Hrozí nám soukromá cenzura? *Časopis pro právní vědu a praxi*. 2023, č. 4, roč. 31, s. 870.

⁶⁷ Srov. Nejvyšší správní soud v rozsudcích č. j. 4 As 206/2022-108 a č. j. 5 As 230/2022-66 nebo Ústavní soud v usneseních sp. zn. Pl. ÚS 5/23 a sp. zn. III. ÚS 2628/23.

⁶⁸ K celé situaci blíže viz MIZEROVÁ, Tina, HARAŠTA, Jakub. Dostupnost mediálního obsahu: blokování dezinformačních webů. *Právník*. 2023, roč. 162, s. 415-430.

prostřednictvím moderace. Pravidla upravují podmínky užití, které musí uživatel odsouhlasit, aby mohl platformu vůbec používat. Platformy si přitom vyhrazují právo je kdykoliv jednostranně změnit. Jedná se o podmínky adhezního typu, tedy uživatel není schopen je jakkoli modifikovat a v podstatě nemá jinou možnost, než je v celkovém znění přijmout (nebo platformu opustit). Vyjednání některých výjimek se podařilo pouze státům (např. Německu),⁶⁹ jejichž vyjednávací pozice je logicky mnohem silnější než pozice běžného uživatele.

Jedná se o smluvní vztah, právo proto běžné uživatele chrání jako spotřebitele (což se netýká např. médií nebo jiných společností). Otázkou zůstává, zda smí sociální síť blokovat obsah nad rámec zákonných požadavků či nikoli, což ukazují např. odlišné závěry německých soudů.⁷⁰ Dalším problémem jsou samotné formulace smluvních podmínek. Ty jsou často velmi vágní, aby obsáhly co nejširší možnosti regulace. Do jisté míry tak záleží na „libovůli“ konkrétního moderátora, který obsah přezkoumává.⁷¹

Taková situace staví mezi projev platformy a uživatele propastný rozdíl. Platforma si teoreticky může stanovit libovolná pravidla. Pokud jsou dostatečně vágní, může jejich výklad přizpůsobit každé jedné situaci. Uživatel pak nemá možnost předvídat, zda konkrétní případ již pravidla porušuje, či se ještě drží v nastavených mantinelech. Takové nejistotě se snaží některé státní autority zabránit: zejm. nastavují pravidla pro moderaci, určují po-

⁶⁹ Viz HANYCH, PIVODA. *Facebook, Twitter a YouTube jako garanti svobodného projevu? Kritika současného systému notice-and-takedown*, s. 194.

⁷⁰ Jedná se o případy *Themel v. Facebook Ireland* a *User v. Facebook Ireland*. V prvním jmenovaném případě soud v Mnichově stanovil, že Facebook blokovat nad rámec nesmí a v druhém dovedl soud v Heidelbergu opak. Blíže viz Koltay. *The Private Censorship of Internet Gatekeepers*, s. 283-285.

⁷¹ Ke sjednocení jejich rozhodování by měly sloužit instrukce s konkrétními příklady porušení podmínek. Některé uniklé instruktážní dokumenty tehdejší společnosti Facebook analyzoval v roce 2018 list *The New York Times*. Poukázal na časté problémy s nejasným výkladem, zmatenými formulacemi a nesystémovými řešeními. Instrukce měly být obsaženy v několika prezentacích a tabulkách vytvořených různými týmy, které spolu příliš nesouvisely a komplexní problematiku nadměru zjednodušovaly. Dalším problémem pak byla také nedostatečná expertíza moderátorů, kteří neznali místní realie nebo nerozuměli jazyku. Blíže viz FISHER, Max. *Inside Facebook's Secret Rulebook for Global Political Speech* [online]. *The New York Times*, 27. 12. 2018 [cit. 19. 3. 2025]. <https://www.nytimes.com/2018/12/27/world/facebook-moderators.html>

vinnou míru transparentnosti nebo vytvářejí možnosti „odvolání“ proti smazání příspěvku.

Lze uzavřít, že blokování nad rámec zákonných požadavků může být projevem platformy jako soukromé osoby. Nelze však obecně stanovit, kdy je takový postup oprávněný. Přestože v judikatuře existují analogické situace,⁷² velké online platformy jsou poměrně unikátním fórem. Pokud uvažujeme o „kvazimonopolním“ postavení několika platform, nemusí pro zablokovaného uživatele existovat odpovídající možnost vyjádřit se jinde. V těchto případech je nutné pečlivě poměřovat mezi právy uživatele i platformy s ohledem na kontext dané situace, jinak stát nedostojí svému pozitivnímu závazku. V následující části ukazují, jak s tímto problémem zákonodárci pracují.

3.3 SNAHA REGULOVAT SOUKROMOU „CENZURU“

EU tyto problémy řeší prostřednictvím DSA,⁷³ které specifikuje práva a povinnosti jak uživatelů, tak platform. Smluvní podmínky musí předem obsahovat informace o veškerých možnostech omezení obsahu a využívaných nástrojích moderace.⁷⁴ Musí být napsány jasně, jednoznačně a uživatelsky uchopitelnou formou,⁷⁵ což je jasnou reakcí právě na praxi vágně formulovaných podmínek.

Při odstranění obsahu musí platforma vždy jeho původci poskytnout vysvětlení, proč k odstranění přistoupila⁷⁶ a v případě, že uživatel není spokojen s tímto odůvodněním, může navíc ve lhůtě 6 měsíců využít interního systému pro vyřizování stížností,⁷⁷ tedy jakéhosi „odvolání“ proti rozhodnutí o odstranění obsahu. Mimo to má možnost využít mimosoudní

⁷² V tomto kontextu lze zmínit závěry případu *Appleby*. ESLP zde dovedl projev vlastníka obchodního centra, který omezil sběr podpisů pod petici. Viz *Appleby proti Spojenému království*, rozhodnutí Evropského soudu pro lidská práva ze dne 6. 5. 2003 č. stížnosti 44306/98.

⁷³ Nařízení Evropského parlamentu a Rady (EU) 2022/2065 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách).

⁷⁴ Dle čl. 14 a 15 DSA.

⁷⁵ Dle čl. 14 odst. 1 DSA.

⁷⁶ Dle čl. 17 DSA.

⁷⁷ Dle čl. 20 DSA.

řešení sporů⁷⁸ u subjektu certifikovaného národním koordinátorem digitálních služeb.⁷⁹ Pravidla však nejsou nastavena pouze ve prospěch uživatele, DSA také stanovuje možnost obrany proti kverulantům: platforma může po předchozím upozornění pozastavit přístup uživateli, který by těchto postupů zjevně zneužíval.⁸⁰

Velmi velké online platformy (“VLOP”) mají také povinnost hodnotit⁸¹ a zmírňovat⁸² tzv. systémová rizika,⁸³ kam budou patřit právě rizika zautomatizovaných procesů kontroly obsahu. Na analýzu systémových rizik dohlíží Evropská komise a národní koordinátoři digitálních služeb, kteří mají možnost zahájit kontrolu a případně udělit sankce až do výše 6 % celosvětového ročního obrátu.⁸⁴ Takovou kontrolou prochází k 17. 2. 2026 26 platforem.⁸⁵ Ukázkovým příkladem je řízení s platformou X, které uložila Komise pokutu 120 mil. EUR mj. pro nedostatek transparentnosti a klamavý design v podobě „modré fajfky“.Vi⁸⁶ Podobně Komise postupuje i v dalších řízeních, např. u platformy Mety prověřuje algoritmické systémy z hlediska návykového designu a ochrany nezletilých osob.⁸⁷

V americkém prostředí se rovněž objevují snahy regulovat soukromou „cenzuru“ platform, zde však narážejí na výše popsané exkluzivní posta-

⁷⁸ Dle čl. 21 DSA.

⁷⁹ Tuto pravomoc ČTÚ do českého právního řádu provede právě projednávaný zákon o digitální ekonomice. (Sněmovní tisk 69/0).

⁸⁰ Dle čl. 23 DSA.

⁸¹ Dle čl. 34 DSA.

⁸² Dle čl. 35 DSA.

⁸³ Jde o dopad na lidská práva, volební procesy, ochranu veřejného zdraví nebo genderově podmíněné násilí a další (dle čl. 34 odst. 1 DSA).

⁸⁴ Dle čl. 52 DSA.

⁸⁵ Viz Supervision of the designated very large online platforms and search engines under DSA [online]. *European Commission* [cit. 24. 3. 2026]. <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>

⁸⁶ Viz Evropská komise. Commission fines X €120 million under the Digital Services Act [online]. Tisková zpráva ze dne 5. 12. 2025 [cit. 24. 3. 2026]. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934

⁸⁷ Viz Evropská komise. Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram Act [online]. Tisková zpráva ze dne 5. 12. 2025 [cit. 24. 3. 2026]. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664

vení svobody projevu. Ukázkou jsou zákony států Texas⁸⁸ a Florida,⁸⁹ které reagovaly na omezování projevů uživatelů po útoku na Kapitol v lednu 2021,⁹⁰ včetně zablokování profilu tehdy dosluhujícího prezidenta Trumpa.⁹¹ Tyto zákony se pokusily omezit možnosti platform moderovat obsah. Platformy měly např. vytvořit systém pro podávání stížností nebo povinně odůvodňovat svá moderační rozhodnutí. Platformy se proti oběma zákonům bránily soudně, právě s odkazem na svobodný projev.⁹² Ačkoliv Nejvyšší soud USA („SCOTUS“) v červenci 2024 vrátil spory nižším instancím k vypořádání námitek, z dosavadních vyjádření většiny soudců vyplývá, že zákony tohoto typu „zřejmě neobstojí“⁹³ a nespadají pod „omezenou autoritu státu.“⁹⁴

Jak u DSA, tak u obou amerických zákonů si lze všimnout určitých podobností. Jsou to zejm. požadavky na transparentnost smluvních podmínek a povinnost zavést systém pro „odvolání“ proti smazaným příspěvkům. Zatímco v EU bylo DSA obecně přijato a nebylo ani ústavněprávně zpochybňováno, americké zákony již prošly řízením před SCOTUS a očekává se, že neobstojí před Prvním dodatkem. To opět ukazuje důsledky jiného chápání rozsahu svobody projevu na obou kontinentech.

⁸⁸ Jedná se o zákon Texas' House Bill 20. USA.

⁸⁹ Jedná se o zákon Florida's Senate Bill 7072. USA.

⁹⁰ Viz McCABE, A *First Amendment Right to Censor: Social Media Regulation and Freedom of Speech in the NetChoice Cases*, s. 28.

⁹¹ Viz JONES, Zoe Christen. Facebook bans Trump for the rest of his presidency [online]. BBC. 7. 1. 2021 [cit. 19. 2. 2025]. <https://www.cbsnews.com/news/facebook-bans-trump-joe-biden-president-inauguration/>

⁹² Případy NetChoice v. Paxton a Moody v. NetChoice. Blíže viz McCabe, B. A First Amendment Right to Censor: Social Media Regulation and Freedom of Speech in the NetChoice Cases. *Columbia Undergraduate Law Review*. 2024, č. 3, roč. 20, s. 28-49.

⁹³ V originálním znění „unlikely to stand“ (překlad autora). DODSON, Samantha. Balancing Act: Navigating First Amendment Rights and Online Content Regulation [online]. *Juris Mentem Law Review*, 14. 11. 2024. https://aura.american.edu/articles/journal_contribution/Balancing_Act_Navigating_First_Amendment_Rights_and_Online_Content_Regulation/27738678?file=50496804

⁹⁴ V originálním znění „limited government authority“ (překlad autora). Viz Dodson, S. *Balancing Act: Navigating First Amendment Rights and Online Content Regulation*.

4. MODERACE NA PLATFORMÁCH METY

Meta je dominantní hráč na poli sociálních sítí. Vlastní jedny z nejpopulárnějších platform, jako je Facebook nebo Instagram. Moderace na těchto platformách proto více či méně ovlivňuje miliony uživatelů po celém světě. Meta používá kombinaci moderace pomocí algoritmů a lidských moderátorů. Konkrétní postup není nikde veřejně upraven, následující řádky proto vyplývají ze zobecněných rozhodnutí orgánu Oversight Board, který přezkoumává rozhodnutí moderátorů a moderačních algoritmů na platformách Mety.

Uživatelé sociální sítě mají možnost potenciálně závadný obsah nahlásit a vybrat, které ustanovení zásad komunity porušil. Algoritmy následně přispěvek buď samy automaticky přezkoumají a rozhodnou o jeho odstranění (příp. zachování), nebo předají rozhodnutí lidským moderátorům (jedná se o zlomek případů). Algoritmy porovnávají zejm. závažnost dopadu případu na širší uživatelskou základnu nebo možnost způsobit „offline“ újmu (tedy újmu v reálném světě) a podle toho přezkum upřednostňují.⁹⁵ „Méně závažné“ případy pak často automaticky uzavírají, aniž by je fakticky přezkoumaly.⁹⁶ Konkrétní podoba algoritmů však není známá, stejně jako u profilování se jedná do jisté míry o neprůhledný algoritmus, u něhož uživatelé nemají možnost zjistit, jak konkrétně funguje.

Uživatel, který není s výsledkem kontroly spokojen, může podat odvolání. V tom případě se celý proces opakuje, a pokud dojde nový kontrolor k opačnému závěru, předá případ třetímu moderátorovi, který obě rozhodnutí zohlední a rozhodne finálně.⁹⁷ Ač by se tento proces mohl zdát do jisté míry podobný např. správnímu procesu, není v případě Mety vytvoře-

⁹⁵ Viz Meta. Zásady komunity: Jak technologie pomáhá upřednostňovat případy ke kontrole. *Meta* [cit. 19. 2. 2025]. <https://transparency.meta.com/cs-cz/enforcement/detecting-violations/technology-helps-prioritize-review/>

⁹⁶ Srov. situaci popsanou v rozhodnutí v dále analyzovaném rozhodnutí *Politician's Comments on Demographic Changes*. Standard Decision Oversight Board ze dne 12. 3. 2024. Plné znění dostupné na <https://www.oversightboard.com/decision/fb-ofs963dz/> [cit. 19. 2. 2025].

⁹⁷ Viz Meta. Zásady komunity: Obsah, u kterého bylo podáno odvolání. *Meta* [cit. 19. 2. 2025]. <https://transparency.meta.com/cs-cz/policies/improving/appealed-content-metric/>

na žádná skupina „odvolacích moderátorů“, kteří by fungovali jako odvolací orgán a disponovali vyšší odborností. To také kritizovala Oversight Board v rozhodnutí *Post in Polish Targeting Trans People*.⁹⁸

Moderace je založena na smluvních podmínkách,⁹⁹ které uživatel odsouhlasí při registraci na sociální síť. Nároky na obsah publikovaných příspěvků pak upravují zásady komunity. Jak popíšu níže, tyto zásady nejsou přesně formulovány, jejich význam proto dotváří rozhodnutí Oversight Board. V následující kapitole tento orgán nejprve charakterizuji, následně přiblížím právní základ jeho rozhodování (včetně relevantních zásad komunity) a nakonec představím vybraná rozhodnutí, která ovlivnila zásady upravující nenávistné chování.

4.1 CHARAKTERISTIKA OVERSIGHT BOARD

Vznik Oversight Board („OB“),¹⁰⁰ iniciovala Meta s vizí, že půjde o její „Nejvyšší soud“.¹⁰¹ V některých ohledech orgán vizi naplnil, v některých ne: nedosáhl např. plné autonomie na Metě. OB je částečně autonomní orgán, který finálně rozhoduje spory ohledně moderace na sociálních sítích Facebook, Instagram¹⁰² a od roku 2023 také Threads.¹⁰³ Jeho jurisdikce je poměrně omezená. Může rozhodovat pouze na základě stížnosti uživatele nebo Mety, nikoli třetí strany. To může být problematické např. v případech ochrany

⁹⁸ Viz *Post in Polish Targeting Trans People*. Standard Decision Oversight Board ze dne 16. 1. 2024. Plné znění dostupné na <https://www.oversightboard.com/decision/fb-uk2rus24/> [cit. 19. 2. 2025].

⁹⁹ Verze pro Facebook je dostupná zde: <https://www.facebook.com/legal/terms/update> [cit. 19. 2. 2025].

¹⁰⁰ V české verzi zásad komunity Meta používá označení „dozorčí rada“. Tento výraz však považuji za zmatečný, protože neodpovídá legální definici pojmu „dozorčí rada“, se kterou pracuje zákon č. 90/2012 Sb., o obchodních korporacích. Dále proto budu používat anglické označení „Oversight Board“.

¹⁰¹ Viz HELFER, Laurence R., LAND, Molly K. The Meta Oversight Board's Human Rights Future. *Cardozo Law Review*. 2023, č. 6, roč. 44, s. 2236.

¹⁰² Viz MAZÚR, Jan, GRAMBLIČKOVÁ, Barbora. New Regulatory Force of Cyberspace: The Case of Meta's Oversight Board. *Masaryk University Journal of Law and Technology*. 2023, č. 1, roč. 17, s. 6.

¹⁰³ Viz Oversight Board. 2023 Annual Report [online]. *Oversight Board* [cit. 19. 2. 2025]. <https://www.oversightboard.com/wp-content/uploads/2024/06/Oversight-Board-2023-Annual-Report.pdf>

osobnosti. OB rozhoduje v podstatě pouze o obsahu ve feedu. Jurisdikce se nevztahuje na další služby jako zprávy, marketplace nebo dating.¹⁰⁴ OB navíc rozhoduje pouze o tom, zda má Meta daný obsah ponechat na sociální síti, nebo ho má odstranit.¹⁰⁵ Případně může dávat Metě doporučení pro další praxi.

Svou činnost orgán zahájil v roce 2020¹⁰⁶ a skládá se ze dvou právních subjektů – trustu a LLC,¹⁰⁷ obou zřízených podle Delawarského práva.¹⁰⁸ Trust je stálý a jeho hlavní funkcí je dohlížet na LLC a spravovat finance. Naproti tomu LLC vykonává běžnou administrativu a provádí právě rozhodovací činnost. Vztah obou subjektů (i vzhledem ke společnosti Meta) definuje základní dokument „Charter“, který upravuje také základy fungování orgánu¹⁰⁹ a díky obtížným postupům ke změně dokumentu slouží jako jakási „ústava“ OB.

OB není striktně vzato nezávislým soudem, protože zřizující společnost Meta má stále velký vliv na jeho fungování. Jednak je OB závislá na jejím financování, jednak má Meta nezanedbatelný vliv na ustanovení jejích členů.¹¹⁰ Některé tyto problémy se Meta snažila při zřízení alespoň částečně překonat, např. investovala do trustu finance pro šest let fungování OB nebo dala současným členům OB a veřejnosti možnost podílet se na ustanovení nových členů (celý proces je ale poměrně nejasně formulovaný).¹¹¹ OB není ani arbitrážní soud, jedná se o orgán stálý a postupující podle vlastní-

¹⁰⁴ Viz HELFER, LAND. *The Meta Oversight Board's Human Rights Future*. s. 2246.

¹⁰⁵ Viz GULATI, Rishi. *Meta's Oversight Board and Transnational Hybrid Adjudication - What Consequences for International Law?* *German Law Journal*. 2023, č. 3, roč. 24, s. 491.

¹⁰⁶ Viz BILLY, Perrigo. *Facebook's Oversight Board Is Reviewing Its First Cases. Critics Say It Won't Solve the Platform's Biggest Problems* [online]. *Time*, 7. 12. 2020 [cit. 19. 2. 2025]. <https://time.com/5918499/facebook-oversight-board-cases/>

¹⁰⁷ V obou případech se jedná o koncepty amerického soukromého práva. Českým ekvivalentem trustu je svěřenský fond podle § 1448 an. o. z., LLC („limited liability company“) je nejpodobnější české společnosti s ručením omezeným podle § 132 an. o. z.

¹⁰⁸ Viz GULATI. *Meta's Oversight Board and Transnational Hybrid Adjudication - What Consequences for International Law?*, s. 479.

¹⁰⁹ Viz Oversight Board. *Oversight Board Charter* [online]. *Oversight Board* [cit. 19. 2. 2025]. https://www.oversightboard.com/wp-content/uploads/2024/03/OB_Charter_March_2024.pdf

¹¹⁰ Viz GULATI. *Meta's Oversight Board and Transnational Hybrid Adjudication - What Consequences for International Law?*, s. 480.

ho procesu a vlastního práva.¹¹² Podle Mazúra a Grambličkové stojí OB z pohledu DSA na pomezí mezi interním přezkumem a mimosoudním řešením sporu,¹¹³ zastřešuje sice interní přezkum jako částečně nezávislá poslední instance, nemá ale certifikaci národním koordinátorem digitálních služeb podle DSA.

Rozhodovací proces OB začíná podáním žádosti o přezkum, kterou může podat buď uživatel nebo Meta. Následně administrativní tým sestaví „long-list“ jednotlivých případů. OB si své případy vybírá, což připomíná proces vybírání případů severskými nejvyššími soudy.¹¹⁴ Stejně jako ony OB zohledňuje zejm. důležitost případu nebo jeho dopad na společnost a projedná tak jen zlomek žádostí.¹¹⁵ Případy vybírá tzv. Case Selection Committee složená z členů OB na rotačním principu, která vybrané případy postoupí pětičlennému panelu. Ten je projedná a vypracuje koncept rozhodnutí. Na závěr rozhoduje celé plénum OB, jehož rozhodnutí je pro Metu závazné.¹¹⁶ Nejběžnějším typem rozhodnutí je „Standard Decision“. V případech naléhavých problémů je možné vydat tzv. „Expedited Decision“, u kterého je celý proces rychlejší. „Summary Decisions“ (shrnutí) pak OB vydává v případech, kdy Meta přehodnotila svůj původní závěr během projednávání případu.¹¹⁷ Pokud se jedná o několik podobných případů, může je OB spojit a vydat tzv. „Multiple Case Decision“.

¹¹¹ Viz GULATI. *Meta's Oversight Board and Transnational Hybrid Adjudication - What Consequences for International Law?*, s. 480.

¹¹² Tamtéž, s. 476-478.

¹¹³ Viz MAZÚR, GRAMBLIČKOVÁ. *New Regulatory Force of Cyberspace: The Case of Meta's Oversight Board*, s. 25.

¹¹⁴ Viz GHAVANI, Anna W., GRENDSTAD, Gunnar, SCHAFFER, John K. Institutions that define the policymaking role of courts: A comparative analysis of the supreme courts of Scandinavia. *International Journal of Constitutional Law*. 2023, č. 21, roč. 3, s. 791. <https://academic.oup.com/icon/article/21/3/770/7250119>

¹¹⁵ Dle výroční zprávy v roce 2023 OB obdržela téměř 400 000 žádostí o přezkum a rozhodla celkem 53 případů (22 standardních, 29 shrnutí, 2 zrychlené). Viz Oversight Board. *2023 Annual Report*.

¹¹⁶ Viz MAZÚR, GRAMBLIČKOVÁ. *New Regulatory Force of Cyberspace: The Case of Meta's Oversight Board*, s. 23-24.

¹¹⁷ Viz Oversight Board. *2023 Annual Report*.

4.2 PRÁVNÍ ZÁKLAD PRO ROZHODOVÁNÍ OVERSIGHT BOARD

Jurisdikce OB je na rozdíl od běžných soudů založena smluvně. OB tak nerozhoduje na základě práva státu, ale podle právního derivátu, který je určen v Charter. Tento derivát nazývá Gulati „hybridním právem“,¹¹⁸ sestává se totiž z kombinace zásad komunity (resp. dalších smluvních podmínek sociální sítě) a „lidskoprávních norem upravujících svobodu projevu“.^{119 120} Toto ustanovení je samo o sobě velmi vágní a nechává OB volnou ruku v tom, jaké lidskoprávní dokumenty bude uplatňovat.¹²¹ Neupravuje ani poměr mezi oběma složkami, avšak ve svých rozhodnutích dává OB konstantně přednost lidskoprávní složce.¹²²

4.2.1 LIDSKOPRÁVNÍ NORMY

OB přijala za svůj názor Zvláštního komisaře OSN¹²³ pro svobodu projevu, tedy že „společnosti nemají povinnosti států, ale jejich dopad na uživatele je enormní, a proto by měly [při zásahu do lidských práv uživatelů] posuzovat stejné otázky jako státy.“¹²⁴ V souvislosti s touto zprávou se Meta zavázala dodržovat Obecné zásady OSN pro podnikání a lidská práva („UNGP“),¹²⁵ které zahrnuje do svých Corporate Human Rights Policy.¹²⁶ Dosud jde o jediný lidskoprávní dokument, který závazně přijala. V případě

¹¹⁸ Viz GULATI. *Meta's Oversight Board and Transnational Hybrid Adjudication - What Consequences for International Law?*, s. 484.

¹¹⁹ Viz HELFER, LAND. *The Meta Oversight Board's Human Rights Future*, s. 2247.

¹²⁰ Viz sec. 2 Oversight Board. *Oversight Board Charter*.

¹²¹ TIEDEKE, Anna S., FERTMANN, Martin. A love triangle? Mapping Interactions between International Human Rights Institutions, Meta and Its Oversight Board. *European Journal of International Law*. 2023, roč. 34, č. 4, s. 916.

¹²² Viz HELFER, LAND. *The Meta Oversight Board's Human Rights Future*, s. 2270.

¹²³ Organizace spojených národů.

¹²⁴ Viz odst. 41, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/74/486 ze dne 9. 10. 2019. *United Nations General Assembly* [cit. 19. 2. 2025]. <https://docs.un.org/en/A/74/486>

¹²⁵ Viz United Nations. Guiding Principles on Business and Human Rights. 2011 [cit. 19. 2. 2025]. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinessshr_en.pdf

¹²⁶ Viz Meta. Corporate Human Rights Policy [online]. *Meta* [cit. 19. 2. 2025]. <https://about.fb.com/wp-content/uploads/2021/03/Facebooks-Corporate-Human-Rights-Policy.pdf>

ostatních smluv si nechává volnou ruku a nijak je konkrétně nespecifikuje.¹²⁷

OB prakticky neodráží hojnou judikaturu regionálních lidskoprávních organizací (např. ESLP) nebo ústavních soudů. Velmi zřídka také používá vyjádření specializovaných mezinárodních institucí jako je Světová zdravotnická organizace, UNESCO nebo Mezinárodní výbor Červeného kříže.¹²⁸ Výsadní postavení se však dostává MPOPP.¹²⁹ Jeho čl. 19 lze vnímat jako základ lidskoprávní argumentace OB, která s ním pracuje ve všech svých rozhodnutích. V souladu s názorem Zvláštního komisaře (viz výše) provádí OB stejný tříprvkový test, jaký je určen výkonné moci. Posuzuje v něm nejprve legalitu (jasnost a dostupnost pravidel), následně legitimní cíl a potřebnost a nakonec proporcionalitu.¹³⁰

4.2.2 ZÁSADY KOMUNITY

Zásady komunity vydává Meta pro své platformy společně a jsou platné pro všechny uživatele bez ohledu na zemi původu.¹³¹ Měly by sloužit jako podklad pro rozhodování o tom, co uživatelé smí na platformách publikovat“.

Přestože by zásady komunity měly sloužit jako jakýsi „zákon“ sociálních sítí, jejich podoba je od zákona odlišná již po vizuální stránce: chybí dělení do paragrafů, součástí jsou různé grafiky apod. Shodně s výkladem poskytnutým v podkapitole 3.2 jsou formulace často poněkud obecné, doplněné následně konkrétními příklady. Jejich výčet je ale již z podstaty věci omezený. Zásady se skládají z úvodní stránky, která poskytuje základní

¹²⁷ TIEDEKE, FERTMANN. *A love triangle? Mapping Interactions between International Human Rights Institutions, Meta and Its Oversight Board*, s. 919.

¹²⁸ Tamtéž, 933.

¹²⁹ Mezinárodní pakt o občanských a politických právech.

¹³⁰ Blíže viz např. část 4.III rozhodnutí *Politician's Comments on Demographic Changes*. Standard Decision Oversight Board ze dne 12. 3. 2024. Plné znění dostupné na <https://www.oversightboard.com/decision/fb-ofs963dz/> [cit. 19. 2. 2025].

¹³¹ Jejich aktuální znění viz Meta. Zásady komunity. *Meta* [cit. 19. 2. 2025]. <https://transparency.meta.com/cs-cz/policies/community-standards/>

vhled do motivace Mety a jejích hodnot, a dalších oddílů upravujících jednotlivé oblasti (kterých je k březnu 2026 celkem 27).¹³²

Pro analýzu rozhodnutí jsou stěžejní zásady upravující nenávistné chování,¹³³ proto je představím podrobněji. Tyto zásady upravují případy, kdy může Meta odstranit nenávistný obsah, typicky tzv. hate speech (nenávistný projev). Aby šlo o zakázaný nenávistný projev ve smyslu těchto zásad, musí se jednat o přímý útok na lidi (nikoli např. na instituce) na základě tzv. chráněné charakteristiky: rasy, národnosti, sexuální orientace, náboženství aj. Dále upravuje výjimky pro „nadávky na gender v souvislosti s ukončením partnerského vztahu“, pro satiru, či kritiku.¹³⁴

Nenávistný projev se dělí do dvou úrovní podle závažnosti. Do první úrovně patří přirovnávání ke zvířatům, obviňování ze závažných trestných činů, opakování škodlivých stereotypů a další. Ve druhé úrovni se pak nachází např. výzvy k segregaci nebo cílené nadávky.¹³⁵ Ve všech případech se jedná o obecné formulace, které následně doplňují četné příklady. Ze zásad však jasně nevyplývá, k čemu vlastně rozdělení do dvou úrovní slouží. Neobsahují žádná procesní pravidla, ani rozdíl v případných sankcích, které se pochopitelně mohou výrazně lišit, jako je tomu např. při stanovení doby zablokování účtu.

4.3 ANALÝZA VYBRANÝCH ROZHODNUTÍ

V následujících řádcích představím vybraná rozhodnutí Oversight Board. Ve všech případech se jedná o rozhodnutí z roku 2024, která nebyla sumarizovaná ve výroční zprávě a veřejnost s nimi dosud nebyla široce seznámena. Pro dokreslení způsobu „dotváření“ zásad komunity jsem zvolil taková rozhodnutí, která rozvíjejí zásady upravující nenávistné chování, přiblížené výše v oddílu 4.2.1. Cílem je představit čtenáři kontext, v jakém

¹³² Viz Meta. *Zásady komunity*.

¹³³ Jejich aktuální znění viz Meta. *Zásady komunity: nenávistné chování*. Meta [cit. 19. 2. 2025] <https://transparency.meta.com/cs-cz/policies/community-standards/hate-speech/>

¹³⁴ Viz Meta. *Zásady komunity: nenávistné chování*.

¹³⁵ Viz Meta. *Zásady komunity: nenávistné chování*.

OB rozhodnutí vydala, způsob tvorby rozhodnutí a dílčí závěry, které z jednotlivých rozhodnutí plynou.

Všechna analyzovaná rozhodnutí jsou tzv. „Standard Decision“ nebo „Multiple Case Decision“, u nichž je na rozdíl od zbývajících typů rozhodnutí dostupné poměrně obsáhlé odůvodnění. Při analýze jsem pracoval s plnými zněními rozhodnutí v angličtině, tedy úředním jazyce OB. Rozhodnutí řadím chronologicky podle data jejich vydání.

4.3.1 POST IN POLISH TARGETING TRANS PEOPLE¹³⁶

V prvním analyzovaném rozhodnutí objasňuje OB rozdíl mezi nenávistným projevem spočívajícím v útoku na instituci a na skupinu jednotlivců a vysvětluje hranice, kdy lze takový útok postihovat. Jde zároveň o jasný příklad tzv. „malign creativity“ (viz dále), kterou algoritmy Mety neumějí příliš efektivně postihovat, což OB opakovaně kritizuje.

Jeden z uživatelů Facebooku nahrál na tuto síť příspěvek s obrázkem zachycujícím vlajku trans osob, která byla zavěšena jako záclona. Tento obrázek dále obsahoval texty „Nová technologie: záclony, které se samy pověsí“ a „jarní úklid <3“.¹³⁷ Daný uživatel měl navíc v popisu svého profilu uvedeno, že je „transfobem“. Uživatelé příspěvek celkem dvanáctkrát nahlásili, ale pouze dvakrát se dostal k lidskému moderátorovi. Ani v jednom případě jej moderátoři nesmazali, a to ani po odvolání.

Lidskoprávní organizace soustavně kritizují Polsko za problematický přístup k sexuálním menšinám. Ve srovnání s členskými státy EU stojí Polsko na posledních příčkách těchto žebříčků. Vůči sexuálním menšinám se hanlivě vyjadřují vrcholní politici (např. z tehdejší vládní strany PiS), v mnoha polských městech byly po roce 2019 zřízeny tzv. „LGBT-free zóny“.¹³⁸ U sexuálních menšin je také větší riziko sebevraždy, což OB dokládá výzkumy z USA.

¹³⁶ Dle *Post in Polish Targeting Trans People*. Standard Decision Oversight Board ze dne 16. 1. 2024. Plné znění dostupné na <https://www.oversightboard.com/decision/fb-uk2rus24/> [cit. 19. 2. 2025].

¹³⁷ V jazyce rozhodnutí „*New technology ... Curtains that hang themselves*“ a „*spring cleaning <3*“, v (původním) polském jazyce „*Nowa technologia... zastony, które wieszają się same*“ a „*wiosenne porządki <3*“. Překlad autora.

Po představení případu OB Meta příspěvek odstranila. Zařadila jej jako nenávistný projev první úrovně právě z důvodu nepřímých výzev k sebevraždám. Podle vyjádření Mety by samotný útok na vlajku trans osob vykládala jako útok na „instituci“, ovšem v kontextu dodatečných textů je zjevné, že „instituce se nemůže oběsit“ a útok tak směřuje na skupinu lidí (trans osob). Popis profilu uživatele, ve kterém sám sebe označuje za „transfoba“ pak Meta vyhodnotila jako nenávistný projev druhé úrovně. Podle ní se zde uživatel sám hlásí k intoleranci vůči chráněné charakteristice, kam patří i gender.

OB ve svém odůvodnění souhlasila s dodatečným vyjádřením Mety. Potvrdila závěr o útoku na skupinu osob a zdůraznila jeho kontext s ohledem na problematickou situaci sexuálních menšin v Polsku a vysokou míru sebevražd. Kritizovala však Metu za nedostatečnou kontrolu nad takovým obsahem, zejm. s ohledem na několikrát přezkoumání takto zjevného útoku různými moderátory. Podle OB by měli mít „odvolací“ moderátoři daleko větší odbornost k rozpoznávání porušení a Meta by měla zapracovat také na odhalování případů tzv. „malign creativity“. Tedy případů, kdy se nenávistný projev snaží maskovat jako humor a satira nebo používá výrazy, které algoritmy nedokáží detekovat.

4.3.2 HOLOCAUST DENIAL¹³⁹

V následujícím rozhodnutí OB objasňuje, zda vůbec a případně za jakých okolností může sociální síť obecně blokovat všechny příspěvky na nějaké konkrétní téma. Vysvětluje tak do jisté míry hranici mezi projevem uživatele a platformy.

Uživatel na Instagramu zveřejnil obrázek zobrazující animovanou postavu Sépiáka z pořadu Spongebob v kalhotách s textovým polem „Fun Facts About The Holocaust“, ve kterém následně zpochybňoval údaje o po-

¹³⁸ Podle Human Rights Watch šlo o místa, „kde místní úřady přijaly diskriminační ‚rodinné charty‘, v nichž se zavázaly ‚chránit děti před morálním úpadkem‘, nebo se prohlásily za osvobozené od ‚LGBT ideologie‘“. Takové zóny vznikly ve více než 100 obcích, polský Nejvyšší soud nařídil v roce 2022 čtyřem z nich jejich zrušení. Blíže viz cit. rozhodnutí *Post in Polish Targeting Trans People*.

¹³⁹ Dle *Holocaust Denial*. Standard Decision Oversight Board ze dne 23. 1. 2024. Plné znění dostupné na <https://www.oversightboard.com/decision/ig-zj7j6d28/> [cit. 19. 2. 2025].

čtu zavražděných Židů a samotnou existenci krematorií v koncentračním táboře Auschwitz.¹⁴⁰ Tento příspěvek uživatelé celkem šestkrát nahlásili, z toho jej čtyřikrát přezkoumal algoritmus a dvakrát fyzikální moderátoři, aniž by shledali rozpor se zásadami komunity. Jeden z uživatelů následně podal odvolání k OB s odkazem na protiprávnost takového obsahu v Německu.

Zásady komunity ohledně této problematiky se postupem času měnily. Do listopadu 2022 byl jejich součástí pouze obecný zákaz nenávistného projevu, následně popírání holokaustu explicitně zakázaly¹⁴¹ jako nenávistný projev 1. úrovně.¹⁴² OB zohledňovala také aspekty omezování svobody projevu s ohledem na popírání holokaustu např. v perspektivě MPOPP a Deklarace OSN.

Při přezkumu porušení standardů OB zohledňovala výjimky, avšak daný příspěvek nenaplnil požadavky na satiru, ani neměl cíl zvyšovat povědomí veřejnosti o dané problematice.¹⁴³ OB shledala, že příspěvek měla Meta odstranit již podle staré obecnější úpravy. Kritizovala Metu, že její algoritmus nedokáže zachytit některé formulace (např. „Holohoax“)¹⁴⁴ a nemá data o funkčnosti detekčního systému.¹⁴⁵ OB dále připomíná lidskoprávní závazky, např. Rezoluci Valného shromáždění OSN 76/250, která výslovně vyzývá k blokování obsahu popírající holokaust a rozhodnutí Faurisson proti Francii (550/1993), ve kterém Výbor pro lidská práva shledal omezení projevu popírajícího holokaust v souladu s MPOPP. Meta se cítí být MPOPP vázána (viz podkapitola 4.2.2), proto by měla těmto požadavkům dostát. OB nakonec dodává, že obecný zákaz příspěvků s určitým tématem musí Meta dostatečně odůvodnit a pravidelně přezkoumávat.

¹⁴⁰ Např. tvrdil, že krematoria v koncentračních táborech byla postavena až po válce nebo že o holokaustu chybí zmínka v pamětech jakéhokoli vrcholného státníka té doby.

¹⁴¹ Je uveden jako příklad „škodlivého stereotypu historicky spojeného se zastrašováním nebo násilím“.

¹⁴² Viz Meta. *Zásady komunity: nenávistné chování*.

¹⁴³ Obě výjimky přímo stanovuje Meta. *Zásady komunity: nenávistné chování*.

¹⁴⁴ Jedná se o slovní hříčku, která pracuje se spojením slov „holocaust“ a „hoax“, což je označení pro falešnou zprávu poplašného charakteru.

¹⁴⁵ Jedná se opět o příklad tzv. *malign creativity*, jehož nedostatečné potírání vytkla OB Metě již v předchozím analyzovaném rozhodnutí.

OB v tomto rozhodnutí nepřímo vysvětluje hranici svobody projevu platformy v otázce moderace obsahu popírajícím holokaust. Nevyjadřuje se k ilegaltě v některých zemích (např. v Německu), ale pouze k aplikaci zásad komunity a lidskoprávních dokumentů OSN. Z těchto dokumentů dovozuje OB nejen možnost takový obsah blokovat, ale i v jistém smyslu povinnost tak činit. Zároveň kritizuje moderační postupy na sociální síti, které jednak nedokázaly příspěvek samy zachytit, přestože jeho závadnost byla zjevná, a jednak ani odstranit po nahlášení příspěvku jinými uživateli.

4.3.3 POLITICIAN'S COMMENTS ON DEMOGRAPHIC CHANGES¹⁴⁶

OB v tomto rozhodnutí definovala hranici, kdy může projev politika (tedy chráněný typ projevu) kritizujícího přístup státu k určité skupině osob přerůst k nenávistnému projevu proti této skupině osob. Navíc řeší otázku, zda označení původu podle světadílu lze podřadit pod stejný stupeň ochrany jako státní nebo etnickou příslušnost.

Éric Zemmour je francouzský politik, který proslul svými výroky silně kritizujícími evropskou migrační politiku, islám nebo ženská práva. Za podobné výroky byl v minulosti postihován francouzskými soudy, jedno z řízení vyústilo také v neúspěšnou stížnost u ESLP. Na svém Facebookovém účtu zveřejnil video obsahující krátkou část jednoho z rozhovorů, který poskytl při kampani na prezidenta. V rozhovoru se vyjadřuje o tom, že v Africe je obrovská populační vlna a přirovnává tuto situaci k populační vlně v Evropě na přelomu 19. a 20. století. Podle něj evropská populační vlna vyústila v kolonizaci Afriky a stejná situace hrozí i dnes, ovšem v opačném směru.

Příspěvek uživatelé nahlásili jako fake news, ale algoritmy neshledaly porušení zásad komunity. Po odvolání ke stejnému závěru dospěli i lidští moderátoři a uživatel podal odvolání k OB. Meta vysvětlovala svůj přístup jednak zařazením imigrantů v rámci zásad komunity do 2. úrovně, která nemá takový stupeň ochrany. Nenávistný projev vyžaduje přímý zásah na chráněnou kategorii, Meta však argumentovala, že „Afričané“ nejsou ná-

¹⁴⁶ Dle *Politician's Comments on Demographic Change*. Standard Decision Oversight Board ze dne 12. 3. 2024. Plné znění dostupné na <https://www.oversightboard.com/decision/fb-ofs963dz/> [cit. 19. 2. 2025].

rod ani etnikum, nýbrž obyvatelé kontinentu a tato ochrana se jich proto netýká.

Argumentaci OB lze rozdělit na dvě části, první zaměřenou na nenávislný projev proti „Afričanům“ a druhou ohledně souvislosti s konspirační teorií „The Great Replacement“. Co se týče první části argumentace, OB opakuje požadavek na přímý útok proti chráněné skupině. V tomto případě video neobsahovalo žádné výzvy k násilí, přímé dehumanizování nějaké skupiny, ani nenávislný projev vůči ohroženým skupinám. OB v souvislosti s projevem o imigrantech požaduje odstranění obsahu pouze u nejzávažnějších projevů, s ohledem na volnost politické debaty. Meta sama totiž v zásadách komunity deklarovala, že chce nechat prostor pro diskusi o imigrační politice států.¹⁴⁷ V souvislosti s lidskoprávními závazky Mety provedla OB test proporcionality ohledně svobody projevu, kterým by omezení takového politického videa dle OB neprošlo. Především by nebyl proporcionální vůči možnosti vést otevřenou debatu na téma imigrační politiky.

Druhá část argumentace se zabývala souvislostí videa s konspirační teorií „The Great Replacement“. Ta rozvíjí názor, že bílí Američané a Evropané jsou účelně nahrazováni ne-bílými imigranty.¹⁴⁸ Zde se členové OB rozcházel. Většina neshledala přímou souvislost mezi rasistickou konspirační teorií a daným příspěvkem, a proto byla proti blokování Menšině stačilo opakování narativů, které taková konspirační teorie předkládá, a blokování prosazovala. Většina také argumentovala praktickým uplatňováním takové doktríny, které by podle ní vyústilo k širokému blokování politického obsahu. OB se nakonec přiklonila k ponechání příspěvku na Facebooku. Hlavními důvody byla nechuť disproportčně omezovat politický projev a nesplnění testu, který požaduje přímý útok proti chráněné skupině.

¹⁴⁷ Viz *Meta*. Zásady komunity: nenávislné chování.

¹⁴⁸ Viz ROSE, Steve. A deadly ideology: how the ‘great replacement theory’ went mainstream [online]. *The Guardian*, 8. 6. 2022 [cit. 19. 2. 2025]. <https://www.theguardian.com/world/2022/jun/08/a-deadly-ideology-how-the-great-replacement-theory-went-mainstream>

4.3.4 POSTS THAT INCLUDE "FROM THE RIVER TO THE SEA"¹⁴⁹

OB zkoumala, zda lze politický slogan s více významy označit za nenávistný projev jen proto, že to jeden z výkladů umožňuje. Rozhodnutí částečně navazuje na již předložené rozhodnutí Holocaust Denial. OB totiž opět řeší, zda lze obecně zakázat určitý druh projevu, zde však jde o frázi (slogan), nikoli o téma.

OB řešila tři příspěvky na Facebooku, které obsahovaly frázi „From the River to the Sea“. Prvním byl komentář s hashtagem¹⁵⁰ a dalšími frázemi vyjadřující podporu Palestině, druhý příspěvek obsahoval vygenerovaný obrázek, kde frázi tvořily kousky vodního melounu¹⁵¹ a třetí příspěvek byl text vyjadřující podporu Palestině a odpor proti „Sionistům“. Všechny tři příspěvky uživatelé nahlásili, algoritmy neshledaly rozpor se zásadami komunity a příspěvky nesmazaly. Fyzičtí moderátoři kontrolovali pouze druhý případ, ale také příspěvek na síti ponechali.

Fráze slouží jako slogan při podpoře Palestiny v rámci aktuálního konfliktu s Izraelem a její četnost na sociálních sítích po 7. 10. 2023 násobně vzrostla (v angličtině z cca 1400 případů během šesti měsíců před útokem na cca 82 000 během stejné doby po něm). OB v rámci kontextu rozebírá aspekty konfliktu (útok Hamásu ze 7. 10. 2023, následnou válku a podezření obou stran z válečných zločinů) a historii fráze, která podle jejího názoru přímo nesouvisí s Hamásem (který samotná Meta řadí mezi 1. skupinu nebezpečných organizací), ale s podporou Palestiny. Dále zmiňuje případy, kdy se výkonná moc snažila o zákaz této fráze, ale soudy následně nedovodily její závadnost (případy ve Spojeném království, Německu i ČR).¹⁵²

¹⁴⁹ *Dle Posts That Include "From the River to the Sea"*. Multiple Case Decision Oversight Board ze dne 4. 9. 2024. Plné znění je dostupné na <https://www.oversightboard.com/decision/bun-86tj0rk5/> [cit. 19. 2. 2025].

¹⁵⁰ Jde o klíčové slovo nebo frázi, které předchází znak „#“ a umožňuje uživatelům snazší hledání podobných příspěvků napříč sociální sítí.

¹⁵¹ Vodní meloun je jedním ze symbolů propalestinského hnutí. Jeho barvy (červená, zelená, černá) totiž odpovídají barvám palestinské vlajky.

¹⁵² Pro konkrétní případy viz analyzované rozhodnutí.

Podle uživatelů, kteří příspěvky nahlásili, samotná fráze propaguje násilí, je sama o sobě nenávistným projevem a vyzývá ke genocidě. Meta argumentuje, že samotná fráze není porušením podmínek, toho by dosáhla až v kombinaci s dalšími prvky: např. s výzvami ke „konečnému řešení“ nebo k „návratu Židů do Polska“.

OB vysvětluje jednotlivé aspekty fráze a argumentuje, že ačkoli fráze „od řeky (Jordán) k moři (Středozemnímu)“ v čistě jazykovém výkladu nepočítá s existujícím Izraelem a lze ji zneužít k vyjádření nenávisti vůči Židům nebo židovskému státu, je sama o sobě politickým projevem, který zasluhuje vyšší úroveň ochrany. Souhlasí s argumentací Mety, že pro závažnost této fráze by byla potřeba kombinace s dalšími prvky, které by měly samy o sobě dostatečnou intenzitu k porušení zásad.

Podle OB tato fráze neodporuje zásadám komunity ani lidskoprávním požadavkům. Nebyla prokázána jasná souvislost mezi užitím fráze a výzvou k násilí (resp. bezprostřední hrozbou v offline světě), ani podněcování k násilí na Židech. Podle názoru většiny OB by Meta příspěvky s touto frází neměla blokovat automaticky, ale měla by prověřit další kontext: např. zda není výzva spojena s dalšími problematickými výroky. V rozhodnutí se objevil také menšinový názor, který požadoval opak; tedy obecně blokaci takových příspěvků, ale s možností výjimek.

4.3.5 CRIMINAL ALLEGATIONS BASED ON NATIONALITY¹⁵³

Podobně jako v rozhodnutí *Post in Polish Targeting Trans People*, i zde OB řešila, kdy se obecné označení vztahuje na instituci a kdy na skupinu osob. V tomto případě šlo o označení národů jako „zločinců“ a OB posuzovala, zda se v konkrétním případě jedná o útok na národ jako skupinu jednotlivců (tedy nenávistný projev) nebo útok na stát, (resp. státní politiku), který Meta toleruje.

OB posuzovala tři případy, každý útočící na jiný národ a uveřejněný na jiné sociální síti. V prvním případě šlo o příspěvek na Facebooku v arabštině, který označoval všechny Rusy a Američany za zločince a dodával, že

¹⁵³ Dle *Criminal Allegations Based on Nationality*. Multiple Case Decision Oversight Board ze dne 25. 9. 2024. Plné znění je dostupné na <https://www.oversightboard.com/decision/bun-fjipx1xo/> [cit. 19. 2. 2025].

„Američané jsou alespoň čestnější zločinci, protože se ke svým zločinům přiznají“. Druhý příspěvek na Threads označoval za zločince všechny Izraelce, jednalo se o komentář pod videem rozebírajícím konflikt v Gaze a zahrnujícím obvinění Izraele z genocidy. V posledním případě šlo o komentář označující všechny Indy za násilníky, který se objevil na Instagramu pod fotkou mužů stojících v hloučku a zírajících na ženu uprostřed.

Ve všech třech případech Meta příspěvky smazala s odkazem na zásady komunity o nenávistném chování, některé příspěvky dokonce přezkoumávala. Ani jeden z jejich autorů se neodvolal k OB, případ jí však předala sama Meta. Ve svém vyjádření vysvětlila, že přímý útok proti skupině osob, který je obecně označuje za zločince, spadá pod 1. úroveň nenávistného projevu. Meta považovala za nejasné, do jaké míry je potřeba zohledňovat kontext těchto označení, např. jak moc je potřeba posuzovat politický kontext vyjádření. Sama hledala hranici mezi odstraňováním obvinění jedinců nebo skupin a kritikou států jako politickým projevem. Předložila několik alternativ, jako je podrobné zkoumání kontextu specialisty nebo různé formy obecného zákazu s určenými výjimkami.

OB dovodila, že označení národa za zločince není nenávistným projevem, pokud je jasná spojitost se státem (resp. jeho představiteli). Především jde o situace, kdy v dané situaci vystupují státní představitelé, jako jsou vojáci nebo policisté, nebo se jedná o zločiny, které může spáchat pouze stát (zejm. zločiny vycházející z Římského statutu). Roli pak také hrají použité jazykové výrazy jako je označení „všichni“ nebo použití určitého členu.

První příspěvek OB nařídila obnovit. S ohledem na expertní vyjádření, podle něhož použité arabské výrazy mohly označovat jak národ, tak stát („všichni Rusové a Američané jsou zločinci“), a následné porovnávání činností států („Američané jsou alespoň čestnější zločinci, protože se ke svým zločinům přiznají“), OB dovodila, že se jedná o kritiku států a nejedná se tedy o zakázaný nenávistný projev. Ve druhých dvou případech nebyla podle OB splněna podmínka jasného propojení kritiky a činnosti státu. U druhého příspěvku OB splnění podmínky nedovodila, podle mého názoru poměrně nepochopitelně. V konfliktu totiž jasně vystupují izraelští

vojáci, tedy představitelé státu (navíc!) nařčeného z genocidy, tedy zločinu podle Římského statutu. OB pouze konstatovala riziko „offline“ újmy vůči Izraelcům v případě ponechání příspěvku na platformě, s ohledem na zvýšenou míru protizidovských a protiizraelských vyjádření ve veřejném prostoru a (ne)splnění podmínek jasné spojitosti se státem blíže nekomentovala, ani se nevyjádřila, zda riziko „offline“ újmy převáží nad projevem kritizujícím jednání státu. Ve třetím případě pak mezi obsahem příspěvku a Indií jako státem nenašla žádnou vazbu.

OB vyžaduje po Metě, aby vytvořila příručku pro moderátory, která by jim pomohla najít hranice mezi kritikou státu a útokem na jeho obyvatele. Takové instrukce musí být jasné a odpovídat nastaveným pravidlům tak, aby byl při přezkumu dodržen princip legality. OB dále doporučila zavedení výjimky pro kritiku vůči státům, k tomu však Meta dosud nepřistoupila.

4.4 SHRnutí ANALYZOVANÝCH ROZHODNUTÍ

Ve všech rozhodnutích lze jasně vidět specifický charakter rozhodovacího orgánu, který je stále v právním prostředí novinkou a do určité míry hledá své místo. Zřejmě i proto si vybírá mediálně vděčná témata, která rezonují ve společnosti a mohla by zvýšit povědomí o samotné existenci orgánu, příp. jeho činnosti. Tuto snahu odráží také volba úderných populárních názvů a vysoká aktivita OB na sociálních sítích (mj. na Instagramu), kde zveřejňuje krátká shrnutí rozhodnutí v uživatelsky přívětivé grafické formě.

Co se obsahu rozhodnutí týče, ve všech případech kladla OB velký důraz na aplikaci lidskoprávních norem. Ty staví proti zásadám komunity a následně rozhoduje na základě kombinace obou složek. Jak vyplývá z rozhodnutí Holocaust Denial, k odstranění příspěvku by OB stačilo porušení samotných lidskoprávních norem zakazujících popírání holokaustu, aniž by byl tento zákaz specificky zmiňovaly zásady komunity. Ve všech případech OB důsledně provádí tříprvkový test a vyjadřuje odpor proti formalistickému jazykovému výkladu pravidel, např. ohledně označení „Afričané“ v rozhodnutí Politician's Comments on Demographic Changes. OB bývá ve svých rozhodnutích poměrně kritická vůči přístupu Mety k moderaci. Opakovaně

vytýká nedokonalost algoritmů a chybovost lidských moderátorů. To lze vidět třeba v problematických případech malign creativity, na které OB opakovaně upozorňuje (viz případ Post in Polish Targeting Trans People).

Samotná rozhodnutí obsahují také menšinové názory členů OB, které představují další zohledňované návrhy a mohou předvídat možný budoucí vývoj rozhodovací činnosti při obměně členů. V rozhodnutích lze vidět také různé formy činnosti orgánu. OB nefunguje pouze jako odvolací orgán, může Metě poskytovat vlastní názory a kontrolovat, jak a zda je implementovala. O takový názor může sama Meta požádat, jako v rozhodnutí Criminal Allegations Based on Nationality. I díky těmto případům dokáže OB poskytovat závazný výklad zásad komunity a dotvářet tak celkový systém. To lze vidět na všech analyzovaných rozhodnutích s ohledem na zásady komunity ve věci nenávistných projevů.

Pokud OB nezmění styl a přístup k rozhodovací činnosti, můžeme očekávat poměrně rozumný stupeň dohledu nad dodržováním zásad komunity a široké zohledňování možných zásahů do lidských práv.

4.5 ZÁVĚRY A NÁMĚTY PRO APLIKAČNÍ PRAXI

Internet je specifickým prostředím, ve kterém je problematické aplikovat všechna dosavadní pravidla tak, jak byla původně nastavena. Představa o jeho „neregulovatelnosti“ z 90. let nebyla naplněna¹⁵⁴ a státy rozšířily své jurisdikce i do tohoto prostředí. To s sebou ale přineslo řadu problémů, jedním z nich je neexistence jednotných internetových pravidel, která by vymáhala specializovaná instituce, jakýsi „mezinárodní internetový soud“. Takový orgán by mohl disponovat lepším odborným zázemím a efektivnějšími nástroji, než je tomu u běžných soudů, dnes už je však jeho zřízení v podstatě nemožné, ať už z důvodu obchodních zájmů platforem či geopolitických zájmů států. Nejblíže k představě „internetového soudu“ je aktuálně právě OB, nelze ji však považovat za soud v pravém slova smyslu. Ačkoli není závislá na žádné světové vládě, do určité míry závisí na zřizující společnosti Meta, která má vliv na její financování a volbu jejích členů. Mezi nedostatky také patří vágnost základních ustanovení o použití lid-

¹⁵⁴ Viz GOLDSMITH, WU. *Kdo řídí Internet? Iluze o světě bez hranic*, s. 10.

skoprávních dokumentů. Na druhou stranu se jedná o první rozhodovací orgán tohoto typu s jurisdikcí čistě na internetu,¹⁵⁵ což přináší řadu novinek.

OB s odkazem na zásady komunity Mety zvládne poměrně dobře pracovat s „internetovými zločiny“.¹⁵⁶ Využívá přesnou definici nenávistného projevu vycházející z „přímého útoku na základě chráněné charakteristiky“, kterou dokáže OB rozumně rozvíjet s ohledem na problematické okolnosti (viz analyzovaná rozhodnutí výše). Je zde zřejmá pozice Mety jako definiční autority: sama si vytvořila „právo“ ve formě zásad komunity a „soud“ ve formě OB, jejichž kombinace vytváří pravidla chování uživatelů na nejpopulárnějších světových sociálních sítích. A nejedná se pouze o případy nenávistného projevu popsané výše, podobně lze nazírat na problematiku šíření misinformací¹⁵⁷ nebo blokování nenávistných profilů a stránek.¹⁵⁸

Naproti tomu u běžných soudů je postup pomalý, drahý a často neefektivní. Pokud sankce v podobě příkazu k odstranění obsahu přijde v řádu měsíců po publikaci na internetu, nemá již pro dotčenou osobu velkou hodnotu. Obsah už se pravděpodobně rozšířil a může ho kdykoli znovu publikovat jiný uživatel. Soudy také řeší pouze konkrétní stížnosti jednotlivců, nikoli systémové problémy (jako je podoba zásad komunity).¹⁵⁹ Takový postup však nemůže efektivně fungovat, což konstatoval SCOTUS již na přelomu 70. a 80. let v případě Sony (viz kapitola 3). Nedává tedy velký smysl

¹⁵⁵ Již v minulosti jsme se setkali se snahou o zřízení jisté formy „internetového soudu“ u problematiky doménových jmen, kdy vznikla speciální pravidla pro arbitrážní spory týkající se „cybersquattingu“ (UDRP). Tyto postupy organizace ICANN však nelze chápat jako „soud“, ale stále jako arbitráž. Zejm. nejde o stálou instituci, která aplikuje vlastní právo, jako je tomu u OB.

¹⁵⁶ Za „internetový zločin“ považují právě prohřešky uživatelů sociálních sítích, které se na nich opakovaně objevují – tedy podněcování k nenávisti vůči skupině osob, šíření poplašné zprávy aj. Záměrně neuvádím pojem „kyberzločin“, jež zahrnuje různé typy hackerských útoků, těm se totiž OB vůbec nevěnuje.

¹⁵⁷ K tomu viz *Removal of COVID-19 misinformation*, Published Advisory Opinion Oversight Board ze dne 20. 4. 2023. Plné znění dostupné zde: <https://www.oversightboard.com/decision/pao-sabu4p2s/> [cit. 19. 2. 2025].

¹⁵⁸ OB se vyjadřovala k zablokování facebookového a instagramového účtu Donalda Trumpa po útoku na Kapitol. Viz *Former President Trump's suspension*, Standard Decision Oversight Board ze dne 5. 5. 2021. Plné znění je dostupné zde: <https://www.oversightboard.com/decision/fb-691qamhj/> [cit. 19. 2. 2025].

soudně řešit konkrétní zásahy do svobody projevu, ale spíše hledat způsob, jak získat vliv na tvorbu nebo změny zásad komunity.

Stále je však potřeba udržet regulaci v rozumných mezích tak, aby se nezměnila v podružnou cenzuru (viz podkapitola 3.2), státy by tedy neměly mít plné právo nařít změnu zásad komunity. Nejlepší a nejefektivnější řešení je samozřejmě dialog mezi státy a platformami, což se v určitých aspektech dařilo mezi Metou a OSN.¹⁶⁰ V současné společnosti však mnohdy nestačí¹⁶¹ a státy musí disponovat nástroji, jak dodržování práva vynutit v mezích daných zákazem cenzury. Právě o to se snaží DSA, které dává Evropské komisi poměrně silnou pravomoc v kontrolování rizikových postupů a udělování pokut (viz podkapitola 3.3). Tento přístup se jeví jako střední cesta mezi oběma extrémy, nějaká regulace a vynutitelnost je totiž nutná. Pokud zůstanou velké sociální sítě efektivně neregulované, nebude možné aplikovat pravidla bránící se demokracie proti narůstajícímu vlivu krajní pravice v Evropě.

S vytvořením jisté formy „internetových soudů“ aktuálně pracuje čl. 21 DSA, který vytváří podklad pro zřizování certifikovaných subjektů pro mimosoudní řešení sporů („ODS“)¹⁶² mezi uživatelem a platformou. Jedná se o soukromé subjekty, kterým udělí národní koordinátor digitálních služeb certifikaci. Nejde sice o plně nezávislý orgán, s ohledem na nejisté financování¹⁶³ a možnost odebrání certifikace, jejich vytvoření je však dobrou zprávou zejm. z hlediska efektivního a odborného řešení internetových sporů. ODS řeší čistě problémy na internetu a přehlaceným soudům by mohly

¹⁵⁹ Zajímavý pohled na věc předkládá Thomson, když platformy na základě jejich postavení připodobňuje k vládám a argumentuje, že by měly také podléhat *judicial review*, jako je tomu u veřejné moci v některých anglosaských státech. Soudní moc by pak mohla hrát zásadní roli pro praktické fungování systému. K tomu více THOMSON, Stephen. Into the Quagmire: Social Media as Regulators and the Limits of Judicial Review. *Public Law*. 2024, Oct, s. 695-718. Dostupné v systému Westlaw Edge UK.

¹⁶⁰ S ohledem na adopci UNGP, blíže viz podkapitola 4.2.

¹⁶¹ Zejm. s ohledem na nedávná vyjádření Elona Muska a Marka Zuckerberga o „omezení cenzury“ na svých sociálních sítích.

¹⁶² Zkratka vychází z anglického označení „Out-of-court dispute settlement bodies“.

¹⁶³ K tomu blíže HOLZNAGEL, Daniel. Art. 21 DSA Has Come to Life [online]. *Verfassungsblog*. 5. 11. 2024 [cit. 19. 3. 2025]. <https://verfassungsblog.de/art-21-dsa-fundamental-rights-certification/>

alespoň částečně ulehčit od nápadu. Na druhou stranu mají rozhodnutí ODS pouze omezenou vynutitelnost a orgány je nemusí zveřejňovat. Aktuální počet ODS je stále nízký (k březnu 2026 šlo o devět subjektů)¹⁶⁴ a implementace pravidel v některých členských státech vážne (v ČR prošel v březnu 2026 návrh zákona prvním čtením v Poslanecké sněmovně).¹⁶⁵

ODS by si do jisté míry mohly vzít příklad ze systému rozhodování OB, avšak je potřeba mít stále na paměti její částečnou závislost na Metě především v otázkách financování a výběru členů, a složitou pozici související s omezenou vynutitelností rozhodnutí. Přesto jsou některé praktické otázky dobře uplatnitelné i zde. Vzhledem k obsáhlým a poměrně kvalitním odůvodněním mohou ODS z jejich závěrů vycházet a ve vlastních rozhodnutích se s jejími argumenty vypořádat, což přispěje k celkové stabilitě a předvídatelnosti systému. Podstatnou vadou jsou neveřejná rozhodnutí ODS, uživatelé tedy nemají možnost předvídat, jak orgány jednotlivé zásady komunity vykládají a zda má jejich stížnost šanci na úspěch. Přitom by stačilo následovat příklad OB a publikovat (minimálně stěžejní) anonymizovaná rozhodnutí, ideálně včetně shrnutí důležitých bodů v uživatelsky přívětivé formě např. na sociálních sítích. ODS by měly výrazněji akcentovat závěry národních soudů, evropských institucí a relevantních lidskoprávních organizací (zejm. ESLP), což je velký nedostatek odůvodnění OB. Propojení těchto systémů by opět přineslo vyšší míru právní jistoty do jejich rozhodování. Nakonec je potřeba zmínit dialog s platformou. ODS mají jedinečnou možnost pomáhat vytvářet tlak na platformy, který může vést ke změnám zásad komunity nebo způsobu jejich vymáhání. Těchto možností ostatně využívá také OB, když dává ve svých rozhodnutích doporučení k takovým změnám a Meta se jimi do určité míry řídí.¹⁶⁶

¹⁶⁴ Seznam včetně odkazů na weby konkrétních ODS je dostupný na webu Evropské komise, viz *Out-of-court dispute settlement bodies under the Digital Services Act (DSA)* [online]. European Commission [cit. 24. 3. 2026]. <https://digital-strategy.ec.europa.eu/en/policies/dsa-out-court-dispute-settlement>

¹⁶⁵ Viz sněmovní tisk 69/0. Vládní návrh zákona o digitální ekonomice a změně některých souvisejících zákonů.

¹⁶⁶ Ke květnu 2024 Meta implementovala celkem 75 z 266 doporučení OB. Viz Oversight Board. *2023 Annual Report*.

5. ZÁVĚR

Sociální sítě hrají ve společnosti velmi důležitou roli, uživatelé na nich tráví několik hodin denně a jejich prostřednictvím nejen komunikují se svým okolím, ale také přijímají zprávy o politice a aktuálním dění ve světě. Všechny příspěvky, které se jim ve feedu zobrazí, však kontroluje algoritmus, který v konečném důsledku rozhoduje o tom, jaký obsah se stane virálním, a jaký se naopak dostane pouze k zanedbatelnému počtu uživatelů. Postup algoritmu je zároveň na rozdíl od lidského moderátora v podstatě nepřezkoumatelný: funguje automaticky a nelze se ho zeptat, proč dané rozhodnutí učinil. Lidských moderátorů navíc ubývá, jejich práce je totiž pro platformy pomalá a drahá. Algoritmická moderace je nedokonalá, nezvládá např. správně zohledňovat kontext v otázkách satiry nebo ochrany menšin, případně může rozhodovat na základě stereotypů. Algoritmus totiž často upřednostňuje extrémní názory, jejichž šíření může vést k radikalizaci společnosti a jiným drastickým důsledkům.

Vědecká obec a úřady mají prakticky velmi malou možnost dohlížet nad fungováním algoritmů a jejich riziky. Platformy si své algoritmy zpravidla hlídají jako obchodní tajemství, stojí na nich totiž jejich komerční model. Ze strany států navíc může být poměrně obtížné přijít s funkčním systémem regulace, který by neomezoval svobodný projev. Většina velkých platform (jako je Facebook, Google nebo X) pochází z USA, kde je pojetí svobody projevu daleko širší než v evropském prostředí. Jedním z faktorů je historická zkušenost s totalitními režimy 20. století a koncept bránící se demokracie, který umožňuje projev v Evropě více omezovat. Pro platformy je americké pojetí velmi výhodné, mohou totiž obsah v podstatě nekontrolovaně moderovat, upřednostňovat příspěvky, které se jim hodí, a jiné mazat. Dokáží tak lépe pracovat s uživatelem, udržet ho na platformě, zobrazit mu reklamy a dostat za něj peníze. Navíc se nemusí zatěžovat dalšími byrokratickými povinnostmi, což rovněž šetří velké množství prostředků. V Evropě je však situace podstatně odlišná a široká argumentace svobodou projevu zde neobstojí, jak jsem ukázal na příkladu Google Shopping.

V Evropě podléhají platformy daleko širší regulaci než v USA, příčinou je právě rozdílné pojetí svobody projevu. Lze to vidět prakticky na všech případech, které jsem v textu rozvíjel. V Evropě funguje systém odpovědnosti ISP, který stanovuje mantinely mezi odpovědností platformy a uživatele. Zdůrazňuje odpovědnost platformy v případě, kdy závadný obsah neodstranila, ačkoli o něm věděla. Naopak americký princip dobrého samaritána vyžaduje pro odpovědnost „přispění“ a pokud jsou platformy v dobré víře, neodpovídají ani za závadný obsah, o kterém věděly. Podobné závěry lze pozorovat také u regulací zaměřených proti libovůli platforem v omezování obsahu uživatelů. Zatímco evropské státy začínají uplatňovat DSA, které mimo jiné umožňuje uživatelům „odvolání“ proti odstranění příspěvku, podobné zákony Texasu a Floridy přezkoumával Nejvyšší soud USA a zřejmě neobstojí před Prvním dodatkem.

Meta svým uživatelům umožňuje jistou formu revize skrze odvolací orgán Oversight Board, čímž se liší od dalších podobných společností. Přestože má tento systém mnoho podstatných nedostatků, jako je nedostatečná nezávislost nebo omezená vynutitelnost rozhodnutí, stále se jedná o zavedený model, ze kterého si lze odnést klíčové zkušenosti pro další rozhodovací praxi. OB je uživatelsky velmi přívětivá, veřejně publikuje svá rozhodnutí a informuje o nich veřejnost jednoduchou formou na sociálních sítích. Jak jsem ukázal na analýze vybraných rozhodnutí, její „judikatura“ je konzistentní, rozumná a poměrně dobře odůvodněná. Proto si z ní lze v některých aspektech vzít příklad třeba pro budoucí fungování nových subjektů pro mimosoudní řešení sporů podle čl. 21 DSA. Ideálně by pak měly orgány vzájemně spolupracovat a přispět k právní jistotě ve sporech mezi uživatelem a platformou.

Pro další vývoj regulace platforem budou z mého pohledu stěžejní dva aspekty. Prvním je postup současné administrativy Donalda Trumpa, která proti regulaci ostře vystupuje. Je proto otázkou, zda nebude vyžadovat po Evropě zmírnění regulace např. výměnou za bezpečnostní záruky, jak na-

značoval viceprezident Vance.¹⁶⁷ Tlak americké strany se objevil také v podobě jednání Výboru pro soudnictví amerického Kongresu.¹⁶⁸ Ta řešila, zda se jedná o nástroj cenzury, který omezuje americké společnosti. Proti zkratkovitým závěrům a neporozumění významu regulace v otevřeném dopise protestovali evropští akademici.¹⁶⁹

Druhým klíčovým aspektem je pak praktické uplatňování a vymáhání DSA v členských státech EU. Všechny nové instituty a instrumenty v Evropě teprve začínají působit a mohou přinést nové možnosti. Důležitým by mohlo být zkoumání systémových rizik vědeckými pracovníky, které může poskytnout větší vhled do celé problematiky algoritmické modrace. S ohledem na samotnou každodenní regulaci je potřeba zmínit nový institut důvěryhodných oznamovatelů a subjektů pro mimosoudní řešení sporů. Ty by měly uživatelům sloužit k efektivnějšímu vymáhání práv po platformách, které jsou vůči nim v nerovném postavení. Všechny tyto možnosti však podléhají aktivnímu přístupu regulátorů, kteří mají stanovená pravidla důsledně vymáhat. To může ztížit jejich nedostatečné personální a finanční zabezpečení, ale též podpora politických hráčů na unijní úrovni i mezi členskými státy.

¹⁶⁷ Viz KILANDER, Gustaf. JD Vance says US could drop support for NATO if Europe tries to regulate Elon Musk's platforms [online]. *The Independent*, 17. 09. 2024 [cit. 19. 11. 2025]. <https://www.independent.co.uk/news/world/americas/us-politics/jd-vance-elon-musk-x-twitter-donald-trump-b2614525.html>

¹⁶⁸ JAHANGIR, Ramsha, LIMA-STRONG, Cristiano. Transcript: US House Judiciary Hearing on Europe's Threat to American Speech and Innovation [online]. The Tech Policy Press, 4. 9. 2025 [cit. 20. 11. 2025]. <https://www.techpolicy.press/transcript-us-house-judiciary-hearing-on-europes-threat-to-american-speechand-innovation/>

¹⁶⁹ HUSOVEC, Martin. Open Letters by Academics on DSA and Censorship – Martin Husovec [online]. Martin Husovec, 05. 09. 2025 [cit. 19. 11. 2025]. <https://husovec.eu/2025/09/open-letters-by-academics-on-dsa-andcensorship/>

SEZNAM ZDROJŮ

KNIHY A KAPITOLY V KNIZE

- [1] BARTOŇ, Michal. *Svoboda projevu a její meze v právu ČR*. Praha: Linde, 2002.
- [2] DUTKIEWICZ, Lidia. Artificial Intelligence and Media. In: *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*. Cambridge: Cambridge University Press, 2025, s. 283-305.
- [3] GOLDSMITH, Jack, WU, Tim. *Kdo řídí Internet? Iluze o světě bez hranic*. Praha: Dokořán, Argo, 2008.
- [4] HUSOVEC, Martin. *Zodpovednosť na internete podľa českého a slovenského práva*. Praha: CZ.NIC, 2014.
- [5] CLOUPKOVÁ, Helena, HOLÝ, Petr, URBÁNEK, Jiří. *Mediální právo*. Praha: C. H. Beck, 2018.
- [6] MYŠKA, Matěj, KOUKAL, Pavel, VLACHOVÁ, Zuzana, WOZNICA, Ondřej. Liability of Hosting ISPs: the Czech Perspective. In: Szostek, D., Załucki, M. (eds). *Internet and New Technologies Law*. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 2021.
- [7] POLČÁK, Radim. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018.
- [8] POLČÁK, Radim. Zákaz cenzury jako zásah do svobody podnikání a svobody projevu internetových platforem. In: Šimíček, Vojtěch. (ed.). *Právo svobodně podnikat*. Praha: Leges, 2023, s. 95-109.
- [9] WAGENROVÁ, Eliška. Čl. 17 (Svobodný projev a právo na informace). In: Wagnerová, Eliška, Šimíček, Vojtěch, Langášek, Tomáš, Pospíšil, Ivo a kol. *Listina základních práv a svobod. Komentář*. Praha: Wolters Kluwer, 2012, s. 323-445.

ČLÁNKY V ODBORNÝCH ČASOPISECH

- [10] AMARIKWA, Melany. Social Media Platforms' Reckoning: The Harmful Impact of TikTok's Algorithm on People of Color. *Richmond Journal of Law & Technology*. 2023, roč. 29, č. 3, s. 69-144.
- [11] BERBEC, Adriana. To What Extent Can Online Service Providers Adopt Voluntary Content Moderation Measures without Losing Their Immunity Shields? A Comparative Analysis of Online Service Providers' Liabilities in the European Union and the United States. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*. 2024, č. 1, roč. 15, s. 13-37.
- [12] GHAVANI, Anna W., GRENDSTAD, Gunnar, SCHAFFER, Johan K. Institutions that define the policymaking role of courts: A comparative analysis of the supreme courts of Scandinavia. *International Journal of Constitutional Law*. 2023, č. 21, roč. 3, s. 770-797. <https://academic.oup.com/icon/article/21/3/770/7250119>

- [13] GULATI, Rishi. Meta's Oversight Board and Transnational Hybrid Adjudication - What Consequences for International Law? *German Law Journal*. 2023, č. 3, roč. 24, s. 473-493.
- [14] HANYCH, Monika, PIVODA, Marek. Facebook, Twitter a YouTube jako garanti svobodného projevu? Kritika současného systému notice-and-takedown. *Revue pro právo a technologie*. 2017, roč. 8, č. 16, s. 177-220.
- [15] HART, Jan. Svoboda projevu v USA a v Evropě. *Právní rozhledy*. 2002, roč. 10, č. 1, s. 28-32.
- [16] HELFER, Laurence R., LAND, Molly K. The Meta Oversight Board's Human Rights Future. *Cardozo Law Review*. 2023, č. 6, roč. 44, s. 2233-2300.
- [17] KIM, Ah Sang. Social Media Algorithms: Why You See What You See. *Georgetown Law Technology Review*. 2017, roč. 1, č. 2, s. 147-154.
- [18] KOLTAY, Andras. The Private Censorship of Internet Gatekeepers. *University of Louisville Law Review*. 2021, roč. 59, č. 255, s. 255-304.
- [19] MAZÚR, Jan, GRAMBLIČKOVÁ, Barbora. New Regulatory Force of Cyberspace: The Case of Meta's Oversight Board. *Masaryk University Journal of Law and Technology*. 2023, č. 1, roč. 17, s. 3-32.
- [20] McCABE, Brigid. A First Amendment Right to Censor: Social Media Regulation and Freedom of Speech in the NetChoice Cases. *Columbia Undergraduate Law Review*. 2024, č. 3, roč. 20, s. 28-49.
- [21] McINTOSH, Daniel. We Need to Talk about Data: How Digital Monopolies Arise and Why They Have Power and Influence. *Journal of Technology Law & Policy*. 2019, roč. 23, č. 2, s. 185-213.
- [22] MIZEROVÁ, Tina, HARAŠTA, Jakub. Dostupnost mediálního obsahu: blokování dezinformačních webů. *Právník*. 2023, roč. 162, s. 415-430.
- [23] POPPEOVÁ, Marie. Odpovědnost zprostředkovatelů za protiprávní projevy na internetu: Hrozí nám soukromá cenzura? *Časopis pro právní vědu a praxi*. 2023, č. 4, roč. 31, s. 870.
- [24] RATHJE, Steve. et al. People Think That Social Media Platforms Do (but Should Not) Amplify Divisive Content. *Perspectives on Psychological Science*. 2024, roč. 19, č. 5, s. 781-795.
- [25] THOMSON, Stephen. Into the Quagmire: Social Media as Regulators and the Limits of Judicial Review. *Public Law*. 2024, Oct, s. 695-718. Dostupné v systému Westlaw Edge UK.
- [26] TIEDEKE, Anna S., FERTMANN, Martin. A love triangle? Mapping Interactions between International Human Rights Institutions, Meta and Its Oversight Board. *European Journal of International Law*. 2023, roč. 34, č. 4, s. 907-938.
- [27] TYMOFEYEVA, Alla. Svoboda projevu právnických osob na internetu z pohledu Evropského soudu pro lidská práva. *Právník*. 2022, roč. 161, č. 2, s. 140-155.
- [28] VLČKOVÁ, Veronika. Svoboda projevu v USA. *Právník*. 2004, roč. 143, č. 3, s. 262-284.

[29] VÖLOKH, Eugene, FALK, Donald M. Google First Amendment for Search Engine Search Results. *Journal of Law, Economics & Policy*. 2012, roč. 8, č. 4, s. 883-899. <https://www2.law.ucla.edu/Volokh/searchengine.pdf>

[30] VÝBORNÝ, Štěpán. Koncept bránící se demokracie v judikatuře Ústavního soudu ČR. *Časopis pro právní vědu a praxi*. 2012, roč. 20, č. 2, s. 157-163.

ELEKTRONICKÉ A OSTATNÍ ZDROJE

[31] Benson, P. J. Moody v. NetChoice, LLC: The Supreme Court Addresses Facial Challenges to State Social Media Laws [online]. *Congressional Research Service*. 11. 11. 2024 [cit. 19. 2. 2025]. <https://crsreports.congress.gov/product/pdf/LSB/LSB11224>

[32] BILLY, Perrigo. Facebook's Oversight Board Is Reviewing Its First Cases. Critics Say It Won't Solve the Platform's Biggest Problems [online]. *Time*, 7. 12. 2020 [cit. 19. 2. 2025]. <https://time.com/5918499/facebook-oversight-board-cases/>

[33] BLAHOŠOVÁ, Jana, LEBEDÍKOVÁ, Michaela, TANCOŠ, Martin, PLHÁK, Jaromír, ŠMAHEL, David, ELAVSKÝ, Steriani, TKACZYK, Michal, SOTOLÁŘ, Ondřej. *Jak čeští adolescenti používají své mobily? Analýza dat z chytrých telefonů*. Brno: Masarykova univerzita, 2023 [cit. 19. 2. 2025]. https://irtis.muni.cz/media/3524142/wp4_report_jak-cesti-adolescenti-pouzivaji-sve-mobily.pdf

[34] BOOTH, Robert. Meta to get rid of factcheckers and recommend more political content [online]. *The Guardian*, 7. 1. 2024 [cit. 19. 2. 2025]. <https://www.theguardian.com/technology/2025/jan/07/meta-facebook-instagram-threads-mark-zuckerberg-remove-fact-checkers-recommend-political-content>

[35] *Criminal Allegations Based on Nationality*. Multiple Case Decision Oversight Board ze dne 25. 9. 2024. Plné znění je dostupné na <https://www.oversightboard.com/decision/bun-fjipx1xo/> [cit. 19. 2. 2025].

[36] DODSON, Samantha. Balancing Act: Navigating First Amendment Rights and Online Content Regulation [online]. *Juris Mentem Law Review*. 14. 11. 2024 [cit. 19. 2. 2025]. https://aura.american.edu/articles/journal_contribution/Balancing_Act_Navigating_First_Amendment_Rights_and_Online_Content_Regulation/27738678?file=50496804

[37] Evropská komise. Commission fines X €120 million under the Digital Services Act [online]. Tisková zpráva ze dne 5. 12. 2025 [cit. 24. 3. 2026]. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934

[38] Evropská komise. Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram Act [online]. Tisková zpráva ze dne 5. 12. 2025 [cit. 24. 3. 2026]. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664

[39] Facebook. Podmínky používání služby [online]. *Facebook* [cit. 19. 2. 2025]. <https://www.facebook.com/legal/terms/update>

- [40] FISHER, Max. Inside Facebook's Secret Rulebook for Global Political Speech [online]. *The New York Times*, 27. 12. 2018 [cit. 19. 3. 2025]. <https://www.nytimes.com/2018/12/27/world/facebook-moderators.html>
- [41] *Former President Trump's suspension*, Standard Decision Oversight Board ze dne 5. 5. 2021. Plné znění je dostupné zde: <https://www.oversightboard.com/decision/fb-691qamhj/> [cit. 19. 2. 2025].
- [42] *Holocaust Denial*. Standard Decision Oversight Board ze dne 23. 1. 2024. Plné znění dostupné na <https://www.oversightboard.com/decision/ig-zj7j6d28/> [cit. 19. 2. 2025].
- [43] HOLZNAGEL, Daniel. Art. 21 DSA Has Come to Life [online]. *Verfassungsblog*. 5. 11. 2024 [cit. 19. 3. 2025]. <https://verfassungsblog.de/art-21-dsa-fundamental-rights-certification/>
- [44] HUSOVEC, Martin. Open Letters by Academics on DSA and Censorship – Martin Husovec [online]. Martin Husovec, 05. 09. 2025 [cit. 19. 11. 2025]. <https://husovec.eu/2025/09/open-letters-by-academics-on-dsa-andcensorship/>
- [45] JAHANGIR, Ramsha, LIMA-STRONG, Cristiano. Transcript: US House Judiciary Hearing on Europe's Threat to American Speech and Innovation [online]. The Tech Policy Press, 4. 9. 2025 [cit. 20. 11. 2025]. <https://www.techpolicy.press/transcript-us-house-judiciary-hearing-on-europes-threat-to-american-speech-and-innovation/>
- [46] JOLER, Vladan, PETROVSKI, Andrej. Human Data Banks and Algorithmic Labour [online]. *labs.rs*, 20. 8. 2016 [cit. 19. 2. 2025]. <https://labs.rs/en/facebook-algorithmic-factory-human-data-banks-and-algorithmic-labour/>
- [47] JONES, Zoe C. Facebook bans Trump for the rest of his presidency [online]. *BBC*, 7. 1. 2021 [cit. 19. 2. 2025]. <https://www.cbsnews.com/news/facebook-bans-trump-joe-biden-president-inauguration/>
- [48] KARI, Paul. Elon Musk reportedly forced Twitter algorithm to boost his tweets after Super Bowl flop [online]. *The Guardian*, 15. 2. 2023 [cit. 19. 2. 2025]. <https://www.theguardian.com/technology/2023/feb/15/elon-musk-changes-twitter-algorithm-super-bowl-slump-report>
- [49] KILANDER, Gustaf. JD Vance says US could drop support for NATO if Europe tries to regulate Elon Musk's platforms [online]. *The Independent*, 17. 09. 2024 [cit. 19. 11. 2025]. <https://www.independent.co.uk/news/world/americas/us-politics/jd-vance-elon-musk-x-twitter-donald-trump-b2614525.html>
- [50] Meta. Corporate Human Rights Policy [online]. *Meta* [cit. 19. 2. 2025]. <https://about.fb.com/wp-content/uploads/2021/03/Facebooks-Corporate-Human-Rights-Policy.pdf>
- [51] Meta. Zásady komunity. *Meta* [cit. 24. 3. 2026]. <https://transparency.meta.com/cs-cz/policies/community-standards/>
- [52] Meta. Zásady komunity: Jak technologie pomáhá upřednostňovat případy ke kontrole. *Meta* [cit. 19. 2. 2025]. <https://transparency.meta.com/cs-cz/enforcement/detecting-violations/technology-helps-prioritize-review/>

- [53] Meta. Zásady komunity: nenávistné chování. *Meta* [cit. 19. 2. 2025]. <https://transparency.meta.com/en-gb/policies/community-standards/hateful-conduct/>
- [54] Meta. Zásady komunity: Obsah, u kterého bylo podáno odvolání. *Meta* [cit. 19. 2. 2025]. <https://transparency.meta.com/cs-cz/policies/improving/appealed-content-metric/>
- [55] NMS Market Research. *Kde si Češi hledají informace? Vedou internetová média. Sociální sítě využívá třetina lidí v Česku* [online]. Tisková zpráva ze dne 5. 11. 2024 [cit. 19. 2. 2025]. <https://nms.global/cz/kde-si-cesi-hledaji-informace-vedou-internetova-media-socialni-site-vyu-ziva-tretina-lidi-v-cesku/>
- [56] Out-of-court dispute settlement bodies under the Digital Services Act (DSA) [online]. *European Commission* [cit. 24. 3. 2026]. <https://digital-strategy.ec.europa.eu/en/policies/dsa-out-court-dispute-settlement>
- [57] Oversight Board. 2023 Annual Report [online]. *Oversight Board* [cit. 19. 2. 2025]. <https://www.oversightboard.com/wp-content/uploads/2024/06/Oversight-Board-2023-Annual-Report.pdf>
- [58] Oversight Board. Oversight Board Charter [online]. *Oversight Board* [cit. 19. 2. 2025]. https://www.oversightboard.com/wp-content/uploads/2024/03/OB_Charter_March_2024.pdf
- [59] *Politician's Comments on Demographic Change*. Standard Decision Oversight Board ze dne 12. 3. 2024. Plné znění dostupné na <https://www.oversightboard.com/decision/fb-ofs963dz/> [cit. 19. 2. 2025].
- [60] *Post in Polish Targeting Trans People*. Standard Decision Oversight Board ze dne 16. 1. 2024. Plné znění dostupné na <https://www.oversightboard.com/decision/fb-uk2rus24/> [cit. 19. 2. 2025].
- [61] *Posts That Include "From the River to the Sea"*. Multiple Case Decision Oversight Board ze dne 4. 9. 2024. Plné znění je dostupné na <https://www.oversightboard.com/decision/bun-86tj0rk5/> [cit. 19. 2. 2025].
- [62] *Removal of COVID-19 misinformation*. Published Advisory Opinion Oversight Board ze dne 20. 4. 2023. Plné znění dostupné zde: <https://www.oversightboard.com/decision/pao-sabu4p2s/> [cit. 19. 2. 2025].
- [63] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression A/74/486 ze dne 9. 10. 2019. *United Nations General Assembly* [cit. 19. 2. 2025]. <https://docs.un.org/en/A/74/486>
- [64] ROSE, Steve. A deadly ideology: how the 'great replacement theory' went mainstream [online]. *The Guardian*, 8. 6. 2022 [cit. 19. 2. 2025]. <https://www.theguardian.com/world/2022/jun/08/a-deadly-ideology-how-the-great-replacement-theory-went-mainstream>
- [65] SOLEA, Anda Iulia. How a little-known far-right candidate manipulated TikTok to rise to the top in the Romanian election [online]. *University of Portsmouth*, 29. 11. 2024 [cit. 19. 2. 2025]. <https://www.port.ac.uk/news-events-and-blogs/blogs/academic-expertise/how-a-little-known-far-right-candidate-manipulated-tiktok-to-rise-to-the-top-in-the-romanian-election>

[66] Supervision of the designated very large online platforms and search engines under DSA [online]. *European Commission* [cit. 18. 3. 2025]. <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>

[67] United Nations. Guiding Principles on Business and Human Rights. 2011 [cit. 19. 2. 2025]. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

[68] WANG, VIVIAN. How Does DeepSeek's A.I. Chatbot Navigate China's Censors? Awkwardly [online]. *The New York Times*. 19. 1. 2025 [cit. 19. 2. 2025]. <https://www.nytimes.com/2025/01/29/world/asia/deepseek-china-censorship.html>

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/RPT2026-1-3>

DOMESTIC PARTNERSHIP OF CAMPOS & MUNOZ: KDO ODPOVÍDÁ ZA VYHALUCINOVANÉ PRECEDENTY?

JAN MARTÍNEK¹

Soud: Odvolací soud, čtvrtý odvolací okres, první oddělení, stát Kalifornie, USA
Věc: Domestic Partnership of Campos & Munoz (D085584)
Datum: 5. 3. 2026
Dostupnost: law.justia.com

1. SKUTKOVÝ STAV

Základem celého sporu byl rozvod Campose a Munoz, o kterém dříve rozhodl rodinný soud. V rozsudku se vypořádal s jejich jméním, ale nijak nerozhodl o jejich domácích mazlíčcích. O dva roky později požádal Campos soud o nařízení sdílené péče a určení návštěv jejich psa.²

2. PRŮBĚH ŘÍZENÍ

Na žádost reagovala Munoz, kterou bezplatně zastupovala její sestřenice, advokátka Bonar. Odmítla Camposovy nároky a odkázala na dva precedenty. První případ „*Manželství Twigg*“ měl dokládat, že emoční blahobyt zúčastněných stran má být určujícím prvkem při stanovení péče. „*Manželství Teegarden*“ směřovalo na důležitost udržení psychické stability ope-

¹ Mgr. Jan Martínek je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity a analytikem Ústavního soudu. Kontaktní e-mail: 508778@muni.cz. ORCID 0009-0008-3151-2259.

² Viz str. 2 anotovaného rozhodnutí.

čovávaných osob.³ Ani jeden z případů nebyl skutečný. *Twigg* vůbec neexistoval a citace odkazovala na nesouvisející trestněprávní případ. Skutečný *Teegarden* pak neodpovídal citaci a řešil nesouvisející otázku výživného mezi manžely.⁴

Ve svém podání Munoz uvedla, že má psa v péči. Odkazovala se na rozhodnutí *Twigg*, které mělo podpořit důraz na její psychické zdraví jako hlavní pečující osoby. S Camposem se vídat nechtěla, střídavá péče by pro ni byla náročná. Campos její důvody rozporoval. Neupozornil však na to, že případ *Twigg* není skutečný.⁵ Soudce vyslechl při líčení obě strany, návštěvy ani střídavou péči nenařídil. Právní zástupce Campose následně na příkaz soudu vyhotovil návrh závěrů z jednání, který soud potvrdil. Návrh cituje oba neexistující precedenty.⁶ Campos se následně odvolal.⁷

Ve vyjádření k odvolání Munoz opět citovala oba neexistující případy. Ve svém druhém podání Campos poprvé upozornil na to, že jsou smyšlené.⁸ Proti tomu protestovala advokátka Bonar a obvinila Campose z neschopnosti používat právní informační systémy. Oba případy zopakovala a doplnila k nim další informace. Uvedla, že chyba v citaci neodůvodňuje nařčení z nesplnění povinností obhájce.⁹ I nově poskytnuté detaily byly fiktivní.

Odvolací soud proto nařídil Bonar poskytnout kopii obou rozhodnutí, ze kterých vychází. Ve své odpovědi Bonar poprvé přiznala, že precedenty neexistují.¹⁰ Údajně si nevzpomínala, jestli z nich vycházela při prvním líčení. Uznala, že si dostatečně neověřila citaci rozhodnutí před odvolacím soudem. Její informace o případu *Twigg* měly pocházet z článku na sociální

³ Viz str. 3 anotovaného rozhodnutí.

⁴ Tamtéž.

⁵ Viz str. 4 anotovaného rozhodnutí.

⁶ Viz str. 4-5 anotovaného rozhodnutí.

⁷ Viz str. 5 anotovaného rozhodnutí.

⁸ Viz str. 5 anotovaného rozhodnutí.

⁹ Viz str. 6-7 anotovaného rozhodnutí.

¹⁰ Viz str. 7 anotovaného rozhodnutí.

síti Reddit.¹¹ Ten však neobsahoval kompletní citace, pouze název údajného rozhodnutí. Původ ostatních informací advokátka nevysvětlila.

Soud jí následně zaslal výzvu k vyjádření, proč by jí neměl udělit sankci za falešné citování a argumentaci neexistujícími precedenty.¹² Na svou obranu pouze uvedla, že to neudělala s úmyslem někoho poškodit a že její chyba nezpůsobila žádnou újmu.¹³ Dále se odvolávala na závěry soudu prvního stupně, kterými se údajně řídila. Soud uzavřel, že Bonar stále nevysvětlila původ dodatečných informací, které se objevily až před odvolacím soudem. Během ústního líčení pouze uvedla, že si nevzpomíná, odkud je čerpala. Uznala, že nedisponuje předplatným právních informačních služeb a při přípravě používala jiné internetové služby včetně AI. Připustila, že fiktivní informace o případech *Twigg* a *Teegarden* mohla získat pomocí AI nástrojů.¹⁴

3. KLÍČOVÉ OTÁZKY

V odvolacím řízení se soud zabýval třemi základními otázkami. První dvě souvisely s odvolacími důvody Campose a třetí s pochybením advokátky Bonar. Soud řešil, zda je rozhodnutí soudu prvního stupně neplatné, pokud se opírá o fiktivní precedenty a zda může odvolací soud přezkoumat důvody pro rozhodnutí soudu prvního stupně, pokud chybí přepis z jednání. Ve vztahu k Bonar řešil, jaké sankce hrozí advokátům v souvislosti s argumentací neexistující judikaturou.

4. PRÁVNÍ ÚPRAVA

Soud vzal v úvahu pravidla stanovená zákonem o rodině,¹⁵ pravidla pro výkon advokátní profese a související precedenty. Důležitá byla především povinnost advokáta využívat pouze prostředky slučitelné s pravdou a nesnažit

¹¹ Viz str. 8 anotovaného rozhodnutí.

¹² Tamtéž.

¹³ Viz str. 9 anotovaného rozhodnutí.

¹⁴ Tamtéž.

¹⁵ Family Code section 2605, viz str. 10 a 14 anotovaného rozhodnutí.

se uvést soudce v omyl nepravdivým tvrzením¹⁶ a zákaz vědomě uvádět nepravdivá tvrzení o právu nebo citovat fiktivní autority.¹⁷

5. POUŽITÍ PRÁVNÍ ÚPRAVY NA SKUTKOVÝ STAV

5.1 CAMPOS NEVZNESL NÁMITKU NEEEXISTUJÍCÍCH PRECEDENTŮ VČAS

Podle Campose soud prvního stupně pochybil, když při rozhodování spoléhal na fiktivní precedenty.¹⁸ Odvolací soud s tím souhlasil a uvedl, že soudy si musí vždy ověřit citace jednotlivých případů ve svých rozhodnutích. A to i pokud vychází z návrhů stran. Spoléhání se na falešné případy je totiž v rozporu s obecnými principy práva.¹⁹ Odvolací soud vytknul pouze formu postupu, nepředjímal potenciální výsledek sporu.²⁰

Zároveň odvolací soud zohlednil kontext současného případu. Campos totiž mohl vznést svůj argument již v prvním řízení. Platí, že v odvolacím řízení nemohou strany vznášet nové argumenty, které již mohly uplatnit dříve. Soud navíc připomněl, že sám Camposův obhájce navrhoval znění soudního rozhodnutí, měl tedy dostatek možností ověřit si citace daných rozhodnutí.²¹ Ostatně povinností advokáta je osobně číst a ověřit citace ve všech podáních, které soudu předkládá. Strany musí upozornit soud na chyby v okamžiku, kdy je ještě může napravit.²² Pokud by Campos vznesl své výhrady včas, k pochybení by nedošlo.²³

Dále Campos nesouhlasil s důvody rozhodnutí v otázce stanovení péče o psa. Soud uzavřel, že Campos neunesl své důkazní břemeno. Ke svému

¹⁶ Business and Professions Code section 6068(d), viz str. 17 anotovaného rozhodnutí.

¹⁷ California Rules of Professional Conduct, rule 3.3, Viz str. 17 anotovaného rozhodnutí.

¹⁸ Viz str. 10 anotovaného rozhodnutí.

¹⁹ Viz str. 10-11 anotovaného rozhodnutí.

²⁰ Viz str. 11 anotovaného rozhodnutí.

²¹ Viz str. 12 anotovaného rozhodnutí.

²² Viz str. 13 anotovaného rozhodnutí.

²³ Viz str. 14 anotovaného rozhodnutí.

odvolání nepřiložil přepis jednání před soudem prvního stupně. Nešlo tedy ověřit, že svou argumentaci vznesl už v prvním řízení.²⁴

5.2 BONAR PORUŠILA POVINNOSTI ADVOKÁTKY

Soud nejprve připomněl povinnosti spojené s povoláním advokáta, především neuvádět soud v omyl nepravdivými tvrzeními.²⁵ Spoléhání se na neexistující právní zdroje lze proto sankcionovat. Bonar uznala, že fiktivní případ *Teegarden* zřejmě vygenerovala AI a případ *Twigg* převzala z diskuze na Redditu. Autor daného příspěvku nebyl advokátem a Bonar si pravdivost informací neověřila.²⁶ Podle odvolacího soudu šlo o neodůvodněné porušení pravidel.

Bonar svou pozici ještě zhoršila, když v odvolacím řízení obhajovala oba případy. Vydávala je za platné a publikované precedenty Nejvyššího soudu Kalifornie a nepřiznala, odkud skutečně pochází.²⁷ Naopak k nim doplnila další smyšlené detaily, které neobsahoval článek na Redditu ani rozhodnutí soudu prvního stupně. Když protistrana nezvládla případy najít, obvinila ji Bonar z neschopnosti provádět základní právní rešerši.²⁸

Bonar tak porušila své povinnosti: uvedla soud v omyl a citovala falešné právo. Soud její chování poměřoval s jinými případy, ve kterých se objevily špatné citace. V současném případě se však Bonar provinila podstatně závažněji. Poskytla soudu nepravdivé informace, na kterých trvala a rozšiřovala je o další nepravdy. Přitom celou dobu věděla, že jsou neověřené. Ani v závěru sporu nevysvětlila, odkud citace a informace pocházejí. Pouze podotkla, že mohou pocházet z AI nástrojů.²⁹

²⁴ Soud podrobně zkoumal použití zákona o rodině, v podrobnostech viz str. 14-17 anotovaného rozhodnutí.

²⁵ Viz str. 17 anotovaného rozhodnutí.

²⁶ Viz str. 18 anotovaného rozhodnutí.

²⁷ Tamtéž.

²⁸ Viz str. 19 anotovaného rozhodnutí.

²⁹ Viz str. 20 anotovaného rozhodnutí.

6. SHRNUÍ ROZHODNUTÍ

V anotovaném případě soud prvního stupně pochybil, když své rozhodnutí opřel o neexistující precedenty.³⁰ Chybu však udělal také odvolatel, který soud na problém včas neupozornil. Jeho vlastní obhájce navíc smyšlené případy zahrnul do návrhu rozhodnutí soudu.³¹ Odvolací soud proto z procesních důvodů ponechal původní rozhodnutí v platnosti.³²

Zároveň potrestal advokátku protistrany, která s neexistujícími případy přišla. Podle odvolacího soudu hrubě porušila své povinnosti.³³ Udělil jí proto pokutu ve výši 5 000 USD. Kopii svého rozhodnutí přeposlal advokátní komoře a nařídil advokátce, aby komoru sama informovala o udělené sankci.³⁴

7. ZÁVĚR A MOŽNÝ PŘESAŇ DO ČESKÉHO PROSTŘEDÍ

Velké jazykové modely a především AI chatboty se během posledních let stávají nedílnou součástí každodenního života. Nevyhýbají se právnické profesi a už vůbec ne justici. Vygenerovaná podání, návrhy smluv a jiné právní texty budou přibývat. Důkazem je databáze *AI Hallucination Cases*,³⁵ na kterou již upozornil Harašta.³⁶ Přibývají v ní soudní rozhodnutí, kde se soudy musely nějakým způsobem vypořádat s halucinacemi. Databáze obsahuje také anotovaný případ.

Současný trend se nevyhýbá ani českým soudům. Citace neexistujících případů v kasační stížnosti řešil v říjnu 2025 Nejvyšší správní soud.³⁷ S nesouvislou argumentací stěžovatele se tehdy vypořádal, ale z rozhodnutí je znát odpor soudu vůči podobným podáním.³⁸ Ústavní soud byl o dva mě-

³⁰ Viz str. 11 anotovaného rozhodnutí.

³¹ Viz str. 12 anotovaného rozhodnutí.

³² Viz str. 14 anotovaného rozhodnutí.

³³ Viz str. 19-20 anotovaného rozhodnutí.

³⁴ Viz str. 20 anotovaného rozhodnutí.

³⁵ Databáze je přístupná na adrese <https://www.damiencharlotin.com/hallucinations/>

³⁶ Viz Harašta, J. Halucinované citace v kasační stížnosti. *Revue pro právo a technologie*. 2025, roč. 16, č. 32, s. 125.

³⁷ Viz rozsudek Nejvyššího správního soudu sp. zn. 3 As 34/2025 - 80 ze dne 15. 10. 2025.

³⁸ Blíže viz anotace J. Harašty citovaná výše.

síce později méně vstřícný.³⁹ Za ústavní stížnost s neexistujícími spisovými značkami udělil advokátovi pořádkovou pokutu ve výši 25 000 Kč. Uvedl, že podobná podání mohou soud nesmyslně zatěžovat.⁴⁰

Soudy se musí naučit na podobné situace reagovat. Jinak může hrozit jejich přehlčení a postupná destrukce právního systému, jak naznačil anotovaný případ. Ve svých závěrech přitom nabízí jedno z možných řešení. Pracuje s modelem, kdy vyhalucinované citace měl odhalit jakýkoli účastník řízení, včetně protistrany. Účastníci mají soudu pomoci v odhalování podobných chyb, jinak jim soud buď nemusí vyhovět, nebo jim může přímo udělit sankci. Soud navíc zohlednil intenzitu zavinění jednotlivých stran. Protistraně „pouze“ nevyhověl, protože měla halucinace odhalit včas. Naproti tomu advokátce/původkyni halucinací přiznal vysokou pokutu a upozornil advokátní komoru na její selhání. Jako přítěžující okolnost zohlednil neochotu advokátky objasnit, odkud neexistující případy pochází.

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>).

³⁹ Viz usnesení Ústavního soudu sp. zn. I. ÚS 3004/25 ze dne 1. 12. 2025.

⁴⁰ Viz bod 4 usnesení.

<https://doi.org/10.5817/RPT2026-1-4>

PŘEHLED AKTUÁLNÍ JUDIKATURY I/2026

*ANNA BLECHOVÁ, MARTIN ERLEBACH, JAKUB HARAŠTA, ANEŽKA
KARPJÁKOVÁ, PAVEL LOUTOCKÝ, TINA MIZEROVÁ, KRISTÝNA
MLČÁKOVÁ, MARTIN PLÁŠEK*

1. SOUKROMÍ A OSOBNÍ ÚDAJE

OSOBNÍ ÚDAJE ZÍSKANÉ PROSTŘEDNICTVÍM KAMERY REVIZORŮ JÍZDENEK VE VEŘEJNÉ DOPRAVĚ

Soud: Soudní dvůr Evropské unie
Věc: C-422/24
Datum: 18. 12. 2025
Dostupnost: curia.europa.eu

Společnost SL¹ je společností působící v oblasti veřejné dopravy ve Stockholmu. Společnost vybavila své revizory osobními kamerami, jejichž účelem bylo dokumentování vyhrocených situací a ověřování totožnosti osob, které odmítaly zaplatit pokutu v případě, kdy neměly platnou jízdenku.² Revizoři mají kamery zapnuté celou směnu a zaznamenaný obsah se automaticky maže po jedné minutě, tuto funkci však mohou revizoři vypnout v určitých případech.³

Švédský Úřad pro ochranu osobních údajů prověřoval, zda společnost SL neporušuje GDPR.⁴ Úřad dospěl k závěru, že společnost SL neposkytla sub-

¹ Společnost AB Storstockholms Lokaltrafik.

² Body 2 a 8 anotovaného rozhodnutí.

³ Body 9 a 10 anotovaného rozhodnutí.

⁴ Bod 9 anotovaného rozhodnutí.

jektům údajů dostatečné informace. Společnosti tak byla uložena pokuta za porušení čl. 13 GDPR.⁵ Společnost SL podala žalobu ke Správnímu soudu, ten ji však zamítl.⁶ Společnost se tedy odvolala ke Správnímu odvolacímu soudu. Ten zrušil rozsudek soudu prvního stupně i Úřadu s argumentací, že čl. 13 se v daném případě neaplikuje, a Úřad tak nebyl oprávněn pokutu uložit.⁷ Úřad proti rozsudku podal kasační opravný prostředek k Nejvyššímu správnímu soudu a dovolával se zrušení odvolacího rozsudku.⁸

Předběžná otázka se týkala výkladu čl. 13 a 14 GDPR⁹. Oba články se věnují problematice informování subjektů údajů, článek 13 se vztahuje na situace, kdy osobní údaje byly získány od samotného subjektu údajů, pokud nikoliv, aplikuje se čl. 14.¹⁰

Soudní dvůr v případě této otázky akcentoval, že pojem získání údajů ve smyslu čl. 13 GDPR nevyžaduje zvláštní úkon od subjektu údajů, pouze od správce.¹¹ Dále upozornil na skutečnost, že cílem GDPR je zajištění ochrany osobních práv fyzických osob a je potřeba vykládat GDPR ve světle tohoto účelu.¹² Relevantním kritériem pro určení působnosti předmětných článků je pouze zdroj osobních údajů.¹³ Z uvedeného vyplývá, že výklad svědčí ve prospěch aplikace čl. 13 GDPR pro situaci, kdy osobní údaje jsou získány prostřednictvím osobních kamer revizorů, a to proto, že údaje jsou získávány přímo od subjektu údajů.¹⁴ V případě připuštění aplikace čl. 14 by subjekt údajů neobdržel žádnou informaci o získávání jeho údajů,

⁵ Bod 11 anotovaného rozhodnutí.

⁶ Bod 12 anotovaného rozhodnutí.

⁷ Bod 13 anotovaného rozhodnutí.

⁸ Bod 14 anotovaného rozhodnutí.

⁹ 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.

¹⁰ Bod 29 anotovaného rozhodnutí.

¹¹ Bod 33 anotovaného rozhodnutí.

¹² Bod 40 anotovaného rozhodnutí.

¹³ Bod 35 anotovaného rozhodnutí.

¹⁴ Bod 36 anotovaného rozhodnutí.

subjekt by tak vůbec netušil, že jsou shromažďovány jeho osobní údaje.¹⁵ Tato situace by byla v hrubém rozporu s účelem nařízení GDPR.

Soudní dvůr tak dospěl k závěru, že v daném případě se aplikuje čl. 13 GDPR.

Autorka: KM

**„BEZPLATNÉ" NEWSLETTERY JAKO PŘÍMÝ MARKETING: SDEU
POTVRZUJE, ŽE POJEM „PRODEJ" MŮŽE BÝT SPOJEN
I S NEPŘÍMOU ODMĚNOU**

Soud: Soudní dvůr Evropské unie

Věc: C-654/23

Datum: 13. 11. 2025

Dostupnost: curia.europa.eu

Společnost *Inteligo Media* je vydavatelem on-line tiskové publikace *avocatnet.ro*¹⁶, na které její uživatele mohli získat šest bezplatných článků měsíčně. Pro přístup k dalšímu obsahu si uživatelé vytvořili bezplatný účet registrací své e-mailové adresy a přijetím podmínek „služby Premium“. Tím získali dva další bezplatné články a bezplatný denní e-mailový newsletter s názvem „Personal Update“. Ten obsahoval redakčně zpracované legislativní změny s hypertextovými odkazy na bezplatné články, ale také odkazy na placený obsah. Newsletter byl koncipován tak, aby uživatele motivoval k zaplacení přístupu k plné verzi. Placené předplatné zpřístupnilo veškerý obsah a obsáhlejší newsletter.¹⁷ Uživatelé měli možnost newsletter při registraci zaškrtnutím příslušného políčka v registračním formuláři odmítnout. Alternativně pak mohli odběr odhlásit při každém obdržení newsletteru skrze tlačítko „Odhlásit odběr“.¹⁸ Rumunský úřad pro ochranu osobních údajů (ANSPDCP) dne 26. září 2019 uložil společnosti pokutu ve výši přibližně 9 000 EUR za nezákonné zpracování osobních údajů (e-

¹⁵ Bod 41 anotovaného rozhodnutí.

¹⁶ Bod 20 anotovaného rozhodnutí.

¹⁷ Bod 21 anotovaného rozhodnutí.

¹⁸ Bod 22 anotovaného rozhodnutí.

mail, heslo, uživatelské jméno) 4 357 uživatelů bez souhlasu podle GDPR, přičemž konstatoval, že údaje byly využity nad rámec původního smluvního účelu.¹⁹

Spor se dostal po částečném potvrzení závěrů ANSPDCP soudy nižší instance až k Odvolacímu soudu v Bukurešti (Curtea de Apel București). Ten požádal SDEU o objasnění, zda praxe společnosti Inteligo spočívající v zasílání bezplatných newsletterů spadá pod výjimku *soft opt-in* ve čl. 13 Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (dále jen „ePrivacy směrnice“). Jinými slovy, soud zkoumal, zda byly e-mailové adresy získány „v souvislosti s prodejem produktu nebo služby“ a představoval newsletter „přímý marketing vlastních obdobných produktů nebo služeb“ ve smyslu čl. 13 odst. 2 směrnice ePrivacy. Následně se soud tázal, zda se v takovém případě uplatní rovněž podmínky zákonnosti zpracování podle čl. 6 odst. 1 GDPR.²⁰

Klíčovým ustanovením je v této souvislosti čl. 13 odst. 1 ePrivacy směrnice, který stanovuje povinnost předchozího souhlasu pro zasílání e-mailů za účelem přímého marketingu. Článek 13 odst. 2 následně vytváří výjimku „soft opt-in“, která se uplatní v případě, že kontaktní údaje byly získány v souvislosti s prodejem produktu nebo služby, marketing se týká vlastních obdobných produktů odesílatele a marketingový e-mail je možné snadno odhlásit (buď při shromáždění údajů nebo v každé marketingové zprávě). Dle čl. 95 GDPR je pak zabráněné ukládání dalších povinností podle GDPR tam, kde jsou stanovené specifické povinnosti jiným právním předpisem.²¹

SDEU v tomto případě dospěl k závěru, že newsletter představuje „přímý marketing“²² navzdory svému informativnímu obsahu²³, neboť jeho účel,

¹⁹ Bod 23 anotovaného rozhodnutí

²⁰ Body 29-33 anotovaného rozhodnutí.

²¹ Body 3-14 anotovaného rozhodnutí.

²² Jak bylo objasněno v předchozí judikatuře (StWL, C-102/20), tento pojem zahrnuje sdělení sledující komerční účel, adresovaná přímo a individuálně spotřebiteli.

²³ Bod 44 anotovaného rozhodnutí.

nikoli obsah, je komerční.²⁴ Newsletter směřuje uživatele k vyčerpání bezplatných kvót a k předplacení.²⁵ K otázce výkladu termínu „v souvislosti s „prodejem““ SDEU konstatoval, že prodej je označuje pojem, kdy dochází zaplacení ceny výměnou za službu.²⁶ Nicméně SDEU dodal, že odměnu za službu poskytovanou poskytovatelem v rámci jeho hospodářské činnosti nemusí nutně hradit osoby, které z ní mají prospěch. Postačuje nepřímá úplata, kdy jsou náklady bezplatné služby zahrnuty v ceně předplatného. Adresy tak byly získány „v souvislosti s prodejem.“ Ačkoli čl. 13 odst. 2 jako výjimka z obecného pravidla vyžaduje striktní výklad, taková striktnost nemůže zmařit jeho účinnost.²⁷ K druhé otázce Soudní dvůr s použitím čl. 95 GDPR shledal, že čl. 13 odst. 2 ePrivacy směrnice komplexně upravuje podmínky, účely a práva subjektů údajů, a ukládá tak „specifické povinnosti,“ takže čl. 6 odst. 1 GDPR se nepoužije.²⁸

Závěrem lze konstatovat, že bezplatné newslettery mohou představovat formu přímého marketingu, registrace bezplatného účtu může být kvalifikována jako „prodej“ prostřednictvím nepřímé úplaty, což výrazně rozšiřuje výklad a působnost čl. 13 odst. 2. Pokud se čl. 13 odst. 2 uplatní, není zapotřebí již aplikovat podmínky zákonného zpracování osobních údajů dle čl. 6 GDPR.

Pokud jde o širší dopady tohoto rozhodnutí, je třeba zdůraznit posun ve vnímání podstaty přímého marketingu a prodeje. Zároveň je třeba zmínit, že ačkoli rozsudek poskytuje jasné právní vodítko pro modely typu freemium, není ho možné vnímat jako univerzální pravidlo pro veškeré „bezplatné“ newslettery. Skutečně bezplatné služby bez jakékoli placené úrovně se tak nachází stále v určitém právním vakuu. Co se týče vztahu s GDPR, jak bylo zmíněno výše, rozhodnutí lze číst tak, že směrnice ePrivacy „vytěšňuje“ ustanovení GDPR. V neposlední řadě je třeba zdůraznit, že i když pro samotný akt odeslání newsletteru není zapotřebí samo-

²⁴ Bod 63 anotovaného rozhodnutí.

²⁵ Bod 45 anotovaného rozhodnutí.

²⁶ Bod 53 anotovaného rozhodnutí.

²⁷ Body 54-57 anotovaného rozhodnutí.

²⁸ Body 64-69 anotovaného rozhodnutí.

statného posouzení zákonnosti podle GDPR, zpracování předcházející odeslání (shromažďování údajů, profilování, transparentnost, posouzení oprávněných zájmů) stále vyžaduje aplikaci GDPR.

Autorka: AB

VZTAH BEZPEČNÉHO PŘÍSTAVU A GDPR PRO POSKYTOVATELE ZPROSTŘEDKOVATELSKÝCH SLUŽEB

Soud: Soudní dvůr Evropské unie

Věc: C-492/23

Datum: 2. 12. 2025

Dostupnost: curia.europa.eu

V původním sporu byl na online tržiště provozovaného společností Russmedia Digital SRL (dále jen „Russmedia“) anonymním uživatelem nahrán inzerát indikující, že paní X poskytuje sexuální služby za úplatu. To se stalo bez vědomí a souhlasu paní X. Jakmile se paní X o inzerátu dozvěděla, vyzvala s odkazem na GDPR²⁹ provozovatele portálu, aby inzerát stáhl, jelikož je založen na protiprávním zpracování jejích osobních údajů a narušuje její osobnostní práva. Inzerát byl do hodiny stažen, ovšem některé další webové stránky v mezích tento stejný inzerát přebíraly, a byl tedy nadále volně dostupný, ovšem mimo kontrolu Russmedia.³⁰

Za toto zveřejnění škodlivého inzerátu musela společnost Russmedia zaplatit odškodné ve výši 7000 euro. Jádrem sporu ovšem je, zda společnost Russmedia neměla být odpovědná také za porušení GDPR,³¹ jak tvrdí paní X, nebo zda se na situaci uplatní výjimka z odpovědnosti pro poskytovatele

²⁹ 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 (obecné nařízení o ochraně osobních údajů).

³⁰ Bod 31 anotovaného rozhodnutí.

³¹ Bod 32 anotovaného rozhodnutí.

zprostředkovatelských služeb podle e-commerce směrnice,³² která byla provedena do národního práva.

V tomto smyslu tedy i příslušný národní soud směřoval své předběžné otázky na Soudní dvůr Evropské unie. Konkrétně bylo smyslem těchto otázek zjistit, zda společnost Russmedia tím, že dovolila zveřejnit daný inzerát, porušila ustanovení GDPR a zda je možné na toto porušení aplikovat režim bezpečného přístavu z článků 12–15 e-commerce směrnice.³³

V tomto kontextu Soudní dvůr odpověděl, že zveřejnění inzerátu obsahujícího osobní údaje bez ověření souhlasu či jiného právního základu pro zpracování daných osobních údajů není přípustné.³⁴ Společnost Russmedia měla podle článku 32 GDPR přijmout přiměřená technická a organizační opatření, aby toto nebylo možné. Stejně tak měla přijmout opatření bránící možnému převzetí škodlivého inzerátu dalšími webovými stránkami. V kontextu rozšíření škodlivého inzerátu i jinam ovšem není možné podle Soudního dvora obecně říci, že pokud se inzerát dostane na další stránky došlo k porušení GDPR, společnost Russmedia totiž měla pouze povinnost vyvinout potřebnou snahu této situaci předejít.³⁵

Ke vztahu mezi e-commerce směrnicí a GDPR Soudní dvůr konstatoval, že GDPR není dotčeno režimem bezpečného přístavu. To znamená, že společnost Russmedia v pozici společného správce³⁶ osobních údajů v daném případě mohla porušit GDPR a za toto porušení nést odpovědnost, i přestože neměla povědomí o konkrétním obsahu nahraném na online tržiště, které provozovala, a který GDPR porušil.³⁷ Rozhodnutí tak významně změnilo dosavadní chápání výjimek z odpovědnosti z článků 12–15 e-commerce směrnice, ale i obdobných výjimek obsažených v člancích 4–6 DSA.³⁸

Autor: ME

³² Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu).

³³ Bod 35 anotovaného rozhodnutí.

³⁴ Bod 93 anotovaného rozhodnutí.

³⁵ Bod 123 anotovaného rozhodnutí.

³⁶ Bod 72 a násl. anotovaného rozhodnutí.

³⁷ Bod 135 anotovaného rozhodnutí.

SHROMAŽDOVÁNÍ BIOMETRICKÝCH ÚDAJŮ V TRESTNÍM ŘÍZENÍ A ODMÍTNUTÍ IDENTIFIKACE JAKO TRESTNÝ ČIN

Soud: Soudní dvůr Evropské unie

Věc: C-371/24

Datum: 19. 3. 2026

Dostupnost: curia.europe.eu

Dne 30. května 2020 pořádkové síly zadržely obviněného při rozptylování klimatických aktivistů na Champs-Élysées.³⁹ Obviněný odmítl sejmutí otisků prstů a pořízení fotografie, přestože byl upozorněn, že jde o trestný čin.⁴⁰ Trestní soud v Paříži jej zprostil obvinění z primárního trestného činu, uznal jej však vinným ze specifického trestného činu odmítnutí identifikace a uložil mu peněžitý trest 300 eur.⁴¹ Odvolací soud v Paříži řízení přerušil a předložil SDEU předběžné otázky.⁴²

Předkládající soud se tázal, zda čl. 10 směrnice 2016/680 ve spojení s čl. 4 odst. 1 písm. a) až c) a čl. 8 brání systematickému shromažďování biometrických údajů u každé důvodně podezřelé osoby, zda vyžaduje odůvodnění naprosté nezbytnosti v každém případě, a zda brání stíhání za odmítnutí identifikace při zproštění obvinění z primárního trestného činu.⁴³

Článek 10 směrnice 2016/680 zajišťuje zvýšenou ochranu biometrických údajů – jejich zpracování je přípustné pouze tehdy, je-li zcela nezbytné a existují-li vhodné záruky práv subjektů údajů.⁴⁴ Podmínka naprosté ne-

³⁸ Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách).

³⁹ Bod 11 anotovaného rozhodnutí.

⁴⁰ Bod 11 anotovaného rozhodnutí.

⁴¹ Bod 13 anotovaného rozhodnutí.

⁴² Bod 14 anotovaného rozhodnutí.

⁴³ Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

⁴⁴ Bod 21 anotovaného rozhodnutí.

zbytnosti musí být posuzována obzvláště přísně s důrazem na zásadu minimalizace a proporcionality, přičemž čl. 54 ve spojení s čl. 47 Listiny zaručuje právo na účinnou soudní ochranu.⁴⁵

SDEU konstatoval, že pouhá existence důvodného podezření naprostou nezbytnost shromažďování biometrických údajů sama o sobě nezakládá a příslušný orgán musí zohlednit povahu trestného činu, trestní minulost i profil osoby.⁴⁶ Národnímu soudu přísluší ověřit, zda francouzská úprava fakticky nevede k systematickému shromažďování.⁴⁷ Bez přiměřeného odůvodnění nelze zajistit účinný soudní přezkum, který tuto povinnost orgánu nahradit nemůže.⁴⁸ Zproštění obvinění z primárního trestného činu není rozhodující, neboť naprostá nezbytnost se posuzuje k okamžiku zamýšleného shromažďování; uložená sankce však musí respektovat zásadu proporcionality dle čl. 49 odst. 3 Listiny.⁴⁹

SDEU rozhodl, že čl. 10 směrnice 2016/680 brání systematickému shromažďování biometrických údajů bez individuálního posouzení naprosté nezbytnosti, přičemž příslušný orgán je povinen tuto nezbytnost odůvodnit. Stíhání za odmítnutí identifikace směrnicí neodporuje, je však podmíněno naplněním naprosté nezbytnosti a proporcionalitou sankce.⁵⁰

Autorka: AK

PRÁVO NA SOUKROMÍ ZAMĚSTNANCE (EMAILOVÁ SCHRÁNKA)

Soud: Nejvyšší správní soud
Věc: 6 Ads 21/2026-27
Datum: 18. 3. 2026
Dostupnost: vyhledavac.nssoud.cz

⁴⁵ Bod 24 anotovaného rozhodnutí.

⁴⁶ Body 28, 64 a 65 anotovaného rozhodnutí.

⁴⁷ Body 34 a 41 anotovaného rozhodnutí.

⁴⁸ Bod 53 anotovaného rozhodnutí.

⁴⁹ Body 71 a 73 anotovaného rozhodnutí.

⁵⁰ Body 86, 88 a 91 anotovaného rozhodnutí.

Nejvyšší správní soud řešil případ zaměstnance ČÚZK, který neoprávněně nakládal s dokumenty z vkladového řízení, u kterých nebyly anonymizovány osobní údaje. Konkrétně zveřejnil vkladovou listinu ve veřejné skupině na Facebooku, návrh na vklad rozeslal jiným zaměstnancům, kteří k dané dokumentaci neměli mít přístup a rovněž i dvěma osobám, které vůbec na ČÚZK zaměstnány nebyly. Kárná komise uložila zaměstnanci snížení platu o 15 % na tři měsíce; odvolací orgán zpřesnil popis skutků a právní kvalifikaci. Zaměstnanec s uloženou sankcí nesouhlasil a bránil se zejména tím, že důkazy z monitoringu služebního e-mailu jsou nezákonné (zaměstnanec byl o daném nedostatečně informován, nebyla naplněna zvláštní povaha vykonávané činnosti, došlo k zásahu do tajemství přepravovaných zpráv).

NSS tak primárně řešil, jestli je kontrola obsahu služebního e-mailové schránky podle § 316 zákoníku práce (ZP) za daných okolností přípustná a zda mohou být takto získané zprávy využity v kárném řízení.

Ustanovení § 316 ZP připouští kontrolu e-mailu jen při závažném důvodu spočívajícím ve zvláštní povaze činnosti, při přiměřenosti a při splnění informační povinnosti; zásah musí respektovat čl. 13 Listiny základních práv a svobod a kritéria proporcionality formulovaná judikaturou ESLP (zejm. ve věci *Bărbulescu*⁵¹).

NSS konstatoval, že monitoring byl legitimní, časově a účelově omezený, a zaměstnanec byl dopředu o daném informován na základě interní směrnice. Navíc zaměstnanec nemohl rozumně očekávat ochranu soukromí v případě, kdy rozesílal dané zprávy ze své emailové adresy hromadně. Navíc NSS zdůraznil, že zaměstnanec zveřejnění informací mj. na Facebooku nijak nerozporoval.

Na základě této argumentace byla kasační stížnost zamítnuta; monitoring i způsob formulace sankce NSS považoval za zákonné.

Autor: PL

⁵¹ *Bărbulescu proti Rumunsku*, 5. 9. 2017, stížnost č. 61496/08.

2. UMĚLÁ INTELIGENCE, DIGITÁLNÍ PLATFORMY, SOCIÁLNÍ SÍTĚ A OSTATNÍ

HALUCINACE AI V ÚSTAVNÍ STÍŽNOSTI

Soud: Ústavní soud
Věc: I. ÚS 3004/25
Datum: 1. 12. 2025
Dostupnost: nalus.usoud.cz

Povinný jako právní zástupce stěžovatele sepsal a doručil Ústavnímu soudu, prostřednictvím datové schránky advokáta, ústavní stížnost. Svou argumentaci podpořil dvanácti rozhodnutími Ústavního soudu a Evropského soudu pro lidská práva.⁵² Ústavní soud však při bližším zkoumání zjistil, že podstatná část citovaných rozhodnutí vůbec neexistuje, nebo je hrubě dezinterpretována.⁵³

V daném případě byla řešena otázka, zda podání ústavní stížnosti, která vykazuje značné nedostatky v důsledku využití generativních modelů umělé inteligence představuje situaci, která natolik ztěžuje postup řízení, že zakládá možnost uložení pořádkové pokuty.

Pro posouzení předmětné otázky je relevantní ustanovení § 61 odst. 1 zákona o Ústavním soudu. Ustanovení stanovuje, že tomu, kdo hrubě ztěžuje postup řízení, může být předsedou senátu uložena pořádková pokuta.⁵⁴

Podání ústavní stížnosti je úkon, který je podmíněn zastoupením advokátem.⁵⁵ Ústavní soud v předmětném rozhodnutí uvedl, že je potřeba, aby komunikace s ÚS probíhala na náležité formální a věcné úrovni.⁵⁶ Účelem zastoupení je ochrana stěžovatele a jeho zájmů.⁵⁷ Úroveň komunikace by byla hrubě narušena v případě, že by právní zástupci stěžovatelů nesmy-

⁵² Bod 1 anotovaného rozhodnutí.

⁵³ Tamtéž.

⁵⁴ Bod 2 anotovaného rozhodnutí.

⁵⁵ Ustanovení § 30 odst. 1 zákona č. 182/1993 Sb., o Ústavním soudu.

⁵⁶ Bod 3 anotovaného rozhodnutí.

⁵⁷ Tamtéž.

slně zatěžovali ÚS podáními, ve kterých argumentují neexistujícími právními prameny.⁵⁸ Ústavní soud se musel podrobně zabývat argumentací povinného, pečlivě zkoumal veškerá uvedená rozhodnutí a zkoumal také možnost výskytu překlepů. Vzhledem k frekvenci, s jakou se nedostatky v ústavní stížnosti objevovaly, však dospěl k závěru, že ústavní stížnost byla s největší pravděpodobností generována modelem umělé inteligence a povinný ji ponechal v této podobě bez nutných následných korekcí.⁵⁹ Povinný jako osoba znalá práva přebírá odpovědnost za případné vady podání v důsledku halucinující argumentace umělé inteligence.⁶⁰

ÚS tak na závěr konstatoval, že povinný uvedl ÚS v omyl a zbytečně tak zkomplikoval a zdržel postup řízení.⁶¹ Z tohoto důvodu tak ÚS uložil povinnému pořádkovou pokutu ve výši 25 000 Kč a vyzval jej k odstranění vad ústavní stížnosti.⁶²

Autorka: KM

INTERPRETACE SYSTÉMOVÝCH RIZIK DLE ČL. 34 ODS. 1 DSA

Soud: Soudní dvůr Evropské unie (Tribunál)
Věc: T-367/23 Amazon EU proti Evropské komisi
Datum: 19. 11. 2025
Dostupnost: eur-lex.europa.eu

Společnost Amazon napadla rozhodnutí komise o zařazení své platformy Amazon Store mezi velmi velké online platformy dle čl. 33 nařízení (EU) 2022/2065 (DSA).⁶³ Dle Amazonu představují požadavky, které DSA velmi velkým online platformám (a především online tržištím) stanoví, značnou zátěž a porušují tak její právo na svobodu podnikání zakotvené v čl. 16. Listiny základních práv EU (Listina). Amazon namítal porušení i dalších práv,

⁵⁸ Bod 4 anotovaného rozhodnutí.

⁵⁹ Body 5-7 anotovaného rozhodnutí.

⁶⁰ Bod 7 anotovaného rozhodnutí.

⁶¹ Bod 8 anotovaného rozhodnutí.

⁶² Body 10 a 11 anotovaného rozhodnutí.

⁶³ Bod 9 anotovaného rozhodnutí.

stěžejní část argumentace a následného rozhodnutí se zaměřila na čl. 16 Listiny.

V žalobě Amazonu jsou důležité tři argumenty. Za prvé Amazon tvrdil, že se na online tržištích nemohou objevit systémová rizika, protože tržiště nepředstavují provázaný systém.⁶⁴ Dle Tribunálu nemá (ne)provázanost online tržišť vliv na výskyt systémových rizik, protože v DSA se systémová rizika odvíjí od nebezpečí, které mohou online platformy představovat pro společnost jako celek.⁶⁵ Tento bod je podstatný proto, že Amazon se ve své argumentaci opíral o evropskou regulaci finančních služeb, která je kromě DSA jedinou evropskou regulací, která také pracuje s konceptem systémových rizik. (Ne)provázanost online tržišť tak Amazon stavěl jako protiklad k provázanému „světovému finančnímu systému.“ Tribunál tuto analogii odmítl, což znamená, že při interpretaci systémových rizik dle DSA nelze z této regulace finančních služeb vycházet.⁶⁶

Za druhé, dle Amazonu se obsah na jím provozovaném online tržišti týká primárně nákupu a projeedu výrobků, nemůže proto představovat riziko pro demokratickou společnost, jak předvídá DSA. Tribunál nesouhlasil, protože sám Amazon ve svých obchodních podmínkách upravuje pravidla k zabránění šíření nezákonného obsahu, obsahu s nepříznivým dopadem na výkon základních práv apod. Dále dle Tribunálu Amazon v rámci žaloby uznal, že tržiště mohou sloužit k prodeji nelegálních výrobků a nepředložil žádný důkaz pro tvrzení, že prodej nelegálních výrobků na platformách s vyšším počtem měsíčních uživatelů je méně závažný než prodej těchto výrobků mimo VLOPs. To znamená, že online tržiště mohou působit řadu systémových rizik dle čl. 34 DSA.⁶⁷

Za třetí, povinnosti stanovené DSA představují dle názoru Amazonu nepřiměřenou zátěž. Dle Tribunálu mírnější opatření, s jejichž pomocí by bylo možné dosáhnout požadovaných cílů, sice existují, nejsou ale dostatečně

⁶⁴ Bod 69 anotovaného rozhodnutí.

⁶⁵ Bod 70 anotovaného rozhodnutí.

⁶⁶ Viz <https://dsa-observatory.eu/2026/05/06/what-makes-a-risk-systemic-the-cjeus-first-interpretation-of-systemic-risks-under-the-digital-services-act/>

⁶⁷ Bod 77 anotovaného rozhodnutí.

efektivní. Existující úprava v DSA tudíž nepředstavuje nepřiměřenou zátěž a neporušuje tak právo svobodně podnikat dle čl. 16 Listiny.⁶⁸ Tribunál následně odmítl i další námitky společnosti Amazon, často s odkazem na nedostatečnou argumentaci. Amazon se proti tomuto rozhodnutí odvolal a případu se tak bude v budoucnu věnovat i Soudní dvůr.⁶⁹

Autorka: TM

BLOKACE RUSKÝCH SOCIÁLNÍCH SÍTÍ VS. PRÁVO NA SVOBODU PROJEVU

Soud: Evropský soud pro lidská práva
Věc: Boyarov proti Ukrajině (stížnost č. 79083/17)
Datum: 3. 3. 2026
Dostupnost: hudoc.echr.coe.int

V roce 2017 přijala Ukrajinská národní a bezpečnostní rada opatření, kterým uvalila sankce na tři ruské společnosti, které provozovaly různé typy zprostředkovatelských služeb, včetně internetového prohlížeče Yandex, sociálních sítí VKontakte a Odnoklassniki a e-mailové služby Mail.ru. Sankce přijaté na základě ukrajinského zákona o sankcích z roku 2014 nařídily ukrajinským poskytovatelům telekomunikační služeb zablokovat přístup k těmto službám, v praxi je tak uživatelé na území Ukrajiny nemohli využívat.⁷⁰ K přijetí sankcí vedlo to, že Rusko používalo tyto služby k ohrožení ukrajinské národní bezpečnosti, například prostřednictvím získávání osobních dat o členech ukrajinských ozbrojených sil a k šíření dezinformací včetně výzev ke státnímu převratu vůči stávající ukrajinské vládě.⁷¹

Celkem čtyři osoby opatření napadly u ukrajinských správních a ústavního soudu. Dva z nich tvrdili, že jim opatření znemožnilo přístup k vlastním účtům, třetí si stěžoval na ztrátu kontaktu se svými příbuznými v Rusku, čtvrtý nevyjasnil, jak služby využívá. ESLP se zabýval otázkou,

⁶⁸ Bod 121 anotovaného rozhodnutí.

⁶⁹ Případ je vedený pod sp. zn. C-47/26 P.

⁷⁰ Bod 17 anotovaného rozhodnutí.

⁷¹ Bod 23 anotovaného rozhodnutí.

zda blokace těchto služeb představuje zásah do práva na svobodu projevu stěžovatelů. Obecně ESLP poukázal na důležitou roli sociálních sítí pro možnost jednotlivců veřejně vyjadřovat své názory, přijímat informace a participovat na veřejném životě.⁷² Zároveň podotkl, že pouhá nemožnost přístupu k sociálním sítím neznamena automatický zásah do práva na svobodu projevu uživatelů. Závěry soudu se u jednotlivých stěžovatelů lišily, všechny ale zamítl jako nepřijatelné. U jednoho ze stěžovatelů byl důvod procesní, protože před podáním stížnosti k ESLP nevyčerpal všechny vnitrostátní opravné prostředky. Další stěžovatel vůbec nevysvětlil, jak blokace těchto služeb omezila jeho aktivity.⁷³ V případě stěžovatele, který argumentoval ztrátou kontaktu s příbuznými na území Ruska došel soud k závěru, že je stížnost nepřipustná, protože se jedná o soukromou konverzaci, ne veřejné vyjadřování a případ tudíž nespadá pod rozsah práva na svobodu projevu dle čl. 10 EÚLP.⁷⁴ Nejpodrobněji se Soud zabýval posledním stěžovatelem, který tyto služby využíval k propagaci vlastních aktivit. Jeho stížnost vyhodnotil ESLP jako neopodstatněnou, kdy zohlednil výjimečnou situaci, v níž se Ukrajina nachází a fakt, že se stěžovatel mohl ke svým účtům dostat za použití VPN nebo využívat alternativní sociální média, která jsou stále dostupná.⁷⁵

Autorka: TM

RYCHLOMĚR JAKO BEZPEČNOSTNÍ OPATŘENÍ V KONTEXTU ZÁKONA Č. 106/1999 SB.

Soud: Nejvyšší správní soud
Věc: 1 As 208/2025-34
Datum: 26. 3. 2026
Dostupnost: vyhledavac.nssoud.cz

⁷² Bod 109 anotovaného rozhodnutí.

⁷³ Bod 51 anotovaného rozhodnutí.

⁷⁴ Body 105 a 106 anotovaného rozhodnutí.

⁷⁵ Bod 120 anotovaného rozhodnutí.

V rámci anotovaného rozhodnutí se Nejvyšší správní soud (dále jen „NSS“) vyjadřoval k možnosti neposkytnout IP adresu prvního serveru, na který rychloměr zasílá fotografie měřených vozidel. Správní orgán odmítnutí poskytnutí informace odůvodnil ohrožením účinnosti bezpečnostního opatření v důsledku poskytnutí informace ve smyslu § 11 odst. 1 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím (dále jen „zákon“). NSS se tak ve svém rozsudku vypořádal s vymezením pojmu bezpečnostního opatření v zákoně a s jednotlivými složkami tohoto pojmu.

Žalobce původně podal u povinné osoby žádost podle zákona, kdy požadoval informace o umístěném rychloměru, zejména ve smyslu identifikace provozovatele, způsobu fungování rychloměru, technické specifikace, přenosu dat a počtu změřených vozidel. Povinná osoba v rámci požadované technické specifikace odmítla sdělit IP adresu prvního serveru, na který rychloměr přenáší pořízené snímky.⁷⁶ Dle správního orgánu (i orgánu nadřízeného) by mohla být IP adresa zneužita k DDoS útoku, přičemž nešlo pouze o hypotetickou možnost, ale o riziko vycházející z jejich praktické zkušenosti.⁷⁷ Žaloba ke krajskému soudu pak byla neúspěšná,⁷⁸ a soud potvrdil závěr správních orgánů.

Proti rozsudku krajského soudu⁷⁹ podal žalobce kasační stížnost, v níž se domáhal jeho zrušení. Hlavním tvrzením bylo, že z napadeného rozhodnutí není zřejmé, které bezpečnostní opatření (resp. jeho účinnost) má být sdělením narušena. Také dle žalobce nebylo zřejmé, který právní předpis označuje rychloměr za bezpečnostní opatření ve smyslu díkce § 11 odst. 1 písm. d) („účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu“).⁸⁰

Vedle vypořádání se s obecnými námitkami žalobce (nepřezkoumatelnost napadeného rozhodnutí) se NSS věnoval vymezení pojmu bezpečnostního opatření ve smyslu zákona. NSS totiž konstatoval, že posouzení

⁷⁶ Bod 2 anotovaného rozhodnutí.

⁷⁷ Bod 3 anotovaného rozhodnutí.

⁷⁸ Bod 4 anotovaného rozhodnutí.

⁷⁹ Konkrétně šlo o rozsudek Krajského soudu v Ústí nad Labem 10. 12. 2025, č. j. 141 A 13/2025-29. Tento rozsudek je také dostupný v databázi NSS na vyhledavac.nssoud.cz.

⁸⁰ Bod 6 anotovaného rozhodnutí.

použitelnosti § 11 odst. 1 písm. d) zákona v tomto kontextu představuje otázku, kterou soud musí prozkoumat z úřední povinnosti.⁸¹ S touto námitkou žalobce se tak soud vypořádal věcně.⁸²

NSS konstatoval, že je z dikce zákona zřejmé, že neposkytnutí podle § 11 odst. 1 písm. d) zákona je možné pouze za kumulativního splnění tří podmínek: (i) musí jít o bezpečnostní opatření, (ii) které má základ ve zvláštním předpise, a (iii) které chrání některý z v ustanovení uvedených cílů.⁸³

K první podmínce NSS zdůraznil, že pojem bezpečnostního opatření je neurčitým právním pojmem, který je vlastní zákonu a nelze tak vycházet z jeho definice v jiném předpise.⁸⁴ NSS se opřel o důvodovou zprávu k ustanovení (resp. příslušný sněmovní tisk).⁸⁵ Z ní NSS dovodil, že je možné ustanovením chránit i „analogové“ formy ochrany, tedy provoz jakéhokoli prostředku, který zajišťuje ochranu zákonem předpokládaného zájmu.⁸⁶ Až tautologicky tak uzavřel, že rychloměr je možné považovat za bezpečnostní opatření ve smyslu zákona, protože jde o nástroj, který směřuje k ochraně bezpečnosti. IP adresa prvního serveru, na který jsou odesílána data, tak je důležitým prvkem systému, jehož vyřazení z provozu by mohlo vést k významnému ohrožení činnosti rychloměru.⁸⁷ Jakkoli NSS komentářovou literaturu nezmínil, dospěl ke stejnému výkladu.⁸⁸

Ke druhé podmínce NSS uvedl, že právní základ rychloměru jako bezpečnostního opatření je možné najít v § 79a zákona č. 361/2000 Sb., o si-

⁸¹ Odkázal přitom na usnesení rozšířeného senátu ze dne 28. 7. 2009, č. j. 8 Afs 51/2007-87 (publikováno jako č. 1926/2009 Sb. NSS).

⁸² Bod 16 anotovaného rozhodnutí.

⁸³ Bod 17 anotovaného rozhodnutí.

⁸⁴ Viz např. § 4 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti nebo § 13 odst. 1 zákona č. 264/2025 Sb., o kybernetické bezpečnosti.

⁸⁵ Bod 18 anotovaného rozhodnutí.

⁸⁶ Bod 20 anotovaného rozhodnutí.

⁸⁷ Bod 21 anotovaného rozhodnutí.

⁸⁸ Viz FUREK, Adam, ROTHANZL, Lukáš, MÍŠEK, Jakub, LUDVÍK, Otakar. § 11 [Další omezení práva na informace]. In: FUREK, Adam, ROTHANZL, Lukáš, MÍŠEK, Jakub, LUDVÍK, Otakar. Zákon o svobodném přístupu k informacím. 2. vydání. Praha: C. H. Beck, 2025, s. 586-587.

lničním provozu. Ač jde o kompetenční normu,⁸⁹ je jí poskytnut právní základ pro provoz rychloměru. Jak uvádí NSS, „není vyloučeno, aby na základě jedné normy byla určitému orgánu svěřena kompetence, definován pojem či někomu stanovena povinnost, a zároveň tatáž norma byla právním podkladem pro stanovení prostředku jako bezpečnostního opatření.“⁹⁰

Konečně ke třetí podmínce NSS uvedl, že měření rychlosti směřuje ke zvýšení bezpečnosti provozu, jelikož „[d]održování rychlosti směřuje k nižší nehodovosti.“ Tím se opatření vztahuje k bezpečnosti osob i majetku. Dále uvedl, že kontrola rychlosti je součástí širší ochrany veřejného pořádku.⁹¹

Dle NSS je tak rychloměr možné považovat za bezpečnostní opatření ve smyslu § 11 odst. 1 písm. d) zákona.⁹²

Za nedůvodnou pak NSS označil námitku žalobce, že poskytnutím IP adresy nedochází k významnému ani přímému ohrožení účinnosti bezpečnostního opatření. Žalobce argumentoval paralelou mezi veřejně známou fyzickou adresou úřadu a IP adresou. NSS k tomu uvedl, že tato paralela je nepřipadná.⁹³ Veřejná znalost IP adresy může být vzhledem k povaze online prostředí (anonymita, možnosti automatizace) nežádoucí.⁹⁴ Míra hrozícího rizika pro řádné fungování rychloměru, která je spojená s poskytnutím IP adresy, překračuje běžná rizika a může vést k tomu, že by rychloměr přestal plnit svou funkci.⁹⁵

NSS tak potvrdil postup správních orgánů i napadený rozsudek Krajského soudu v Ústí nad Labem ze dne 10. 12. 2025, č. j. 141 A 13/2025-29.

Jako závěrečnou informaci této anotace je pak nutné uvést, že osoba žalobce v anotovaném rozhodnutí je přes totožné iniciály odlišná od osoby autora této anotace. Tato shoda je náhodná, byť pozoruhodná.

⁸⁹ Bod 23 anotovaného rozhodnutí.

⁹⁰ Tamtéž.

⁹¹ Bod 26 anotovaného rozhodnutí.

⁹² Bod 27 anotovaného rozhodnutí.

⁹³ Bod 30 anotovaného rozhodnutí.

⁹⁴ Body 31-33 anotovaného rozhodnutí.

⁹⁵ Bod 37 anotovaného rozhodnutí.

Autor: JH

POUŽITELNOST DŮKAZŮ ZÍSKANÝCH POLICISTOU V UTAJENÍ V ON-LINE PROSTŘEDÍ

Soud: Evropský soud pro lidská práva
Věc: Helme proti Estonsku (stížnost č. 3023/22)
Datum: 7. 10. 2025
Dostupnost: hudoc.echr.coe.int

Dne 19. září 2019 bylo estonskou policií zahájeno trestní řízení, a to na základě několika obdržených podnětů, které naznačovaly, že některé osoby využívaly vybrané internetové stránky k vedení on-line konverzací sexuální povahy s osobami mladšími 14 let; jednalo se přitom o stránky www.facebook.com a stránku www.armastusesaal.org, což v překladu znamená síň lásky.⁹⁶ Na základě těchto informací bylo povoleno použití policisty v utajení, který měl pod pseudonymem „Marleen12“ pod fiktivní identitou dvanáctileté dívky jménem Marleen za využití chatovacích místností shromáždit relevantní informace pro předmětné řízení.⁹⁷ S Marleen navázal komunikaci stěžovatel, který konverzace opakovaně inicioval a vnášel do nich sexuální témata.⁹⁸ Stěžovatel byl poté odsouzen za trestný čin sexuálního svádění nezletilé osoby.⁹⁹

Protože bylo rozhodnutí okresního soudu následně potvrzen soudem odvolacím i Nejvyšším soudem Estonska,¹⁰⁰ podal stěžovatel stížnost k ESLP, v níž namítal především porušení práva na spravedlivý proces.¹⁰¹ Ve své stížnosti uvedl, že trestní stíhání bylo zahájeno na základě obecných informací s cílem podněcovat osoby k páčání trestné činnosti;¹⁰² zejména použi-

⁹⁶ Bod 5 anotovaného rozhodnutí.

⁹⁷ Body 6 a 7 anotovaného rozhodnutí.

⁹⁸ Bod 10 anotovaného rozhodnutí.

⁹⁹ Bod 11 anotovaného rozhodnutí.

¹⁰⁰ Body 18 a 22 anotovaného rozhodnutí.

¹⁰¹ Viz článek 6 odst. 1 Úmluvy o ochraně lidských práv a základních svobod.

¹⁰² Bod 36 anotovaného rozhodnutí.

tý pseudonym Marleen12, který naznačoval, že je Marleen osobu nezletilou, byl podle stěžovatele zvolen za účelem podněcování.¹⁰³

ESLP ve svém rozhodnutí především uvedl, že samotné použití policisty v utajení samo o sobě nepředstavuje porušení práva na spravedlivý proces.¹⁰⁴ Hlavní otázkou, kterou se ESLP zabýval nicméně bylo, zda se orgány činné v trestním řízení omezily na vyšetřování toliko pasivním způsobem, tj. zda ze strany policisty v utajení nedocházelo k podněcování k páčání trestné činnosti.¹⁰⁵

Ve vztahu k použitému pseudonymu ESLP došel k závěru, že jeho použití nepředstavovalo nezákonné podněcování ze strany orgánů činných v trestním řízení.¹⁰⁶ K tomuto závěru ESLP došel zejména s přihlédnutím k tomu, že to byl právě stěžovatel, kdo vždy inicioval konverzace s Marleen a vnášel do nich sexuální témata;¹⁰⁷ ESLP tak uzavřel, že policista v utajení neopustil požadovaný pasivní přístup při vyšetřování a stěžoval k trestné činnosti podněcován nebyl.¹⁰⁸ Ve vztahu k on-line prostředí ESLP rovněž uzavřel, že s ohledem na náročnost odhalení skutečné identity pachatelů v on-line prostředí postačuje v takových případech k zahájení vyšetřování již pouhá existence objektivního podezření na páčání trestné činnosti, týkající se definovaného a vymezeného virtuálního prostoru.¹⁰⁹

Ačkoliv se ESLP již použitím policisty v utajení a podněcováním k trestné činnosti zabýval, případ Helme proti Estonsku představuje první případ, ve kterém se ESLP zabýval podněcováním k trestné činnosti v on-line prostředí. V tomto případě nicméně ESLP porušení práva stěžovatele na spravedlivý proces neshledal.

Autor: MP

¹⁰³ Bod 37 anotovaného rozhodnutí.

¹⁰⁴ Bod 47 anotovaného rozhodnutí.

¹⁰⁵ Bod 53 anotovaného rozhodnutí.

¹⁰⁶ Bod 87 anotovaného rozhodnutí.

¹⁰⁷ Bod 85 anotovaného rozhodnutí.

¹⁰⁸ Bod 86 anotovaného rozhodnutí.

¹⁰⁹ Bod 82 anotovaného rozhodnutí.

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>).

LIFE IN THE DATASPHERE: THE NEW ALWAYS- ONLINE SELF¹

ADÉLA MERTOŮVÁ²

1. INTRODUCTION

People used to have two separate realms in which they expressed themselves: the private interior of personal life, dedicated to themselves and their closest ones, and the public exterior of social interactions. Nowadays, these two worlds are not only colliding, but also blending. Our online and offline lives merged into the “always-online self” in the new environment called “the datasphere”. It’s a digital omnipresent ecosystem of devices and platforms that collects, analyzes, and uses our everyday actions and intentions [both online and offline]. From smartphones tracking our movements to smart watches collecting data about our health condition or even so-called smart-houses. In the datasphere, the offline experiences are gradually transported into digital traces, used to personalize our online activities.³

As a result, fundamental concepts like privacy and identity went through a profound transformation. Both privacy and identity have become co-determined by the technologies we use, the platforms that mediate our interactions. The boundary between private and public, external and internal self is dissolving. What once separated the intimate from the exposed, and the inner self from its outward expression, is now eroding, leaving indivi-

¹ Esej byla zpracována v podzimním semestru 2025 v rámci předmětu MVV1368K Privacy and Personal Data.

² Studentka 3. ročníku Právnické fakulty Masarykovy univerzity. Kontaktní e-mail: 547211@muni.cz

³ HUMPHREYS, Stephen. Conscience in the datasphere. In: *openDemocracy* [online]. 14.3.2016. [cit. 18. 1. 2026]. Available at: <https://www.opendemocracy.net/en/digital-liberties/conscience-in-datasphere/>

duals transparent to systems that were never designed to understand them as whole human beings.

This essay focuses on the blended experience where offline life is tracked and used by digital systems and how it reshapes our perception of privacy, personality, and most importantly identity. It mainly aims at how people feel, think and experience themselves in a world where the data produced by daily life carries persistent consequences: in the datasphere, privacy as we know it becomes a technically unmanageable concept, and identity becomes an algorithmic construct.

2. THE EMERGENCE OF THE DATASPHERE⁴

“Datasphere”, as mentioned, refers to the virtually limitless digital environment in which our personal data circulates. Smartphones, wearables, home assistants, digital services, and so on gather data about what we do, where we go, how long we sleep, what we buy, etc. This concept, alas the interconnection of everyday objects via the internet, is called the Internet of Things [IoT]. IoT technologies are the prime example of how digital data collection has become omnipresent, blending into homes, cities, and workplaces. Due to these information being collected and shared throughout the datasphere, it’s easy for the device to appeal to our liking, meaning that various algorithms they manage to personalize everything we come across online. Seemingly mundane objects like thermostats are able to customize themselves automatically to our liking by all the information gathered about us.

The first technological shift from the concept of two separate worlds of being online and offline lies in the continuous exposure and ambient connectivity. As stated, everyday objects contain certain sensors that operate silently and continuously, turning ordinary life and experiences into digital traces. That being said, under such conditions, the concept of “being offline” becomes rather fictional. A user may turn off their phone, but their

⁴ More about datasphere and IoT in general see: NIŽETIČ, Sandro, et al. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. In: *Journal of Cleaner Production* [online]. 2020, vol. 274. [cit. 18. 1. 2026]. ISSN 0959-6526. Available at: <https://www.sciencedirect.com/science/article/pii/S095965262032922X>

watch, car, or home assistant continues collecting and transmitting data. This everlasting data collection blurs the boundaries between public and private spaces and it goes beyond our general comprehension of privacy. Instead of the old dualism of “offline world” and “online world”, the “real world” is now an extension of the digital domain.

Not only does this always-on collection of information alter how we understand our privacy, but it also reshapes our understanding of our own identities. Rather than living a discrete life offline and separately, the self that we increasingly know and come across is the one that’s been mediated and interpreted by the digital world. By “seeing” this self, the one analyzed by algorithms, the more these characteristics deepen their roots within us.

3. IDENTITY IN THE DATASPHERE: SELF AS ALGORITHMIC PROJECTION

As was mentioned, our identities in the digital ecosystems are not mirrors, they are not cohesive or reflective like the narrative self. By now, the identity has been thoroughly constructed by the algorithmic interpretation. Every click, search, and purchase becomes a person’s fragment and becomes fuel to an algorithmic model that tries to predict or influence future behavior. These models create a version of us that is legible for computing, meaning it organizes learned values. The more data we generate, the more complete the digital portrait becomes.

Of course, the outcome of the “characterization” process is not objectively us. It is shaped by platforms’ interests and goals, especially commercial ones. That itself is not an “identity” as we understand, but it’s rather a product instead, predictable and profitable. It’s a new form of selfhood: “the always-online self” or “data identity”: a profile constructed by algorithms. Corporations, or even governmental systems rely on these profiles to make decisions about creditworthiness, desirability [as a consumer], or risk assessment. As a result, individuals’ opportunities may increasingly depend on the algorithmic categorization rather than genuine self-expression. In the context of global powers, these data identities are assigned different purposes. For example, systems in China integrate data identities

into state governance, helping the government monitor and control its citizens and their behavior. On the other hand, the United States of America use data identities for consumer personalization. In every case, the most important outcome remains in the fact, that identity is shaped externally through the algorithm-based processes rather than by people themselves.⁵

Understandably, this creates a psychological and social tension. The identity as we know, is an internal set of stories and facts individuals construct to define their role in life, begins to diverge from the algorithmic identity, which dictates how institutions perceive and treat us. For example, someone who self-identifies as financially responsible although not having a large income may be algorithmically labeled as high-risk. Can we fight this unfair labeling? Hardly. These algorithmic classifications are rather unchallengeable. The reality set by the algorithm is that individuals are known by systems more thoroughly and consequently than by themselves.

To enforce the “real” purpose of an identity as we know, there’s a concept of digital self-determination. This concept concerns the autonomy of individuals and follows their interest in how their digital identities are shaped and used. The digital identity is therefore influenced by the users’ control over the narrative of their own selves. That is also apparent in the context of IoT technologies. In this realm, our data are analyzed and often aggregated, which ignores the individuality of users. All the data collected is prone to being more likely than not incorrect. By aggregation, platforms are able to infer things about us that we haven’t directly disclosed. These interferences can even relate to our personal and even intimate facts, such as our health conditions, emotional states, and political preferences. Thus, the platforms fill the gaps using a certain general condition learned from the data collected, reshaping our digital identity as something that’s not expressed by users, but what the platform wants to be expressed. It means that our digital identity does not emerge primarily

⁵ FINGER, Matthias. Book review: Digital Empires. In: *Center for Digital Trust (C4DT), EPFL* [online]. [cit. 18. 1. 2026]. Available at: <https://c4dt.epfl.ch/article/book-review-digital-empires/> (The original book: Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology*. Oxford, New York: Oxford University Press, 2023. ISBN 978-0-19-764926-8.)

from deliberate self-expression but from automated data-generation. What we think of identity, as unique facets of ourselves, the digital ecosystems treat it as a variable fit to be manipulated for the purpose of being predictable, rather than being individual.⁶

4. LIVING IN AN OMNIPTICON: THE PSYCHOLOGICAL PRESSURE AND FRAGMENTATION OF IDENTITY^{7 8}

The datasphere also reshapes our identity through continuous observation, described as the emergence of an “omnicon”. It’s a distributed form of visibility in which individuals are potentially watched by everyone, corporations, governments, people in general, and algorithms, and are aware of it. This observance subtly changes individuals’ behavior, internalizing the possibility of surveillance and adjust their actions or behavior accordingly, avoiding risk or controversy. Our actions simply become a cautious performance designed to avoid possible algorithmic misinterpretation or backlash from peers.⁹

At the same time, the online self becomes a “victim” of personalization. These systems refine what we see, from news feed to search results based on our previous interactions and activity. The system gathers our preferences and interests and uses them to hand-feed us content based on them. People adapt to these incentives, expressing themselves as the platform urges

⁶ VERHULST, Stefaan G. Operationalizing digital self-determination. In: *Data & Privacy* [online]. 2023. [cit. 18. 1. 2026]. Available at: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/C320AA7491A6F301BDFCB53EE2C7C5D7/S2632324923000111a.pdf/operationalizing-digital-self-determination.pdf>

⁷ The concept of filter bubbles thoroughly explained by: BRUNS, Axel. Filter bubble. In: *Internet Policy Review* [online]. 2019. [cit. 18. 1. 2026]. Available at: <https://policyreview.info/concepts/filter-bubble>

⁸ The same issue was also covered by: FLETCHER, Richard. The truth behind filter bubbles: Bursting some myths. In: *Reuters Institute for the Study of Journalism* [online]. 24.1.2020. [cit. 18. 1. 2026]. Available at: <https://reutersinstitute.politics.ox.ac.uk/risj-review/truth-behind-filter-bubbles-bursting-some-myths>

⁹ SERDAR, Mehmet. Transformation of the Surveillance Society from Panopticon to Omnicon: The Case of Black Mirror’s Episode „Nosedive“. *OPUS Journal of Society Research* [online]. 2023, p. 403-420. [cit. 18. 1. 2026]. Available at: https://www.researchgate.net/publication/371315466_Transformation_of_the_Surveillance_Society_from_Panopticon_to_Omnicon_The_Case_of_Black_Mirror's_Episode_'Nosedive'

and encourages them to. This process is often described as the “filter bubble”. The process practically wraps us into a closed environment of personalized content that reinforces our already existing views. A “filter bubble” can cause individuals to perceive themselves and the world in a very narrow and selective way, all due to algorithmic systems that keep delivering a tailored content.

The severity of these bubbles is mixed. In worst cases, it might lead to a complete ideological isolation. What is undeniable is that personalization deepens the effect of digital identity being a part of an algorithm. It’s important to see how algorithms narrow the informational and social environments in which identity develops. In these bubbles happen repeated exposures to similar viewpoints and narratives occur that reinforce certain identity traits and marginalize others. What’s practically happening is that algorithmically curated spaces selectively expose individuals to content aligned with their past behavior. The self is reflected back to the individual in increasingly homogeneous forms, creating a feedback loop. The process reshapes our self-perception. Individuals start to see their preferences, beliefs or attitudes as more fixed, more absolute, than they actually are. Exposure to different or opposing opinions becomes rarer and, when encountered, more emotionally charged.

In this sense, filter bubbles do not simply isolate individuals from alternative viewpoints. They harden the established identity and constrain the imaginative space in which identity can evolve. The outcome is that individuals in general become less exploratory and more confirmatory, prioritizing affirmation over personal growth.

Ultimately, the psychological pressure exerted by algorithmic visibility and filter bubbles reshapes identity not through force but through subtle habituation and normalization. Individuals adapt gradually, seeing content appealing to their already established opinion or belief, often without recognizing it’s effects on their self-understanding. That being said, the individuals remain formally free, yet increasingly guided by invisible auto-

mented decisions of the platform that reward users' conformity and engagement.¹⁰

5. PRESERVING PERSONHOOD IN THE AGE OF ARTIFICIAL INTELLIGENCE¹¹

The challenges posed by life in the datasphere do not end with privacy erosion linked with data collection or digital identity as an algorithm construct. AI systems not only collect data, interpret and predict it but they also increasingly decide on behalf of humans. That obviously raises a question: how can a “real” identity be preserved when our experiences are translated into data and processed by a rather autonomous system?

While self-reflection and expression of oneself are essential, the core of identity is further defined by moral judgement and contextual understanding. These qualities are hardly captured by computing models. They can reflect or try to impersonate, which makes them seem valid, however at its core it cannot be sincere and, most importantly, individual. AI systems operate by reducing individuals to probabilities and patterns.

The datasphere constructs digital identities through aggregation. AI intensifies this process by acting upon those identities, shaping what opportunities individuals see and how the individuals are categorized or treated across social, economic, and political realms.

A humane approach to AI and preserving personhood therefore requires reaffirming human privacy in decision-making and resist the normalization of human reductionism. Nowadays, we might feel that advanced AI systems could erode people by making decisions faster and on a larger scale than humans ever could. Such situation means that autonomy is fragile because

¹⁰ JOSEPH, Jeena. The algorithmic self: how AI is reshaping human identity, introspection, and agency. *Frontiers in Psychology* [online]. 2025, roč. 16, čl. 1645795. [cit. 18. 1. 2026]. Available at: <https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2025.1645795/full>

¹¹ More about this topic: NIZAMANI, Mir Muhammad, ZHANG, Hai-Li and LAI, Zhongping. Human-centered AI: advancing ethical, transparent, and context-aware systems for sustainable development. *Technology in Society* [online]. 2026, vol. 84. [cit. 18. 1. 2026]. Available at: <https://www.sciencedirect.com/science/article/pii/S0160791X25003112>

systems subtly absorb our judgment and creativity, and we slowly and willingly accept this shift as convenience or natural progress.¹²

Despite the undeniable increased efficiency and speed, it is human intervention that gives all the work produced its meaning and value. Again, AI can optimize processes, recognize patterns and generate outputs but it cannot understand why those outputs matter nor can it grasp the human consequences they carry. When decision-making is transferred to automated systems, there is an issue of responsibility becoming diffused and accountability fading, which might lead us to feel numb and detached from outcomes that nonetheless affect our lives. To prevent this and keep our identity present, it is important to keep humans “in the loop” both technically and, most importantly, existentially. Decisions shaping identities, social participations, and so on must remain grounded in human judgment, empathy, and contextual understanding. Instead of allowing AI to define what’s valuable or desirable, society needs to stay on track and insist on the main purpose of technologies: to serve us humans, not the other way around. In doing so, the always-online self remains capable of reflection and resistance within an increasingly automated world.

That being said, keeping our identities present in this world, we must defend it culturally and ethically, not technically or legally. As long as human non-measurable qualities like ambiguity, morality, and vulnerability remain the most important values, humans cannot be sidelined. Reassuring personhood means valuing our specifically humane qualities explicitly. With that, we can design AI systems that support human self-understanding, rather than supplant.

6. CONCLUSION

Life in the datasphere transforms privacy and identity by dissolving the boundary between offline experience and digital interpretation, producing an always-online self that is continuously observed, categorized, and

¹² The challenges associated with AI reshaping our world were aptly described by: KISSIGNER, Henry A., SCHMIDT, Eric and HUTTENLOCHER, Daniel. The challenge of being human in the age of AI. [online]. 2021. [cit. 18. 1. 2026]. Available at: <https://www.henrykissinger.com/articles/the-challenge-of-being-human-in-the-age-of-ai/>

even actively shaped by algorithmic systems, subtly narrowing the space for autonomy and self-definition. With this transformation, privacy as a technical concern is not the only threat there is. There is also the risk of reducing human personhood to a set of computable, quantifiable traits.

Preserving identity in this environment therefore requires resisting the reduction of human personhood to data alone and reaffirming the importance of human judgment and morality. The central challenge is not to reject digital technologies, but to ensure that identity within the digital realm remains a human process rather than an algorithmic outcome. Identity must remain a human process, preserving our unique qualities. Keeping people involved in decisions shaping their social participation and opportunities is an ethical necessity, not a design preference. Ultimately, it is up to society to decide whether the future of the always-online self lies in allowing technology to define humanity, or whether these systems remain grounded in humane values and responsibilities.

BIBLIOGRAPHY

- [1] HUMPHREYS, Stephen. Conscience in the datasphere. In: *openDemocracy* [online]. 14.3.2016. [cit. 18. 1. 2026]. Available at: <https://www.opendemocracy.net/en/digital-liberties/conscience-in-datasphere/>
- [2] NIŽETIČ, Sandro, et al. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. In: *Journal of Cleaner Production* [online]. 2020, vol. 274. [cit. 18. 1. 2026]. ISSN 0959-6526. Available at: <https://www.sciencedirect.com/science/article/pii/S095965262032922X>
- [3] FINGER, Matthias. Book review: Digital Empires. In: *Center for Digital Trust (C4DT), EPFL* [online]. [cit. 18. 1. 2026]. Available at: <https://c4dt.epfl.ch/article/book-review-digital-empires/> (The original book: Anu Bradford, Digital Empires: The Global Battle to Regulate Technology. Oxford, New York: Oxford University Press, 2023. ISBN 978-0-19-764926-8.)
- [4] VERHULST, Stefaan G. Operationalizing digital self-determination. In: *Data & Privacy* [online]. 2023. [cit. 18. 1. 2026]. Available at: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/C320AA7491A6F301BDFCB53EE2C7C5D7/S2632324923000111a.pdf/operationalizing-digital-self-determination.pdf>
- [5] BRUNS, Axel. Filter bubble. In: *Internet Policy Review* [online]. 2019. [cit. 18. 1. 2026]. Available at: <https://policyreview.info/concepts/filter-bubble>
- [6] FLETCHER, Richard. The truth behind filter bubbles: Bursting some myths. In: *Reuters Institute for the Study of Journalism* [online]. 24.1.2020. [cit. 18. 1. 2026]. Available at: <https://reutersinstitute.politics.ox.ac.uk/risj-review/truth-behind-filter-bubbles-bursting-some-myths>
- [7] SERDAR, Mehmet. Transformation of the Surveillance Society from Panopticon to Omnip-ticon: The Case of Black Mirror's Episode „Nosedive“. *OPUS Journal of Society Research* [online]. 2023, p. 403-420. [cit. 18. 1. 2026]. Available at: https://www.researchgate.net/publication/371315466_Transformation_of_the_Surveillance_Society_from_Panopticon_to_Omnip-ticon_The_Case_of_Black_Mirror's_Episode_'Nosedive'
- [8] JOSEPH, Jeena. The algorithmic self: how AI is reshaping human identity, introspection, and agency. *Frontiers in Psychology* [online]. 2025, roč. 16, čl. 1645795. [cit. 18. 1. 2026]. Available at: <https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2025.1645795/full>
- [9] NIZAMANI, Mir Muhammad, ZHANG, Hai-Li and LAI, Zhongping. Human-centered AI: advancing ethical, transparent, and context-aware systems for sustainable development. *Technology in Society* [online]. 2026, vol. 84. [cit. 18. 1. 2026]. Available at: <https://www.sciencedirect.com/science/article/pii/S0160791X25003112>
- [10] KISSIGNER, Henry A., SCHMIDT, Eric and HUTTENLOCHER, Daniel. The challenge of being human in the age of AI. [online]. 2021. [cit. 18. 1. 2026]. Available at: <https://www.henryakissinger.com/articles/the-challenge-of-being-human-in-the-age-of-ai/>

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 I/2026

OBSAH SEKCE

Martin Erlebach: HONKOVÁ, J.: <i>Koordinátor digitálních služeb</i>	128
Irena Holcová: PEJCHA, M.: <i>Videomapping z pohledu autorského práva</i>	133
Irena Holcová: SITÁRIKOVÁ, B.: <i>Digitální obsah jako věc v právním smyslu</i>	138
Irena Holcová: ŠTUKSOVÁ N.: <i>Využití chytrých smluv v autorském právu</i>	142
Adam Jareš: HUDEOVÁ, K.: <i>Elektronický systém spisové služby: Legislativní požadavky a praktické problémy implementace</i>	147
František Kasl: STOJAN, J.: <i>Data access pursuant to the Data Act in the context of personal data protection</i>	151
Pavel Loutocký: STEINER, K.: <i>Právní aspekty digitalizace dotačního řízení v programech financovaných z EU fondů</i>	156
Ondřej Málek: STROUHA, V.: <i>Právní rámec pro aplikaci umělé inteligence a velkých jazykových modelů při správě daní</i>	159
Matúš Mesarčík: HARŠÁNIOVÁ, V.: <i>Prenos osobných údajov mimo Európsku úniu</i>	165
Jakub Míšek: RŮŽIČKA, M.: <i>Zero trust security v právní úpravě ochrany osobních údajů a kybernetické bezpečnosti</i>	169

HONKOVÁ, J.: KOORDINÁTOR DIGITÁLNÍCH SLUŽEB

MARTIN ERLEBACH¹

Honková, J.: Koordinátor digitálních služeb. 2026, diplomová práce, Masarykova univerzita, Právnická fakulta, 101 s.

ANOTACE

Diplomová práce se zabývá rolí národního koordinátora digitálních služeb, kterým byl jmenován Český telekomunikační úřad (ČTÚ). Tento nově vzniklý právní institut do českého práva přináší Akt o digitálních službách (DSA). Teoretická část se soustředí na analýzu současné regulace digitálních služeb se zaměřením na nové povinnosti náležité péče pro poskytovatele zprostředkovatelských služeb a principy nařízení DSA, které se týkají činnosti ČTÚ jako národního koordinátora. Zvláštní část analyzuje nové pravomoci a povinnosti ČTÚ, včetně postupů pro nahlašování a odstraňování nelegálního uživatelského obsahu a možnosti napadnout rozhodnutí online platforem o moderaci obsahu. Cílem práce je identifikovat možné problematické aspekty národní transpozice Aktu o digitálních službách do českého právního řádu.

KLÍČOVÁ SLOVA

Digitální služby; internet; koordinátor digitálních služeb; ČTÚ; Akt o digitálních službách; DSA; moderace obsahu; certifikace; důvěryhodný oznamovatel; subjekt pro mimosoudní řešení sporů; prověřený výzkumný pracovník; zákon o digitální ekonomice; správní trestání

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 the role of the Digital Services Coordinator, designated by the Czech Telecommunication Office (ČTÚ), a position established under Czech law pursuant to the Digital Services Act (DSA). The theoretical part focuses on an analysis of the current regulatory framework for digital services, with particular attention to the new due diligence obligations imposed on providers of intermediary services and to the principles of the DSA relevant to the activities of the CTU in its capacity as the National Digital Services Coordinator. The analytical section explores the new competences and obligations conferred upon the ČTÚ, including mechanisms for the notification and removal of illegal online content, and procedures for contesting content moderation decisions made by on-line platforms. The principal aim of the thesis is to identify and assess potential legal and practical challenges associated with the transposition of the Digital Services Act into the Czech legal order.

KEYWORDS

Digital Services; Internet; Digital Services Coordinator; CTU; Digital Services Act; DSA; Content Moderation; Certification; Trusted Notifier; Alternative Dispute Resolution Entity; Verified Researcher; Digital Economy Act; Administrative Penalties

Plná verze práce je dostupná z: <https://is.muni.cz/th/r40ke/>

Autorka zvolila pro svou práci poměrně náročné téma vyžadující orientaci v navržené legislativě na národní úrovni ale zároveň i v relativně novém evropském nařízení o digitálních službách. Přestože různé rozborů nařízení DSA jsou poměrně rozšířené v zahraničí, v české právní doktríně je povědomí o tomto nařízení stále na nižší úrovni. O to více je nutné ocenit snahu autorky zabývat se tím, jak bude nařízení provedeno do českého právního řádu. Téma, které autorka zvolila, vyžaduje hlubokou orientaci v zahraničních zdrojích i silné teoretické zázemí, hodnotím proto téma práce jako velmi náročné.

Práce se dle autorky zaměřuje zejména na analýzu nového právního rámce pro online zprostředkovatelské služby, a to jak obecně, tak se zaměřením na koordinátora digitálních služeb. Dále si autorka vytyčila za cíl zabývat se kriticky zhodnotit navrženou implementační úpravu v ČR v podobě návrhu zákona o digitální ekonomice. V rámci tohoto zákona se specificky zaměřila na nová práva a povinnosti koordinátora digitálních služeb, kterým mají být Český telekomunikační úřad a Úřad pro ochranu osobních údajů. Kromě takto obecně vymezených cílů si autorka nepokládá žádnou konkrétní výzkumnou otázku. Pro obecně vymezené cíle popsané zde je možné konstatovat, že autorka je naplňuje zcela, pouze část textu věnující se kriticky návrhu zákona o digitální ekonomice je kratší. Z daného tedy vyplývá, že je práce nutně poměrně popisná, což je způsobeno už jejím prvotním zaměřením, vytyčené cíle ale plní v celém rozsahu.

Práce je rozdělena do 3 rozsáhlých kapitol s mnoha podkapitolami, úvodu a závěru. Autorka vhodně postupuje od obecného popisu regulace obsažené v DSA a cílů této regulace ke konkrétním právním a povinnostem koordinátora digitálních služeb až po navrženou úpravu práv a povinností koordinátora digitálních služeb v návrhu zákona o digitální ekonomice.

Jak již bylo naznačeno výše je text z větší části popisný. Na druhé straně ale autorka demonstruje opravdu výbornou znalost aktuální akademické diskuze ohledně kontroverzních téma navázaných na nařízení DSA jako jsou například obavy z tzv. „over blockingu“ nebo na lokální české úrovni nezávislosti Českého telekomunikačního úřadu jako koordinátora digitálních služeb a problémy s opožděnou implementací DSA v ČR. Kromě těchto témat autorka výborně poukazuje i na širší teoretická témata související s oblastí regulovanou DSA jako je virtualizace mezilidských vztahů nebo koncepty jako „Brussels effect“ a funkce platform jako definičních autorit. Takový vhled je pro tento typ práce silně nadstandardní. Tento rozhled v existující literatuře autorka demonstruje častými přímými citacemi zdrojů, které ovšem nepůsobí rušivě a jsou vhodně zakomponovány do celkového textu.

Po obsahové stránce je ale možné v některých případech najít drobné nekonzistence, namátkou autorka uvádí, že dozor nad velmi velkými online

platformami je výlučně v gesci Evropské komise podle čl. 65 DSA, což ovšem není zcela pravda. Nařízení DSA už přímo v čl. 65 ale i v následujících upravuje mechanismy spolupráce národních koordinátorů s Evropskou komisí při vymáhání nařízení DSA. Kromě toho bych v práci v úvodní části uvítal alespoň zběžnou definici toho, které subjekty podle DSA je možné považovat za ony velmi velké platformy nebo vyhledávače. Neznalému čtenáři by absence alespoň drobného vysvětlení mohla ztížit orientaci v textu. Stejně tak autora blíže nevysvětluje, co je možné si podle DSA představit pod pojmem zprostředkovatelské služby, přestože na jejich druhy během textu odkazuje. I pro tento pojem tak platí stejné výhrady jako pro VLOP a VLOSE.

Jako další konkrétnější chyby lze uvést například spojování čl. 16 DSA s institutem důvěryhodných oznamovatelů na straně 56, kteří v daném článku nejsou vůbec zmíněni nebo souvislost článku 16 DSA s mimosoudním řešením sporů ze strany 54 práce, přestože z tohoto článku není žádná souvislost přímo zjevná.

Jako poslední drobnou výtku zde uvádím, že když se autorka zajímavě zabývá extrateritorialitou DSA neuvádí, ve které části DSA kromě obecného „Brussels effect“ tuto extrateritorialitu v DSA spatřuje.

Z mého pohledu se kritice implementačního zákona v ČR a aktuální situaci v ČR autorka věnuje spíš střídmě, těsně před závěrem práce. Ocenil bych kdyby autorka své poznatky o možných nevýhodách zvolených rozhodnutí v rámci návrhu zákona o digitální ekonomice více rozvinula, ovšem kvůli předchozímu poměrně dlouhému popisu už na takový postup v práci nezůstává příliš místa. Přesto nepochybuji o odborných znalostech autorky a její schopnosti tyto kritiky formulovat již podle znění předchozího výborného textu v práci.

Na druhou stranu je ale třeba pozitivně hodnotit velmi přesný popis aktuálního stavu dozoru podle DSA v ČR. Autorka výslovně zmiňuje fakt, že Český telekomunikační úřad už provádí neformální kroky podobné správnímu řízení i přes to, že ještě není účinný implementační zákon, a jde tak o určitou „dobrou vůli“ tohoto úřadu a jeho snahu o přípravu na plnou roli koordinátora digitálních služeb v budoucnosti.

Současně chci také ocenit zahrnutí podrobných, ale stále přehledných shrnutí kapitol na konci každé ze stěžejních kapitol práce. Autorka v nich dokazuje, že dokáže vhodně identifikovat podstatné informace a čtenáři je koherentně předat.

Celkově tak práce může sloužit jako zdařilý úvod do problematiky pro zájemce i s povedenými ukazateli toho kam směřovat dále pokud ho zajímají problematičtější aspekty předpokládané činnosti koordinátora digitálních služeb.

Na tomto místě bych ještě jednou chtěl zdůraznit, že autorka opravdu skvěle pracuje s širokým rozsahem odborných i vysoce teoretických zdrojů. Uznání si zaslouží i drobná odbočka autorky k americkému a britskému právnímu systému a zdrojům pocházejícím z anglosaské právní tradice. Citací standard je také vhodně dodržen.

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>).

PEJCHA, M.: VIDEOMAPPING Z POHLEDU AUTORSKÉHO PRÁVA

IRENA HOLCOVÁ¹

Pejcha, M.: Videomapping z pohledu autorského práva. 2026, diplomová práce, Univerzita Karlova, Právnická fakulta, 76 s.

ANOTACE

Diplomová práce se zabývá právním posouzením videomappingu z pohledu českého autorského práva. Videomapping představuje moderní multimediální formu uměleckého vyjádření, která propojuje audiovizuální obsah, výtvarné prvky, zvuk, digitální technologie a konkrétní fyzický objekt, typicky architektonické dílo nebo jiný prostorově vymezený objekt. Práce reaguje na skutečnost, že platná česká právní úprava videomapping jako svébytný druh uměleckého díla výslovně neupravuje, a jeho právní kvalifikace je proto závislá na výkladu obecných ustanovení zákona č. 121/2000 Sb., autorského zákona, jakož i na judikatuře a odborné literatuře.

Cílem práce je teoreticky vymezit pojem videomappingu, analyzovat jeho právní povahu z pohledu autorského práva a posoudit, zda a za jakých podmínek může být považován za autorské dílo ve smyslu autorského zákona. Pozornost je věnována naplnění definičních znaků autorského díla, tedy tvůrčí činnosti autora, jedinečnosti výsledku a objektivního vyjádření díla, a dále otázkám originality v kontextu judikatury českých soudů a Soudního dvora Evropské unie. Práce se rovněž zabývá určením autorství a spoluautorství u videomappingu, právní povahou jeho jednotlivých složek a rozlišením tvůrčích a technických prvků.

¹ JUDr. Irena Holcová je akademickou pracovnicí Centra práva duševního vlastnictví (předchozí označení do roku 2022 Ústavu autorského práva, práv průmyslových a práva soutěžního) na Právnické fakultě Univerzity Karlovy. Kontakt: holcova@prf.cuni.cz

Významná část práce se zaměřuje na možnosti právní kvalifikace videomappingu jako audiovizuálního díla, případně jako díla výtvarného či multimedialního, a reflektuje relevantní rozhodovací praxi českých soudů. Součástí analýzy jsou rovněž otázky způsobů užití videomappingu, licencování, kolektivní správy práv a vztahu projekce k architektonickým dílům, která mohou sama podléhat autorskoprávní ochraně nebo památkové regulaci.

Metodologicky je práce založena na analýze platné právní úpravy, odborné literatury a judikatury českých soudů a Soudního dvora Evropské unie. Vzhledem k rozvoji digitálních technologií a absenci výslovné právní úpravy videomappingu se práce neomezuje pouze na výklad platného práva, ale identifikuje i jeho limity. V závěru jsou proto formulovány návrhy *de lege ferenda* směřující k přesnějšímu vymezení tzv. multimedialních děl v českém autorském právu a k posílení právní jistoty v oblasti moderních forem multimedialní tvorby.

KLÍČOVÁ SLOVA

Videomapping; multimedialní dílo; audiovizuální dílo

ABSTRACT

Thesis examines the legal assessment of videomapping from the perspective of Czech copyright law. Videomapping represents a contemporary multimedia form of artistic expression that combines audiovisual content, visual art elements, sound, digital technologies, and a specific physical object, typically an architectural work or another spatially defined structure. The thesis responds to the fact that the current Czech legal framework does not expressly regulate videomapping as an autonomous category of artistic work, and its legal qualification therefore depends on the interpretation of the general provisions of Act No. 121/2000 Sb., autorsky zakon, as well as on relevant case law and legal doctrine.

The aim of the thesis is to provide a theoretical definition of videomapping, analyse its legal nature, and assess whether and under what conditions it may be regarded as a copyrighted work within the meaning of the Copyright Act. Particular attention is paid to the fulfilment of the defining characteristics of a copyrighted work, namely the creative activity of the author, the uniqueness of

the result, and the objective expression of the work, as well as to issues of originality in the context of the case law of Czech courts and the Court of Justice of the European Union. The thesis further addresses the determination of authorship and co-authorship in videomapping projects, the legal nature of its individual components, and the distinction between creative and technical elements.

A substantial part of the thesis focuses on the possibilities of legally classifying videomapping as an audiovisual work, or alternatively as a visual or multimedia work, and reflects the relevant decision-making practice of Czech courts. The analysis also covers issues related to the modes of use of videomapping, licensing, collective rights management, and the relationship between the projection and architectural works, which may themselves be subject to copyright protection or heritage preservation regulation.

*Methodologically, the thesis is based on an analysis of the applicable legal framework, relevant academic literature, and the case law of Czech courts and the Court of Justice of the European Union. In light of the dynamic development of digital technologies and the absence of explicit legal regulation of videomapping, the thesis does not limit itself to an interpretation of the law in force but also identifies its shortcomings. The concluding part therefore formulates *de lege ferenda* proposals aimed at a more precise definition of so-called multimedia works in Czech copyright law and at strengthening legal certainty in the field of modern forms of multimedia works.*

KEYWORDS

Videomapping; Multimedia Works; Audiovisual Works

Plný text práce dostupný z: <https://dspace.cuni.cz/handle/20.500.11956/206713>

Téma práce cílené na problematiku videomappingu z pohledu autorského práva je s ohledem na absenci kvalitních odborných pramenů a rozsah využití v praxi velmi aktuální. Práce může přispět k odborné diskuzi k právní povaze videomappingu, neboť i přes komparativně zajímavé zahraniční pra-

meny je řešení výzkumné otázky v českém právním prostředí specifické. Téma tak je vysoce vhodné nejen z pohledu právní vědy, ale též aplikační právní praxe.

Téma vykazuje vyšší míru náročnosti. Vyžaduje seznámení se s odbornou literaturou, včetně cizojazyčné, s legislativou EU i legislativou tuzemskou a zásadní relevantní judikaturou českou a SDEU. K analýze a detekování problémů je potřebná dobrá orientace ohledně věcné stránky tématu. Diplomant volí především metodu deskriptivní, analytickou, komparativní a syntetickou.

Cílem diplomové práce je posouzení právní povahy videomappingu z hlediska autorskoprávního, z pohledu českého autorského práva s cílem vymezit pojem videomappingu, analyzovat jeho právní povahu z pohledu autorského práva a posoudit, zda a za jakých podmínek může být považován za autorské dílo ve smyslu autorského zákona. Zejména se zaměřuje s ohledem na povahu videomappingu na možnost jeho kvalifikace jako díla audiovizuálního v souladu s rozhodovací praxí českých soudů, či díla výtvarného nebo souborného, či zda jde o novou kategorii tzv. multimediálního díla. V rámci analýzy se diplomant zabývá též způsoby užití videomappingu, licencováním, kolektivní správou práv a vztahem projekce k architektonickým dílům, která mohou podléhat autorskoprávní ochraně a/nebo veřejnoprávní regulaci. Práce reflektuje též aktuální vliv digitálních technologií na videomapping a s ohledem na absenci výslovné právní úpravy videomappingu práce kromě výkladu platného práva identifikuje i jeho limity. Diplomant tak v závěru práce formuluje návrhy *de lege ferenda* k přesnějšímu vymezení tzv. multimediálních děl v českém autorském právu a k posílení právní jistoty v oblasti moderních forem multimediální tvorby. Autor prokázal velmi dobrou orientaci v problematice, schopnost propojit teoretické znalosti s praxí včetně porozumění aktuálním trendům v oblasti práva a splnil tak cíle práce. V práci nenalézám zásadních pochybení. Práce je v zásadě prostá formálních chyb, obsahuje funkční poznámkový aparát. Práce může sloužit jako cenný zdroj informací pro odbornou veřejnost i praxi.

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>).

SITÁRIKOVÁ, B.: DIGITÁLNÍ OBSAH JAKO VĚC V PRÁVNÍM SMYSLU

IRENA HOLCOVÁ¹

Sitáriková, B.: Digitální obsah jako věc v právním smyslu. 2026, diplomová práce, Univerzita Karlova, Právnická fakulta, 57 s.

ANOTACE

Předkládaná diplomová práce se zabývá právní povahou digitálního obsahu. Cílem práce je komplexní zpracování tématu digitálního obsahu jako věci v právním smyslu. Digitální obsah analyzuje v kontextu autorského práva, vycházejíc ze skutečnosti, že ve většině případů má povahu autorského díla, a zabývá se jeho právním režimem, včetně úvah o možné aplikaci věcných práv. Zároveň reflektuje zahraniční koncepční přístupy k jeho uchopení a související úvahy de lege ferenda.

Práce sestává z pěti částí. První část se zaměřuje na vymezení základních pojmů, přičemž analyzuje digitální obsah napříč relevantními právními prameny, včetně evropského a mezinárodního kontextu, a současně vymezuje pojem věci v právním smyslu ve vztahu k digitálnímu obsahu.

Druhá část se zabývá vztahem autorského díla a věci v právním smyslu, a to s ohledem na častý průnik kategorií digitálního obsahu a autorského díla. V této souvislosti se dále zabývá dualitou autorského díla a jeho nosiče, zejména v digitálním prostředí.

Třetí část představuje tzv. teorii vrstev jako koncepční přístup k uchopení digitálního obsahu, nacházející uplatnění v části zahraniční právní nauky. Jsou

¹ JUDr. Irena Holcová je akademickou pracovnicí Centra práva duševního vlastnictví (předchozí označení do roku 2022 Ústavu autorského práva, práv průmyslových a práva soutěžního) na Právnické fakultě Univerzity Karlovy. Kontakt: holcova@prf.cuni.cz

zde představeny jednotlivé vrstvy digitálního obsahu, aplikace dané teorie a analýza právní povahy těchto vrstev, přičemž pozornost je zaměřena zejména na logickou vrstvu digitálního obsahu, a to i v kontextu digitálního obsahu jako autorského díla.

Čtvrtá část otevírá otázku možné aplikace věcných práv na digitální obsah pro případ, že by určitá forma digitálního obsahu byla shledána věcí v právním smyslu, a uvádí argumenty pro i proti takové aplikaci.

Pátá část popisuje vybrané aspekty současné praxe v oblasti digitálního obsahu a nastíní relevantní úvahy de lege ferenda, reflektované zejména v zahraniční právní nauce.

KLÍČOVÁ SLOVA

Digitální obsah; věc v právním smyslu; autorské dílo

ABSTRACT

This thesis examines the legal nature of digital content. The aim of the thesis is to provide a comprehensive analysis of digital content as a thing in the legal sense. Digital content is analysed in the context of copyright law, reflecting the fact that it takes the form of copyrighted works in most cases, and its legal regime is addressed, including considerations concerning the possible application of property law. Additionally, it reflects foreign conceptual approaches to the legal understanding of digital content and related de lege ferenda considerations.

The thesis consists of five parts. The first part focuses on defining basic concepts and addresses the concept of digital content in relevant legal sources, including the European and international context. Furthermore, it deals with the definition of a thing in the legal sense in relation to digital content.

The second part examines the relationship between copyrighted works and things in the legal sense, with regard to the frequent overlap between digital content and copyrighted works. In this context, it further addresses the duality of copyrighted works and their carriers, particularly in the digital environment.

The third part presents the layer theory as a conceptual approach to the understanding of digital content, which has been widely applied by foreign legal scholars. It introduces the layers of digital content, the application of the theory

and analyses their legal nature, with particular emphasis on the logical layer, including in cases where digital content takes the form of copyrighted works.

The fourth part raises the question of possible property law application to digital content in cases where particular forms of digital content would be considered things in the legal sense, and sets out arguments for and against such application.

The fifth part describes relevant aspects of the current practice regarding digital content and outlines de lege ferenda considerations, reflected primarily amongst foreign legal scholars.

KEYWORDS

Digital Content; Thing in the Legal Sense; Copyrighted Work

Plná verze práce je dostupná z: <https://dspace.cuni.cz/handle/20.500.11956/206705>

Téma práce cílené na digitální obsah jako věc v právním smyslu je s ohledem na jeho zcela zásadní význam a rozsah využití v praxi velmi aktuální. Aktuálnost i v českém právním prostředí souvisí zejména nyní, kdy je digitální obsah všudypřítomný v zásadě ve všech oblastech života člověka a je i předmětem každodenních transakcí. Práce může přispět k odborné diskuzi k právní povaze digitálního obsahu, neboť i přes komparativně zajímavé zahraniční prameny je řešení výzkumné otázky podle autorky „nutně jurisdikčně specifické“. Téma tak je vysoce vhodné nejen z pohledu právní vědy, ale též aplikační právní praxe.

Téma vykazuje vyšší míru náročnosti. Vyžaduje seznámení se s odbornou literaturou, včetně cizojazyčné, s legislativou EU i legislativou tuzemskou a zásadní relevantní judikaturou zejména zahraniční. K analýze a detekování problémů je potřebná dobrá orientace ohledně věcné stránky tématu včetně procesu analýzy textů nebo dat. Diplomantka volí především metodu deskriptivní, analytickou, komparativní a syntetickou.

Cílem diplomové práce je analýza právní povahy digitálního obsahu, a to zvláště v kontextu autorského práva s ohledem na to, že ve většině pří-

padů má povahu autorského díla, včetně úvah o možné aplikaci věcných práv. Zároveň reflektuje zahraniční koncepční přístupy k jeho uchopení a související úvahy *de lege ferenda*. Kromě úvodního výkladu a vymezení základních pojmů s analýzou digitálního obsahu v kontextu českého, evropského a mezinárodního práva, se práce zaměřuje v následujících stěžejních částech na vztah autorského díla a věci v právním smyslu s ohledem na to, že digitální obsah je velmi často autorským dílem, i s ohledem na dualitu autorského díla a jeho nosiče, též v digitálním prostředí. Za velmi přínosné považuji následné představení tzv. teorie vrstev části zahraniční právní nauky coby koncepčního přístupu k výkladu digitálního obsahu. Autorka zde představuje jednotlivé vrstvy digitálního obsahu, aplikace dané teorie a analýzu právní povahy těchto vrstev, přičemž pozornost je zaměřena zejména na logickou vrstvu digitálního obsahu, a to i v kontextu digitálního obsahu jako autorského díla. S možnou aplikací této teorie v českém právním prostředí lze sice polemizovat, ale je potřebné ji znát. Práce nepomíjí ani otázku možné aplikace věcných práv na digitální obsah v případě, že by určitý digitální obsah byl věcí v právním smyslu, a uvádí argumenty pro i proti takové aplikaci. Za přínosnou lze považovat též poslední část věnovanou popisu vybraných aspektů současné praxe v oblasti digitálního obsahu včetně nástinu relevantních úvah *de lege ferenda* čerpajících zejména ze zahraniční právní nauky. Autorka prokázala velmi dobrou orientaci v problematice, schopnost propojit teoretické znalosti s praxí včetně porozumění aktuálním trendům v oblasti práva a splnila tak cíle práce. V práci nenalézám zásadních pochybení. Práce je prostá formálních chyb, obsahuje funkční a rozsáhlý poznámkový aparát. Práce může sloužit jako cenný zdroj informací i pro odbornou veřejnost. Předložená práce jak rozsahem, tak obsahem nesporně splňuje požadavky kladené na tento typ prací a lze ji doporučit k ústní obhajobě.

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>).

ŠTUKSOVÁ, N.: VYUŽITÍ CHYTRÝCH SMLUV V AUTORSKÉM PRÁVU

IRENA HOLCOVÁ¹

Štuksová, N.: Využití chytrých smluv v autorském právu. 2026, diplomová práce, Univerzita Karlova, Právnická fakulta, 56 s.

ANOTACE

Tato diplomová práce se věnuje technologii chytrých smluv (smart kontraktů) a možnostem jejich využití ve specifických institutech českého autorského práva. Hlavním cílem textu je zhodnotit, zda lze technologii smart kontraktů, fungující na bázi blockchainu, využít v oblasti kolektivní správy autorských práv a u licenčních smluv souvisejících s kolektivní správou při respektování české právní úpravy. Text se zaměřuje na potenciál zefektivnění a zrychlení ekonomických transakcí v digitálním prostředí, kde autorskoprávní ochrana čelí novým výzvám, včetně rozmachu generativní umělé inteligence. Práce je strukturována do čtyř kapitol, které postupně analyzují technickou podstatu chytrých smluv, jejich praktickou aplikaci v rámci kolektivní správy, poté v rámci licenčních smluv a závěrem řeší související právní i technické obtíže, jež brání širšímu zapojení chytrých smluv do praxe.

Analýza ukazuje, že největší potenciál pro využití chytrých smluv spočívá v jejich zapojení do procesů stávajících kolektivních správců, zejména u kolektivních správce OSA, a to především pro práva v režimu smluvní kolektivní správy. Technologie by mohla výrazně podpořit nezávislé hudební umělce tím, že zvýší efektivitu finančních transakcí a sníží náklady na převod autorských odměn. V oblasti licenčních smluv se jako reálné jeví provádění hromadných licencí

¹ JUDr. Irena Holcová je akademickou pracovnící Centra práva duševního vlastnictví (předchozí označení do roku 2022 Ústavu autorského práva, práv průmyslových a práva soutěžního) na Právnické fakultě Univerzity Karlovy. Kontakt: holcova@prf.cuni.cz

s uživateli, případně i přeshraničních licencí, ačkoliv u nich je technické provedení zatím spíše hypotetické. Klíčovým zjištěním je, že v současných podmínkách chytré smlouvy fungují spíše jako doplněk k tradiční smluvní dokumentaci, nikoliv jako její úplná náhrada, a to kvůli nutnosti jasně definovat práva, povinnosti a odpovědnost při selhání technologie.

Pro instituty autorského práva je nejrealističtější řešením využití chytrých smluv na soukromém nebo konsorciovém blockchainu, přestože tyto varianty postřádají úplnou decentralizaci. Hlavní překážkou širšího přijetí jsou nedostatky v propojení databází s hudebními díly. Práce dochází k závěru, že plné využití této technologie vyžaduje určité a srozumitelné právní nastavení a případné změny v národních i nadnárodních předpisech. Přestože chytré smlouvy nabízejí značnou optimalizaci transakcí, jejich budoucí role v oblasti autorského práva bude záviset na vyjasnění právního rámce a ochotě klíčových subjektů tuto inovaci aktivně podporovat a implementovat do svých vnitřních procesů

KLÍČOVÁ SLOVA

Chytré smlouvy; kolektivní správa; licenční smlouva

ABSTRACT

This Master's thesis examines smart contract technology and its potential application within specific institutes of Czech copyright law. The primary objective of the research is to evaluate whether blockchain-based smart contracts can be effectively utilised in the fields of collective rights management and related licensing agreements, while respecting the existing Czech legal framework. The study focuses on the potential for streamlining and accelerating economic transactions in a digital environment where copyright protection faces novel challenges, including the rise of generative artificial intelligence. The thesis is structured into four chapters, which sequentially analyse the technical nature of smart contracts, their practical application within collective management and licensing agreements, and finally, the legal and technical obstacles hindering more extensive practical implementation.

The analysis demonstrates that the greatest potential for smart contracts lies in their integration into the processes of existing collective management organi-

sations (CMOs), specifically OSA, particularly regarding rights under the voluntary collective management regime. This technology could significantly support independent musical artists by increasing the efficiency of financial transactions and reducing the costs associated with the transfer of royalties. Within the sphere of licensing, the execution of mass licensing agreements with users, or potentially cross-border licences, appears feasible, although the technical implementation of the latter remains largely hypothetical. A key finding of the research is that, under current conditions, smart contracts serve as a supplement to traditional contractual documentation rather than a complete replacement, due to the necessity of clearly defining rights, obligations, and liability in the event of technological failure.

For copyright institutes, the most viable solution appears to be the use of smart contracts operating on private or consortium blockchains, despite these variants lacking full decentralisation. The primary obstacle to broader adoption remains the insufficient interconnection of musical work databases. The thesis concludes that the full utilisation of this technology requires a certain and intelligible legal framework, as well as potential amendments to both national and supranational regulations. Although smart contracts offer substantial transactional optimisation, their future role in copyright law will depend on the clarification of the legal environment and the willingness of key stakeholders to actively support and implement this innovation within their internal processes.

KEYWORDS

Smart Contracts; Collective Management, Licensing Agreement

Plná verze práce je dostupná z: <https://dspace.cuni.cz/handle/20.500.11956/206716>

Téma práce věnované technologii chytrých smluv (smart kontraktů) a jejich využití v autorském právu, kdy je navíc hlavním cílem práce analýza a zhodnocení využití technologie smart kontraktů, fungující na bázi blockchainu, v oblasti kolektivní správy autorských práv a licenčních smluv souvisejících s kolektivní správou podle české právní úpravy, je s ohledem na

jeho stále se zvyšující význam a rozsah využití v praxi vysoce aktuální. Práce může velmi přispět též k odborné diskuzi k možnostem využití uvedených technologií právě v tomto segmentu. Téma tak je vysoce vhodné nejen z pohledu právní vědy, ale též aplikační právní praxe.

Téma vykazuje vyšší až vysokou míru náročnosti. Vyžaduje seznámení se s odbornou literaturou (kdy cílené na využití smart kontraktů v kolektivní správě mnoho není), včetně cizojazyčné, s legislativou EU i legislativou tuzemskou a zásadní relevantní judikaturou zejména zahraniční. K analýze a detekování problémů a účely analýzy je potřebná jak dobrá orientace ohledně věcné stránky tématu, tak ale i zjištění praxe kolektivních správců. Diplomantka volí především metodu deskriptivní, analytickou, komparativní a syntetickou.

Cílem diplomové práce je analýza využití chytrých smluv v českém autorském právu, a to se soustředěním na dvě klíčové oblasti, kde lze uvažovat praktické uplatnění této technologie, a to v rámci kolektivní správy autorských práv a licenčních smluv při jejím výkonu využívaných. Kromě úvodního technického výkladu a vymezení základních pojmů, který je zcela nezbytný s ohledem na zaměření a cíle práce pro další rozbor, se práce zaměřuje v následujících stěžejních částech na téma samé. Druhá kapitola je věnována využití smart kontraktů v rámci kolektivní správy, kdy jednotlivé vybrané modelové situace přicházející do úvahy jsou předmětem výkladu jednotlivých subkapitol. Součástí této kapitoly jsou pro analýzu i závěry z ní plynoucí velmi přínosné výklady obsažené ve vyjádřeních zástupce kolektivního správce OSA k této problematice. Navazující třetí kapitola pak rozebírá dva typy licenčních smluv, využívaných v kolektivní správě, pro které by technologie chytrých smluv mohla být relevantní, a jež souvisí s výkonem kolektivní správy. Poslední kapitola pak obsahuje shrnutí analyzovaných situací, z analýzy vyplývající závěry a rozbor souvisejících problémů, ať již právních či technických, spojených s aplikací chytrých smluv bránících jejich širší aplikaci v praxi. Autorka prokázala velmi dobrou orientaci v problematice, a to se zjevnou znalostí věcných konsekvencí, schopnost propojit teoretické znalosti s praxí včetně porozumění aktuálním trendům v oblasti práva a splnila tak plně cíle práce. V práci

nenalézám zásadních pochybení. Práce je prosta formálních chyb, obsahuje funkční a rozsáhlý poznámkový aparát. Práce může sloužit jako cenný zdroj informací i pro odbornou veřejnost a lze doporučit s ohledem na absenci kvalitních výkladů na uvedené téma její publikaci v některém z recenzovaných odborných periodik zařazených např. v databázích WoS nebo Scopus. Předložená práce jak rozsahem, tak obsahem nesporně splňuje, ale i převyšuje, požadavky kladené na tento typ prací.

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>).

HUDEOVÁ, K.: ELEKTRONICKÝ SYSTÉM SPISOVÉ SLUŽBY: LEGISLATIVNÍ POŽADAVKY A PRAKTICKÉ PROBLÉMY IMPLEMENTACE

ADAM JAREŠ¹

Hudeová, K.: Elektronický systém spisové služby: Legislativní požadavky a praktické problémy implementace. 2026, závěrečná práce programu LL.M. v právu informačních a komunikačních technologií, Masarykova univerzita, Právnická fakulta, 84 s.

ANOTACE

Závěrečná práce analyzuje legislativní požadavky na elektronický systém spisové služby (eSSL) ve veřejné správě České republiky a upozorňuje na problematické aspekty jejich implementace. Obecná část představuje eSSL jako nástroj spisové služby a vymezuje jeho právní rámec na národní i nadnárodní úrovni. Zvláštní část se soustředí na praktické problémy spojené s implementací tohoto právního rámce, zejména v oblastech uchovávání elektronických dokumentů a atestace eSSL. Cílem je kriticky zhodnotit právní úpravu v kontextu praxe a nastínit možné směry dalšího vývoje.

KLÍČOVÁ SLOVA

Veřejná správa; elektronický dokument; důkazní spolehlivost; nařízení eIDAS; elektronický systém spisové služby; atestace; transakční protokol

¹ JUDr. Adam Jareš, Ph. D. je externím spolupracovníkem Ústavu práva a technologií na Masarykově univerzitě v Brně a zakladatel platformy Legální kód. Kontakt: adam@legal-nikod.cz.

ABSTRACT

The thesis analyses legislative requirements for the electronic filing system (eSSL) in public administration in the Czech Republic and points out problematic aspects of their implementation. The general part presents eSSL as a tool of records management and defines its legal framework at national and supranational levels. The special part focuses on practical problems of implementation, particularly the pre-servation of electronic documents and the attestation of eSSL. The aim is to critically assess the legal regulation in practice and outline possible directions for future development.

KEYWORDS

Archiving by Design; Public Administration; Electronic Document; Evidentiary Reliability; eIDAS Regulation; Electronic Filing System; Certification; Transaction Log

Plná verze práce je dostupná z: <https://is.muni.cz/th/qi08v/>

Informační systémy veřejné správy a elektronické systémy spisových služeb představují podle mého názoru tu nejsložitější a nejhůře uchopitelnou právní úpravu v rámci předpisů, které lze řadit mezi předpisy upravující eGovernment. Uchazečka si jako své téma vybrala „Elektronický systém spisové služby: Legislativní požadavky a praktické problémy implementace“. S určitou mírou nadsázky musím ocenit její odvahu vypořádat se s tímto tématem. Jeho úprava je totiž značně nepřehledná a začíná v rámci regulace informačních systémů veřejné správy, pokračuje přes úpravu archivnictví a spisové služby, až po vyhlášku o podrobnostech výkonu spisové služby a Národní standard elektronické spisové služby. A platí, že žádný z těchto předpisů není napsán příliš uživatelsky přívětivě. Také je nutné pro pochopení tématu pochopit i technické a uživatelské souvislosti elektronický systém u spisových služeb. K tématu navíc neexistuje mnoho použitelné literatury.

Uchazečka vymezila cíl takto: „Cílem práce je nejen analyzovat aktuální legislativní požadavky kladené na eSSL, ale také kriticky zhodnotit problematické aspekty jejich implementace do praxe a nastínit možné směry dalšího vývoje.“ Jelikož byl cíl práce stanoven takto široce, uchazečka jej splnila. Osobně bych nicméně preferoval, pokud byl cíl vymezen více specificky a ideálně v rámci tématu stanoveny i výzkumné otázky.

První část práce je velmi popisná bez většího vlastního hodnocení zkoumané problematiky. To nemusí být nutně na škodu, pokud je takový zdoluhavý popis následně podkladem pro vlastní závěry a zjištění v dalších částech textu. Uchazečka v této první části navíc prokázala dostatečně hlubokou znalost tématu a přehled o jeho různých aspektech. Na ni navazuje druhá část s velmi praktickým textem plným vlastních závěrů uchazečky. Tato druhá část je velmi povedená, a celkově tak lze hodnotit práci velmi pozitivně.

Obecně lze konstatovat, že není důvod uchazečce přisuzovat nějaké nedostatky závěrečné práce. Osobně pouze bojuji s textem na straně 20, ze kterého vyplývá že čistě vizuální nebo zvukové stopy neunesou informaci. Není mi příliš jasné, z čeho takto uchazečka usuzuje. Je v této souvislosti také vhodné připomenout, že v rámci elektronických spisových služeb lze pracovat i s video formáty, zvukovými formáty i audiovizuální formáty. Ocenil bych také rozlišení mezi pojmy „data“ a „informace“, jelikož jsem přesvědčený, že je nelze směřovat.

Vyzdvihnout lze například část práce, která se zabývá praktickými problémy spojenými s atestací elektronických systémů spisových služeb. Nejde přitom o jednoduchou otázku, která má ale zásadní dopady na výkon spisové služby veřejnoprávních původců a na trh subjektů nabízejících elektronické systémy spisových služeb.

Uchazečka pro svoji práci využila řadu legislativních i nelegislativních zdrojů včetně důvodových zpráv a metodických materiálů. V rámci tématu není dostupné větší množství literatury a toto omezené množství uchazečka využila velmi vhodně. V rámci tohoto specifického tématu byla schopná čerpat i z cizojazyčných zdrojů. Uchazečka píše text velmi srozumitelně

i v rámci tohoto složitého a vysoce technického tématu. Text je i z jazykového pohledu v podstatě bez jakýchkoliv nesprávností.

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>).

STOJAN, J.: DATA ACCESS PURSUANT TO THE DATA ACT IN THE CONTEXT OF PERSONAL DATA PROTECTION

FRANTIŠEK KASL¹

Stojan, J.: Data access pursuant to the Data Act in the context of personal data protection. 2026, diplomová práce, Masarykova univerzita, Právnická fakulta, 98 s.

ANOTACE

Diplomová práce se zabývá otázkou přístupu k údajům podle soukromého práva v rámci nařízení (EU) 2023/2854 (Nařízení o datech) v kontextu práva na ochranu osobních údajů podle nařízení (EU) 2016/679 (GDPR). Cílem práce je identifikovat základní principy a povinnosti vyplývající z těchto nařízení a analyzovat jejich vzájemný vztah v kontextu současné právní situace v Evropské unii. Autor bude vycházet z předpokladu, že současná široká interpretace pojmu „osobní údaje“ způsobuje uplatnitelnost protichůdných povinností vyplývajících z těchto dvou nařízení, což v praxi může vést k situaci, kdy splnění jedné povinnosti (povinnosti zveřejnit) automaticky vede k porušení druhé (povinnosti chránit) a naopak. Výzkumnou otázkou práce bude: „Jaké jsou konflikty mezi povinnostmi vyplývajících ze zákona o datech a GDPR a jak lze tyto konflikty vyřešit legislativně a interpretačně?“

KLÍČOVÁ SLOVA

Nařízení o datech; GDPR; Ochrana osobních údajů; Přístup k datům; Internet věci

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

ABSTRACT

The thesis addresses the issue of private law access to data under Regulation (EU) 2023/2854 (Data Act) in the context of the right to personal data protection under Regulation (EU) 2016/679 (GDPR). The aim of the thesis is to identify the basic principles and obligations arising from these regulations and to analyse their mutual relationship in the context of the current legal situation in the European Union. The author will work on the assumption that the current broad interpretation of the term "personal data" causes the applicability of conflicting obligations arising from these two regulations, which in practice can lead to a situation where the fulfilment of one obligation (the obligation to disclose) automatically results in a violation of the other (the obligation to protect) and vice versa. The research question of the thesis will be: "What are the conflicts between the obligations arising from the Data Act and the GDPR, and how can these conflicts be resolved legislatively and interpretatively?"

KEYWORDS

Data Act; GDPR; Personal Data Protection; Data Access; Internet of Things

Plná verze práce je dostupná z: <https://is.muni.cz/th/b2b98/>

V této práci se autor rozhodl zpracovat téma v současné době v odborném diskurzu nedořešené a tudíž náročné na uchopení. Zhostil se ho zdárně a přínos vidím nejen v rozboru, který v práci poskytl, ale ve skutečnosti, že text je psaný anglicky a může tedy snadno sloužit jako podklad pro další kvalitní odbornou činnost.

Cílem práce bylo odhalit, zda existuje výkladový či aplikační konflikt mezi Nařízením o datech (dále jen "DA") a Obecným nařízením o ochraně osobních údajů (dále jen "GDPR"). K tomuto cíli práce jako celek konzistentně směřuje, autor řadu napětí a výkladových výzev identifikuje a v rámci diskuzní části práce se s nimi zdařile vypořádává.

Autor předložil ambiciózní akademický počín, ve kterém se nezalekl náročného tématu a předložil kvalitně zpracovanou a myšlenkově bohatou práci, která mě svým důsledným a systematickým pojetím a zpracováním vedla k důslednějším zamyšlením nad prezentovanými pnutími a výkladovými výzvami mezi GDPR a DA. To, že je práce takto "thought-provoking" pokládám za velmi pozitivní. Autor zdárně poukázal na výkladovou náročnost zvolené problematiky a vhodně popsal její současnou dynamiku. Svou prací přispívá do živoucího odborného diskurzu, ve kterém je řada otázek stále nevyjasněných a rozdílnost váhy či závažnosti, který je ve výkladu ustanovení DA při kontrastu s GDPR zvolen, může vést k odlišným závěrům, které lze v současné době sledovat v odborných kruzích.

Struktura práce je jasná a systematická a zvolené čtyři obsahové kapitoly představují odlišné, ale vhodně propojené bloky, ve kterých autor nejprve v kapitole 2 výstižně zachycuje širší kontext, poté v kapitole 3 představuje relevantní právní rámec, načež v kapitole 4 zdůrazňuje identifikované výkladové výzvy, se kterými se v kapitole 5 s pomocí vhodně formulovaného modelového příkladu diskuzně a argumentačně vypořádává.

Kapitola 2 může být vnímána jako příliš široký úvod k tématu, když se autor vydává poměrně dávno do historie k původu digitálního zachycení dat, pokládám to však za vhodné prokázání, že má autor širší chápání základů a podstaty prostředí, na které se následně analyzované regulační rámce vztahují i čtenářsky zajímavé střípky informací, které dokreslují celistvé uchopení zkoumané otázky. Zároveň oceňuji, že autor prokázal velmi efektivní způsob koncentrace informací, kdy stručně, výstižně, ale přitom informačně hutně popisuje klíčové aspekty a jejich podstatu či původ. Autor důsledně editoval a provázal text, který obsahuje výstižné úvody ke kapitolám shrnující jejich roli v rámci práce, vhodné oslí můstky a přechody a výstižná průběžná shrnutí. V textu také pravidelně odkazuje napříč kapitolami, ať pro zdůraznění, proč je určitý pojem na daném místě rozebírán nebo odkázání na podrobnější analýzu v pozdější části práce. Zde je ovšem škoda, že autor zpravidla odkazuje poměrně obecně, což poněkud znesnadňuje nalezení příslušné reference v dané části textu práce.

I kapitola 3 začíná poměrně podrobným historickým exkurzem k základům, na kterých řešená právní úprava stojí a důvodech a okolnostech, které vedly k jejímu vzniku a přijetí v její současné podobě. Oceňuji práci autora s judikaturou Soudního dvora i rozhodovací praxí Evropské komise, např. výstižný rozbor rozhodnutí ve věci Google a Fitbit.² Ze shrnutí vývoje úpravy neosobních údajů je zřejmé, že se autor orientuje v širším regulačním rámci EU pro digitální služby a chápe vztahy mezi jednotlivými předpisy i jejich odlišné role a cíle.

Je vhodné, že autor napříč prací pracuje s návrhem nařízení Digital Omnibus, byť méně, než bych očekával. V závěru kapitoly též autor dle mého názoru příliš lpí na tom, že pro neosobní údaje by měl platit stejný režim volného toku jako pro osobní údaje a regulace v EU tedy tuto mezeru dohání.

Základním pnutím, které autor mezi DA a GDPR v kapitole 4 identifikuje, je problém vymezení osobních údajů. Jak výstižně shrnuje, k tomuto bylo napsáno odbornou veřejností a odjudikováno Soudním dvorem již mnohé a hlavní pozornost se nyní váže k důsledkům rozhodnutí Soudního dvora ve věci C-413/23P EDPS proti SRB. Dále autor upozorňuje na pnutí mezi principy GDPR a DA. Na tomto místě práce je ovšem dle mého názoru nedostatečně zohledňovaný bod odůvodnění 7 DA, který stanoví prioritu hodnot chráněných GDPR. To je umocněno bodem odůvodnění 8, který upřesňuje, že při identifikaci významného rizika pro jednotlivce je klíčové dodržení principu minimalizace dat. To dále posiluje bod odůvodnění 34, kdy je na smíšené datasety nutno nahlížet jako na datasety osobních údajů a z toho vyplývajících omezení výkladu ustanovení DA. Autor s těmito ustanoveními pracuje, přesto v některých částech až poněkud tvrdošíjně hledá přetrvávající výkladové nedostatky, které by mohly i přes tyto body odůvodnění přetrvávat.

V kapitole 5 autor vhodně využívá modelové případové studie, aby zpřehlednil náročné datové vazby, které mezi subjekty mohou být a aplikoval na ně dosavadní zjištění a testoval pnutí, která mezi GDPR a DA odhalil.

² Viz s. 37 závěrečné práce.

K problému smíšených datasetů³ si dovolím poznamenat, že na výrobce dopadá povinnost dle článku 3 odst. 1 DA designu produktu tak, aby umožňoval sdílení dat ve stanoveném formátu, míří tedy na odstranění technických překážek, které by mohly později bránit sdílení dat, ale nevede k povinnosti sdílet data. K tomu slouží režim článku 4 DA, který skrze zmíněný odst. 12 omezuje povinnost sdílet osobní údaje (resp. smíšené datasety, protože je s nimi nutno nakládat stejně), pokud pro to není doložen či proaktivně ze strany držitele dat zajištěn právní základ dle článku 6 (resp. 9) GDPR. Jeho absence přitom bude pouze v případě, že uživatel není subjekt údajů (jinak je základem jeho souhlas vyplývající ze žádosti o tato data), a toto omezení se s ohledem na prioritu hodnot ochrany soukromí jeví jako zcela záměrné omezení dosahu DA (nedopadá totiž na technická metadata či jiná neosobní data).

Doporučení, která autor formuluje⁴ jsou dobrým teoretickým základem pro vodítko, které v podstatě vychází ze standardního posouzení zpracování dle GDPR, vyhodnocení jeho přiměřenosti, zákonnosti, rizik a limitů. Byl bych ovšem opatrný s hodnocením, jaký je podíl osobních údajů v datasetu a vyvozováním právních důsledků z tohoto poznatku, jelikož početně

malý podíl může přesto být významný co do dopadů na práva dotčených subjektů údajů a kvantifikace toho, co představuje jeden osobní údaj může být také poměrně problematická a těžko zobecnitelná.

Závěrem bych chtěl tedy vyzdvihnout, že práce je zde mého značně zdařilá. Autor se projevil jako způsobilý hloubkové analýzy právní úpravy a hodnotného přispění do odborného diskurzu k této stále živý a dynamicky se vyvíjející problematice.

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>).

³ Viz s. 69 závěrečné práce.

⁴ Viz podkapitola 5.3.1. závěrečné práce.

STEINER, K.: PRÁVNÍ ASPEKTY DIGITALIZACE DOTAČNÍHO ŘÍZENÍ V V PROGRAMECH FINANCOVANÝCH Z EU FONDŮ

PAVEL LOUTOCKÝ¹

Steiner, K.: Právní aspekty digitalizace dotačního řízení v v programech financovaných z EU fondů. 2026, závěrečná práce programu LL.M. v právu informačních a komunikačních technologií, Masarykova Univerzita, Právnická fakulta, 80 s.

ABSTRAKT

Tato práce je zaměřená na právní i praktickou stránku digitalizace poskytování evropských dotací v ČR. Současné dotační řízení je pro projekty financované z EU fondů sjednoceno a vedeno ve společném elektronickém systému. V první řadě shrnuje práce vývoj obecného právního rámce řízení o poskytnutí dotace pro nastolení kontextu. V další části je rozebrán právní rámec pro řízení související s implementací dotačních projektů. Hlavní část práce se pak věnuje procesu digitalizace řízení vedených v souvislosti s implementací dotačních projektů a programů a popisu aktuální praxe digitalizovaného dotačního řízení. V závěru se práce zaměřuje na identifikaci dalších možných kroků, které by vedly k vytvoření komplexního a efektivního prostředí pro implementaci dotací jak z úhlu pohledu žadatelů a příjemců dotací, tak z pohledu potřeb poskytovatelů dotací a dalších subjektů v implementační struktuře.

¹ JUDr. Pavel Loutocký, PH.D., BA (Hons) je odborným asistentem na Ústavu práva technologií Právnické fakulty Masarykovy Univerzity. Kontakt: loutocky@muni.cz.

KLÍČOVÁ SLOVA

Dotace z EU fondů; řízení o poskytnutí dotace; eGovernment; informační systémy státní správy; digitalizace dotačního řízení

ABSTRACT

This thesis focuses on the legal and practical sides of the digitalisation of the procedure for granting EU funded subsidies in the Czech Republic. The current procedure for EU granted projects is unified and managed in a shared electronic system. The first part of the thesis provides context by summarising the development of the general legal framework for grant procedures. In the following part, the legal framework for procedures related to the implementation of subsidy schemes is described. The central part of the thesis concentrates on the digitalisation of procedures related to the implementation of subsidy schemes and programmes, and delineates current practices in the digitalised subsidy procedure. The final chapters identify potential next steps to create a comprehensive, effective environment for implementing subsidies for applicants and beneficiaries, as well as subsidy providers and other entities within the implementation framework.

KEYWORDS

Frants from EU Funds; Grant Award Procedures; eGovernment; Government Information Systems; Digitization of Grant Award Procedures

Plná verze práce je dostupná z: <https://is.muni.cz/th/nampk/>

Volbu tématu považuji za zdařilou a aktuální. Problematika digitalizace dotačního řízení ve vztahu k fondům Evropské unie je odborně náročná, dynamická a současně i prakticky významná (a to mj. s ohledem na rozsah čerpání prostředků EU v České republice a kontinuálně se vyvíjející právní i technologický rámec). Autorka se této problematice ujala vhodně, do zpracování práce se zřetelně projevila její dlouhodobá praktická zkušenost v dané oblasti. Ačkoliv práce příliš neakcentuje hlubší doktrinní diskusi,

v tomto případě to z mého pohledu nepůsobí jako nedostatek. Silnou stránkou práce je schopnost převést komplexní právní a metodické prostředí do podoby srozumitelné, kontextualizované a reflektující praxi administrace dotací.

Práce poskytuje podrobný popis vývoje národní i komunitární úpravy až po současný systém MS2014+ a MS2021+. Obzvláště oceňuji podrobný popis praktického fungování monitorovacích systémů, propojení s dalšími systémy veřejné správy a zachycení interakcí mezi poskytovatelem a příjemcem dotace. Výstupy z monitorovacích systémů jsou popsány věcně, z textu je patrné pochopení jejich významu pro správu dotací. Přínosem práce je rovněž identifikace problematických aspektů digitalizovaného řízení – zejména otázky vedení spisu, napojení na spisovou službu, roztržitost právního rámce či přetrvávající nesouladu mezi procesní realitou a požadavky správního řádu.

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>).

STROUHA, V.: PRÁVNÍ RÁMEC PRO APLIKACI UMĚLÉ INTELIGENCE A VELKÝCH JAZYKOVÝCH MODELŮ PŘI SPRÁVĚ DANÍ

ONDŘEJ MÁLEK¹

Strouha, V.: Právní rámec pro aplikaci umělé inteligence a velkých jazykových modelů při správě daní. 2026, diplomová práce, Univerzita Karlova, Právnická fakulta, 90 s.

ANOTACE

Diplomová práce zkoumá, v jaké míře současný právní řád umožňuje využití umělé inteligence, včetně velkých jazykových modelů, při správě daní v České republice a jaké jsou hlavní právní limity a požadavky, které musí taková implementace splnit. Na základě právně-dogmatické analýzy, judikatury a komparativní metody je vyložen ústavní rámec (princip legality, proporcionality a právo na spravedlivý proces), relevantní právo Evropské unie (zejména AI Akt a GDPR), mezinárodní standardy (OECD a Rada Evropy) a národní právní úprava (správní řád a daňový řád).

Práce ukazuje, že české právo již určitou míru automatizace připouští, a to převážně v podpůrných režimech, jako je například: analytika, třídění podání, vytipování rizik, generování podkladů. Klíčovou hranicí zůstává vydávání meritorních rozhodnutí, kde procesní pravidla nadále předpokládají lidské posouzení, přezkoumatelné odůvodnění a možnost odvolání. Současné jsou identifikována specifická rizika nasazení AI ve správě daní, zejména: netransparenčnost, systematické zkreslení, halucinace a otázky mlčenlivosti, odpovědnosti

¹ JUDr. Ondřej Málek, Ph.D. je odborným asistentem Katedry finančního práva a finanční vědy na Právnické fakultě Karlovy univerzity v Praze. Kontakt: malek@prf.cuni.cz

a auditovatelnosti a jsou popsány nástroje jejich řízení (dokumentace, testování, logování, průběžné vyhodnocování a pravidelné audity).

V aplikační části jsou posouzeny možnosti a limity automatizace daňové kontroly a správního trestání. Na tuto analýzu poté navazují návrhy *de lege ferenda*. Jádrem doporučení je postupná, právně ukotvená implementace: využívat AI přednostně pro standardizované a rutinní úkony (screening, analytika, generování podkladů a prvoinstanční rozhodnutí s možností lidského přezkumu a jednoduchého zrušení rozhodnutí podáním opravného prostředku, obdobně jako u institutů platebního rozkazu nebo trestního příkazu). V části *de lege ferenda* je navržen dvoustupňový model změn kombinující automatizační klauzuli v daňovém řádu (stanovující minimální procesní záruky, zejména: transparentnost, auditovatelnost a možnost účinného přezkumu), navazující specifikace u vybraných daní (konkretizující, pro které agendy a v jakém rozsahu lze AI využít) a návrh na rozšíření daňové mlčenlivosti i na dodavatele technických řešení.

KLÍČOVÁ SLOVA

Správa daní; umělá inteligence; velké jazykové modely; automatizované rozhodování; AI Akt; GDPR; daňový řád

ABSTRACT

This master's thesis examines the extent to which the current legal framework allows the use of artificial intelligence, including large language models, in the tax administration in the Czech Republic, and identifies the key legal limits and requirements that such implementation must meet. Based on doctrinal legal analysis combined with case-law and comparative methods, the thesis outlines the constitutional framework (the principles of legality and proportionality and the right to a fair trial), the relevant EU law (notably the AI Act and the GDPR), international standards (OECD and the Council of Europe), and the national procedural framework (the Administrative Procedure Code and the Tax Procedure Code).

The thesis shows that Czech law already allows for a certain degree of automation, mainly in supportive functions such as analytics, filing sorting, risk identification, and support documents generation. A key boundary remains the is-

suance of substantive decisions, where procedural rules still presume human assessment, reviewable reasoning, and effective means of defence. At the same time, the thesis identifies specific risks of deploying AI in tax administration (especially lack of transparency, systematic bias, hallucinations, and issues of confidentiality, liability, and auditability) and describes instruments for mitigating these risks (documentation, testing, logging, continuous evaluation, and regular audits).

In the applied section, the thesis assesses the options and limits of automating tax audits and administrative punishment (administrative penalties). This analysis is followed by proposals de lege ferenda. The core recommendation is a gradual, legally embedded implementation: prioritising AI for standardised and routine tasks (screening, analytics, generation of supporting materials, and first-instance decisions subject to human review and easy annulment through a remedial instrument), similar to the mechanisms of a payment order or a criminal penalty order. The de lege ferenda section proposes a two-tier model of reform combining (i) an automation clause in the Tax Procedure Code establishing minimum procedural safeguards (particularly transparency, auditability, and the possibility of effective review) and (ii) subsequent specification in selected tax statutes, defining the agendas and scope in which AI may be used, together with a proposal to extend tax confidentiality obligations to suppliers of technical solutions.

KEYWORDS

Tax Administration; Artificial Intelligence; Large Language Models; Automated Decision-Making; AI Act; GDPR; Tax Code

Plná verze práce je dostupná z: <https://dspace.cuni.cz/handle/20.500.11956/207733>

Téma využití umělé inteligence (včetně velkých jazykových modelů) ve správě daní je vysoce aktuální – jednak z důvodu rychlého praktického rozšíření generativní AI po roce 2022, jednak pro intenzivní tlak na modernizaci a efektivitu veřejné správy, a zároveň pro nárůst regulatorních

požadavků (AI Act, GDPR apod.). Autor zasazuje téma „rychlosti vývoje“ AI do kontextu (právní) připravenosti na využití AI ve veřejné správě.

Aktuálnost je v práci podložena i konkrétním a poměrně dobře testovatelným vymezením cíle a výzkumné otázky. Autor zkoumá „v jaké míře umožňuje současná legislativa implementaci umělé inteligence ve správě daní a jaké jsou hlavní právní limity“.

Za drobnou metodickou rezervu považují, že autor neformuluje explicitně několik dílčích výzkumných otázek (resp. hypotéz). Dílčí otázky však fakticky nahrazuje systematickým rozvržením kapitol, které k naplnění cíle směřují.

Zvolené téma je náročné jak teoreticky, tak metodologicky. Vyžaduje orientaci v daňovém právu a procesních institutech správy daní, v obecném správním právu, v ústavních limitech výkonu veřejné moci a ve významné části unijní regulace (AI Act, GDPR) včetně judikatury. Náročnost dále zvyšuje nezbytný přesah do technického vysvětlení fungování AI/LLM, bez něž nelze kvalifikovaně hodnotit otázky transparentnosti, přezkoumatelnosti, „halucinací“ či systematického zkreslení.

Metodicky diplomant volí právně-dogmatický přístup doplněný judikturní a komparativní analýzou; v aplikační části hodnotí možnosti automatizace v daňové kontrole a správním trestání a doplňuje práci hloubkovým rozhovorem se zástupci GŘŘ. Zvolené metody odpovídají stanovenému cíli (mapování právního rámce + kritické vyhodnocení + návrhy *de lege ferenda*) a vedou k poměrně konkrétním závěrům o tom, co je již dnes právně možné a kde jsou limity.

Diplomant v úvodu vymezuje kontext rychlého rozvoje AI a jeho dopady na veřejnou správu, odůvodňuje relevanci tématu pro správu daní a formuluje výzkumnou otázku a cíl práce. Dále stručně popisuje postup zpracování a použité metody, včetně uvedení limitů (rychle se vyvíjející praxe a neúplná empirická data).

Druhá část práce systematicky definuje klíčové pojmy. Nejprve autor vysvětluje technické pojmy (digitalizace, automatizace, AI, strojové učení, generativní AI a LLM, regulační sandbox), poté přidává právní ukotvení

(daň, správa daní, daňová a finanční správa). Tím vytváří společný pojmový základ pro další právní analýzu.

Třetí, nejobsáhlejší část mapuje relevantní právní rámec. Diplomant postupuje od ústavních principů a judikatury (legalita, proporcionalita, spravedlivý proces, soukromí) přes unijní regulaci (zejména AI Act a GDPR) a mezinárodní standardy až k národní úpravě (správní řád, daňový řád). Průběžně uvádí implikace těchto pravidel pro automatizaci a AI a doplňuje je tabulkovými shrnutími závěrů.

Následně diplomant kombinuje komparaci zahraničních přístupů a popis praktického rámce využitelnosti AI ve správě daní. Využívá zahraniční inspiraci (včetně modelů umožňujících automatizaci při omezení správní diskrce a důrazu na soudní přezkum) a propojuje ji s českou realitou (technické možnosti, institucionální limity, praxe Finanční správy).

Pátá kapitola identifikuje klíčová rizika implementace AI ve správě daní (netransparentnost, systematické zkreslení, „halucinace“, otázky mlčenlivosti, odpovědnosti a auditovatelnosti) a popisuje nástroje jejich řízení (dokumentace, testování, logování, průběžné vyhodnocování a audit). Autor se snaží tato rizika převést do konkrétních požadavků na právní i technické nastavení systémů.

V poslední kapitole diplomant hodnotí možné aplikační scénáře (zejména daňová kontrola a správní trestání) a na jejich základě formuluje návrhy změn de lege ferenda. Jádrem návrhů je myšlenka postupné a kontrolované automatizace s důrazem na procesní záruky, lidský dohled a přezkoumatelnost. V textu se objevuje i návrh „dvoustupňového“ legislativního modelu kombinujícího obecné zmocnění a úpravy v oborových zákonech.

V závěru diplomant výslovně uvádí, že odpověděl na výzkumnou otázku. Shrnuje, že české právo připouští určitý stupeň automatizace, zejména v podpůrných režimech (analytika, třídění podání, tipování rizik, generování podkladů), avšak jako klíčovou hranici označuje vydávání meritorních rozhodnutí, u nichž procesní pravidla předpokládají lidské posouzení, odůvodnění a opravné prostředky.

Členění práce je v logické a systematické. Diplomant postupuje od základních pojmů přes pozitivněprávní úpravu k aplikaci, identifikaci rizik

a následně k návrhům de lege ferenda. V závěru shrnuje výsledky a vztahuje je k cíli práce. Pozitivně hodnotím práci s tabulkami, které kondenzují závěry a zvyšují přehlednost.

Za drobnou formální nesrovnalost považuji, že popis jednotlivých částí v úvodu nekoresponduje s finálním pořadím částí v práci (prohozená část k rizikům a komparaci). Jde však o detail, který nemění věcnou návaznost argumentace a jinak poctivou systematiku práce.

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>).

HARŠÁNIOVÁ, V.: PRENOS OSOBNÝCH ÚDAJOV MIMO EURÓPSKU ÚNIU

MATÚŠ MESARČÍK¹

Haršániová, V.: Prenos osobných údajov mimo Európsku úniu. 2026, diplomová práca, Univerzita Palackého v Olomouci, Právnická fakulta, 61 s.

ANOTACE

Diplomová práca sa zaoberá právnym rámcom prenosu osobných údajov do tretích krajín podľa kapitoly V GDPR, so zameraním na jeho vývoj po rozhodnutiach Schrems I a Schrems II. Vychádza z platnej právnej úpravy, relevantnej judikatúry Súdneho dvora EÚ a vykonávacích aktov Európskej komisie. Osobitná pozornosť je venovaná štandardným zmluvným doložkám, povinnosti vykonávať posúdenie vplyvu prenosu a požiadavke zabezpečenia "v podstate rovnocennej" úrovne ochrany. Samostatná časť práce analyzuje EU-U.S. Data Privacy Framework ako rozhodnutie o primeranosti, jeho právne záruky a doterajšie formy administratívneho a súdneho preskúmania. Cieľom práce je zhodnotiť praktickú udržateľnosť súčasných mechanizmov prenosu osobných údajov.

KLÍČOVÁ SLOVA

GDPR; prenos osobných údajov; tretie krajiny; rozhodnutie o primeranosti; štandardné zmluvné doložky (SCC); Transfer Impact Assessment (TIA); Schrems I; Schrems II; EU-U.S. Data Privacy Framework (DPF)

¹ JUDr. Matúš Mesarčík, PhD. LL.M je odborný asistentem Ústavu práva informačných technológií a práva duševného vlastníctva, Univerzita Komenského v Bratislave, Právnická fakulta. Kontakt: matus.mesarcik@flaw.uniba.sk

ABSTRACT

This thesis examines the legal framework for transfers of personal data to third countries under Chapter V of the GDPR, focusing on its development after the Schrems I and Schrems II judgments. It is based on the applicable legislation, relevant CJEU case law and European Commission acts. Particular attention is paid to Standard Contractual Clauses, Transfer Impact Assessments and the requirement of an "essentially equivalent" level of protection. A separate part analyses the EU-U.S. Data Privacy Framework as an adequacy decision, including its safeguards and review mechanisms. The thesis aims to assess the practical sustainability of current data transfer mechanisms.

KEYWORDS

GDPR; International Personal Data Transfers; Third Countries; Adequacy Decision; Standard Contractual Clauses (SCCs); Transfer Impact Assessment (TIA); Schrems I; Schrems II; EU-U.S. Data Privacy Framework (DPF)

Plná verze práce je dostupná z: <https://theses.cz/id/kbhq2i/>

Diplomantka si pre spracovanie svojej diplomovej práce zvolila mimoriadne aktuálnu a prakticky významnú tému, ktorá dlhodobo patrí medzi najproblematickejšie oblasti práva ochrany osobných údajov v Európskej únii. Prenos osobných údajov do tretích krajín, najmä do Spojených štátov amerických, predstavuje jednu z kľúčových výziev súčasného európskeho dátového práva, a to tak z hľadiska ochrany základných práv, ako aj z hľadiska právnej istoty dotknutých osôb a povinných subjektov.

Pozitívne hodnotím skutočnosť, že diplomantka nepristupuje k téme iba deskriptívne, ale jasne vymedzuje analytický cieľ práce a formuluje konkrétne výskumné otázky. Zvolené tematické zúženie na transatlantické prenosy osobných údajov je racionálne, odborne obhájiteľné a umožňuje hlbší a systematickejší rozbor judikatúry Súdneho dvora Európskej únie, najmä vo veciach Schrems I a Schrems II, ako aj nového rámca EU-US Data Privacy Framework.

Práca sa vyznačuje premyslenou štruktúrou a koncepčným uchopením problému, pričom diplomantka preukazuje schopnosť zasadiť analyzovanú problematiku do širšieho ústavnoprávneho a unijného kontextu ochrany základných práv. Výber témy aj spôsob jej spracovania preto hodnotím veľmi pozitívne.

Obsahová stránka diplomovej práce zodpovedá náročnosti a komplexnosti zvolenej témy. Práca je logicky členená a jednotlivé kapitoly na seba systematicky nadväzujú. Diplomantka najskôr vytvára solídny teoreticko-normatívny základ v podobe rozboru kapitoly V GDPR, následne analyzuje kľúčovú judikatúru Súdneho dvora EÚ a v ďalšej časti sa venuje aktuálnemu rámcu EU-US Data Privacy Framework a jeho doterajšiemu hodnoteniu.

Za výrazný prínos práce považujem najmä:

- detailný rozbor materiálneho testu „v podstate rovnocennej ochrany“,
- systematické spracovanie dopadov rozsudku Schrems II na využívanie štandardných zmluvných doložiek a povinnosť vykonávať Transfer Impact Assessment,
- kritické zhodnotenie dlhodobej udržateľnosti rámca EU-US Data Privacy Framework a úvahy o možnom budúcom súdnom preskúmaní (tzv. Schrems III).

Práca tak nepôsobí len ako zhrnutie známych záverov odbornej literatúry, ale prináša vlastnú syntézu a hodnotiacu rovinu. Diplomantka preukazuje veľmi dobrú orientáciu v judikatúre, sekundárnej literatúre aj aplikáčnej praxi a je schopná pracovať s argumentmi na odbornej úrovni.

Z formálneho hľadiska je práca spracovaná na veľmi dobrej úrovni. Text je prehľadný, štylisticky kultivovaný a logicky štruktúrovaný. Diplomantka vhodne pracuje s odbornou terminológiou a dokáže ju zrozumiteľne vysvetliť. Pozitívne hodnotím aj systematické vymedzovanie pojmov a priebežné zhrnutia čiastkových záverov.

Práca spĺňa všetky formálne náležitosti kladené na diplomovú prácu, pracuje s dostatočným množstvom relevantných prameňov, vrátane judikatúry Súdneho dvora EÚ, stanovísk Európskeho výboru pre ochranu údajov

(EDPB) a odbornej cudzojazyčnej literatúry. Čo je však nutné vytknúť je, že diplomová práca pracuje s nižším množstvom vedeckých článkov z kľúčových časopisov zaoberajúcich sa témou diplomovej práce ako napríklad European Data Protection Law Review, International Data Privacy Law alebo Computer and Security Law Review. Citácie sú spracované korektne a transparentne. Jazyková úroveň práce je veľmi dobrá, bez závažnejších štylistických alebo gramatických nedostatkov.

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>).

RŮŽIČKA, M.: ZERO TRUST SECURITY V PRÁVNÍ ÚPRAVĚ OCHRANY OSOBNÍCH ÚDAJŮ A KYBERNETICKÉ BEZPEČNOSTI

JAKUB MÍŠEK¹

Růžička, M.: Zero Trust Security v právní úpravě ochrany osobních údajů a kybernetické bezpečnosti. 2026, závěrečná práce LL.M. programu v právu informačních a komunikačních technologií, Masarykova univerzita, Právnická fakulta, 87 s.

ANOTACE

Práce se zabývá modelem Zero Trust Security (ZTS) jako technicko-organizačním přístupem k řízení kybernetické bezpečnosti v kontextu evropské a české právní regulace. Cílem je posoudit soulad principů ZTS s požadavky GDPR, směrnice NIS2 a zákona o kybernetické bezpečnosti. Analýza se zaměřuje na plnění povinností v oblasti ochrany osobních údajů, řízení přístupů a monitoringu. Zvláštní pozornost je věnována dopadům ZTS na soukromí zaměstnanců a řízení rizik v dodavatelském řetězci. Práce hodnotí ZTS jako nástroj pro zajištění compliance a prokazování náležité péče organizace.

KLÍČOVÁ SLOVA

Zero Trust Security; compliance; kybernetická bezpečnost; GDPR; NIS2; zákon o kybernetické bezpečnosti; ochrana osobních údajů; monitoring zaměstnanců; řízení dodavatelského řetězce

¹ JUDr. MgA. Jakub Míšek, Ph.D. je odborným asistentem Ústavu práva a technologií-Právnické fakulty Masarykovy univerzity. Kontakt: jkb.misek@mail.muni.cz

ABSTRACT

This thesis examines Zero Trust Security (ZTS) as a technical and organizational approach to cybersecurity management within EU and Czech regulations. The goal is to assess the alignment of ZTS with GDPR, the NIS2 Directive, and the Cybersecurity Act. The analysis focuses on fulfilling obligations in data protection, access management, and monitoring. Specific attention is paid to the impact of ZTS on employee privacy and supply chain risk management. The thesis evaluates ZTS as an effective tool for ensuring regulatory compliance and demonstrating an organization's due diligence.

KEYWORDS

Zero Trust Security; compliance; cybersecurity; NIS2 Directive; Cybersecurity Act; Personal Data Protection; Employee Monitoring; Supply Chain Management

Plná verze práce je dostupná z: <https://is.muni.cz/th/ww30p/>

Téma hodnocené závěrečné práce je aktuální a bez pochyby náročné. Kvalitní zpracování takového textu totiž vyžaduje jednak dobrou znalost předmětné právní úpravy, která je navíc poměrně široká a zasahující do několika oblastí práva, a jednak dobrou znalost technického fungování zkoumaného problému. Stejně tak je zásadní autorova dovednost tyto oblasti propojit a kriticky aplikovat. Autor pak v práci dokázal, že se tohoto úkolu zhostil úspěšně.

Cíle práce jsou formulovány na s. 19 a 20 v podobě vyjádření tří výzkumných otázek, které práce zodpovídá. Vzhledem k formulaci výzkumných otázek není jasně argumentován vztah mezi otázkou č. 1 a otázkou č. 2. Otázka č. 2 totiž věcně spadá pod obecnější otázku č. 1. Bez jasného vymezení toho, proč se autor rozhodl tyto dvě otázky takto rozdělit, je zvolené řešení matoucí. Obecně by pro větší přehlednost textu bylo vhodné jasně indikovat, které kapitoly práce směřují primárně k zodpovězení které výzkumné otázky. Postrádám rovněž jednoznačné výslovné zohlednění cílů formulovaných v zadání práce. Uvedené nedostatky jsou částečně vyřešeny

v Závěru práce, kde autor zmíněné vazby prezentuje. To je však z hlediska přehlednosti práce jako celku pozdě, protože to je role Úvodu, který však v tomto směru selhává. Cíle práce nicméně byly naplněny a výzkumné otázky vhodně zodpovězeny.

Práce je celkově zpracována kvalitně. Její struktura je na obecné úrovni přehledná a (s výše uvedenou výhradou) odpovídá vymezeným cílům a výzkumným otázkám.

V kapitole 2 autor přehledně a srozumitelně popisuje věcný a technický rozměr principu zero trust security. Podkapitola 2.4 je systematicky umístěna nevhodně, protože pojednává o právních a etických limitech a přínosech ZTS, přičemž ale v dosavadním výkladu se práce těmto otázkám vůbec nevěnovala. Kapitola 3 se věnuje základní analýze relevantních právních předpisů, které se problematiky ZTS dotýkají, ať už proto, že obsahují požadavky, které mohou být prostřednictvím ZTS naplňovány, nebo proto, že představují limity pro nasazení ZTS. Oba dva rozměry však autor poněkud míchá mezi sebou bez jasného strukturálního oddělení. Je třeba vyzdvihnout, že se autor vyvaroval obvyklému problému příliš širokého výkladu a text vhodně konkrétně navazuje na konkrétní projevy v rámci ZTS (viz např. přehled zásad zpracování osobních údajů na s. 29 a následující). Ve vztahu k ochraně osobních údajů mám dílčí výhrady. Kapitola 3.2.2 (právní základy/ tituly dle GDPR) není vhodně uchopena. Není účelné uvažovat o ZTS jako o samostatném procesu zpracování osobních údajů, ať už ve vztahu k právním titulům pro zpracování nebo například pro provádění DPIA, jak autor naznačuje na s. 33. Vhodné zarámování autor nabízí, když ZTS prezentuje jako technický prostředek pro zajištění zabezpečení zpracování a snížení jeho rizika. Ve vztahu k naplnění konkrétního účelu pak bude rovněž nezbytné posuzovat vhodnost a nezbytnost nasazení přístupu ZTS, respektive jeho konkrétní realizaci. Od daného se pak budou odvozovat i právní tituly (případně další povinnosti vyplývající z GDPR), protože tituly se vážou na účely zpracování, přičemž ZTS vždy bude součástí širšího řešení pro dosažení vybraného účelu. V kontextu výkladu právní úpravy ochrany osobních údajů postrádám úvahu o možnosti realizace práv subjektů údajů ve smyslu čl. 12 - 22 GDPR.

Kapitola 4 vhodně propojuje předchozí kapitoly a obecně popisuje praktické aspekty implementace ZTS. Kapitola 5 se specificky zaměřuje na nasazování ZTS v kontextu pracovněprávních vztahů. Práce dobře popisuje jak obecnější evropský rámec právní úpravy, tak její praktickou realizaci v podobě § 316 ZP. Oceňuji, že autor do argumentace zahrnul relevantní judikaturu ESLP. Naopak, umístění speciální podkapitoly věnované judikatuře českých soudů (5.2.5) je z hlediska výkladu spíše nevhodné a daná rozhodnutí měla být argumentačně zahrnuta přímo do výkladu (jde však o drobnost). Kapitola 6 se věnuje specifickému problému nasazení principů ZTS v rámci řízení dodavatelského řetězce. Vedle nasazení v kontextu pracovněprávního vztahu jde o další praktický rozměr, který je jednak aktuální a jednak jeho zahrnutí do práce přímo vyplývá ze zadání závěrečné práce. Velká část kapitoly je věnována obecným právním požadavkům na řízení dodavatelského řetězce. Konkrétní aplikace principů ZTS je pak přehledně vyložena zejména prostřednictvím vložených tabulek a stručného přehledu technických opatření. Zvolený způsob výkladu je vhodný, protože umožňuje přehledně předat již značně komplexní informace.

Závěr práce zodpovídá na výzkumné otázky a dává práci jako celku nezbytné ukotvení. Celkově je tedy možné shrnout, že až na dílčí nedostatky jde o velice zdařilý text, který zajímavým způsobem komplexně pojednává o aktuálním a důležitém tématu.

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>).

YEUNG, K., RANCHORDÁS, S.: AN INTRODUCTION TO LAW AND REGULATION: TEXT AND MATERIALS

ONDŘEJ BÖHM¹

YEUNG, K., RANCHORDÁS, S. *An introduction to law and regulation: text and materials. Second edition. ed. Cambridge, UK New York: Cambridge University Press, 2024. Law in context. ISBN 978-1-009-37903-8.*

1. ÚVOD

Recenzovaná publikace ze série *Law in Context* nabízí komplexní konceptuální mapu a kritický úvod do studia regulace, přičemž propojuje právní perspektivu s poznatky společenských věd, zejména politologie, ekonomie a sociologie. Autorky volí metodologický přístup kombinující vlastní teoretický a analytický komentář s rozsáhlými úryvky z klíčových akademických textů jiných autorů. Konceptuální rámec publikace je ukotven v předpokladu, že nadnárodní společnosti nelze vnímat jako pasivní adresáty norem, nýbrž jako mocenské aktéry, kteří aktivně využívají svého politického a hospodářského vlivu k ovlivňování regulačních mechanismů, jež jsou vůči nim uplatňovány.² Tento fenomén poté autorky vykreslují jako velmi zásadní, a to zejména v kontextu velkých technologických společností.³

Současný socioekonomický vývoj je charakterizován bezprecedentním nárůstem vlivu nadnárodních technologických společností, masivním využí-

¹ Mgr. Ondřej Böhm je doktorandem a výzkumníkem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. E-mail: Ondrej.Bohm@law.muni.cz

² Srov. YEUNG, K., RANCHORDÁS, S. *An introduction to law and regulation: text and materials*. Cambridge, UK New York: Cambridge University Press, 2024, s. 8–10.

³ Ibid., s. 85–89.

váním systémů umělé inteligence ke zpracování dat a postupnou platformizací služeb,⁴ v důsledku které mají stále větší množství uživatelských dat pod kontrolou právě jejich poskytovatelé. Na této infrastruktuře dnes neběží pouze drtivá většina soukromých interakcí, ale rovněž veřejné služby, které ve velkém využívají nástroje a služby poskytované velkými technologickými společnostmi.⁵ Jestliže před dvaceti lety platilo, že nikdo nevypne internet, dnes můžeme říct, že nikdo nevypne Google. Tato ústřední role technologických společností se poté projevuje i v jejich neodmyslitelném dominantním postavení a tržní síle, která těmto společnostem umožňuje takřka cokoliv. Kromě toho, tyto společnosti utvářejí digitální služby prostřednictvím kódu, který jako zásadní modalita regulace přímo ovlivňuje, co uživatelé mohou a nemohou dělat. Velké technologické společnosti tak v podstatě utváří svůj vlastní regulační rámec, který konkuruje tradiční právní regulaci.⁶ Na tyto výzvy a s nimi spojená rizika pro veřejný zájem reaguje zákonodárce přijímáním komplexních veřejnoprávních předpisů, jejichž příkladem může být např. evropské Nařízení o digitálních službách (Digital Services Act, dále jen „DSA“). V rámci doktrinálního právního výzkumu tak vyvstává fundamentální otázka, zda a jakým způsobem tyto nové regulační rámce skutečně ovlivňují chování dominantních platform a do jaké míry je reálně nutí respektovat právem chráněné hodnoty. Ústředním problémem legislativy i právní vědy se stává hledání odpovědi na otázku, *jak konceptualizovat právní regulaci, aby chování velkých technologických společností nebylo svévolné a aby se donucovací mechanismy nestaly pouze kalkulovaným nákladem na provozování platformy.*

K nalezení odpovědi na tuto otázku je nezbytné opustit izolovaný pohled na texty konkrétních nařízení a podrobit kritické reflexi samotné teoretické

⁴ K platformizaci viz např. CHIA, A. et al. Platformisation in game development. *Internet Policy Review*. 2020, roč. 9, č. 4. DOI: 10.14763/2020.4.1515

⁵ Srov. YEUNG, K., RANCHORDÁS, S. *An introduction to law and regulation*, s. 104–106.

⁶ Ibid., s. 185–192. Publikace zde vychází z Lessiga, ale nezabývá jeho teorií kódu jako stěžejní modalitě regulace, místo toho se soustředí na procesní aspekty algoritmické moderační, kterou předkládá Yeungová ve svých dalších dílech. Srov. LESSIG, L. *Code: version 2.0*. New York: Basic books, 2006, s. 120–125.

základy právního státu, tedy vázanost státu i subjektů právem. Právě z tohoto důvodu je předmětem této recenze publikace *An Introduction to Law and Regulation: Text and Materials* autorek K. Yeung a S. Ranchordás. Ačkoliv se jedná o obecnější teoretické dílo, jeho analytický aparát poskytuje zcela klíčová východiska pro studium moderní digitální regulace. Jak již bylo uvedeno, publikace vychází z premisy, že velké korporace disponují asymetrickou politickou a ekonomickou mocí, kterou využívají, resp. mohou využívat, k formování a ovlivňování regulačního rámce. Prostřednictvím dekonstrukce tradičních nástrojů příkazu a kontroly (*command-and-control*) v kontextu jednotlivých modalit regulace a analýzy konceptu hybridních nástrojů regulace (*hybrid instruments*) kniha přesvědčivě teoretizuje, proč klasické finanční sankce u velkých technologických společností mohou selhávat.⁷ Pochopení těchto limitů, které publikace systematicky mapuje, je proto stěžejní pro jakýkoliv další doktrinní výzkum zaměřený na regulaci online platform a algoritmických systémů.

Vzhledem k tomu, že tato kniha byla autorkami pojata z části také jako základní učební text do úvodu práva, obsahuje kniha mnoho velmi obecných pasáží, např. celou část první, která se zabývá vysvětlením základních ekonomických konceptů. Přestože nijak nezpochybňuji přínos i těchto částí publikace, můj zájem v rámci této recenze byl věnován výhradně teorii regulace v kontextu výše položené otázky.

Tato recenze tedy podrobně analyzuje teoretický přínos publikace se specifickým zaměřením na část druhou, zejména poté na čtvrtou (*Theories of Regulation*) až sedmou (*Hybrid Instruments and Experimental Regulations*) kapitolu díla, a to právě v kontextu limitů právní regulace ve vztahu k technologickým společnostem, pro něž běžné finanční sankce za porušení práva mnohdy nepředstavují odrazující trest, nýbrž pouhý náklad na podnikání.⁸

Stěžejním analytickým nástrojem pro uchopení tohoto problému je v recenzovaném díle detailní komparace mezi ekonomickým a neekonomickým

⁷ YEUNG, K., RANCHORDÁS, S. *An introduction to law and regulation*, s. 119–123.

⁸ Ibid.

(politickým) pojetím veřejného zájmu v rámci teorií regulace.⁹ Tato komparace odhaluje hluboké koncepční rozdíly v tom, jaké cíle má regulace sledovat, jakou roli v ní hraje právo a proč u velkých společností tradiční sankční mechanismy selhávají.

2. TEORIE REGULACE JAKO ANALYTICKÉ VÝCHODISKO

Autorky v úvodu čtvrté kapitoly definují teorii regulace jako soubor propozic či hypotéz o tom, proč regulace vzniká, jací aktéři k jejímu vzniku přispívají a jaké jsou typické vzorce interakcí mezi těmito aktéry. Čtvrtou kapitolu autorky strukturují do tří hlavních teoretických oddílů: teorie veřejného zájmu (*public interest theories*), teorie soukromého zájmu (*private interest theories*) a institucionální přístupy (*institutionalist theories*).

Pro zkoumanou problematiku korporátního compliance je zásadní teorie veřejného zájmu, jež regulátorům a legislativě přisuzuje snahu prosazovat kolektivní cíle s úmyslem podporovat obecný blahobyt společnosti. Tato kategorie se však vnitřně štěpí na dvě zásadně odlišné větve: na přístup vycházející z ekonomického blahobytu (*welfare economics*) a na přístupy zdůrazňující hodnotové, resp. politické cíle.¹⁰ Zkoumání rozdílů mezi těmito dvěma koncepty a jejich vzájemné provázanosti poskytuje klíč k pochopení toho, za jakým účelem je tradiční právní regulace přijímána, a směrem k jakému cíli je formulována. Pochopením tohoto poté autorky dochází k závěru, že v kontextu velkých technologických společností není tento cíl nastaven vhodně a nabízí alternativu v podobě již zmíněných hybridních nástrojů.

3. EKONOMICKÉ POJETÍ VEŘEJNÉHO ZÁJMU A SANKCE JAKO NÁKLAD

Ekonomická verze teorie veřejného zájmu chápe regulaci striktně jako reakci na nedokonalosti trhu, takzvaná tržní selhání (*market failures*). Jak vysvětluje A. Ogus, korekce těchto selhání zvyšuje obecný blahobyt, a je tedy

⁹ Ibid., s. 121–136.

¹⁰ Ibid., s. 121–130.

ve veřejném zájmu. Ekonomický blahobyt je pouhým výsledkem efektivity alokace zdrojů, tedy stavu, kdy jsou zdroje využívány k nejhodnotnějšímu účelům. Regulace je ospravedlněna pouze tehdy, pokud volný trh tuto efektivitu zajistit nedokáže.¹¹

Ogus podrobně rozebírá typická tržní selhání, jimiž jsou monopoly, veřejné statky, externality a informační deficit. V kontextu výše položené otázky je klíčová analýza externalit a informačních asymetrií. Pokud korporace svou činností způsobuje negativní technologické externality (například znečištění; v kontextu technologických společností poté např. únik uživatelských dat nebo nezákonné profilování), neplatí skutečné společenské náklady své činnosti a dochází k chybné alokaci zdrojů. Ekonomickým řešením, a tedy cílem regulace z pohledu této teorie, je donutit korporaci tuto externalitu „internalizovat“, tj. tyto skutečné společenské náklady zaplatit.¹²

Právě zde se vyjevuje fundamentální příčina toho, proč je sankce vnímána pouze jako poplatek. Z pohledu ekonomického pojetí veřejného zájmu je hlavním cílem dosažení efektivity, nikoliv morální odsouzení jednání. Pokud je regulace nastavena formou ekonomických nástrojů (jako jsou daně či poplatky) nebo finančních sankcí za nedodržení předpisů,¹³ racionálně jednající korporace, z logiky věci, provádí kalkulaci. Aplikuje-li se ekonomická teorie, říkají autorky, pak v situaci, kdy jsou náklady na eliminaci negativního jevu (tzv. *abatement costs*) vyšší než pokuta či poplatek za jeho tolerování, je pro korporaci z hlediska jejích individuálních zájmů efektivnější zaplatit sankci.¹⁴

V ekonomickém modelu je právo vnímáno přísně instrumentálně, plní facilitativní roli jako nástroj k formování sociálního chování s cílem maximalizovat alokační efektivitu. Pokud právní předpis zakáže určité chování

¹¹ OGUS, A. I. *Regulation: Legal Form and Economic Theory*. London: Bloomsbury Publishing Plc, 2004, s. 30–40. Srov. YEUNG, K., RANCHORDÁS, S. *An introduction to law and regulation*, s. 122.

¹² OGUS, A. I. *Regulation: Legal Form and Economic Theory*, s. 30–40.

¹³ Což autorky rozebírají v šesté kapitole jako tzv. *command-and-control* mechanismy a nástroje založené na konkurenci. Viz YEUNG, K., RANCHORDÁS, S. *An introduction to law and regulation*, s. 169–171.

¹⁴ Ibid., s. 209–211.

pod hrozbou pokuty, ekonomický přístup to vnímá tak, že právo pouze stanovilo „cenu“ za toto chování. Pokud korporace tuto cenu (pokutu) zaplatí a pokračuje v činnosti, z hlediska ekonomického pojetí veřejného zájmu vlastně nedochází k anomálii. Regulace je tak zároveň předmětem určitého vyjednávání.

Autorky k ekonomickému pojetí veřejného zájmu nepřijímají jednostranné stanovisko, nýbrž k němu přistupují s analytickým odstupem. Ekonomickou teorii blahobytu a koncept tržních selhání na jednu stranu vnímají jako legitimní teorii, zároveň však kriticky reflektují limity tohoto přístupu. Upozorňují, že čistě ekonomické směry, které nahlízejí na právo jako na nástroj k efektivnímu řešení alokace prostředků, vykazují tendenci potlačovat některé hodnoty, instituce a ideály, jež jsou inherentní samotnému principu právního státu. Vlastní přístup Yeungové tedy spočívá v doplnění ekonomických základů o politický a ústavní kontext, který reflektuje zmínované hodnoty.¹⁵ Tyto dvě teorie, na rozdíl např. od Sunsteina, nestaví do vzájemného protikladu.

4. NEEKONOMICKÉ A POLITICKÉ POJETÍ VEŘEJNÉHO ZÁJMU

Publikace následně staví výše uvedený ekonomický model do kontrastu s politickými verzemi teorie veřejného zájmu. Tyto přístupy, podle autorek, do účelu a smyslu regulace zahrnují hodnoty jako sociální a distributivní spravedlnost, paternalismus nebo inherentní hodnotu participace v demokratickém dialogu. Komplexní veřejný zájem se zde formuje prostřednictvím určité deliberace. Autorky zde vycházejí jednak z Blackové, která jako předmět i legitimní důvody pro regulaci vnímá určitá společenská rizika, a jednak z Benhabiba, který jako legitimní důvod regulace vnímá nezbytnost ochrany lidských práv.

V případech společenských rizik autorky identifikují problematickou nestálost názoru společnosti v tom, co společenské riziko představuje.¹⁶ Absence jednotného a všeobecně akceptovaného přístupu k tomu, co tato rizika re-

¹⁵ Yeungová tento přístup zaujímá již v předchozím vydání publikace, kde uvedené vysvětluje na dichotomii facilitativní a expresivní funkce regulace. Blíže k tomu viz MORGAN, B., YEUNG, K. *An introduction to law and regulation: text and materials*. Cambridge, UK New York: Cambridge University Press, 2012, s. 3–7.

álně konstituuje, a vzhledem k tomu, že pojem rizika v sobě nese jak deskriptivní, tak normativní dimenzi, vyvolává tato pojmová nejednotnost neustálé proměny v samotných metodách a technikách regulace. Tento fluidní stav následně v praxi podněcuje paralelní nárůst jak nových, často nekonceptních regulací, tak protichůdných tendencí směřujících k „anti-regulaci“ a k ideologickým střetům o samotný rozsah legitimních státních zásahů. Výsledná dynamika, charakterizovaná nestabilitou a neustálým napětím mezi expertním tlakem na snižování rizik a politickým odporem vůči omezování autonomie subjektů, pak z pohledu právní jistoty a systémové efektivity reálně nepředstavuje ideální ani stabilní stav regulačního rámce.¹⁷

Argument ochrany lidských práv poté autorky, s odkazem na Benhabiba, považují za robustnější oporu pro smysl a účel regulace, která obecně limituje autonomii vůle soukromých subjektů. Na tomto místě je ale argumentace poněkud nejasná a chybí mi nějaké substantivnější odůvodnění. Autorky se v této části nevěnují např. pojednání Casse Sunsteina, který škálu neekonomických, hodnotových cílů regulace definuje konkrétněji. Sunstein tvrdí, že trh nedokáže plně zachytit to, co lidé od společnosti skutečně chtějí, protože je nutí jednat ve svém individuálním zájmu sledujíc okamžitý prospěch. Sunstein proto identifikuje několik kategorií veřejného zájmu, kde se projevuje ochranná funkce regulace, např. ochrana slabších stran před kolektivní újmou, meta-preference (prosazení dlouhodobých cílů před okamžitým prospěchem) nebo boj proti sociální podřízenosti. Volný trh poté není smyslem regulace, ale jen jednou z dalších právem chráněných hodnot.¹⁸

Aplikujeme-li Sunsteinovo pojetí veřejného zájmu na problém korporátního compliance, situace, kdy korporace vnímá sankci jen jako náklad tedy není otázkou nastavení „ceny“ ze strany státu, ale představuje selhání

¹⁶ Tento aspekt ostatně přiznává i sama Blacková, viz BLACK, J. The Role of Risk in Regulatory Processes. In: BLACK, J. *The Oxford Handbook of Regulation*. Oxford University Press, 2010, s. 306–308. DOI: 10.1093/oxfordhb/9780199560219.003.0014

¹⁷ YEUNG, K., RANCHORDÁS, S. *An introduction to law and regulation*, s. 123–126.

¹⁸ SUNSTEIN, C. R. *After the rights revolution: reconceiving the regulatory state*. Cambridge - Massachusetts: Harvard university press, 1990.

hodnotového nastavení právního řádu, aniž by došlo k zásahu do základních lidských práv nebo ve společnosti panovala shoda na tom, zda příslušná regulace chránila před nějakým společenským rizikem. V hodnotovém pojetí, vrátím-li se k dichotomii Yeungové,¹⁹ tedy právo neplní pouze facilitativní roli, ale má i silný expresivní charakter.

Pokud tedy korporace platí pokuty jako poplatek za porušování práva, jedná v rozporu s hodnotami, ke kterým se demokratická společnost prostřednictvím regulace zavázala. Jak ale autorky tvrdí, volba korporace mezi *abatement costs* a uhrazením sankce je zcela racionální a nelze se domnívat, že společnost čistě z vlastního smyslu pro morálku zvolí dražší možnost, tím spíš, pokud z porušení právní povinnosti benefituje její obchodní model. V případě online platform tak např. typicky půjde o nedostatek transparentnosti ve vztahu k algoritmickým doporučovacím systémům, což odporuje DSA.

Kritikou společnou oběma teoriím veřejného zájmu je poté autorkami předkládané tvrzení, že teorie veřejného zájmu je sice schopná objasnit, proč je regulace přijímána a pomáhá nám tak identifikovat, k čemu by měla směřovat, a tedy posoudit, zda je nedodržování právních povinností v rozporu s tímto cílem (hodnotové pojetí) či nikoliv (ekonomické pojetí), ale již není schopná objasnit, proč v praxi není tohoto veřejného zájmu dosahováno, tj. proč dochází k porušování právních povinností korporacemi.²⁰ Z toho důvodu předkládají autorky konkurenční teorii, a to teorii soukromého zájmu.

5. TEORIE SOUKROMÉHO ZÁJMU

Autorky diskusi o veřejném a soukromém zájmu na regulaci vykreslují v zásadě jako dichotomii. Na pomezí těchto přístupů lze však ještě vymezit např. tzv. procedurální veřejný zájem podle Prossera, který vychází z Habermasovy teorie „ideální řečové situace“ (*ideal speech situation*), tvrdí, že ústředním zájmem regulace má být rozvoj institucí, které podporují sociální učení prostřednictvím participativního dialogu. Z tohoto úhlu pohledu

¹⁹ MORGAN, B., YEUNG, K. *An introduction to law and regulation*, s. 3–7.

²⁰ YEUNG, K., RANCHORDÁS, S. *An introduction to law and regulation*, s. 130.

korporace, jež redukuje compliance na cost-benefit analýzu, ignoruje požadavek odpovědnosti a racionálního diskurzu, který demokratický proces tvorby norem předpokládá. Právo zde slouží jako arbitr (*image of law as umpire*), jenž má utvářet prostor pro svobodnou a rovnou interakci.²¹

Jak popisuje Croley, teorie veřejného zájmu modelují politický proces jako trh, kde jsou regulace nabízeny a poptávány.²² Organizované úzké zájmové skupiny (např. nadnárodní korporace) mají na rozdíl od rozptýlených spotřebitelů silnou motivaci a prostředky k ovlivňování legislativy. Fenomén *regulatory capture* poté vede k tomu, že sankční limity či formy prosazování práva jsou od počátku nastaveny tak, aby korporace neohrožily, což podle autorek teoreticky vysvětluje, proč finanční sankce často nejsou skutečně odrazující.²³

6. HYBRIDNÍ REGULATORNÍ NÁSTROJE JAKO ŘEŠENÍ

Šestá kapitola recenzované publikace systematicky opouští představu, že pro vynucení žádoucího chování existuje jeden univerzální právní nástroj. Autorky zde rozvíjejí klasifikaci několika regulačních nástrojů, které dělí do pěti základních modalit kontroly, jimiž jsou příkaz, konkurence, konsensus, komunikace a již zmiňovaný kód.²⁴ Z analýzy těchto nástrojů vyplývá, že vůči velkým korporacím je spoléhání se na izolované nástroje neúčinné a preferovaným přístupem autorek je jejich určitá kombinace, jejímž výsledkem jsou tzv. hybridní nástroje popsane v kapitole 7.²⁵

Tradiční regulace, v níž stát autoritativně stanoví pravidlo a hrozí sankcí za jeho porušení,²⁶ naráží, dle autorek, u velkých subjektů na zásadní pře-

²¹ PROSSER, T. Theorising Utility Regulation. *The Modern Law Review*. 1999, roč. 62, č. 2. DOI: 10.1111/1468-2230.00201

²² CROLEY, S. P. Theories of Regulation: Incorporating the Administrative Process. *Columbia Law Review*. Columbia Law Review Association, Inc., 1998, roč. 98, č. 1. DOI: 10.2307/1123396

²³ YEUNG, K., RANCHORDÁS, S. *An introduction to law and regulation*, s. 130–136.

²⁴ *Ibid.*, s. 168–193.

²⁵ *Ibid.*, s. 194–231.

²⁶ Dle Daintitha označováno jako *imperium*. Viz DAINTITH, T. The techniques of government. In: JOWELL, J. L., OLIVER, D. *The changing constitution*. Oxford: Clarendon press, 1994, s. 209–236.

kážky.²⁷ Jakmile navíc korporace splní stanovený standard, klasický právní příkaz jí neposkytuje žádnou motivaci k tomu, aby své chování dále zlepšovala.²⁸

Smyslem hybridních nástrojů je poté jejich základ postavený alespoň zčásti na modalitách alternativních k tradičnímu příkazu. Zásadním alternativním přístupem je v publikaci např. využití tržních sil a nástrojů založených na konkurenci.²⁹ Ekonomické nástroje, jako daně, poplatky či obchodovatelná práva, které uvalují finanční zátěž na nežádoucí aktivitu a nutí korporace internalizovat jejich společenské náklady. Tím podle autorek ovlivňují soutěžní prostředí, protože korporacím zvyšují výdaje, což ovlivňuje jejich postavení na trhu. Tyto nástroje proto vytvářejí tlak na vývoj levnějších metod eliminace škodlivých projevů, což zároveň podporuje inovaci.³⁰

V kontextu velkých technologických společností však stěžejní roli hraje koncept samoregulace. Principem samoregulace je přijímání vlastních pravidel regulovanými subjekty, často prostřednictvím zájmových sdružení či subjektů odvozených od regulovaných korporací. Mezi velkými platformami lze jmenovat např. Oversight Board Mety nebo např. věkové ratingové systémy ve videoherním průmyslu, např. PEGI, ke kterému přistupují velké platformy jako např. Steam nebo Roblox. Výhodou samoregulace je dle autorek zejména individuální nastavení povinností vhodné pro jednotlivá odvětví a dobrovolnost dodržování těchto limitů, kritikou poté naopak nízká míra nezávislosti dohledových subjektů a absence donucení. Autorky tvrdí, že samoregulace je projevem čistě soukromého, nikoliv veřejného zájmu na regulaci, což v kontextu velkých technologických

²⁷ Autorky mj. odkazují na Daintitha a Oguse. Daintith upozorňuje na nedostatečnou kontrolu subjektů, Ogus zase na alokační neefektivitu. Ogus argumentuje, že legislativa nezohledňuje např. rozdílné náklady na dosahování souladu s právními předpisy. Tuto myšlenku lze ale považovat za v praxi překonanou, např. klauzulemi o vyloučení menších a mikropodniků v evropské legislativě. Viz např. čl. 19 DSA.

²⁸ YEUNG, K., RANCHORDÁS, S. *An introduction to law and regulation*, s. 152–156; 169–170. Srov. MORGAN, B., YEUNG, K. *An introduction to law and regulation*, s. 80–85.

²⁹ Autorky zde využívají kombinace ekonomického i hodnotového přístupu, jak již bylo nastíněno výše.

³⁰ YEUNG, K., RANCHORDÁS, S. *An introduction to law and regulation*, s. 171–174.

společností vzhledem k jejich vlivu představuje vysoké riziko *regulatory capture* a tyto subjekty tak mohou snadno ovlivňovat regulatorní rámec ve svůj prospěch,³¹ mnohdy pak na úkor menších společností a vzniká tak nežádoucí asymetrie. V rámci tohoto pojednání mi schází koncept „vynucené samoregulace“, který Yeungová představila v předchozím vydání knihy.³² Domnívám se, že představuje efektivnější nástroj, avšak není zde vysvětleno, proč jej autorky opustily. Vynucená samoregulace se vyhýbá riziku *regulatory capture* integrací příkazu a konsenzu. Stát v tomto modelu nestanovuje přesné uniformní standardy jako u příkazu, ani neponechává regulaci výhradně na zájmových sdruženích a korporacích, ale vede korporace k přijetí vlastní sady pravidel, které regulátor následně schvaluje. Autorky zde navíc argumentují, že asymetrie mezi korporacemi je v tomto ohledu naopak výhodou, neboť po velkých korporacích může stát legitimně vyžadovat mnohem přísnější standardy než po menších podnicích.³³

Významným doplňkem pro regulaci velkých technologických společností je rovněž využití komunikace. Jak rozebírá Yeungová, stát může využít informační nástroje, například povinné zveřejňování informací (*mandatory disclosure*), které odrážejí korporace od riskantního chování z obavy reakce spotřebitelů. V praxi lze tento nástroj vidět např. v povinnosti transparentnosti platform dle čl. 24 DSA. Do těchto nástrojů ale může být zahrnuta i cílená negativní publicita (tzv. *naming and shaming*).³⁴

Knihy se rovněž zabývá nástroji vyplývajícími z kódu jako páté modality regulace, zejména tzv. algoritmickou regulací, jako např. algoritmické rozhodovací procesy. V díle je však tento nástroj analyzován ve vztahu platforma – uživatel, nikoliv ve vztahu regulátor – platforma. Kniha tudíž neposkytuje pojednání o tom, zda lze prostřednictvím kódu zefektivnit compliance. Přestože kód je v literatuře tradičně vnímán jako nejefektivnější modalita, jeho aplikace na zmíněný vztah je problematická hned

³¹ Ibid., s. 175–178.

³² MORGAN, B., YEUNG, K. *An introduction to law and regulation*, s. 105–109.

³³ Legitimita této pozitivní asymetrie zde může vycházet např. z teorie společenského rizika dle Blackové.

³⁴ YEUNG, K., RANCHORDÁS, S. *An introduction to law and regulation*, s. 178–185.

na několika úrovních. Jednak je prostředí internetu silně decentralizované a jednak jsou kódy jednotlivých služeb chráněné jako autorská díla nebo obchodní tajemství. Implementace algoritmické regulace (státní) by znamenala zásah do mnoha chráněných hodnot, ať už do práv duševní vlastnictví, svobody podnikání nebo např. práva na soukromí uživatelů.

7. ZÁVĚR A ZHODNOCENÍ

Recenzovaná publikace představuje přínosnou a komplexní konceptuální mapu pro pochopení limitů tradičních donucovacích mechanismů vůči velkým technologickým společnostem. Autorky velmi dobře a srozumitelně definují dichotomii mezi ekonomickým a politickým pojetím veřejného zájmu, přičemž s oporou o A. Oguse a analýzu tržních selhání přesvědčivě objasňují, že korporace často vnímají finanční sankce pouze jako kalkulovaný náklad na podnikání. Podobně zdařilá je, s využitím S. Croleyho, i demonstrace fenoménu *regulatory capture* v rámci teorie soukromého zájmu, která zase objasňuje, proč ke zkoumanému fenoménu dochází. Jako určité východisko, přestože publikace není koncipována jako *de lege ferenda* analýza, poté slouží detailní rozbor hybridních regulatorních nástrojů. Na druhou stranu lze jmenovat oblasti, kde by teoretický výklad mohl a měl být obsáhlejší, obzvláště u hodnotových a neekonomických cílů regulace. Přestože se autorky v této souvislosti odvolávají na S. Benhabiba a nezbytnost ochrany lidských práv, jejich argumentace není dostatečně přesvědčivá a postrádá oporu o robustnější teorie, např. Casse Sunsteina. Kniha také v rámci dělení veřejného a soukromého zájmu opomíjí koncept procedurálního veřejného zájmu podle T. Prossera. Na škodu je poté také to, že kniha nevysvětluje, proč Yeungová oproti předchozímu vydání opustila koncept vynucené samoregulace, který považují za zajímavé východisko, a že zkoumání modality kódu omezuje pouze na vztah platforma – uživatel.

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>).

VAN CLEYNENBREUGEL, P., GROZDANOVSKI, L.
(EDS). THE STANDARDS OF FAIRNESS IN DIGITAL
LAW: THE NORMATIVE FOUNDATIONS OF THE
DATA, DATA GOVERNANCE, DIGITAL SERVICES,
DIGITAL MARKETS AND ARTIFICIAL INTELLIGENCE
ACTS.

MARTIN ERLEBACH¹

Van Cleynenbreugel, P., Grozdanovski, L. (eds). *The Standards of Fairness in Digital Law: The Normative Foundations of the Data, Data Governance, Digital Services, Digital Markets and Artificial Intelligence Acts*. In: Van Cleynenbreugel, P., Grozdanovski, L. (eds). *The Standards of Fairness in Digital Law*. Edward Elgar Publishing, 2025. ISBN 978-1-0353-3868-9.

1. ÚVOD

Recenzovaná kniha si klade velmi ambiciózní cíl, analyzovat koncept „*fairness*“, tedy férovosti nebo v českých překladech pravidelněji spravedlnosti, napříč novou evropskou digitální legislativou. Přestože v českých překladech dotčených předpisů je možné nalézt slova „*spravedlnost*“ nebo „*spravedlivý*“, bude kvůli distinkci provedené autory i v této recenzi použito slovo „*férovost*“.

¹ Mgr. Martin Erlebach je prezenčním doktorandem na Ústavu práva a technologií, Právnické fakulty Masarykovy univerzity, kontaktní email: 480066@mail.muni.cz

Konkrétně se autoři zaměřují na nařízení o datech (DA),² akt o správě dat (DGA),³ nařízení o digitálních trzích (DMA),⁴ akt o umělé inteligenci (AI Act)⁵ a nařízení o digitálních službách (DSA).⁶ Není ovšem možné opomenout, že autoři se často také odvolávají na znění Obecného nařízení o ochraně osobních údajů (GDPR).⁷ Kapitola knihy zabývající se DGA a DA je přitom přímo založená na porovnávání těchto dvou nařízení a významu férovosti v nich se zněním GDPR. Kniha vyšla v režimu open access na konci roku 2025 a představuje tak zejména rozsáhlý vhled do aktuálních akademických debat týkajících se těchto nařízení.

Premisou knihy je, že se koncept férovosti prolíná a formuje všechna zmíněná nařízení, aniž by byl přesně definovaný. Kniha jako celek si klade za úkol na základě určité metodologie a rozsáhlého filozofického základu⁸ popsat jakou roli tato férovost v jednotlivých nařízeních plní, a co by pod ní měl čtenář chápat. Autoři pracují s konceptem férovosti autonomně pro každé ze zmíněných nařízení, je tak třeba zmínit to, co prozíravý čtenář re-

² Nařízení Evropského parlamentu a Rady (EU) 2023/2854 ze dne 13. prosince 2023 o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání a o změně nařízení (EU) 2017/2394 a směrnice (EU) 2020/1828 (nařízení o datech) (dále jen „DA“).

³ Nařízení Evropského parlamentu a Rady (EU) 2022/868 ze dne 30. května 2022 o evropské správě dat a o změně nařízení (EU) 2018/1724 (akt o správě dat) (dále jen „DGA“).

⁴ Nařízení Evropského parlamentu a Rady (EU) 2022/1925 ze dne 14. září 2022 o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví a o změně směrnic (EU) 2019/1937 a (EU) 2020/1828 (nařízení o digitálních trzích) (dále jen „DMA“).

⁵ Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci) (dále jen „AI Act“).

⁶ Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách) (dále jen „DSA“).

⁷ 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 (obecné nařízení o ochraně osobních údajů) (dále jen „GDPR“).

⁸ Viz Van Cleynenbreugel, P., Grozdanovski, L. (eds). *The Standards of Fairness in Digital Law: The Normative Foundations of the Data, Data Governance, Digital Services, Digital Markets and Artificial Intelligence Acts*. In: Van Cleynenbreugel, P., Grozdanovski, L. (eds). *The Standards of Fairness in Digital Law*. Edward Elgar Publishing, 2025. s. 10 a násl.

cenze již jistě sám tuší, a sice že férovost napříč těmito nařízeními neznamená totéž.

Všechny pozitiva i negativa této publikace, která budou předmětem této recenze, pramení snad právě z ambiciózních cílů a jejich provedení v rámci kolektivní monografie. Samotný koncept férovosti je v právním kontextu⁹ i ve filozofii obecně¹⁰ široce diskutovaný už mnoho let a neexistuje pro něj jednotné vymezení.¹¹ Stejně tak dotčená nařízení jsou velmi různorodá a pokrývají širokou škálu právních vztahů a odvětví práva, kde může zkoumaný koncept nabírat širokou škálu podob, což ostatně kniha reflektuje. K tomu se potom ještě přidává složitý faktický aspekt práce na knize. Autorský kolektiv je rozsáhlý a disciplinárně různorodý, kniha je totiž kolektivní monografií. Není proto divu, že soudržnost textu recenzované knihy je menší, než by byla u klasické monografie. Považuji ovšem za nevhodné, aby u tohoto typu publikace editoři v předmluvě prohlašovali, že je kniha naopak „pozoruhodně koherentní“.¹²

2. FÉROVOST A METODA ZKOUMÁNÍ

Vzhledem k vymezení cílů knihy není asi divu, že nezanedbatelná část úvodních stran je věnovaná právě definici férovosti a filozofickému či právně-filozofickému základu tohoto konceptu. Hned úvodní kapitola se má zabývat filozofickým vymezením férovosti a následně metodologií zkoumání, kterou budou naplňovat následující kapitoly věnované konkrétním nařízením.¹³ Jak již bylo řečeno v úvodu tato část knihy ani nemůže nabídnout ucelenou definici férovosti. Proto její role spočívá zejména v re-

⁹ Viz např. FENNELL, Lee Anne a Richard H. MCADAMS. *Fairness in Law and Economics: Introduction* [online]. Rochester, NY: Social Science Research Network, 2013 [cit. 16. 5. 2026]. Dostupné z: <https://papers.ssrn.com/abstract=2504819>

¹⁰ Viz např. asi nejznámější dílo k této tématice RAWLS, John. *Justice as Fairness. The Philosophical Review*. [Duke University Press, Philosophical Review], [online]. 1958, roč. 67, č. 2 [cit. 16. 5. 2026]. s. 164–194. DOI: 10.2307/2182612

¹¹ Tamtéž, s. 5. Také ale např. právě RAWLS, John. *Justice as Fairness. The Philosophical Review*. [Duke University Press, Philosophical Review], [online]. 1958, roč. 67, č. 2 [cit. 16. 5. 2026]. s. 164–194 a další.

¹² Překlad autor, v originále „remarkably coherent“. Tamtéž s. xii.

¹³ Tamtéž, s. 31 a násl.

kapitulaci dosavadní odborné debaty nad významem tohoto konceptu napříč historií. V tomto ohledu je třeba ocenit, jak se autor této části publikace snaží zakomponovat právě legislativu, která bude předmětem zbytku knihy, do výkladu a jak přirozeně na sebe jeho text navazuje. To činí mnohdy složitý filozofický text srozumitelným i pro právníky, kteří jsou adresáty knihy. Výklad o historickém vývoji je vhodně doplněn také o chápání férovosti v právních kontextech i v opozici s právem¹⁴ nebo je srozumitelně rozebráno, jak se filozofie dívá právě na vztah férovosti a spravedlnosti. Konkrétněji například někteří autoři tyto koncepty směšují a někteří zase trvají na jejich oddělitelnosti. Pro potřeby této konkrétní knihy je pojmem spravedlnost nebo spravedlivost přisuzován význam institucionálně zakotvené férovosti, férovost samotná je přitom více etickou kategorií zaměřenou na rovnost.¹⁵ Férovost je přitom v knize popisována skrze její distributivní nebo korektivní atributy.¹⁶ V právním kontextu je pak možné hovořit o férovosti procesní nebo materiální či substantivní.¹⁷

Na tento robustní filozofický základ je pak navázáno metodologií, která má napomoci zkoumat férovost ve vymezeném právním kontextu. Metodologie se skládá z pěti kroků a postupuje od zkoumání výskytu férovosti v dotčených předpisech a jejich případné shlukování do významových skupin¹⁸ až po konkrétní aplikovatelné instance férovosti v digitální legislativě, které mají být předmětem zbytku knihy.¹⁹ Působí ale poněkud zvláště, že většina kroků je „vyřešena“ již v metodologické kapitole a zbytek knihy je konstruován jen jako příklady toho, jak je možné zkoumat konkrétní význam férovosti. Zřejmě tak jde o pokus dodat knize na soudržnosti a zasadit jednotlivé kapitoly do uceleného metodologického rámce.

¹⁴ Tamtéž, s. 22.

¹⁵ Tamtéž, s. 15.

¹⁶ Tamtéž, s. 4.

¹⁷ Tamtéž, s. 27 ale také s. 219.

¹⁸ Tamtéž, s. 33.

¹⁹ Tamtéž, s. 60.

3. DOTČENÁ REGULACE A OBSAH

Většinu obsahu knihy tvoří právě zmíněné kapitoly rozebírající zmínky o férovosti z daných nařízení. Kromě DGA a DA²⁰ se vždy jedna kapitola věnuje jednomu nařízení. Trochu zvláště ovšem působí, že po kapitolách věnujících se konkrétním nařízením kniha obsahuje ještě čtyři samostatné kapitoly, které se buď věnují znovu již rozebraným nařízením, jen z jiného úhlu pohledu anebo přinášejí kapitolu o již staženém návrhu směrnice o odpovědnosti za AI²¹ a směrnici o odpovědnosti za vadné výrobky.²² Dochází tak ke zvláštním duplicitám výkladu. Jeden autor rozebírá například DMA v obecné rovině, ale v poslední třetině knihy se nachází ještě jedna kapitola pojednávající o specifickém aspektu regulace obsažené v DMA a souvislosti tohoto aspektu s procesními aspekty férovosti. V rámci knihy jsou tyto čtyři kapitoly zařazeny s cílem dosáhnout lepšího uchopení procesního aspektu férovosti. Tento cíl ovšem nekoresponduje s metodologií, která se v rámci knihy váže ke všem kapitolám předcházejícím těmto nesystematicky zařazeným „procesním“ kapitolám. Je zde tedy poněkud zvláštní napětí mezi skutečným obsahem knihy a tím, co od autorů jednotlivých kapitol ona metodologie požaduje. Tím se nesnažím říct, že by texty těchto kapitol nebyly kvalitní, naopak jsou dle mého názoru jednou z nejlepších částí celé knihy, jejich zařazení však působí velmi nesystematicky. V rámci struktury textu je zahrnutí těchto kapitol zdůvodněno tím, že po rozboru standardu férovosti v substantivních rozměrech je třeba analyzovat také procesní aspekt férovosti v evropské digitální legislativě. Pokud tomu ovšem skutečně tak je, není zřejmé, proč je výčet dotčených nařízení v této části knihy odlišný od předchozího, ani proč procesní aspekty nemohly být zahrnuty přímo do

²⁰ Tamtéž, s. 91–128, kapitola je představena jako férovost v „datovém právu“, které podle autorů představuje DA, DGA ale také GDPR.

²¹ Návrh Směrnice Evropského parlamentu a Rady o přizpůsobení pravidel mimosmluvní občanskoprávní odpovědnosti umělé inteligenci (směrnice o odpovědnosti za umělou inteligenci) (dále jen „směrnice o odpovědnosti za AI“).

²² Směrnice Evropského parlamentu a Rady (EU) 2024/2853 ze dne 23. října 2024 o odpovědnosti za vadné výrobky a o zrušení směrnice Rady 85/374/EHS (dále jen „směrnice o odpovědnosti za vadné výrobky“).

předchozích kapitol, které je často samy zmiňují.²³ Nadto je třeba zmínit, že ony kapitoly věnující se substantivním aspektům férovosti již mnohdy zmínky o procesních aspektech obsahují. Tyto duplicity pak při čtení knihy jako celku působí přinejmenším rušivě. Tuto kritiku je sice možné z velké části přičíst specifickému charakteru, který kolektivní monografie má, nelze už ale zdůvodnit, proč jsou tyto kapitoly vynechány z oné jednotící metodologie, ani proč k ní nijak nerefereují.

To ale není jediná duplicita, kterou v knize můžeme nalézt. Jednotlivé kapitoly věnující se digitální legislativě v některých případech samy obsahují drobný exkurs do filozofie a historie konceptu férovosti.²⁴ Autoři kapitol volí výklad, který pro onen koncept budou používat, a zvláště se tak odchylují od výkladu provedeného v úvodní části. Koheze textu s úvodní metodologií je ostatně ve většině knihy poměrně nízká. Metodologická kapitola z úvodu přesně vymezuje, jak by měl probíhat výzkum konkrétní podoby konceptu férovosti v daných digitálních regulacích. Jednotliví autoři kapitol ale často tento postup nenásledují nebo na něj nijak nerefereují. Text proto působí dojmem, že byla metodologie formulována buď paralelně s psaním ostatních kapitol nebo dokonce až zpětně.

Celkově je možné také konstatovat, že kapitoly se silně liší co do kvality obsahu. Přestože například nařízení DMA obsahuje o férovosti díky aplikaci podmínek FRAND²⁵ velkou řadu zmínek,²⁶ první kapitola věnující se DMA působí spíš jako rekapitulace nařízení s vypíchnutím částí, kde se

²³ Viz Van Cleynenbreugel, P., Grozdanovski, L. (eds). *The Standards of Fairness in Digital Law: The Normative Foundations of the Data, Data Governance, Digital Services, Digital Markets and Artificial Intelligence Acts*. In: Van Cleynenbreugel, P., Grozdanovski, L. (eds). *The Standards of Fairness in Digital Law*. Edward Elgar Publishing, 2025. s. 95 pro DGA a DA.

²⁴ Např. tamtéž, s. 268.

²⁵ Podmínky FRAND jsou zkratka pro ustanovení vyžadující, aby byla určitá data zpřístupněna dle podmínek, které jsou v angličtině uváděny jako „*fair, reasonable and non-discriminatory*“, tedy spravedlivé nebo férové, přiměřené a nediskriminační.

²⁶ Viz Van Cleynenbreugel, P., Grozdanovski, L. (eds). *The Standards of Fairness in Digital Law: The Normative Foundations of the Data, Data Governance, Digital Services, Digital Markets and Artificial Intelligence Acts*. In: Van Cleynenbreugel, P., Grozdanovski, L. (eds). *The Standards of Fairness in Digital Law*. Edward Elgar Publishing, 2025. s. 68 nebo např. přímo čl. 6 odst. 12 DMA.

tyto zmínky nacházejí. Takový text nepřináší příliš přidané hodnoty. Oproti tomu text k DSA má silnou základnu citovaných odborných publikací a samotný text je v některých částech i poměrně inovativní. Je jen škoda, že patří k nařízení, kde je ona férovost, která měla být hlavním motivem knihy, zmíněna v závazné části textu nařízení jen několikrát. Celá kapitola se tak věnuje spíše jiným problematikám v DSA než právě hledání významu férovosti. Zřejmě proto, že ona férovost téměř žádnou roli v tomto nařízení nehraje.

To vede k dalšímu zvláštnímu rozhodnutí, které editoři při kompletaci knihy učinili. Ještě v úvodních stránkách knihy je čtenáři představena prostá jazyková analýza dotčených právních předpisů a počtu zmínek klíčových slov, která byla zvolena. Tato klíčová slova jsou nepřekvapivě „férovost“ nebo „neférovost“ a obdobné tvary souvisejících slov. Tabulka má zřejmě ilustrovat, že daná legislativa je zmínkami o férovosti protkaná. Ve většině případů je přitom nutno dát této myšlence za pravdu, v případě DSA ovšem tabulka eviduje v závazném textu nařízení jen dvě zmínky. Jak již bylo zmíněno, výklad se tak u tohoto nařízení na férovost příliš nezaměřuje. Editoři měli možná vyhodnotit menší míru relevantnosti DSA pro jejich publikaci a spíše ho z rozsahu knihy vyřadit či lépe zdůvodnit jeho zahrnutí. Ve finálním textu totiž zahrnutí DSA po tomto zjištění působí jako snaha zahrnout do knihy všechny novější digitální právní předpisy z EU, aby byla výsledná kniha atraktivnější.

Podobně zvláštním rozhodnutím je zahrnutí již výše zmíněné kapitoly týkající se práva na spravedlivý proces, ve které je princip férovosti v procesním smyslu rozebírán na návrhu směrnice o odpovědnosti za AI, který byl již k datu vydání knihy oficiálně stažena,²⁷ a směrnicí o odpovědnosti za vadné výrobky, která je v knize snad poprvé zmíněna právě až v této kapitole. Snaha zabývat se procesní spravedlností, jejíž odraz se mohl nejvíce projevit v kontextu nových technologií u směrnice o odpovědnosti za AI, je pochopitelná. Nemění ale nic na tom, že kapitola působí jako neaktuální

²⁷ Viz např. European Parliament Legislative train schedule. [online] c 2026 [cit. 19. 4. 2026]. Dostupné z: <https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-ai-liability-directive>

přílepek. Možná by bylo vhodnější pokusit se do knihy zahrnout text týkající se připravovaného aktu o digitální spravedlnosti, v angličtině „*Digital Fairness Act*“.²⁸

V knize je ale možné nalézt i místa, která je potřeba vyzdvihnout. Pokud pomineme to, že kapitola zaměřená na DMA by se měla věnovat zmínkám o férovosti v rámci tohoto nařízení, je tato kapitola zdařilým přehledem aktuální diskuze o funkčnosti nástrojů, které DMA nabízí k regulaci velkých technologických společností.²⁹ V kapitole o DGA a DA je část věnující se DA velmi kvalitní a podrobně rozebírá kritéria FRAND specificky pro toto nařízení, včetně individualizace nejen férovosti, ale i ostatních součástí FRAND.³⁰ Kromě toho je tato část kapitoly i dobře napojena na metodologickou kapitolu a postupuje přesně tak, jak úvodní metodologie vymezila. O to horší je, když se druhá část, věnovaná DGA a zjevně psaná převážně jiným autorem, omezí jen na popis fungování DGA a o něco bližší analýzu ustanovení obsahujících klíčová slova bez většího vhledu do toho jakou roli koncept férovosti v nařízení hraje.

Vyzdvihnout je také třeba kapitolu o AI Actu, ten obdobně jako DSA obsahuje jen minimum zmínek o férovosti v textu. Autor kapitoly to přímo přiznává, ale celá kapitola je postavená na myšlence, že by oněch zmínek mělo být spíše více. Zejména autor poukazuje na to, jak férovost podkrešuje nároky na systémy AI podle daného nařízení, jako je například nutnost používat pro vývoj AI systémů reprezentativní data nebo zákaz diskriminace.³¹ Poukazuje tak na to, že férovost se v AI Actu objevuje spíše jako blíže specifikovaný faktický požadavek než jako procesní férovost. Procesní aspekty autor vnímá zejména ve vztahu k právu na vysvětlitelnost, jinak už příliš ne.

²⁸ Viz European Parliament Legislative train schedule. [online] c 2026 [cit. 16. 5. 2026]. Dostupné z: <https://www.europarl.europa.eu/legislative-train/theme-protecting-our-democracy-upholding-our-values/file-digital-fairness-act>

²⁹ Viz Van Cleynenbreugel, P., Grozdanovski, L. (eds). *The Standards of Fairness in Digital Law: The Normative Foundations of the Data, Data Governance, Digital Services, Digital Markets and Artificial Intelligence Acts*. In: Van Cleynenbreugel, P., Grozdanovski, L. (eds). *The Standards of Fairness in Digital Law*. Edward Elgar Publishing, 2025. s. 66.

³⁰ Tamtéž, s. 110.

³¹ Tamtéž, s. 191-193.

Za zmínku také stojí druhá iterace kapitoly věnující se DSA, tentokrát spadající mezi poslední čtyři výše zmíněné kapitoly o procesní férovosti. Tato kapitola na příkladu DSA blíže zkoumá procesy přístupu ke spravedlnosti a práva na přezkum, která hrají ve vztahu k příjemcům služby v DSA významnou roli. Velká část dané kapitoly je věnována opět přehledu regulace obsažené v DSA, jež kniha už v mnohem větším rozsahu obsahuje. Jakmile se ale kapitola přikloní k rozboru práv příjemce služeb ve vztahu k moderačním rozhodnutím učiněným platformou,³² demonstruje její autorka vhléd a vhodnou kritiku textu i aktuálního fungování práv příjemců služby.

4. ZHODNOCENÍ

S celkovým hodnocením knihy jsem na vážkách. Není pochyb, že autorský kolektiv rozumí analyzované legislativě a kniha je prostá faktických chyb. Stylistika se samozřejmě v jednotlivých kapitolách znatelně liší podle toho, kdo je autorem, ale jazyková úroveň je velmi dobrá a texty často příjemně plynou. Některé kapitoly jsou popisnějšího charakteru, jiné zase vyzdvihují u jednotlivých nařízení konkrétní a zajímavé myšlenky. Stále mám ale problém s celým rámováním knihy. Již na začátku knihy je odhaleno, že koncept férovosti, se kterým kniha pracuje, je natolik vágní, že nelze nalézt jednu interpretaci, která by mohla sloužit pro všechny rozebírané regulace. Cílem jednotlivých kapitol tak je najít autonomní významy tohoto pojmu v konkrétních právních předpisech, aniž by bylo možné v knize kromě slova „*fairness*“ vnímat příliš propojujících linií. I poslední čtyři kapitoly knihy působí poněkud nesystematicky: mají se zabývat procesními aspekty férovosti, ale buď v nařízeních, která už byla analyzována i co do procesní části, anebo zahrnují rozbor regulace, která již není relevantní a jejíž význam není pro cíle knihy zřejmý. Přitom tyto kapitoly ani přímo nezapadají do metodologie, která se měla knihou prolínat. Metodologie, která měla knize na soudržnosti přidat, proto kvůli zařazení těchto kapitol spíš podtrhuje nedostatky v soudržnosti textu jako celku. Moje hlavní kritika tak směřuje k jevům typickým pro kolektivní monografie, a to hlavně proto, že pu-

³² Tamtéž, s. 213 a násl.

blikace obsahuje snahu prostřednictvím metodologii tyto neduhy zmírnit. To se bohužel ale ve výsledku, dle mého názoru, nepodařilo.

Knihu bych doporučil čtenáři, který chce získat obecný přehled o novější digitální regulaci v EU, ale pro takové potřeby jistě existují lepší publikace. Snad nejlepší využití si umím představit tak, že potenciální čtenář má zájem o konkrétní nařízení a vysvětlení konceptu férovosti v něm. Pak může být kniha poměrně přínosná, pokud tedy onen čtenář nejeví zájem o DMA. Obecně je možné knihu shrnout slovy, která používají sami autoři a jež si dovolím zde volně přeložit jako „*férovost je koncept závislý na kontextu*“. Nelze proto od knihy očekávat příliš jednotících závěrů.

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>).

CASAROSA, F., PSYCHOGIOPOULOU, E. (EDS.):
SOCIAL MEDIA, FUNDAMENTAL RIGHTS AND
COURTS: A EUROPEAN PERSPECTIVE

JAN MARTÍNEK¹

CASAROSA, Federica, PSYCHOGIOPOULOU, Evangelia (eds.): Social Media, Fundamental Rights and Courts: A European Perspective. New York: Routledge, 2023, 274 s. ISBN 9781032074696.

1. ÚVOD

Prostředí sociálních sítí je v mnoha ohledech odlišné od dosavadní formy veřejné komunikace, specifická pravidla však dlouho chyběla. Soudy proto musely komplexní problémy řešit pomocí analogické aplikace dosavadních předpisů.² Ty však vznikaly pro jiné prostředí, což v praxi naráží na mnohé problémy. V podobných situacích se projevuje výhoda společné evropské právní kultury, kterou sjednocuje judikatura nadnárodních soudů. Díky srovnatelným základům můžeme čerpat inspiraci ze zkušeností soudů napříč kontinentem a v podobných případech funkční argumentaci převzít. Recenzovaná publikace přichází s cenným zmapováním těchto zkušeností. Téma je vysoce aktuální i s ohledem na nové nařízení o digitálních službách³ (DSA), které vytváří pravidla pro uplatnění „offline práva“ v online prostředí. Dosavadní soudní praxe může být stěžejní jak pro výklad někte-

¹ Mgr. Jan Martínek je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity a analytikem Ústavního soudu. Kontaktní e-mail: 508778@muni.cz. ORCID 0009-0008-3151-2259.

² Viz s. 3 recenzované publikace.

³ Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (nařízení o digitálních službách).

rých neurčitých článků DSA,⁴ tak pro řešení konkrétních případů v nových procesech podle tohoto nařízení.⁵

Na vzniku publikace spolupracovalo celkem dvacet evropských akademiků a akademiků, včetně editorek.⁶ Jejich cílem bylo zodpovědět otázku, zda evropské soudy interpretují základní práva v případech spojených se sociálními sítěmi a případně jak.⁷ V úvodu editorky shrnují důvody pro vznik publikace, její cíle a dosavadní vývoj evropské regulace v podobě směrnice o elektronickém obchodu,⁸ audiovizuálních mediálních službách,⁹ boji proti terorismu¹⁰ a dalších právních předpisů. Kniha se dále dělí do dvou částí. První analyzuje judikaturu vrcholných evropských soudů: Soudního dvora Evropské unie (SDEU) a Evropského soudu pro lidská práva (ESLP). Druhá část představuje soudní praxi ve vybraných evropských státech.¹¹

2. EVROPSKÁ PERSPEKTIVA: JUDIKATURA SDEU A ESLP

První část odráží dosavadní vývoj v judikatuře SDEU a ESLP, jejichž závěry se následně promítají do praxe jednotlivých národních soudů. Obě kapitoly obsahují klíčové judikáty v oblasti sociálních sítí, které mnohdy posloužily

⁴ Např. pro povinnost zohlednit základní práva jednotlivců při vytváření a aplikaci interních podmínek užití, čl. 14/4 DSA.

⁵ Jedná se zejm. o interní systém platform pro vyřizování stížností podle čl. 20 DSA, řízení před orgány pro mimosoudní řešení sporů podle čl. 21 DSA nebo vyřizování stížností pro porušení DSA, které probíhá před státními dozorčími orgány podle čl. 53 DSA.

⁶ Pro jejich přehled viz s. ix-x recenzované publikace.

⁷ Viz s. 7, tamtéž.

⁸ Směrnice Evropského parlamentu a Rady (EU) 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu ("směrnice o elektronickém obchodu").

⁹ Směrnice Evropského parlamentu a Rady 2010/13/EU ze dne 10. března 2010 o koordinaci některých právních a správních předpisů členských států upravujících poskytování audiovizuálních mediálních služeb (směrnice o audiovizuálních mediálních službách).

¹⁰ Směrnice Evropského parlamentu a Rady (EU) 2017/541 ze dne 15. března 2017 o boji proti terorismu, kterou se nahrazuje rámcové rozhodnutí Rady 2002/475/SVV a mění rozhodnutí Rady 2005/671/SVV.

¹¹ Jmenovitě jde o Estonsko, Finsko, Francii, Německo, Maďarsko, Irsko, Itálii, Slovinsko, Španělsko a Spojené království.

jako základní kameny následné regulace. Tato část je cenná především tím, že judikáty přehledně shrnuje a vysvětluje souvislosti mezi nimi.

Z pohledu uplatňování evropských regulací je důležitý pohled SDEU, který evropské právo vykládá. S ohledem na přijetí Listiny základních práv EU má SDEU silnou pozici i v uplatňování základních práv. Judikáty se dělí do několika podoblastí podle témat, která řeší. Kapitola předkládá přehlednou analýzu judikátů k odpovědnosti zprostředkovatelů (*Telekabel Wien*), zákazu obecného monitoringu (*YouTube v. Cyando*) nebo správě osobních údajů (*Schrems*) a dalších. Kriticky se vyjadřují k neochotě SDEU pracovat důsledně se základními právy, jimž se v některých judikátech vyhýbá (*Glawischnig-Piesczek*).¹²

Naopak ESLP z podstaty věci musí pracovat přímo s analýzou lidskoprávní stránky případu. Jeho závěry lze proto uplatnit na širokou škálu problémů. Tomu odpovídá i velké množství judikátů v této části, které různě velkou mírou souvisí s problémem sociálních sítí. Leitmotivem je především snaha vztáhnout jednotlivé principy na nové prostředí sociálních sítí. To se mnohdy daří, jako např. v argumentaci pro blokování příspěvků, které neodpovídají světonázoru zájmových fór, s ohledem na závěry případu *Pusy Riot (Mariya Alekhina)*. Naopak jiné případy reflektují spíše problémy na sociálních sítích, aniž by bylo zřejmé, čím se liší od projevu v offline světě (*Beizeras a Levickas*). U některých témat představuje tato část ucelený přehled vývoje, který následně reflektují „národní části“ publikace, jedná se např. o odpovědnost zprostředkovatelů služeb informační společnosti (*Delfi, MTE, Høiness, Sanchez* aj.). Nad rámec přehledu otevírá též zajímavé právní otázky: zda lze vnímat omezení dosahu jako méně invazivní prostředek, příp. jak pracovat s projevem automatizovaných botů. Bohužel na ně neodpovídá.

¹² Viz s. 35 a násl. recenzované publikace.

3. NÁRODNÍ PERSPEKTIVA: JUDIKATURA VYBRANÝCH EVROPSKÝCH STÁTŮ

Těžištěm publikace je analýza judikatury vybraných evropských států. Výběr konkrétních zemí je vždy problematický a zpravidla vykazuje větší či menší deficit, zde je však volba racionální. Odráží zkušenosti států, kde velké platformy většinou sídlí (Irsko), států s dlouholetou snahou o jejich regulaci (Německo) nebo naopak se zkušeností kratší (Slovinsko), případně států, jejichž soudy stály u vzniku aktuální doktríny (Estonsko s případem *Delfi*). Samotné editorky navíc výběr odůvodňují geografickou odlišností (západ i východ Evropy) a různými tradicemi ochrany základních práv (např. britská zkušenost s nepsanou ústavou).¹³ Jednotlivé kapitoly drží společnou strukturu: přibližují podobu soudní soustavy v daném státě, popisují klíčové případy spojené se sociálními sítěmi, a nakonec hodnotí dialog národních soudů s oběma evropskými soudy. Ze struktury je zjevná snaha editorek o přehlednost jednotlivých podkapitol a jejich navázání na předchozí část o SDEU a ESLP. Tomuto cíli však brání nesjednocené přístupy jednotlivých autorů a autorek.

Některé části zbytečně dlouze opakují případy popsané v první části, jako je *Delfi* v části věnované Estonsku nebo *MTE* v případě Maďarska. Naopak vysoce relevantní jsou zkušenosti německých soudů, které čerpají z aplikace zákona o prosazování práva v síti (NetzDG),¹⁴ jedné z prvních legislativních snah o regulaci platforem. Rozdělení mezi jednotlivé státy působí v konečném důsledku nevyváženě právě proto, že se jejich zkušenost s tématem i hloubka řešených problémů podstatně liší. Jednotliví autoři navíc často zmiňují spíše případy *na sociálních sítích*, tedy starý koncept, který se pouze vyskytl v jiném prostředí, ale v podstatě se neodlišuje (např. případy pomluvy z Maďarska).¹⁵ Celkové využitelnosti cenných informací by prospělo rozdělení případů podle témat, např. pomocí přehledné tabulky v příloze publikace. Ta by čtenáři umožnila rychlou orientaci mezi jednot-

¹³ Viz s. 11, tamtéž.

¹⁴ *Netzwerkdurchsetzungsgesetz* ze dne 1. září 2017 (BGBl. I S. 3352). Viz s. 121 recenzované publikace.

¹⁵ Viz s. 142, tamtéž.

livými případy a pomohla mu jednoduše porovnat, jak jednotlivé státy řeší obdobné problémy.

Přesto přináší srovnání jednotlivých přístupů velmi cenné informace pro další výzkum v souvislosti s regulací sociálních sítí. Zajímavá je v tomto ohledu například nesourodost přístupu k uplatnění regulace klasických médií vůči sociálním sítím, která je zjevná v případě Maďarska (aplikuje ji)¹⁶ a Itálie (neaplikuje).¹⁷ A to i s ohledem na rozsudky ESLP ve věcech *Times Newspapers Ltd.* nebo *Pravoye Delo*, které automatickou aplikaci vylučují. Závěry soudů se liší též v otázce shromažďování důkazů z veřejných profilů na sociálních sítích, kdy ve Francii šlo ze strany daňového orgánu o porušení soukromí,¹⁸ porušení však neshledaly španělské soudy v případě podněcování k terorismu.¹⁹ V otázce uplatňování základních práv na vztah mezi sociálními sítěmi a samotnými uživateli lze ve značné míře vycházet z německé judikatury. Ta dovodila jejich horizontální efekt s ohledem na kvazi-monopolní postavení velkých sociálních sítí.²⁰ Zákonodárci na specifika online prostředí reagovali i v trestním právu. Ve Slovinsku²¹ či Španělsku²² vytvořili speciální skutkové podstaty pro trestné činy páchané na sociálních sítích, které lépe odrážejí jejich reálný průběh.

4. ZÁVĚR

Kniha přináší velmi cenný vhled do judikatury vybraných evropských států. Trpí však především nesourodostí jednotlivých částí, která je zřejmě dána rozdílným přístupem jednotlivých autorů a autorek. Největší přidanou hodnotu vykazují méně známé případy národních soudů (zejm. těch německých), které řeší vysoce relevantní problémy pro budoucí regulaci sociálních sítí. Knize by prospělo větší propojení jednotlivých částí, i kdyby se

¹⁶ Viz s. 148, tamtéž.

¹⁷ Viz s. 171, tamtéž.

¹⁸ Viz s. 110, tamtéž.

¹⁹ Viz s. 209, tamtéž.

²⁰ Viz s. 124, tamtéž.

²¹ Viz s. 189, tamtéž.

²² Viz s. 206, tamtéž.

mělo jednat jen o případný přehled zmíněných případů a jejich rozdělení podle témat.

Přesto je publikace cenným zdrojem nejen pro akademickou obec, ale i pro soudní personál, či rozhodce orgánů pro mimosoudní řešení sporů podle čl. 21 DSA. Právě pro ně bude klíčové pochopit nuance mezi „offline“ judikaturou a specifiky sociálních sítí. S ohledem na zavedení nových procesních možností skrze DSA lze do budoucna počítat s nárůstem případů, u nichž bude potřeba zohlednit unikátní aspekty prostředí sociálních sítí, a je nutné, aby při jejich řešení jednotlivé orgány zohledňovaly závěry dosavadní soudní praxe. Jen tak lze docílit udržitelnosti systému a rovného uplatňování základních práv.

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/RPT2026-1-5>

AKTUÁLNÍ OTÁZKY POSTIHOVÁNÍ DEEPFAKES

ZDENĚK FIALA¹, PAVEL MATES² A MAREK PAČMAG³

ABSTRAKT

Příspěvek se zabývá aktuálně diskutovaným tématem, jímž je tvorba deepfakes ve spojení s vyvozením trestněprávní či správněprávní odpovědnosti. První část příspěvku představuje obecná východiska v oblasti deepfakes, způsoby jejich tvorby a jejich rizikovost pro společnost.

V následujících částech se již autoři podrobněji zaměřují na deepfakes se sexuální kontextem, kdy přibližují právní kvalifikaci materiálů zobrazující děti, dospělé osoby a známé osobnosti. Závěrečná část příspěvku pojednává o specifických otázkách spojených s odhalováním, prověřováním a dokazováním těchto deepfakes. Jednotlivé části reflektují a zprostředkovávají poznatky a zkušenosti z aplikační praxe.

KLÍČOVÁ SLOVA

Deepfakes; trestní právo; trestný čin; přestupek

ABSTRACT

The article deals with the currently discussed topic of deepfakes creation in connection with the imposition of criminal or administrative liability. The first part of the article presents general principles in the field of deepfakes, methods of creation and risk to society.

¹ doc. JUDr. PhDr. Zdeněk Fiala, CEVRO univerzita, Policejní akademie České republiky v Praze

² doc. JUDr. Pavel Mates, Vysoká škola ekonomická a správní Praha, FSE UJEP.

³ Mgr. Marek Pačmag, MBA, LL.M., doktorand na Českém vysokém učení technickém v Praze, Fakulta biomedicínského inženýrství.

In the following sections, the authors focus in more detail on deepfakes with a sexual context, where they explain the legal qualification of materials depicting children, adults and celebrities. The final part of the article discusses specific issues related to the detection, verification and evidence of these deepfakes. The individual sections reflect and convey knowledge and experience from application practice.

KEYWORDS

Deepfakes; Criminal Law; Crime; Offence

1. ÚVOD

Umělá inteligence se poměrně rychle stala součástí moderní společnosti. Pro její značný potenciál lze do budoucna nejspíše předpokládat další rozvoj a její kontinuální pronikání do soukromého i veřejného sektoru, tak i běžného občanského života.

Nicméně i zde bohužel platí, že každý „vynález“ vytvořený primárně k pozitivním účelům, může být v konečném důsledku zneužit. Příkladem může být tvorba podvodných deepfakes.

O deepfakes jako novodobém problému se začalo vážněji diskutovat zejména ve spojení s šířením falešných pornografických fotografií a videí veřejně známých osobností.⁴ V posledních letech se lze v prostředí Internetu, již běžně setkat s podvodnými videi, vybízejícími k zvláště výhodným finančním investicím. V roce 2024 se stal objektem těchto videí i prezident České republiky Petr Pavel.⁵ V tomto směru platí, že tak jak se rozšiřuje dostupnost a sofistikovanost generátorů deepfakes, tak se úměrně zvyšuje i riziko jejich zneužití, a to nejen co do možností, ale i okruhu potenciálních pachatelů a obětí. Obětí deepfakes se dnes nestávají výhradně ve-

⁴ Srov. např. KIETZMANN, J. a kol. Deepfakes: Trick or treat? *Business Horizons*. 2020, Vol. 63, No. 2, s. 136.

⁵ ŠVIHEL, P. *Přišli jsme o všechno a stydíme se. Pár uvěřil, že investice zaštiťuje Petr Pavel*. In: Seznam Zprávy [online]. 25. 4. 2023 [cit. 2025-10-10]. Dostupné zde: <https://www.seznamzpravy.cz/clanek/domaci-zivot-v-cesku-podvodnici-se-zastitili-prezidentovym-jmenem-seniorsky-par-prisel-o-vsechno-229909>

řejně známé osoby (celebrity), ale stále častěji i běžní občané.⁶ Pochmurná vize V. Smejkal o tom, že do budoucna lze očekávat masivní zneužívání Internetu k šíření nepravdivých údajů jak vůči osobám fyzickým, tak právnickým, jakož i šíření protizákonných (nenávistných) ideologií a jiných informací, směřujících k poškozování lidských práv a jiných norem práva vnitrostátního i mezinárodního, se dnes ukazuje bohužel jako více než realistická. Internet patří k nástrojům, které sblíží svět, nabízí možnosti k usnadnění svobody projevu a komunikace, ale také k šíření hoaxů, rasistických, xenofobních a nenávistných myšlenek a to tím spíše, že se tak mnohdy děje v podmínkách anonymity.⁷

Problematika deepfakes se proto dostává čím dál tím více do pozornosti odborné veřejnosti, a to jak v zahraničí⁸, tak tuzemsku⁹. Kontinuálně napříč vědními obory (zejména technickými, psychologickými a právními)

⁶ Srov. např. BENÍŠKOVÁ, E. „Někdo hodil mou fotku do AI, aby mě svlékl.“ *Tři české influencerky o své zkušenosti s novou formou sexuálního obtěžování*. In: HEY FOMO [online]. 22. 10. 2023 [cit. 2025-10-10]. Dostupné na: <https://heyfomo.cz/nekdo-hodil-mou-fotku-do-ai-aby-me-svlekl-tri-ceske-influencerky-o-sve-zkusenosti-s-novou-formou-sexualniho-obtezovani>.

⁷ SMEJKAL, V. *Kybernetická kriminalita*. 3 vyd. Plzeň: Aleš Čeněk 2022, s. 845; GRIVNA, T., POLČÁK, R. (eds.) *Kriminalita a právo*. Praha: Auditorium 2008, s. 145; KASL, F. *Porušení bezpečnosti osobních údajů v kontextu Internetu věcí*. Brno: Masarykova univerzita, 2021, s. 151-154.

⁸ Srov. např. ANTOGNINI, A. – WOODS, A. K. Shallow Fakes. *Penn State Law Review*. 2023, Vol. 128, No. 69; BENGIO, Y. – HINTON, G. – LECUN, Y. Deep learning. *Nature*. 2015, Vol. 521, No. 7553; JUEFEI-XU, F. a kol. Countering Malicious DeepFakes: Survey, Battleground, and Horizon. *arXiv*. 2022, No. 2103.00218, GOODFELLOW, I. a kol. *Generative Adversarial Nets*. In: GHAFRAMANI, Z. – WELLING, M. a kol. (eds.). *Advances in Neural Information Processing Systems 27 (NIPS 2014)*. Montreal: Curran Associates, 2014, s. 2672, KIETZMANN, J. a kol. Deepfakes: Trick or treat? *Business Horizons*. 2020, Vol. 63, No. 2

⁹ Srov. např. FIRK, A. – HANÁČEK, P. – MALINKA, K. Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. *Heliyon*. 2023, Vol. 9, No. 4, MIZEROVÁ, T. Právo a deepfakes. In: *AUCI*, č. 2, roč. 2025; POBOŘILOVÁ, M. Virtuální dětská pornografie, *AUCI*, č. 4, roč. 2012, s. 88; BARTOŇ, M. Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. *Právní rozhledy*, č. 17, roč. 2008, ZÁMEK, D. *Rizika zneužití umělé inteligence ke generování sexuálně explicitního obsahu*. In: *QUAERE 2023* - Recenzovaný sborník příspěvků interdisciplinární mezinárodní vědecké konference doktorandů a odborných asistentů. Hradec Králové: MAGNANIMITAS, 2023. p. 306 - 313. vol. 13. ISBN 978-80-87952-38-2., ČESKÁ ASOCIACE UMĚLÉ INTELIGENCE. *Manuál DEEPFAKE 2024: Obranná strategie pro české firmy*. Online. 2023, aktualizace 27.12.2023. Dostupné z: <https://asociace.ai/deepfake-2024/>. [cit. 2025-10-20].

se hledají efektivní způsoby, nástroje a opatření, jež by mohly další šíření deepfakes a jejich negativní dopady eliminovat či alespoň omezit. Právní regulace sehrává při tomto úsilí důležitou roli.

Preventivní „regulace deepfakes v AI aktu”¹⁰ a dalších předpisech nezabrání rizikovým využitím deepfakes a s odstraněním negativních důsledků jejich šíření pomůže jen částečně. Aktéři zneužívající deepfakes mohou stále šířit neoznačené deepfakes, a navíc využívat pokročilejší generátory, které mohou oklamat detektory. Dalším nástrojem dopadajícím na nezákonná šíření deepfakes je tak trestní právo. Deepfakes lze stíhat pomocí existujících skutkových podstat nebo nových jako deep porn.¹¹

V návaznosti na tyto závěry je cílem tohoto příspěvku rozpracování aktuálních otázek spojených s vyvozením trestněprávní, popřípadě správněprávní odpovědnosti, a to na základě poznatků z aplikační praxe a tím přiblížit i nejčastější hrozby, s nimiž se mohou uživatelé na Internetu setkat.

2. OBECNÁ VÝCHODISKA DEEPFAKES¹²

Pokud jde o právní vymezení pojmu deepfakes nabízí se poukázat zejména na čl. 3 odst. 60 AI aktu, který jej definuje jako „obrazový, zvukový nebo video obsah vytvořený nebo manipulovaný umělou inteligencí, který se podobá existujícím osobám, objektům, místům, subjektům či událostem a který by se dané osobě mohl nepravdivě jevit jako autentický nebo pravdivý.“ Z oblasti technických věd lze zmínit např. definici GAO¹³, jež charakterizuje

¹⁰ Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci)

¹¹ MIZEROVÁ, T. Právo a deepfakes. In. AUCI, č. 2, roč. 2025, str. 131. POZN. autorů: autorka rozebírá v souvislosti s regulací digitálního prostoru a šíření deepfakes úpravu směřující na detektory deepfakes (GDPR a AI akt), šíření deepfakes na platformách (DSA a s ním související předpisy), a spojenou s označováním syntetického obsahu a deepfakes (AI akt).

¹² Obsah kapitoly vychází z aktuálně zpracovávané disertační práce spoluautora Marka Pačmaga s názvem "Vybrané problémy ochrany dětí před sexuálním zneužíváním v kyberprostoru", na Fakultě biomedicínského inženýrství Českého vysokého učení technického v Praze.

¹³ Zkratka GAO znamená „U.S. Government Accountability Office“ v překladu Úřad pro odpovědnost vlády Spojených států amerických blíže <https://www.gao.gov/>.

deepfakes jako „video, fotografii nebo zvuková nahrávku, která se zdá být skutečná, ale byla upravena pomocí umělé inteligence. Základní technologie může nahradit obličej, manipulovat s výrazem obličeje, syntetizovat obličej a syntetizovat řeč. Deepfakes mohou zobrazovat někoho, jak říká nebo dělá něco, co ve skutečnosti nikdy neřekl nebo neudělal“.¹⁴

Jak vidno citované **definice** jsou si v mnoha aspektech podobné a jsou vystavěny na následujících **pojmových znacích** (atributech)¹⁵:

- způsob vytvoření deepfakes – obsah je vytvořen za pomoci umělé inteligence (rychlost a snadnost zpracování)
- podoba deepfakes – jde o obrazový, zvukový, textový nebo audiovizuální záznam
- předmět deepfakes – vyobrazuje existující osoby, události, objekty, místa, atp.
- autentičnost deepfakes – jeví se jako skutečný, realistický (způsobílost oklamat). Díky této vlastnosti deepfakes představují aktuálně tak velký problém, neboť jsou velmi přesvědčivé a obtížně ověřitelné (rozpoznatelné).¹⁶

K vyvození trestněprávní odpovědnosti (v širším slova smyslu) za deepfakes je nezbytné, aby zneužití (šíření) deepfakes dosahovalo takové míry společenské škodlivosti, že nepostačuje uplatnění odpovědnosti podle jiného právního předpisu s odkazem na zásadu subsidiarity trestní represe a princip ultima ratio z ní vyplývající.¹⁷ Nepřijatelné jsou proto zejména deepfakes vytvořené s úmyslem poškodit jiného nebo se na jiném obohatit. Deepfakes mohou přitom směřovat jak vůči jednotlivci (např. vytvoření pornografického snímku politicky činné osoby či jiné veřejně známé osoby), ale i celé společnosti (například v podobě diskreditace voleb do Parla-

¹⁴ U.S. GOVERNMENT ACCOUNTABILITY OFFICE. *Science & Tech Spotlight: DEEPFAKES*. Online. 2020. Dostupné z: <https://www.gao.gov/assets/gao-20-379sp.pdf>. [cit. 2025-10-20].

¹⁵ Obdobně např. ŁABUZ, M. Regulating Deep Fakes in the Artificial Intelligence Act. *Applied Cybersecurity & Internet Governance*. 2023, Vol. 2., s. 5–6.

¹⁶ Srov. např. GEISE, S. *Visual Framing*. In: RÖSSLER, P. (ed.). *The International Encyclopedia of Media Effects*. Chichester: Wiley Blackwell, 2017, s. 2054.

¹⁷ ŠÁMAL, P. *Trestní zákoník: komentář*. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. ISBN 978-80-7400-893-1. s. 230.

mentu České republiky nebo v rámci sociálního inženýrství). Na druhé straně se zpravidla nepovažují za závadné (natolik společensky škodlivé) materiály, používané k ironizování politicky činných osob, anebo naopak společensky přínosné, tj. sloužící např. k rekonstrukci historických událostí nebo demonstrování možností daného oboru.

V souvislosti s deepfakes lze v současné době identifikovat následující **typy zneužití**:

- manipulace s video nahrávkami, ve kterých je tvář nebo tělo nahrazeno jinou tvář, tělem či uměle generovaným obsahem pomocí AI technologií (Decline in Trust of Visual Evidence);
- manipulace se statickým obrazem, přičemž dochází k úpravě fotografií či jiného vizuálního obsahu (Reputation Damage & Character Assassination);
- manipulace s textem, kdy je část textu nebo celý text vytvořen za pomoci AI
- audio deepfake, při kterém dochází k vytvoření věrohodného hlasového záznamu za použití několikaminutového autentického záznamu;
- propagace falešných zpráv: extremistické skupiny mohou nahrávat videa svých vůdců podporujících agendu falešných zpráv nebo předstírat nově uniklé dokumenty, aby vyvolaly konfliktní nálady ve společnosti s cílem způsobit významné politické nebo sociální otřesy (Promoting Fake News).¹⁸

Při tvorbě obrazových deepfakes se lze nejčastěji setkat s technologií generativních adversariálních sítí, tzv. GANs. Jedná se o typ pokročilého strojového učení, při kterém nejprve dochází k trénování modelu (dvě neuronové sítě spolu interagují způsobem, kdy jedna vytváří realistické obrazy nebo videa a druhá usiluje o rozlišení mezi skutečnými a uměle vygenerovanými daty). Ve fázi, kdy již není druhá neuronová síť schopna rozlišit

¹⁸ VIZOSO, Á; VAZ-ÁLVAREZ, M. a LÓPEZ G., Xosé. *Fighting Deepfakes: Media and Internet Giants' Converging and Diverging Strategies Against Hi-Tech Misinformation*. Online. *Media and Communication*. 2021, vol. 9, no. 1, s. 291-300. ISSN 2183-2439. Dostupné z: <https://doi.org/10.17645/mac.v9i1.3494>. [cit. 2025-10-21].

mezi skutečností a tím, co je vygenerováno, je model použit například k výměně tváře cílové osoby ve videu či na obrázku. Model si zmapuje rysy obličeje cílové osoby s obličejem osoby ve zdrojovém podkladu. Nakonec jsou generované výstupy modifikovány pomocí softwaru pro úpravu videa, aby působily realisticky dochází k manipulaci s barvami, jasnem a podobně.¹⁹

U **audio deepfakes** je využíváno obdobných technologií jako u obrazových. U těchto ještě důrazněji platí pravidlo – čím více je dostupných zvukových nahrávek cílové osoby, tím zdařilejší bude finální produkt. U politicky činných osob nebo interpretů populární hudby se zpravidla zajišťují desítky rozhovorů a dalších audiovizuálních stop z veřejně dostupných zdrojů. Kromě výše zmíněných generativních adversariálních sítí se používají také konvoluční neuronové sítě (CNNs) či hluboké neuronové sítě (DNNs). Cílem je napodobování rysů hlasu cílové osoby. Je notorietou, že každý člověk disponuje sadou specifik ve svém mluveném projevu. Při postprodukci se u uměle generovaných zvukových nahrávek následně vylepšuje intonace či rychlost řeči.²⁰

Textové deepfakes jsou tvořeny prostřednictvím zpracování přirozeného jazyka (tzv. NLP) a generativních modelů. Poté, co se shromáždí velké množství textových dat dané osoby (články, blogy, emaily, sociální média), jsou data využívána k tréninku generativního modelu. Shodně, jako u hlasových projevů platí, že každý má specifické rysy ve svém písemném projevu, ať už to je slovní zásoba, obsah nebo syntaxe, které si osvojuje postupně a jakkoli se během života mění, zůstávají relativně trvalé. Nebezpečí těchto deepfakes představuje skutečnost, že takto může být vytvořena nejen

¹⁹ ABBAS, F. a TAEIHAGH, A. *Unmasking deepfakes: A systematic review of deepfake detection and generation techniques using artificial intelligence*. Online. Expert Systems with Applications. 2024, vol. 252 Part B. ISSN 0957-4174. Dostupné z: <https://doi.org/10.1016/j.eswa.2024.124260>. [cit. 2025-10-22].

²⁰ KHANJANI, Z.; WATSON, G. a JANEJA, V. P. *Audio deepfakes: A survey*. Online. Frontiers in Big Data. 2023, roč. 5 - 2022. ISSN 2624-909X. Dostupné z: <https://doi.org/10.3389/fdata.2022.1001063>. [cit. 2025-10-22].

část textu, ale i celé rozsáhlé dokumenty, které cílová osoba nikdy reálně nenapsala.²¹

3. AKTUELNÍ OTÁZKY POSTIHOVÁNÍ DEEPFAKES – HMOTNĚPRÁVNÍ OTÁZKY

Z předchozího textu plyne, že způsobů, kterými může být deepfakes zneužito, je vícero, stejně tak rozdílný může být okruh potenciálních obětí, jakož různorodé mohou být i dopady do jejich osobnostní sféry. Lze si představit tvorbu deepfake za účelem obohacení, poškození dobré pověsti, falšování důkazů, zásahu do inteligentních systémů či ovlivňování veřejného mínění aj.

Príspevek se v následující části zaměřuje na deepfakes zobrazující osoby a to především ty se sexuálním kontextem, a tyto s ohledem na poznatky z policejní praxe pro účely řešení otázek spojených s vyvozováním trestněprávní odpovědnosti člení na základě způsobu provedení a předmětu, proti němuž deepfakes míří, do tří kategorií:

1. deepfakes zobrazující děti
2. deepfakes zobrazující dospělé
3. deepfakes zobrazující známé osobnosti

3.1 DEEFAKE ZOBRAZUJÍCÍ DĚTI²²

Na tomto úseku se nejčastěji v policejní praxi setkáváme se zneužíváním svlékacích aplikací ze strany pubescentů a adolescentů, jež zaznamenaly v posledních letech značný vzestup. D. Zámek upozorňuje, že vývoj těchto aplikací se posunul již natolik, že na první pohled je jen velmi obtížené roz-

²¹ HELMUS, T. C., *Artificial Intelligence, Deepfakes, and Disinformation: A Primer*. Santa Monica, CA: RAND Corporation, 2022. Dostupné z: <https://www.rand.org/pubs/perspectives/PEA1043-1.html>. [cit. 2025-10-23].

²² Obsah kapitoly vychází z aktuálně zpracovávané disertační práce spoluautora Marka Pačmaga s názvem "Vybrané problémy ochrany dětí před sexuálním zneužíváním v kyberprostoru", na Fakultě biomedicínského inženýrství Českého vysokého učení technického v Praze.

lišit, zda-li se jedná o fikci, přičemž výsledné fotomontáže se jeví velmi realisticky.²³

Relativně typické jsou proto situace, kdy jsou za využití aplikace Undress.app nebo Promptchan.ai vytvořeny z fotografií zveřejněných na instagramových účtech – např. spolužačky mladší 18 let - deepfakes, na kterých je tato již vyobrazena s vysvěceným tělem, přičemž tyto fotografie jsou následně zveřejněny ve skupině na sociální síti.

O deepfakes zobrazujících nahé děti se nabízí uvažovat jako o **dětské pornografii**. V rámci této právní kvalifikace však bude nezbytné takovéto deepfakes hodnotit z hlediska znaků příslušné skutkové podstaty, jež je zakotvena v ustanovení § 192 **trestního zákoníku**.²⁴ Nadto trestní zákoník v současné době nepodává legální definici pojmu dětská pornografie. V tomto směru se vychází z judikatury Nejvyššího soudu České republiky, konkrétně Usnesení ze dne 28.12.2004, vydané pod spisovou značkou 7 Tdo 1077/2004, podle kterého lze „za pornografické dílo zobrazující dítě pokládat např. snímky obnažených dětí v polohách **vyzývavě předvádějících pohlavní orgány za účelem sexuálního uspokojení, dále pak snímky dětí zachycující polohy skutečného či předstíraného sexuálního styku s nimi, popř. i jiné obdobně sexuálně dráždivé snímky dětí**“. Byť se jedná o rozhodnutí staršího data, Nejvyšší soud České republiky na něj stále ve svých rozhodnutích přímo odkazuje.

Na základě rozboru předmětné skutkové podstaty ve spojení s citovaným rozhodnutím lze za deepfakes, naplňující znaky dětské pornografie, označit pouze **1. počítačové pornografické dílo, 2. které zobrazuje dítě nebo osobu, jež se jeví být dítětem, 3. vyzývavě předvádějící pohlavní orgány, 4. a to primárně k sexuálním účelům**.

²³ ZÁMEK, D. *Rizika zneužití umělé inteligence ke generování sexuálně explicitního obsahu* In: QUAERE 2023 - Recenzovaný sborník příspěvků interdisciplinární mezinárodní vědecké konference doktorandů a odborných asistentů. Hradec Králové: MAGNANIMITAS, 2023. p. 306 - 313. vol. 13. ISBN 978-80-87952-38-2.

²⁴ Citace plného znění ustanovení: „vyrobí,....nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá dítě nebo osobu, jež se jeví být dítětem.

Srov. např. Usnesení Nejvyššího soudu České republiky ze dne 30.07.2025, spis. značka 3 Tdo 587/2025.

Posouzení otázky, zda určité deepfakes tyto znaky splňuje, je samozřejmě záležitostí právní povahy. Role příslušných orgánů veřejné moci, především pak soudů²⁵, je zde nenahraditelná. AI nedokáže určit, kdy se dílo ještě pohybuje v mezích uměleckého a kdy již sklouzlo do oblasti pornografie.²⁶ Každé deepfake přitom musí být hodnoceno individuálně s ohledem na místo, čas, kontext, v nichž bylo prezentováno.²⁷

Aplikujeme-li výše identifikované pojmové znaky dětské pornografie na v úvodu této části příspěvku předestřený skutkový děj, lze dojít k následujícím závěrům.

²⁵ K otázce místní příslušnosti soudu při Zneužití dítěte k výrobě pornografie srov. Usnesení NS 7 Td 9/2025 ze dne 26.2.2025: „Místem spáchání trestného činu (ve smyslu § 18 odst. 1 tr. ř.) jsou všechna místa, kde došlo ke skutečností (k dějům) naplňujícím některé znaky objektivní stránky skutkové podstaty trestného činu. Takovými místy jsou v případě trestného činu zneužití dítěte k výrobě pornografie podle § 193 odst. 1 tr. zákoníku jak místo, kde pachatel jednal způsobem předpokládaným v ust. § 193 odst. 1 tr. zákoníku, tj. kde přiměl, zjednal, najal, zlákal, svedl nebo zneužil dítě k výrobě pornografického díla nebo kde kořistil z účasti dítěte na takovém pornografickém díle, ale také místo, kde dítě bylo některým z uvedených způsobů přivedeno (pohnuto) k účasti na pornografickém díle, resp. na jeho výrobě, a kde se na něm takto zúčastnilo. V posuzovaném případě tudíž bylo místem spáchání jednak místo, ze kterého obviněný prostřednictvím internetu navazoval s poškozenou kontakt přes sociální síť a požadoval po ní uvedené fotografie, tedy jeho bydliště ve městě XY, okres Bruntál (a případně další místa, která nebyla zjištěna), a jednak místo, kde poškozená pořídila a ze kterého odeslala (opět prostřednictvím internetu) předmětné fotografie obviněnému. Toto místo z obžaloby nevyplývá, ale z obsahu spisu (konkrétně z protokolu o výslechu svědka, č. l. 32 a násl.) je zřejmé, že poškozená posílala fotografie ze svého domova, jenž se nachází ve XY, okres Litoměřice.

²⁶ Zevrubně se touto problematikou věnoval ABELOVSKÝ T. Počítač jako sudce, *Revue pro právo a technologie*, č. 14, roč. 2016, s. 35-36.

²⁷ Existuje samozřejmě množství definic pornografie v encyklopediích, odborné a komentářové literatuře a judikatuře, které vesměs používají neurčité pojmy a žádná z nich si nezískala všeobecné přijetí. Jako příklad lze uvést usnesení Nejvyššího soudu sp. zn. 8 Tdo 1002/2012 „V obecné rovině lze za pornografické dílo považovat takové dílo, které jednak u normálního jedince vyvolává aktualizaci sexuálního pudu, jednak překračuje většinově uznávané morální normy“. V často citovaném rozsudku Nejvyššího soudu USA ve věci Samuel Roth versus United States, 354, U.S. 476 je kladen důraz na to, že pornografický materiál má tendenci mravně kazit čtenáře vyvoláváním lascivních myšlenek či podněcováním chlípné touhy (<https://supreme.justia.com/cases/federal/us/354/476/>); obsáhlý rozbor této problematiky viz Smejkal, V., cit práce, s. 266-315. Poněkud nevázně lze uzavřít, že jako nejvýstižnějším se jeví slova soudce Nejvyššího soudu USA Pottera Stewarta, které pronesl v roce 1964: „Nedokážu definovat pornografii, ale poznám ji, když ji vidím.“

První požadavek v podobě počítačového pornografického díla, zobrazující dítě byl naplněn, neboť za počítačově vytvořené pornografické dílo se považuje i dílo vytvořené prostřednictvím speciálního softwaru.²⁸

Stejně tak druhý požadavek, když „*dítětem se podle ustanovení § 126 trestního zákoníku rozumí osoba mladší osmnácti let, pokud trestní zákon nestanoví jinak*“. V souvislosti s deepfakes zobrazující děti lze uvažovat nicméně i otázky, jak by tomu bylo s trestností v případě, pokud deepfakes zobrazují dítě pouze virtuální (neexistující). K tomu lze uvést, že ke vzniku odpovědnosti zde postačuje, pokud by deepfake zobrazovalo osobu, jež se jeví být dítětem. Jde o konstrukci zdání, resp. zdánlivého věku, který by se i u virtuální osoby určoval na základě jejích vnějších znaků, jako je např. vzhled, oblečení a vystupování, přičemž určení zdánlivého věku by mělo být nesporné.²⁹ Důležitý aspekt tu bude samozřejmě sehrávat i míra přesvědčivosti vytvořených deepfakes z hlediska průměrně informovaného pozorovatele (např. (ne)odpovídající vzezření pohlavních orgánů jako velikost poprsí, délka pohlavního údu či vývoj genitálií u dívek).

Třetí znak dětské pornografie vyžadující vyzývavé předvádění pohlavních orgánů mnohá deepfakes zobrazující děti na základě poznatků z policejní praxe již nenaplnují, a to pro svou nedostatečnou „kvalitu“ (zpravidla neostrost). Příkladem zde může být případ, ve kterém byla využita z internetu stažená fotografie dívky stojící v nevyzývavé pozici před tabulí ve třídě, výsledný deepfake následně vyobrazoval dívku sice nahou, avšak se značně neostrou oblastí genitálií. Příčinu deepfakes nižší kvality lze patrně hledat v nedostupnosti takovýchto fotografií oběti.

U většiny deepfakes zobrazující děti absentuje i požadavek na motiv, neboť podvodná videa a fotografie neslouží primárně k uspokojování sexuálních potřeb, důvodem jejich vzniku je zpravidla nešťastná láska, šikana. Cílem bývá oběť zdiskreditovat, zesměšnit.

²⁸ Srov. ŠÁMAL, P. *Trestní zákoník: komentář*. II, § 140-271. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. ISBN 978-80-7400-893-1. s. 2390.

²⁹ POBOŘILOVÁ, M. Virtuální dětská pornografie, In. *AUCI*, č. 4, roč. 2012, s. 88; BARTOŇ, M. Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. In. *Právní rozhledy*, č. 17/2008, s. 621.

Pokud deepfakes zobrazující nahé děti nenaplní znaky trestného činu dětské pornografie, je na místě uvažovat o alternativní právní kvalifikace v podobě **Poškození cizích práv podle ustanovení § 181 trestního zákonníku**. Tyto trestné činy však na problematiku nekonsenzuální deepfake pornografie nedopadají přímo. Trestného činu se dopustí ten „*Kdo jinému způsobí vážnou újmu na právech tím, že uvede někoho v omyl, nebo využije něčího omylu*“. Na úvod je nezbytné uvést, že subjekt uvedený v omyl a subjekt, jemuž byla způsobena vážná újma na právech, nemusí být a zpravidla nebývá identický.³⁰ Vážná újma na právech bude založena v negativním dopadu do různých oblastí lidského života (rodinný, postavení v zaměstnání, pověsti a dobrého jména, a v neposlední řadě v oblasti sexuálního života).³¹ Šíření (nejen) intimních deepfakes dětské oběti, se kterými se může seznámit blíže neurčený okruh adresátů z řad spolužáků, učitelského sboru nebo v rámci sportovních uskupení, budou znamenat vážné narušení intimity soukromí, zachování cti, lidské důstojnosti a dobré pověsti. Důsledky budou převážně psychologického charakteru s tendencemi k sebevražedným sklonům.³² Znak v podobě uvedení v omyl je jednání, kterým pachatel předstírá okolnosti, které nejsou v souladu se skutečným stavem věci.³³ V případech intimních deepfake materiálů budou konzumenti uvedeni v omyl tím, že se domnívají, že pozorují skutečné tělo vyobrazeného dítěte, což je v rozporu se skutečným stavem.³⁴

Na tomto místě je s ohledem na dobu vzniku tohoto textu nezbytné upozornit i na legislativní změnu spočívající v zavedení nové skutkové podstaty trestného činu s názvem „**Zneužití identity k výrobě pornografie a její**

³⁰ Usnesení Nejvyššího soudu České republiky ze dne 22. 7. 2014, sp. zn. 4 Tdo 815/2014

³¹ ŠÁMAL, P. *Trestní zákoník: komentář. II*, § 140-271. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. s. 2278.

³² BARKER, C; FORD, S.; EGLINTON, R.; QUAIL, S. a TAGGART, D. *The truth project paper one —how did victims and survivors experience participation? Addressing epistemic relational inequality in the field of child sexual abuse*. Online. *Frontiers in Psychiatry*. 2023, vol. 2023, no. 14, s. 12. ISSN 1664-0640. Dostupné z: <https://doi.org/10.3389/fpsyt.2023.1128451>. [cit. 2025-10-01].

³³ ŠÁMAL, P. *Trestní zákoník: komentář. II*, § 140-271. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. ISBN 978-80-7400-893-1. s. 2279.

³⁴ Usnesení Nejvyššího soudu ze dne 22. 7. 2014, sp. zn. 4 Tdo 815/2014

šíření“, která nově dopadne právě na deepfakes, která jsou v současné době z výše rozebraných důvodů právně kvalifikované jako poškození cizích práv. Tato nová skutková podstata bude včleněna do Hlavy III trestního zákoníku (trestné činy proti lidské důstojnosti v sexuální oblasti) pod nové ustanovení § 191a s účinností ode dne 1. 1. 2026.³⁵ Nový trestný čin je konstruován obdobně jako stávající skutková podstata trestného činu šíření pornografie podle § 191 trestního zákoníku ve znění „*Kdo vyrobí, doveze, vyveze, proveze, nabídne, učiní veřejně přístupným, zprostředkuje, uvede do oběhu, prodá nebo jinak jinému opatří fotografické, filmové, počítačové, elektronické nebo jiné pornografické dílo, které zobrazuje nebo jinak využívá osobu, o které ví, že k takovému zobrazení nebo využití nedala souhlas*“. Návrh generálně nebrojí proti samotné tvorbě deepfakes. Vychází ze zachování respektu k ústavně zaručenému právu na svobodu projevu, včetně například satiry, kde může mít i deepfake své místo, a to s přísným dodržáním všech ústavních či zákonných podmínek.³⁶ Deepfakes tyto limity již ze své podstaty dalece překračují. I s ohledem na hmotněprávní korektiv v podobě subsidiarity trestní represe bude třeba použít prostředky nejzávažnější, tedy prostředky trestního práva.³⁷ Shodně i Akční plán prevence domácího a genderově podmíněného násilí na období roků 2023 až 2026, který byl dne 23. srpna 2023 schválen vládou České republiky, podporuje potřebu efektivně bojovat proti deepfakes pornografií přijetím přílehlající právní úpravy, respektive nového trestného činu dopadajícího na tuto oblast.³⁸

³⁵ ČESKÁ TELEVIZE. *Prezident podepsal novelu trestního zákoníku*. Online. 2025. Dostupné z: <https://ct24.ceskatelevize.cz/clanek/domaci/prezident-podepsal-novelu-trestniho-zakoniku-363072>. [cit. 2025-10-23].

³⁶ BROZ, J. Karikatura v judikatuře Ústavního soudu: ochrana důstojnosti versus svoboda projevu. [online]. *Časopis pro právní vědu a praxi*, 2018, roč. 26, č. 3. Dostupné z: <https://doi.org/10.5817/CPVP2018-3-6> [cit. 2025-10-10]

³⁷ JELÍNEK, J. *Trestní právo hmotné: obecná část, zvláštní část*. 9. aktualizované vydání. Student. Praha: Leges, 2025. ISBN 978-80-7502-799-3. s. 136-137.

³⁸ ÚŘAD VLÁDY ČESKÉ REPUBLIKY. *Akční plán prevence domácího a genderově podmíněného násilí na léta 2023–2026*. Online. 2023. Dostupné z: https://vlada.gov.cz/assets/ppov/rovne-prilezitosti-zen-a-muzu/dokumenty/AP_DGPN-2023_final.pdf. [cit. 2025-10-25].

3.2 DEEPFAKES ZOBRAZUJÍCÍ DOSPĚLÉ OSOBY

Tvorba sexuálně motivovaných deepfakes zobrazujících dospělé osoby v některých aspektech vychází z předchozí části. **Primárně trestněprávní ochranu dospělých osob před deepfakes poskytuje ustanovení § 181 trestního zákoníku.**

Jako typický příklad z této kategorie, lze uvést situaci, kdy pachatel vytvoří na erotické seznamce uživatelský účet s vloženými sexuálně explicitními deepfake materiály zobrazující jeho bývalou partnerku, toho času pracovníci významné nadnárodní korporace, včetně uvedení kontaktních údajů v rozsahu e-mailové adresy a účastnického telefonního čísla, na základě kterého pak budou zájemci obtěžovat oběť nabídkami o schůzky či sexuální aktivity v podobě telefonátů, e-mailů a SMS zpráv.

Společenskou škodlivost takového jednání, a to i ve vztahu k dospělé osobě, lze hodnotit nepochybně jako vysokou. V rámci obhajoby pachatelů je mnohdy navrhováno využití jiných odvětví práva, než práva trestního. V této otázce je soudní rozhodování v zásadě rigidní. Soudy opakovaně deklarují zásah do osobnostních práv obětí v těchto případech natolik závažným, že subsidiaritu trestní represe nelze aplikovat.³⁹ V kontextu uvedeného však Ústavní soud připomíná, že *„kvalifikaci určitého jednání, které má soukromoprávní základ, jako trestného činu je třeba považovat za ultima ratio, ...je však nepřijatelné, aby tuto ochranu aktivně přebíraly orgány činné v trestním řízení, jejichž úkolem je ochrana převážně celospolečenských hodnot, nikoliv přímo konkrétních subjektivních práv jednotlivce, jež svou povahou spočívají v soukromoprávní sféře“*.⁴⁰

Shodně, jako tomu je deepfakes zobracující děti, bude i zde rozhodným kritériem posuzování trestnosti „kvalita“ vytvořených deepfakes.

U případů, v nichž nedojde k způsobení požadované újmy vlivem naznačeného atributu, bude v praxi možné uvažovat o odpovědnosti za přestupky. Podle obsahu (charakteru) deepfakes se bude jednat nejčastěji o přestupky proti občanskému soužití či proti majetku, přestupky na úseku

³⁹ Usnesení Nejvyššího soudu ze dne 22. 7. 2014, sp. zn. 4 Tdo 815/2014

⁴⁰ Nález Ústavního soudu ze dne 28. 4. 2010, sp. zn. I. ÚS 541/10

zákona o ochraně osobních údajů (zejména použití podobizny bez souhlasu). Na úrovni občanského práva se uvedené dotýká zejména § 81, § 82 občanského zákoníku (popř. § 2956 občanského zákoníku z hlediska povinnosti odčinění újmy při zásahu do přirozeného práva konkrétní osoby).

3.3 DEEPFAKES ZOBRAZUJÍCÍ VEŘEJNĚ ZNÁMÉ OSOBNOSTI

Specifickou množinu představují deepfakes zobrazující veřejně známé osobnosti (tzv. public figures) jako jsou např. politici, herci, zpěváci či sportovci. Specifikum zde vyplývá z jejich společenského statusu, s nímž se pojí povinnost strpět větší míru veřejné kritiky, včetně ironizace, tolerovat, že každé jejich slovo může být podrobeno veřejné kritice ze strany masových médií a široké veřejnosti než jiní občané a to tím spíše, že tak činí dobrovolně.⁴¹

Z toho ovšem neplyne, že by veřejně známé osobnosti museli snášet jakoukoli kritiku, zejména, je-li jejím cílem pouhé zneuctění osoby či uražení. To uznal i Evropský soud pro lidská práva, když těmto osobám přiznal právo na ochranu osobnosti a právo na soukromí před nepravdivými a dehonestujícími útoky, navíc tam, kde se kritika netýkala jejich veřejné činnosti. Ústavní soud k tomu dodává, že nelze takovým projevům poskytnout legitimitu poukazem na ústavní ochranu svobodou projevu, jestliže byly motivovány především touhou poškodit difamovanou osobu, jehož autoři se nepostarali o prověření, je-li obsah pravdivý.⁴²

Motivů pro tvorbu deepfakes zobrazující známé osobnosti lze nalézt celou řadu. K nejčastějším patří finanční obohacení, diskreditace oběti⁴³ a uspokojení sexuální potřeby. Materiály pro finanční obohacení útočníků jsou využívány v rámci sociálního inženýrství.⁴⁴

⁴¹ Nález Ústavního soudu ze dne 26.06.2024, sp. zn. I. ÚS 2946/23 #1

⁴² Např. Nález Ústavního soudu sp. zn. I. ÚS 367/03, nález Ústavního soudu sp. zn. I. ÚS 1586/09; Oberschlik verus Rakousko, stížnost. č. 20834/92; MATES, P. (ed.) a kolektiv: *Ochrana osobnosti, soukromí a osobních údajů*. Praha: Leges: 2019, s. 15 a následující; SIMON G. *Persönlichkeitsschutz Gegen Herabsetzende Karikaturen in Deutschland Und Frankreich*: Frankfurt an Main, Peter Lang AG, 1994; např. rozsudek Evropského soudu pro lidská práva ve věci Tammer versus Estonsko, stížnost č. 41205 a ve věci Lešník versus Slovensko, stížnost č. 35640/97.

Jak již bylo uvedeno v úvodu tohoto příspěvku, historicky první případy výskytu deepfakes celebrit se objevily v souvislosti s pornografií. Jeden z nejznámějších internetových portálů - MrDeepFakes⁴⁵ - je využíván k shromažďování právě tohoto typu materiálů. Odtud ostatně pochází samotné označení deepfakes. Celkově lze vyhledat na obdobných internetových portálech přes čtyři tisíce materiálů se známými osobnostmi.⁴⁶

V posledních let prudce vzrostl počet politicky motivovaných deepfakes, které jsou využívány především v rámci dezinformačních kampaní před volbami. Tyto případy byly registrovány i v rámci České republiky již v souvislosti s volbami prezidenta republiky v roce 2023, kdy byla šířena zpráva o náhlém úmrtí Petra Pavla, a později volbami do Evropského parlamentu.⁴⁷ Vysoké oblibě se rovněž těší již zmíněná deepfakes lákající k investičním příležitostem. Dalším příkladem jsou deepfakes, jejímž cílem je zdiskreditovat stát a jeho politiku v očích veřejnosti, jejichž tvůrci jsou v současnosti často ruští nebo prokremelští hackeři, kteří se snaží vyvolat antipatie vůči zemím, podporujícím Ukrajinu ve válce proti Rusku. Jako příklad lze uvést video ukrajinského prezidenta Volodymyra Zelenského vy-

⁴³ ČESKÁ TELEVIZE. *Nejen Taylor Swiftová. Deepfake pornografie s celebritami je stále větší problém.* Online. 2024, aktualizace 25.3.2024. Dostupné z: <https://ct24.ceskatelevize.cz/clanek/kultura/nejen-taylor-swiftova-deepfake-pornografie-s-celebritami-je-stale-vetsi-problem-347491>. [cit. 2025-10-21]; lze se setkat i s různými kombinacemi, např. při tzv. sextorzi, hrozí úročník, že zveřejní jím údajně získané informace o tom, že dotyčný sleduje pornografii a tím ho bude difamovat a žádá výkupné za to, že tak neučiní.

⁴⁴ Sociální inženýrství znamená „v obecném smyslu způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace“ srov. KOLOUCH, J. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. s. 186.

⁴⁵ NPR NETWORK. *Major deepfake porn site shuts down.* Online. 2025, aktualizace 6.5.2025. Dostupné z: <https://www.npr.org/2025/05/06/nx-s1-5388422/mr-deepfakes-porn-site-ai-shut-down>. [cit. 2025-10-25].; známým se stal zejména malwer, vytvořený ve Spojených státech amerických, zveřejněný do světa v roce 2011, nabízející vytvoření kompromitujících nahých fotografií známých osobností

⁴⁶ THE GUARDIAN. *Nearly 4,000 celebrities found to be victims of deepfake pornography.* Online. 2024. Dostupné z: <https://www.theguardian.com/technology/2024/mar/21/celebrities-victims-of-deepfake-pornography>. [cit. 2025-10-25].

⁴⁷ CNN PRIMA NEWS. *Nevěřte všemu, co vidíte. Do evropských voleb promluví i „naklonovaní“ politici, varují experti.* Online. 2024, aktualizace 29.5.2024. Dostupné z: <https://cnn.iprima.cz/deepfake-evropske-volby-dezinformace-videa-check-point-438230>. [cit. 2025-10-26].

zývajícího národ ke složení zbraní s cílem podkopat vůli pomáhat Ukrajincům v boji s agresorem, které lze označit přímo jako nástroj hybridní války.

Otázka ochrany veřejně známých osob proti deepfakes je složitější, než u dětí či jiných dospělých osob. Otázkou tu je to, jak intenzivně jsou případné deepfakes, způsobilé zasáhnout do jejich vztahů s rodinnými příslušníky a dalšími příbuznými i přáteli a negativně tak ovlivnit jejich společenské, pracovní a osobní postavení.⁴⁸ V rámci tvorby deepfakes se totiž tyto osoby přímo nekritizují, nýbrž dostávají se do pozic, že jsou jejich jménem šířeny mnohdy lživé informace a podobně.

Pro vyvození postihu podle trestního práva, popřípadě správního práva, je tak klíčové obsahové zaměření deepfakes. Tak např. deepfakes nabízejí výhodné investice lze právně kvalifikovat jako podezření ze spáchání **podvodu podle ustanovení § 209 trestního zákoníku** nebo jeho pokusu. Skutková podstata uvedeného přečinu neklade žádné požadavky na „kvalitu“ podvodného sdělení. Významným aspektem pro posouzení však bude výše způsobené škody (musí dosahovat nejméně 10.000,- Kč, u nižší se bude jednat o přešůpek proti majetku), neboť prostředí Internetu umožňuje oslovit blíže neurčený okruh adresátů.⁴⁹ Veřejně známá osoba může být dále zneužita k **šíření poplašné zprávy**, kdy například „*prezident republiky Petr Pavel na deepfake nahrávce dostupné na Internetu sděluje, že Česká republika bude napadena ze strany Ruské federace odpálením raket hromadného ničení na dosud blíže neučených místech v České republice*“. Sdělení z úst prezidenta republiky je způsobilé zapříčinit vážné znepokojení alespoň u části obyvatelstva šířením poplašné zprávy na nepravdivém základu. Poplašnou zprávou je třeba rozumět „*objektivně nepravdivou zprávu, která je způsobilá vyvolat obavy z nějakých, byť i neurčitých budoucích událostí, zasahujících nepříznivě do života alespoň části obyvatelstva nějakého místa*“.⁵⁰ Pachatel bude ohrožen trestní sazbou podle § 357 TrZ až na dvě léta.

⁴⁸ Viz k tomu KASL, F. *Porušení bezpečnosti osobních údajů v kontextu Internetu věcí*. Brno: Masarykova univerzita, 2021, s. 43.

⁴⁹ SMEJKAL, V. *Kybernetická kriminalita*. 3. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. ISBN 978-80-7380-849-5. s. 219.

⁵⁰ Usnesení Nejvyššího soudu ze dne 18.01.2017, spis. zn. 3 Tdo 40/2017

Nelze vyloučit ani to, že deepfakes by mohla představovat i incident podle § 5 zákona o kybernetické bezpečnosti (zák. č. 264/2025 Sb.), protože může představovat hrozbu pro bezpečnost České republiky. Jako příklad lze uvést vystoupení guvernéra České národní banky, který oznamuje zhroucení naší měny, které může vyvolat u nemalé části obyvatel paniku, vést k runu na banky, kolapsu internetového bankovníctví a dalším negativním důsledkům. Dalším příkladem může být takto vytvořené vystoupení politika v televizním vysílání, v němž prezentuje údajný volební program svojí strany s cílem ovlivnit výsledky voleb, čímž jsou podkopávána ústavnost státu a demokracie.⁵¹

4. AKTUÁLNÍ OTÁZKY POSTIHOVÁNÍ DEEPPFAKES – SPECIFIKA ODHALOVÁNÍ, PROVĚŘOVÁNÍ A DOKAZOVÁNÍ

Výchozím ústavněprávním principem při výkonu trestní pravomoci je princip zákonnosti. V oblasti hmotného práva tento princip naplňuje zásada *nullum crimen sine lege, nulla poena sine lege* - žádný trestný čin bez zákona a žádný trest bez zákona.⁵² Procesním protějškem pak je zásada řádného zákonného procesu (*nullus processus criminalis sine lege*) - proti nikomu nesmí být vedeno řízení jinak, než ze zákonných důvodů a pouze způsobem, který stanoví zákon.⁵³

Trest za trestný čin či přestupek tak lze uložit toliko osobě, která je jeho pachatelem, bylo jí spáchání činu v trestním či přestupkovém řízení náležitě prokázáno⁵⁴, a neuplynula lhůta stanovená zákonem pro jeho uložení.

Hlavní těžiště těchto řízení proto představuje dokazování, neboť má zásadní význam pro řádné zjištění skutkového stavu věci, které je **základním předpokladem objektivního rozhodnutí**.

⁵¹ Mastroianni Fake news, frees speech and democracy: a (bad) lesson from Italy? Southwestern Journal of International Law, No.2/2019 s. 67-68

⁵² JELÍNEK, J. *Trestní právo hmotné: obecná část, zvláštní část*. 9. aktualizované vydání. Student. Praha: Leges, 2025. ISBN 978-80-7502-799-3. s. 35-36.

⁵³ FENYK, J.; CÍSAŘOVÁ, D. a GRIVNA, T. *Trestní právo procesní*. 8. vydání. Praha: Wolters Kluwer, 2024. ISBN 978-80-7676-898-7. s. 70. nebo srov. PRÁŠKOVÁ, H. *Správní trestání*. In HENDRYCH, D. a kol. *Správní právo*. Obecná část. 9. vyd. C. H. Beck, Praha, 2016, s. 297.

Dokazování lze charakterizovat jako souhrn (sled) „*dílčích procesních úkonů prováděných z úřední povinnosti s cílem zajistit, aby rozhodnutí odpovídalo okolnostem daného případu a bylo v souladu se zákony a ostatními právními předpisy*“.⁵⁵ Podstatou přitom je aplikace příslušných právních norem na konkrétní skutkovou situaci, což nemusí být mnohdy jednoduché, a proto tento proces často vyžaduje odborné znalosti a nadhled z hlediska skutkových a právních úvah souvisejících se správností a spravedlivostí z tohoto procesu vzešlého rozhodnutí. Formálně jde vždy o zákonem upravený postup příslušného orgánu veřejné moci (v našich podmínkách orgánu činného v trestním řízení, případně správního orgánu), kterým se získávají poznatky o rozhodných skutečnostech.

Při vyvozování trestněprávní či správněprávní odpovědnosti za deepfakes bude proto nezbytné soustředit se na prokázání/zodpovězení zejména následujících skutečností/otázek:

1. Existence zásahu/protiprávnost

- Zjištění o existenci uměle vytvořené či upravené fotografie, videu či jiného materiálu vyobrazující osobu v nahotě či sexuálním kontextu, popřípadě jinak zneužívající určitou osobu (např. k podvodnému jednání). Deepfakes budou vždy představovat nezákonný obsah, pokud obsahují dětskou pornografii, obsah podporující terorismus, nebo zasahují do autorskoprávní ochrany či osobnostních práv. Na tomto místě je však třeba zdůraznit, že vytvoření deepfake, resp. jeho existence sama o sobě ještě nezakládá právní odpovědnost (s výjimkou výroby pornografie), naplnění příslušných skutkových podstat je třeba spojovat až s jeho užitím/šířením.

⁵⁴ Povinnost prokázat vinu obviněného nade vší pochybnost plyne ze základního procesního principu presumpce nevin, přičemž konstatování v podobě „*největší pravděpodobnosti*“ nemůže obstát jako výsledný důkazní standard pro prokázání viny, jelikož na základě zákona, judikatury i trestněprávní doktríny je za takový standard stabilně považována praktická jistota, neboli jistota bez důvodných pochybností srov. Nález Ústavního soudu ze dne 1. dubna 2015, pod spis, značkou I. ÚS 2726/14.

⁵⁵ Srov. Rozhodnutí Krajského soudu v Hradci Králové ze dne 15. 2. 2007, sp. zn. 51 Ca 9/2006-27, popřípadě KALVODOVÁ, V. a HRUŠÁKOVÁ, M. *Dokazování v trestním řízení - právní, kriminologické a kriminalistické aspekty*. Spisy Právnické fakulty Masarykovy univerzity v Brně. Řada teoretická, Edice Scientia. Brno: Masarykova univerzita, 2015. ISBN 978-80-210-8072-0. s. 29.

Ostatně je třeba připustit, že deepfake může vytvořit i automat (včetně námětu).

2. Identifikovatelnost osoby

- Na základě obsahu lze poznat/určit o jakou konkrétní osobu se jedná (např. podle obličeje, speciálních morfologických znaků⁵⁶, hlasu či jiných markantů).

3. Zveřejnění

- Záznam je bez souhlasu dotčené osoby zpřístupněn třetím osobám (např. umístěním na sociální síti, erotických seznamkách či jiných obdobně zaměřených platformách) nebo jinak šířen (na temné vrstvě Internetu s názvem DarkWeb, přičemž i šíření sexuálně explicitních materiálů v rámci této vrstvy bylo předmětem rozhodování o náhradě nemajetkové újmy poškozených ze strany Ústavního soudu České republiky⁵⁷).

4. Následek (poškození práv)

- Posuzování následku, jakožto obligatorního znaku objektivní stránky trestného činu/přestupku, je propojeno s již uvedeným zveřejněním, deepfakes, které nebudou zveřejněny (pachatel je bude mít uloženy pouze ve svém počítači či mobilním přístroji) bude podstatně snižovat následek, pokud však dojde k masivnímu šíření sociálními médii, tak se následek bude exponencionálně zvyšovat (jak již bylo uvedeno u trestného činu poškození cizích práv musí být naplněn znak „způsobení vážné újmy), u způsobeného následku je významné posuzovat také to, do jakého práva na ochranu osobnosti je zasahováno (čest, pověst, důstojnost, soukromí)⁵⁸, zá-

⁵⁶ Morfologické znaky lze charakterizovat jako kvalitativní a individuální znaky, u nichž je pravděpodobnost jejich výskytu u dvou nebo více jedinců v populaci velmi nízká (jizvy, vrásky, tetování) srov. STRAUS, J. *Kriminalistická technika*. 3., rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN 978-80-7380-409-1. s. 63.

⁵⁷ Ústavní soud v nedávné době rozhodoval o požadavku stěžovatelky na náhradu nemajetkové újmy, neboť její nevlastní otec stěžovatelku během sexuálních praktik fotil a natáčel, tyto snímky pak nahrával do sítě tzv. temného webu (dark web či darknet) k tomu srov. Nález Ústavního soudu ze dne 30. července 2025, pod spis. značkou IV. ÚS 1323/25.

⁵⁸ ŠÁMAL, P. *Trestní zákoník: komentář*. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023. ISBN 978-80-7400-893-1. s. 2277-2279.

vážnost emocionální újmy, popř. materiální škody, vzniklá škoda přitom nemusí být nutně vyčíslena, zcela postačí, že nastal zásah.

5. Zavinění ve formě úmyslu

- Pachatel bude jednat úmyslně, tj. věděl, že zveřejňuje deepfake, dále věděl, že nemá souhlas vyobrazené osoby pro takové zveřejnění, a chtěl tím způsobit újmu, nebo byl alespoň srozuměn s tím, že tím poškodí čest, vážnost nebo soukromí jiné osoby. Uvedený souhlas ze strany vyobrazené osoby, tedy potenciální poškozené, je stěžejní z důvodu posuzování trestněprávní či správněprávní odpovědnosti, neboť trestný čin/ přestupek nespáchá „kdo jedná na základě svolení osoby, jejíž zájmy, o nichž tato osoba může bez omezení oprávněně rozhodovat, jsou činem dotčeny“ podle § 30 trestního zákoníku nebo „jestliže někdo jedná na základě svolení osoby, jejíž zájmy, o nichž tato osoba může bez omezení oprávněně rozhodovat, jsou činem dotčeny“ podle § 26 zákona o odpovědnosti za přestupky a řízení o nich.

Materiály, u kterých vyvstane podezření, že byly vytvořeny nebo modifikovány za pomoci nástrojů umělé inteligence, se dostávají do dispozice příslušných orgánů několika způsoby.

Nejčastějším způsobem je oznámení, učiněné přímo dotčenou osobou, případně jinou osobou z řad široké veřejnosti, která v prostředí Internetu zjistila výskyt deepfakes.

Druhá kategorie případných oznamovatelů zahrnuje poskytovatele internetových služeb. Platformy jakými jsou tzv. VLOPs – Very Large Online Platforms⁵⁹ mají na základě Nařízení o digitálních službách (ve zkratce DSA) povinnost přijímat opatření k šíření nezákonného obsahu, pod nějž lze deepfakes nesporně subsumovat. Do této kategorie lze zařadit i poskytovatele služeb, kteří zjistí výskyt deepfakes ve svých službách v rámci dobrovolné moderace obsahu na své síti.⁶⁰ V této souvislosti lze zmínit například snahy populární platformy Youtube, která „od 21. října 2025 zpří-

⁵⁹ Jedná se o platformy, které jsou užívány ze strany více než 45 milionů aktivních uživatelů v Evropské unii, srov. EU DIGITAL SERVICE ACT. *Digital Services Act (DSA)| Updates, Compliance*. Online. 2025. Dostupné z: <https://www.eu-digital-services-act.com/>. [cit. 2025-10-26].

stupňuje vybraným tvůrcům v Partner Program nový AI nástroj nazvaný *Likeness Detection*, který automaticky vyhledává videa obsahující neoprávněně vytvořené deepfake záběry s jejich tvářemi. Tvůrci mohou podezřelá videa po ověření identity přímo nahlásit k odstranění prostřednictvím YouTube Studio⁶¹.

Poslední skupinu představují poznatky z vlastní operativní činnosti, a to ze strany vybraných bezpečnostních sborů či zpravodajských služeb.⁶² Příkladem je proaktivní činnost⁶³ Policie České republiky v prostředí Internetu a vyhledávání informací z veřejně přístupných zdrojů (tzv. OSINT).⁶⁴

V rámci prošetřování/prověřování došlých oznámení a poznatků z vlastní činnosti jsou příslušné orgány povinny provést veškerá potřebná šetření s cílem zjistit veškeré údaje směřující k identifikaci poskytovatele služby, v rámci které byl závadový obsah „vyvěšen“. Poskytovatel služeb je povinen na podkladě žádosti policejních orgánů poskytnout tzv. registrační a lokalizační údaje (údaje poskytnuté uživatelem – bývají ve většině případů smyšlené), který si službu zřídil, včetně platebních údajů v případech zpoplatněných služeb a přístupových logů ke službě. Shodně, jako u kybernetické kriminality v obecném pojetí, lze očekávat, že pachatelé zpravidla disponují potřebnými vědomostmi a znalostmi, jak v prostředí Internetu efek-

⁶⁰ KOLOUCH, J. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7. s. 109 a následující.

⁶¹ MARIGOLD.CZ. *YouTube spouští AI nástroj pro detekci deepfake videí tvůrců obsahu*. Online. 2025, aktualizace 21.10.2025. Dostupné z: <https://www.marigold.cz/tech-news/youtubes-ai-likeness-detection-tool-is-searching-f/>. [cit. 2025-10-28].

⁶² Vyplývá z ustanovení § 158 odst. 1 trestního řádu s odkazem na § 12 odst. 2 trestního řádu.

⁶³ Požadavek na zintenzivnění vlastní činnosti Policie České republiky k vyhledávání trestné činnosti v kyberprstoru byl ze vznesen na 16. schůzi Senátu Parlamentu České republiky ze strany JUDr. Lenky Bradáčové, PhD., viz z SENÁT PARLAMENTU ČESKÉ REPUBLIKY. Stenozáznam z 1. dne 16. schůze. Online. 2025. Dostupné z: <https://www.senat.cz/xqw/xervlet/pssenat/hlasovani?action=steno&O=15&IS=7769&D=16.10.2025>. [cit. 2025-10-26].

⁶⁴ Zkratka OSINT znamená v anglickém jazyce „Open Source Intelligence“, neboli vyhledávání informací ve veřejných zdrojích blíže srov. RÁLIŠ, P. *Zpravodajský odposlech jako důkaz v trestním řízení*. Online. Trestněprávní revue. 2024, roč. 23, č. 4, s. 224-232. ISSN 1213-5313. [cit. 2025-10-21].

tivně zakrýt stopy vedoucí ke zjištění jejich totožnosti, například používáním speciálního vyhledávače s názvem TOR či VPN.⁶⁵

Další šetření bude závislé na sofistikovanosti konkrétního pachatele či skupiny pachatelů. K zjištění navazujících informací k bankovním účtům poskytuje ustanovení § 8 odst. 2 trestního řádu legitimní titul. Ve vztahu k zjištěným logům⁶⁶ či účastnickým telefonním číslům lze také dále vyžadovat potřebné informace.⁶⁷ Je však nezbytné při vyžadování reflektovat data retention lhůtu v České republice, která činí šest měsíců.⁶⁸

Bude-li třeba vyžádat od poskytovatelů služeb původní (originální, nezměněné) materiály za účelem jejich následného srovnání s deepfakes, bude nezbytné zajistit tzv. obsahová data. Pro další procesní postup bude významné, který poskytovatel předmětnými daty disponuje. U poskytovatelů služeb z České republiky lze obsahová data vyžádat za využití ustanovení § 158d odst. 3 trestního řádu. U zahraničních poskytovatelů pak lze využít evropský vyšetřovací příkaz nebo formou právní pomoci ve smyslu zákona o mezinárodní justiční spolupráci v trestních věcech.⁶⁹

U přestupků spáchaných na Internetu jsou zákonné možnosti vyžadování pomoci od fyzických a právnických osob či jiných orgánů nepochybně užší, než je tomu u trestných činů. Při tzv. předšetření přestupků nelze například nařídit uchování nebo znepřístupnění dat jiným osobám (§ 7b TŘ), odposlouchávat budoucí či probíhající zájmové komunikace (§ 88 TŘ), vyžadovat údaje o telekomunikačním provozu (§ 88a TŘ), sledovat obsah e-mailových schránek a cloudových úložišť (§ 158d TŘ). Vzhledem ke skutečnosti, že ve většině případů půjde o přestupky proti občanskému soužití

⁶⁵ Bližší informace k těmto nástrojům na internetových stránkách <https://www.torproject.org/> nebo <https://www.eset.com/cz/vpn/>.

⁶⁶ Ustanovení § 88a odst. 1 trestního řádu, k tomu blíže ŠÁMAL, P. *Trestní řád: komentář*. 7., dopl. a přeprac. vyd. Velké komentáře. V Praze: C.H. Beck, 2013. ISBN 978-80-7400-465-0. s. 1223 a následující.

⁶⁷ Ustanovení § 66 odst. 2 zákona o Policii České republiky, k tomu blíže VANGELI, B. *Zákon o Policii České republiky: komentář*. 2. vyd. Beckovy komentáře. V Praze: C.H. Beck, 2014. ISBN 978-80-7400-543-5. s. 279-280.

⁶⁸ Plenární nález Ústavního soudu ze dne 22.03.2011, pod spis. značkou Pl. ÚS 24/10 #1.

⁶⁹ NOVOTNÁ, J. *Právní pomoc v cizím státu v přípravném řízení trestním*. 3. vydání. Právní praxe. V Praze: C.H. Beck, 2015. ISBN 978-80-7400-568-8. s. 23 – 28.

či majetku, tj. přestupky, u nichž má orgán policie dle § 74 zákona o odpovědnosti za přestupky povinnost konat nezbytná šetření, se právním základem stává zákon o policii. Zejména lze poukázat na ustanovení § 18 ve spojení s ustanovením § 114 citovaného zákona. Tím je zajištěna explicitní povinnost dotčených subjektů, aby na oprávněné žádosti orgánů policie o poskytnutí potřebných informací (registračních údajů) řádně a včas reagovaly.⁷⁰

Výzvou při samotném dokazování deepfakes bude posouzení jejich technologického a efektního aspektu.

V prvním případě otázka zní, zda jde o nový materiál generovaný pomocí nástrojů umělé inteligence. V tomto směru lze využít například stylometrickou analýzu, analýzu pixelů a zvukových vln či již předtřénované modely strojového učení. Pro identifikaci manipulovaných médií se využívají pokročilé metody digitální forenzní analýzy např. analýza vizuálních artefaktů, která detekuje nesrovnalosti, jako jsou např. nepravidelnosti v texturách pleti, chyby ve stínech nebo nepřirozené pohyby obličejových rysů, biometrická analýza, která monitoruje fyziologické znaky, jako je frekvence mrkání nebo synchronizace pohybu rtů s audio stopou, další metodou je „*error level analysis*“, která analyzuje úroveň komprese a odhaluje rozdíly v úpravě různých částí obrazu. V neposlední řadě lze podrobit deepfake srovnávat i s původním (originálním) materiálem, což přichází v úvahu např. získá-li jej příslušný orgán od dotčené osoby.

Uspokojivé zodpovězení této podstatné otázky pro rozhodnutí je však z právního pohledu prozatím značně problematické, neboť doposud neexistuje spolehlivý a univerzálně uznávaný detektor s funkcionalitou posouzení materiálů tzv. „nadevší pochybnost.“ V současnosti se prozatím nacházíme ve fázi vytváření a případně testování takovýchto nástrojů. Příkladem je projekt NABOSO, zabývající se mimo jiné tvorbou nástrojů umožňujících efektivní boj proti škodlivému použití hlasových deepfakes s dobou trvání do 31.12.2026.⁷¹ Dalším je projekt DETEKTOR, který se bude primárně za-

⁷⁰ Podrobněji FIALA, Z. a M. PAČMAG. *ICT a nové trendy v procesu dokazování v řízení o přestupku*. FORENZNÍ VĚDY, PRÁVO, KRIMINALISTIKA, roč. 2020, č. 2, str. 195 -209.

bývat vývojem specializovaných nástrojů pro detekci manipulace s médii – deepfakes. Projekt byl zahájen dne 1. listopadu 2025 s dobou trvání 3 let.⁷²

Aktuálně dostupné nástroje jsou schopné identifikovat deepfakes s procentuálním vyjádřením přibližně mezi 60 až 80 procenty. Studie s názvem „*Comprehensive Evaluation of Deepfake Detection Models: Accuracy, Generalization, and Resilience to Adversarial Attacks*“ z roku 2025 uvádí výsledky pro některé metriky přes 88 %. Jedná se však zatím o výzkumné údaje pro různé modely.⁷³ V kontextu s již zmíněnou povinností příslušných orgánů prokázat vinu tzv. „nadevší pochybnost“, se jeví takové procentuální vyjádření jako nedostatečné pro rozhodnutí o vině, pokud nebudou k dispozici další relevantní skutečnosti (například doznání pachatele).⁷⁴ Nadto lze očekávat, že dotčená osoba, dokud nebude tato problematika dostatečně judikována, bude využívat všechny dostupné opravné prostředky.⁷⁵

Z naznačených důvodů se proto praxe prozatím neubírá cestou znaleckých posudků (např. Odbor kriminalistické techniky a expertízy Policie České republiky, potažmo Kriminalistický ústav, nebo externí znalce). Perspektivou s ohledem na zásadu hospodárnosti⁷⁶ řízení se jeví účelnější

⁷¹ PHONEXIA. *Nástroje boje proti hlasovým deepfakes (NABOSO)*. Online. c2025. Dostupné z: <https://www.phonexia.com/cz-projects-grants/>. [cit. 2025-10-28].

⁷² EUROPEAN COMMISSION: CORDIS - EU RESEARCH RESULTS. *Deepfake Evidence and Technology for Forensic Content Oversight and Research*. Online. c2025. Dostupné z: <https://cordis.europa.eu/project/id/101225942>. [cit. 2025-10-28].

⁷³ MONTEIRO, S.; WANZELLER, C. a CALDEIRA, F. *Performance Analysis on Deep Fake Detection*. Online. Communications of the IBIMA. 2024. ISSN 1943-7765. Dostupné z: <https://doi.org/10.5171/2024.457767>. [cit. 2025-10-26].

⁷⁴ Při nedostatku přímých důkazů aplikační praxe vyžaduje větší množství nepřímých důkazů tak, aby tvořily uzavřený „řetěz“, tj. bez mezer, jenž sám o sobě nežaduje přímého důkazu blíže srov. FENYK, J.; CÍSAŘOVÁ, D. a GRIVNA, T.. *Trestní právo procesní*. 8. vydání. Praha: Wolters Kluwer, 2024. ISBN 978-80-7676-898-7. s. 317.

⁷⁵ SIVÁK, J. *Efektivní obhajoba*. Právo prakticky. Praha: Wolters Kluwer ČR, 2024. ISBN 978-80-7676-901-4. s. 59-62.

⁷⁶ Zásada hospodárnosti směřuje k tomu, aby soudní řízení proběhlo co nejefektivněji, tedy pokud možno rychle a s vynaložením pokud možno nejmenších nákladů jak ze strany účastníků, tak ze strany státního rozpočtu k tomu srov. HENDRYCH, D. *Právní slovník*. 3., podstatně rozš. vyd. Beckovy odborné slovníky. V Praze: C.H. Beck, 2009. ISBN 978-80-7400-059-1. nebo například JEMELKA, L., PONDĚLÍČKOVÁ, K., BOHADLO, D.: *Správní řád. Komentář*. 7. vydání. Praha: C. H. Beck, 2023, ISBN: 978-80-7400-751-4, s. 60-61.

přibrání specializovaných pracovišť Policie České republiky ve smyslu odborných vyjádření.

V druhém případě jde o posouzení míry autentičnosti (způsoblosti klamat), neboť se jedná o otázku do jisté míry značně subjektivní. Zde bude nutné vycházet vedle samotného technického provedení (kvality) deepfake rovněž z povahy prostředí zveřejnění (místa šíření – např. otevřené vs. uzavřené skupiny) ve spojení s okruhem jeho uživatelů a jejich znalostí, resp. rozpoznávací schopnosti (např. profesní skupiny), přičemž jde o to, aby jejich běžný návštěvník nebyl schopen rozpoznat deepfake od reality.

Zajímavou otázkou z pohledu dokazování se jeví i předložení deepfake jako důkazního prostředku.⁷⁷ Naznačené obtíže s posouzením technologického aspektu deepfake platí plně i zde. V případě prokázání předložení falešného důkazu lze uvažovat zejména o odpovědnosti za trestný čin podle ustavení § 347a trestního zákoníku (maření spravedlnosti) či přestupku podle § 2 zákona o některých přestupcích (Přestupky proti pořádku ve státní správě vyskytující se na více úsecích státní správy) v závislosti na typu projednávané věci (řízení).

5. ZÁVĚR

O deepfakes jako novodobém problému se začalo vážněji diskutovat zejména ve spojení s šířením falešných pornografických fotografií a videí veřejně známých osobností. Nicméně tak jak se rozšiřuje dostupnost a sofistikovanost generátorů deepfakes, tak se úměrně zvyšuje i riziko jejich zneužití, a to nejen co do možností a forem zneužití, ale i okruhu potenciálních pachatelů a obětí. Daná problematika se proto dostává čím dál tím více do pozornosti odborné veřejnosti, kdy napříč vědními obory se hledají efektivní způsoby, nástroje a opatření, jež by mohly další šíření deepfakes a jejich negativní dopady eliminovat či alespoň omezit.

Preventivní právní nástroje (zejména regulace digitálního prostoru, úprava směřující na detektory deepfakes, regulace šíření deepfakes

⁷⁷ Podrobněji viz POLČÁK, R., PÚRY, F. HARAŠTA, J. a kol. *Elektronické důkazy v trestním řízení*. Brno: Masarykova Univerzita, Právnická fakulta, 2015. ISBN 978-80-210-8073-7, zejména kapitoly I. 6 – I.8: Opomenutý důkaz, Nástroje praktické jistoty, Důkazní spolehlivost.

na platformách, povinnost označování syntetického obsahu a deepfakes přispívají k tomuto cíli pouze částečně a logicky musí být podpořeny i sankčními nástroji.

Významný nástroj dopadající na nezákonná šíření deepfakes tak představují normy trestního práva. Deepfakes lze podle jejich obsahu a zaměření stíhat jak pomocí existujících skutkových podstat trestných činů (zejména § 181 Poškození cizích práv, § 209 Podvod, příp. přestupků, anebo jako tzv. deep porn (§ 192 Výroba a jiné nakládání s dětskou pornografií, a od 1.1.2026 též § 191a (Zneužití identity k výrobě pornografie a její šíření). V rovině trestního práva hmotného lze stávající úpravu hodnotit jako vyhovující, reagující na vývojové změny.

Stěžejní problém při postihování tvorby deepfake a jeho nezákonného užití/šíření tkví v procesních aspektech, zejména dokazování a posouzení jejich technologického aspektu.

Aktuálně dostupné nástroje (detektory) jsou totiž schopné identifikovat deepfakes s procentuálním vyjádřením přibližně mezi 60 až 80 procenty. V kontextu s povinností prokázat vinu tzv. „nadevší pochybnost“, se jeví takové procentuální vyjádření jako nedostatečné pro rozhodnutí o vině, pokud nebudou k dispozici další relevantní skutečnosti (například doznání pachatele).

Při prokazování viny se tak prozatím nelze opírat o technologie, ale předně o jiné důkazy a zjištěné skutečnosti poukazující na nepravdivost obsahu šířeného materiálu.

SEZNAM ZDROJŮ

- [1] ABBAS, F. a TAEIHAGH, A. Unmasking deepfakes: A systematic review of deepfake detection and generation techniques using artificial intelligence. Online. *Expert Systems with Applications*. 2024, vol. 252 Part B. ISSN 0957-4174. Dostupné z: <https://doi.org/10.1016/j.eswa.2024.124260>. [cit. 2025-10-22].
- [2] ABELOVSKÝ T. Počítač jako sudce, *Revue pro právo a technologie*, č. 14, roč. 2016.
- [3] ANTOGNINI, A. – WOODS, A. K. Shallow Fakes. *Penn State Law Review*. 2023, Vol. 128, No. 69.

- [4] [BARKER, C; FORD, S.; EGLINTON, R.; QUAIL, S. a TAGGART, D. The truth project paper one—how did victims and survivors experience participation? Addressing epistemic relational inequality in the field of child sexual abuse. Online. *Frontiers in Psychiatry*. 2023, vol. 2023, no. 14. ISSN 1664-0640. Dostupné z: <https://doi.org/10.3389/fpsyt.2023.1128451>. [cit. 2025-10-01].
- [5] BARTOŇ, M. Virtuální pornografie, limity svobody umělecké tvorby a svobody projevu a trestní zákon. *Právní rozhledy*, č. 17, roč. 2008,
- [6] BENGIO, Y. – HINTON, G. – LECUN, Y. Deep learning. *Nature*. 2015, Vol. 521, No. 7553
- [7] BENÍŠKOVÁ, E. „Někdo hodil mou fotku do AI, aby mě svlékl.“ Tři české influencerky o své zkušenosti s novou formou sexuálního obtěžování. In: HEY FOMO [online]. 22. 10. 2023 [cit. 2025-10-10]. Dostupné na: <https://heyfomo.cz/nekdo-hodil-mou-fotku-do-ai-aby-me-svlekl-tri-ceske-influencerky-o-sve-zkusenosti-s-novou-formou-sexualniho-obtezovani>
- [8] BROZ, J. Karikatura v judikatuře Ústavního soudu: ochrana důstojnosti versus svoboda projevu. [online]. *Časopis pro právní vědu a praxi*, 2018, roč. 26, č. 3. Dostupné z: <https://doi.org/10.5817/CPVP2018-3-6> . [cit. 2025-10-26]
- [9] CNN PRIMA NEWS. Nevěřte všemu, co vidíte. Do evropských voleb promluví i „naklonovaní“ politici, varují experti. [online]. 2024,. Dostupné z: <https://cnn.iprima.cz/deepfake-evropske-volby-dezinformace-videa-check-point-438230>. [cit. 2025-10-26]
- [10] ČESKÁ ASOCIACE UMĚLÉ INTELIGENCE. *Manuál DEEPFAKE 2024: Obranná strategie pro české firmy*. [online]. 2023. Dostupné z: <https://asociace.ai/deepfake-2024/>. [cit. 2025-10-20].
- [11] ČESKÁ TELEVIZE. *Prezident podepsal novelu trestního zákoníku*. [online]. 2025. Dostupné z: <https://ct24.ceskatelevize.cz/clanek/domaci/prezident-podepsal-novelu-trestniho-zakoniku-363072>. [cit. 2025-10-23].
- [12] ČESKÁ TELEVIZE. *Nejen Taylor Swiftová. Deepfake pornografie s celebritymi je stále větší problém*. [online] 2024. Dostupné z: <https://ct24.ceskatelevize.cz/clanek/kultura/nejen-taylor-swiftova-deepfake-pornografie-s-celebritami-je-stale-vetsi-problem-347491>. [cit. 2025-10-21]
- [13] EUROPEAN COMMISSION: CORDIS - EU RESEARCH RESULTS. *Deepfake Evidence and Technology for Forensic Content Oversight and Research*. [online]. 2025. Dostupné z: <https://cordis.europa.eu/project/id/101225942>. [cit. 2025-10-28]
- [14] FIALA, Z. a M. PAČMAG. ICT a nové trendy v procesu dokazování v řízení o přestupku. *FORENZNÍ VĚDY, PRÁVO, KRIMINALISTIKA*, roč. 2020, č. 2, str. 195 -209.
- [15] FIRIC, A. – HANÁČEK, P. – MALINKA, K. Deepfakes as a threat to a speaker and facial recognition: An overview of tools and attack vectors. *Heliyon*. 2023, Vol. 9, No. 4
- [16] FENYK, J.; CÍSAŘOVÁ, D. a GRIVNA, T. *Trestní právo procesní*. 8. vydání. Praha: Wolters Kluwer, 2024.
- [17] GEISE, S. Visual Framing. In: RÖSSLER, P. (ed.). *The International Encyclopedia of Media Effects*. Chichester: Wiley Blackwell, 2017.

- [18] GOODFELLOW, I. a kol. *Generative Adversarial Nets*. In: GHAHRAMANI, Z. – WELLING, M. a kol. (eds.). *Advances in Neural Information Processing Systems 27 (NIPS 2014)*. Montreal: Curran Associates, 2014.
- [19] HELMUS, T. C., *Artificial Intelligence, Deepfakes, and Disinformation: A Primer*. Santa Monica, CA: RAND Corporation, 2022. Dostupné z: <https://www.rand.org/pubs/perspectives/PEA1043-1.html>. [cit. 2025-10-23].
- [20] HENDRYCH, D. a kol. *Správní právo. Obecná část*. 9. vyd. C. H. Beck, Praha, 2016
- [21] JELÍNEK, J. *Trestní právo hmotné: obecná část, zvláštní část*. 9. aktualizované vydání. Student. Praha: Leges, 2025.
- [22] JEMELKA, L., PONĎELÍČKOVÁ, K., BOHADLO, D. *Správní řád. Komentář*. 7. vydání. Praha: C. H. Beck, 2023
- [23] JUEFEI-XU, F. a kol. Countering Malicious DeepFakes: Survey, Battleground, and Horizon. *arXiv*. 2022, No. 2103.00218
- [24] KASL, F. *Porušení bezpečnosti osobních údajů v kontextu Internetu věcí*. Brno: Masarykova univerzita, 2021.
- [25] KALVODOVÁ, V. a HRUŠÁKOVÁ, M. *Dokazování v trestním řízení - právní, kriminologické a kriminalistické aspekty*. Spisy Právnické fakulty Masarykovy univerzity v Brně. Řada teoretická, Edice Scientia. Brno: Masarykova univerzita, 2015
- [26] KHANJANI, Z.; WATSON, G. a JANEJA, V. P. Audio deepfakes: A survey. [online] *Frontiers in Big Data*. 2023, roč. 5 - 2022. ISSN 2624-909X. Dostupné z: <https://doi.org/10.3389/fdata.2022.1001063>. [cit. 2025-10-22].
- [27] KIETZMANN, J. a kol. Deepfakes: Trick or treat? *Business Horizons*. 2020, Vol. 63, No. 2
- [28] KOLOUCH, J. *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016
- [29] ĽABUZ, M. Regulating Deep Fakes in the Artificial Intelligence Act. *Applied Cybersecurity & Internet Governance*. 2023, Vol. 2
- [30] MIZEROVÁ, T. Právo a deepfakes. In. *AUCI*, č. 2, roč. 2025.
- [31] MARIGOLD.CZ. *YouTube spouští AI nástroj pro detekci deepfake videí tvůrců obsahu*. [online]. Dostupné z: <https://www.marigold.cz/tech-news/youtubes-ai-likeness-detection-tool-is-searching-f/>. [cit. 2025-10-28].
- [32] MONTEIRO, S.; WANZELLER, C. a CALDEIRA, F. Performance Analysis on Deep Fake Detection. Online. *Communications of the IBIMA*. 2024. ISSN 1943-7765. Dostupné z: <https://doi.org/10.5171/2024.457767>. [cit. 2025-10-26].
- [33] MATES, P. (ed.) a kolektiv: *Ochrana osobnosti, soukromí a osobních údajů*. Praha: Leges: 2019
- [34] NOVOTNÁ, J. *Právní pomoc v cizím státu v přípravném řízení trestním*. 3. vydání. Praha: C.H. Beck, 2015.

- [35] NPR NETWORK. *Major deepfake porn site shuts down*. [online]. Dostupné z: <https://www.npr.org/2025/05/06/nx-s1-5388422/mr-deepfakes-porn-site-ai-shut-down>. [cit. 2025-10-25].
- [36] PHONEXIA. *Nástroje boje proti hlasovým deepfakes (NABOSO)*. [online]. Dostupné z: <https://www.phonexia.com/cz-projects-grants/>. [cit. 2025-10-28].
- [37] POBOŘILOVÁ, M. Virtuální dětská pornografie, *AUCI*, č. 4, roč. 2012
- [38] POLČÁK, R., PÚRY, F. HARAŠTA, J. a kol. *Elektronické důkazy v trestním řízení*. Brno: Masarykova Univerzita, Právnická fakulta, 2015.
- [39] SIMON G. *Persönlichkeitsschutz Gegen Herabsetzende Karikaturen in Deutschland Und Frankreich: Frankfurt an Main*, Peter Lang AG, 1994
- [40] SMEJKAL, V. *Kybernetická kriminalita*. 3 vyd. Plzeň: Aleš Čeněk 2022, s. 845; GRÍVNA, T., POLČÁK, R. (eds.) *Kriminalita a právo*. Praha: Auditorium 2008
- [41] RÁLIŠ, P. Zpravodajský odposlech jako důkaz v trestním řízení. Online. *Trestněprávní revue*. 2024, roč. 23, č. 4, s. 224-232. ISSN 1213-5313. [cit. 2025-10-21].
- [42] SIVÁK, J. *Efektivní obhajoba. Právo prakticky*. Praha: Wolters Kluwer ČR, 2024.
- [43] ŠÁMAL, P. *Trestní zákoník: komentář*. 3. vydání. Velké komentáře. V Praze: C.H. Beck, 2023
- [44] STRAUS, J. *Kriminalistická technika*. 3., rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013
- [45] ŠVIHEL, P. *Přišli jsme o všechno a stydíme se. Pár uvěřil, že investice zaštituje Petr Pavel*. In: Seznam Zprávy [online]. 25. 4. 2023 [cit. 2025-10-10]. Dostupné zde: <https://www.seznamzpravy.cz/clanek/domaci-zivot-v-cesku-podvodnici-se-zastitili-prezidentovym-jmenem-seniorsky-par-prisel-o-vsechno-22990>
- [46] THE GUARDIAN. *Nearly 4,000 celebrities found to be victims of deepfake pornography*. [online]. Dostupné z: <https://www.theguardian.com/technology/2024/mar/21/celebrities-victims-of-deepfake-pornography>. [cit. 2025-10-25]
- [47] ÚŘAD VLÁDY ČESKÉ REPUBLIKY. Akční plán prevence domácího a genderově podmíněného násilí na léta 2023–2026. [online]. Dostupné z: https://vlada.gov.cz/assets/ppov/rovne-prilezitosti-zen-a-muzu/dokumenty/AP_DGPN-2023_final.pdf. [cit. 2025-10-25].
- [48] VANGELI, B. *Zákon o Policii České republiky: komentář*. 2. vyd. Praha: C.H.Beck, 2014.
- [49] VIZOSO, Á; VAZ-ÁLVAREZ, M. a LÓPEZ G., Xosé. Fighting Deepfakes: Media and Internet Giants' Converging and Diverging Strategies Against Hi-Tech Misinformation. [online]. *Media and Communication*. 2021, vol. 9, no. 1, s. 291-300. ISSN 2183-2439. Dostupné z: <https://doi.org/10.17645/mac.v9i1.3494>. [cit. 2025-10-21].
- [50] ZÁMEK, D. *Rizika zneužití umělé inteligence ke generování sexuálně explicitního obsahu*. In: QUAERE 2023 - Recenzovaný sborník příspěvků interdisciplinární mezinárodní vědecké konference doktorandů a odborných asistentů. Hradec Králové: MAGNANIMITAS, 2023. p. 306 - 313. vol. 13.

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 17 | YEAR 2026 | NUMBER 33

DISCUSSION

- Eva Fialová, Veronika Příbáň Žolnerčíková, Ján Matejka, Tereza Novotná:** Legal Limits on the Use of Data for Training and Operating Artificial Intelligence Systems 3
- Jan Martínek:** How Can Algorithmic Moderation Be Regulated Fairly? Balancing User and Platform Input in the Decision-Making Process of an Oversight Board 39

ANNOTATION

- Jan Martínek:** Domestic partnership of Campos & Munoz: Who is responsible for these hallucinated precedents?..... 85
- A. Blechová, M. Erlebach, J. Harašta, A. Karpjáková, P. Loutocký, T. Mizerová, K. Mlčáková, M. Plášek:** Overview of current caselaw I/2026 93

ESSAYS

- Adéla Mertová:** Life in the datasphere: The new always-online self..... 115

THESIS REVIEW

- M. Erlebach, I. Holcová, A. Jareš, F. Kasl, P. Loutocký, O. Málek, M. Mesarčík, J. Míšek:** Thesis review I/2026 127

BOOK REVIEW

- Ondřej Böhm:** YEUNG, K., RANCHORDÁS, S.: An introduction to law and regulation: Text and materials 173
- Martin Erlebach:** VAN CLEYNENBREUGEL, P., GROZDANOVSKI, L. (eds). The Standards of Fairness in Digital Law: The Normative Foundations of the Data, Data Governance, Digital Services, Digital Markets and Artificial Intelligence Acts 185
- Jan Martínek:** CASAROSA, Federica, PSYCHOGIOPOULOU, Evangelia (eds.): Social Media, Fundamental Rights and Courts: A European Perspective 195

TOPIC

- Zdeněk Fiala, Pavel Mates, Marek Pačmag:** Current Issues in the Prosecution of Deepfakes 201

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 30th June 2026.

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: Mgr. 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 Grivna, Ph.D., prof. JUDr. Josef Kotásek, Ph.D., JUDr. Bc. Zdeněk Kučera, Ph.D., Mgr. Ing. Zbyněk Loebl, 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 Ptašík, 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

Journal © Masaryk University, 2026

papers are solicited to the following streams (work-in-progress papers are also welcome):

Law: Cybersecurity, Cyberwarfare, *chair: Václav Stupka*, indicative topics: cyber security; cyber warfare; active countermeasures; response teams; EU cybersecurity legislation; cybersecurity certification, usable security.

Law: Cybercrime, Electronic Evidence, *chair: Aleš Završník*, indicative topics: digital forensics; European Investigation etc. Orders; cybercrimes; AI aspects; cross-border challenges; Budapest Convention; space aspects.

Law: Financial Fraud, *chair: Tihomir Katulić*, indicative topics: online payment fraud; AI-enabled fraud; AML/CFT; crypto-asset fraud; KYC and digital identity; fraud-as-a-service; virtual asset fraud and abuse; money muling.

Law: eGovernment, eJustice, *chair: Pavel Loutocký*, indicative topics: digital public services; AI in public administration; automation of processes and decision making; digital identity and citizen access; data governance and data spaces; open / participatory governance; eJustice.

Legal Informatics, *chairs: Erich Schweighofer, Jakub Harašta*, indicative topics: legal information retrieval; deployment of LLMs for legal information retrieval; human-computer interaction; robots and agents; access to law; legal knowledge representation; AI for justice.

Law: Intellectual Property On-Line, *chairs: Andreas Wiebe, Matěj Myška*, indicative topics: software/AI protection and OSS; data rights and access rights; AI: training, output and IP Protection; IP enforcement in the digital economy; trademarks and digital economy; European digital regulation and IP

International Internet Law, *chair: Dan Svantesson*, indicative topics: keywords: public international law and the Internet; private international law and the Internet, extraterritoriality online; cross-border data flows, law enforcement cross-border access to data, cross-border ecommerce.

Law: Privacy and Personal Data, *chairs: Jakub Míšek, Bettina Bacher*, indicative topics: GDPR (incl. national implementations); privacy-by-design; anonymisation and pseudonymisation; risk assessment; Data Governance; data processing in the context of AI technology; privacy and ethics.

Law: eHealth *chair: Michal Košík*, indicative topics: Medical Robotics; Privacy-Enhancing Technologies; Health Surveillance; Digital Therapeutics; MDR; EHDS.

Gaming and Entertainment Law, *chair: František Kasl*, indicative topics: age assurance, digital fairness, loot boxes, e-sports, influencer advertising, generative AI in game development, AI-driven personalization.

New Media: Culture, Politics and Society, *Chairs: Monika Metyková, Jakub Macek*, indicative topics: new media and audiences; new media and journalism; political economy of new media; new media and political communication; new media, democracy

Psychology of Cyberspace, *chairs: David Šmahel, Hana Macháčková*, indicative topics: impact of digital media on wellbeing; online risks (e.g., cyberaggression, online addiction); online socializing and relationships (e.g. digital parenting); AI usage and effects on AI users; digital skills and literacy.

AI Technologies: generative, destructive, *chairs: Herbert Hrachovec, Andreas Kirchner*, indicative topics: use and abuse of AI technologies; mindless intelligence; creative AI technologies?: collaboration, innovation, loss of trust; constraining AI technologies with law, software, and by civil society; data politics: collection, filtering, labeling

Special tracks:

New EU digital regulatory frameworks: challenges & opportunities, *chair: Nikolaus Forgó*.

Large Language Models in Law: Opportunities for Legal Practice, *chairs: Stefan Eder, Tereza Novotná*.

Online Platforms and Copyright Enforcement, *chair: Ondřej Woznica*

ODR, *chair: Zbyněk Loebel*

Law: Digitising Cultural Heritage, *chair: Matěj Myška*

full papers are not mandatory, but are welcome by the following associated peer-reviewed journals

Masaryk University Journal of Law and Technology, print and on-line, listed in SCOPUS (Q2), EBSCO, Hein Online, ERIH PLUS

Cyberpsychology, on-line, listed in WoS (Q2), SCOPUS, EBSCO, ERIH PLUS, Directory of OA Journals

Diskuze

Eva Fialová, Veronika Příbaň Žolnerčíková, Ján Matejka, Tereza Novotná: **Právní limity využití dat pro trénink a provoz systémů umělé inteligence**

Jan Martínek: **Jak spravedlivě regulovat algoritmickou moderaci? Vyvažování projevu uživatelů a platformy v rozhodovací praxi Oversight Board**

Anotace

Jan Martínek: **Domestic partnership of Campos & Munoz: Kdo odpovídá za vyhalucinované precedenty?**

A. Blechová, M. Erlebach, J. Harašta, A. Karpjáková, P. Loutocký, T. Mizerová, K. Mlčáková, M. Plášek: **Přehled aktuální judikatury I/2026**

Essays

A. Mertová: **Life in the datasphere: The new always-online self**

Recenze závěrečných prací

M. Erlebach, I. Holcová, A. Jareš, F. Kasl, P. Loutocký, O. Málek, M. Mesarčík, J. Míšek:

Recenze závěrečných prací I/2026

Recenze

Ondřej Böhm: YEUNG, K., RANCHORDÁS, S.: **An introduction to law and regulation: Text and materials**

Martin Erlebach: VAN CLEYNENBREUGEL, P., GROZDANOVSKI, L. (eds). **The Standards of Fairness in Digital Law: The Normative Foundations of the Data, Data Governance, Digital Services, Digital Markets and Artificial Intelligence Acts**

Jan Martínek: CASAROSA, Federica, PSYCHOGIOPOULOU, Evangelia (eds.): **Social Media, Fundamental Rights and Courts: A European Perspective**

Téma

Zdeněk Fiala, Pavel Mates, Marek Pačmag: **Aktuální otázky postihování deepfakes**

MUNI
PRESS

