28

REVUE PRO PRÁVO A TECHNOLOGIE

Ústav práva a technologií Právnické fakulty Masarykovy univerzity

Ročník 14 / Rok 2023 / Číslo 28

Revue.law.muni.cz

Celoživotní vzdělávání na
Právnické fakultě Masarykovy univerzity

LL.M. V PRÁVU INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

MODERNÍ OBSAH - INOVATIVNÍ METODY VÝUKY - ELITNÍ VYUČUJÍCÍ

Informace o zahájení přihlašování pro rok 2024:

Centrum dalšího vzdělávání
Jana Buchalová

llm@law.muni.cz
+ 420 731 591 249

www.llm.law.muni.cz

REVUE PRO PRÁVO A TECHNOLOGIE

ROČNÍK 14 | ROK 2023 | ČÍSLO 28

Revue pro právo a technologie
Odborný recenzovaný časopis pro technologické obory práva a právní vědy zařazený na Seznamu recenzovaných neimpaktovaných periodik vydávaných v České republice a v databázi ERIH PLUS.
Recenzovány jsou příspěvky v sekci Diskuze a Téma.
Vychází dvakrát ročně. Toto číslo vyšlo 31. 12. 2023.
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
Zástupkyně šéfredaktora: Mgr. Anna Blechová
Redakce: JUDr. Mgr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek, Ph.D.
Editor: Mgr. Martin Erlebach
Redakční rada: prof. JUDr. Radim Polčák, Ph.D. (čestný předseda), JUDr. Zuzana Adamová, Ph.D., prof. JUDr. Michael Bogdan, B.A., LL.M., jur. dr. (Lund), JUDr. Marie Brejchová, LL.M., JUDr. Jiří Čermák, prof. JUDr. Bc. Tomáš Gřivna, Ph.D., doc. 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 Ptašnik, Ph.D., JUDr. Danuše Spáčilová, JUDr. Eduard Szattler, Ph.D., JUDr. Tomáš Ščerba, Ph.D.
Grafická úprava: Mgr. Martin Loučka, doc. JUDr. Matěj Myška, Ph.D.
Tisk: POINT CZ, s.r.o., Milady Horákové 20, 602 00 Brno
Vydání tohoto čísla časopisu Revue pro právo a technologie bylo financováno z projektu „Právo a technologie XI“, MUNI/A/1293/2022.

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 690:2011.

Způsob citování a praktické příklady jsou dostupné v interpretacích normy ISO 690:2011, které jsou dostupné např. na adrese www.ezdroje.muni.cz/prehled/zdroj.php?lang=cs&id=441

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

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/RPT2023-2-1

MOŽNOSTI TRESTNEJ ČINNOSTI V METAVERSE

NORBERT HALAS[1]

ABSTRAKT

Autor sa v predmetnom článku zaoberá trestnou činnosťou spojenou s čoraz viac skloňovanou technológiou metaverse. S predmetnou problematikou je možné stretnúť sa aj na pôde Europolu a Rady EÚ, pričom autor poukazuje na aktuálny vplyv, ktorý môže mať metaverse a technológie, na ktorých je založený, na trestnú činnosť. V ďalšom rozoberá, čo táto technológia znamená pre následne presadzovanie práva a aké rizika so sebou môže priniesť v podobe trestnej činnosti.

KĽÚČOVÉ SLOVÁ:

Metaverse, neoprávnené nakladanie s osobnými údajmi, legalizácia výnosu z trestnej činnosti, obťažovanie, terorizmus, extrémizmus.

ABSTRACT

The author of this article addresses criminal activities associated with the increasingly discussed metaverse technology. This issue is also a subject of discussion within Europol and Council of the European Union, and the author highlights the current impact that the metaverse and its underlying technologies may have on criminal activities. Furthermore, the author explores what this technology means for subsequent law enforcement and the potential risks it may bring in the form of criminal activities.

[1] JUDr. Norbert Halas, Ph.D., je vyšším súdnym úradníkem pri Okresným súdem Vranov nad Topľou. Kontaktní e-mail: norbert.halas13@gmail.com

KEYWORDS:

Metaverse; Unauthorized Handling of Personal Data; Money Laundering; Abusement; Terrorism; Extremism

1. ÚVOD

S vývojom technológii sa rovnako vyvíja aj internet, ktorý je každodennou súčasťou nášho života, či už pracovného, alebo súkromného, a denne na ňom trávime niekoľko hodín. V súčasnosti sa v spojení s internetom začína čoraz viac skloňovať pojem metaverse, ktorý sa dostal do popredia najmä v čase, keď Mark Zuckerberg v októbri 2021 oznámil, že spoločnosť Facebook zmení obchodný názov na Meta Platforms, Inc.[2] Predmetné vyhlásenie prinieslo koncept metaverse do pozornosti verejnosti. Tomuto počinu svedčí aj fakt, že rovnako aj ďalšie technologické spoločnosti ohlásili veľké investície namierené do tejto technológie.[3]

To, že metaverse predstavuje výzvu aj pre trestné právo potvrdzuje aj to, že danou problematikou sa zaoberalo aj Inovačné laboratórium Europolu, ktoré v júni 2022 zorganizovalo podujatie o metaverse pre orgány presadzovania práva a justičné orgány členských štátov Európskej únie, aby pomohli pochopiť vplyv, ktorý môže mať metaverse a technológie, na ktorých je založený, na trestnú činnosť a ako sa budú musieť jednotlivé orgány prispôsobiť novým bezpečnostným potrebám občanov. Počas podujatia sa odborníci z viacerých odvetví podelili o výsledky svojho výskumu ľudského správania v digitálnom prostredí, rozvíjajúcich sa ekonomických ekosystémov súvisiacich s týmito prostrediami a s metaverse. Rovnako diskutovali aj o skúsenostiach a myšlienkach týkajúcich sa výziev, aké môže metaverse predstavovať z hľadiska bezpečnosti a o spôsoboch, ako môžu jednotlivé orgány prispôsobiť svoje postupy. Na podujatí sa zúčastnilo viac ako 120 zástupcov orgánov presadzovania práva a justičných orgánov z celej Európ-

[2] Introducing Meta: A social technology company. [online]. 2021. [18. 03. 2023]. Dostupné z: https://about.fb.com/news/2021/10/facebook-company-is-now-meta/

[3] Which companies are investing in the metaverse? 7 stocks to watch. [online]. [18. 03. 2023]. Dostupné z: https://finance.yahoo.com/news/companies-investing-metaverse-7-stocks

skej únie. V sérii prezentácii účastníci vyjadrili jasnú potrebu zdrojov, ktoré by jednotlivým policajným zložkám v členských štátoch EÚ pomohli lepšie pochopiť riziká a príležitosti, ktoré predstavuje metaverse a s ním súvisiace technológie.[4]

V súčasnosti je náročné predvídať skutočné dôsledky trestnej činnosti v spojení s predmetnou technológiou, nakoľko metaverse má v súčasnej dobe aplikačnú vrstvu len veľmi limitovanú. Tieto nové výzvy si budú vyžadovať inovatívne riešenia a spoluprácu medzi technologickým odvetvím a orgánmi činnými v trestnom konaní, aby sa zabezpečilo bezpečné a dôveryhodné prostredie pre používateľov. Preto je už teraz potrebné predstaviť si možné rizika spojené s metaverse. Cieľom tohto príspevku je systematicky preskúmať a kriticky analyzovať narastajúce hrozby a možnosti trestnej činnosti v kontexte metaverse, ktorý sa stáva stále významnejším aktérom v súčasnom digitálnom ekosystéme. Tento príspevok sa ďalej sústreďuje na jednotlivé technológie, ktoré sú základom pre metaverse, ich následné zneužívanie a na dôležité aspekty bezpečnosti a etických záležitostí, ktoré vznikajú v dôsledku rastúcej komplexity a interakcie medzi fyzickým a virtuálnym svetom v rámci metaverse.

2. TECHNOLÓGIE SPOJENÉ S METAVERSE

Metaverse sa často opisuje ako ďalší medzi stupienok vývoja internetu, ktorý by mohol vytvoriť jediný univerzálny virtuálny svet, resp. kyberpriestor, ktorý ponúka používateľom pohlcujúci zážitok a ktorý má svoje základy v reálnom svete. V najnovšej definícii metaverse sa tento koncept stáva ešte ambicióznejším, keďže môže zrušiť hranice medzi fyzickým a virtuálnym svetom a vytvoriť jednu integrovanú realitu. V súčasnosti je metaverse zameraný len na virtuálnu realitu (VR - Virtual Reality), ale čoraz viac sa definuje aj z hľadiska rozšírenej reality (AR - Augmented Reality) alebo zmiešanej reality (XR - Extended Reality).[5]

---

[4] Policing in the metaverse: what law enforcement needs to know. [online]. 2022. [18. 03. 2023]. Dostupné z: https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know

[5] What is the metaverse and how will it work? [online]. [18. 03. 2023]. Dostupné z: https://blog.servermania.com/what-is-metaverse/

Z prezentovaných vízií metaverse ponúka prísľub umožniť ľuďom vychutnať si zážitky bez fyzických obmedzení a disponovať väčšou autonómiu vďaka decentralizovanej technológii. Navrhované aplikácie presahujú možnosť online zábavy, tak ako ju poznáme dnes, a zahŕňajú zlepšenie produktivity práce, interaktívne vzdelávacie prostredia, elektronický obchod a i. Zdá sa pravdepodobné, že metaverse bude zahŕňať digitálnu ekonomiku, vďaka ktorej budú môcť používatelia vytvárať, nakupovať a predávať tovar podobne ako je to pri mnohých online hrách, akými sú napr. World of Warcraft. V súčasnosti sa už stretávame s virtuálnymi svetmi v rôznych aplikáciách alebo na webových stránkach, akou je aj napr. platforma Roblox[6], platforma Second Life[7], Fortnite alebo aj Minecraft, kde jednotliví užívatelia medzi sebou vzájomne komunikujú a zároveň aj obchodujú.

Metaverse a súvisiace technológie sú predstavované rôznymi spôsobmi, ale zdieľajú spoločný koncept celkového alebo čiastočného virtuálneho sveta, ktorý prenáša zážitky z fyzického sveta do virtuálnej sféry. Na základe tohto konceptu bol navrhnutý tzv. „internet zmyslov“ [8] a zároveň prebieha vývoj implantovaných čipov, ktoré umožňujú úplné ponorenie sa do virtuálneho sveta. [9] S týmito rozhraniami môže v budúcnosti vzniknúť situácia, kedy bude ťažké alebo dokonca nemožné rozlíšiť virtuálny svet od toho fyzického.

V súčasnosti je ťažké predpovedať, či sa koncept metaverse uchytí ako spoločná technológia viacerých spoločnosti, alebo si každá spoločnosť vytvorí svoju vlastnú verziu. Ako však poznamenáva dokument analytického

---

[6] Roblox je online hracia platforma, umožňujúca hráčom vytvárať vlastné hry s otvoreným svetom a zdieľať ich s ostatnými. Hra je dostupná pre Android, iOS, MacOS, Windows, Xbox One a Fire OS.

[7] Second Life je online multimediálna platforma, ktorá umožňuje ľuďom vytvoriť si avatara a následne komunikovať s ostatnými používateľmi a používateľmi vytvoreným obsahom v rámci online virtuálneho sveta pre viacerých hráčov.

[8] Internet of senses (internet zmyslov) poskytuje rozšírené videnie, sluch, hmat a čuch. Umožňuje užívateľom spájať multisenzorické digitálne zážitky s miestnym prostredím a komunikovať so vzdialenými používateľmi, zariadeniami a pod., ako keby boli priamo pri nich.

[9] Elon Musk má veľké plány: Čochvíľa začne testovať Neuralink aj na ľuďoch! [online]. 2022. [cit. 19. 03. 2023]. Dostupné z: https://www.techbyte.sk/2022/12/elon-musk-zacne-testovat-neuralink-ludoch/

a výskumného tímu Rady Európskej únie týkajúci sa metaverse *„dopyt po technológii vytvorí jej následnú ponuku“*[10]*,* čo vlastne platí pri všetkých najnovších technológiách. Navyše, so spojeným trhom pre VR a AR v odhadovanej hodnote 4 miliardy eur, pričom do budúcna sa odhaduje, že táto čiastka vzrastie na 36 miliárd eur,[11] mnohé spoločnosti neváhajú investovať do tejto vznikajúcej technológie za účelom zisku a tým priniesť metaverse do každodenného života. Aj keď predmetné investície nie sú zárukou jeho prijatia, značné investície od širokého spektra technologických spoločností zvyšujú pravdepodobnosť prijatia aspoň niektorých aspektov s ním spojených. Metaverse je nadviazaný na ďalšie samostatné technológie, ktoré tvoria jeho súčasť a ktoré je potrebné si na účely tohto príspevku aj patrične ozrejmiť.

2.1 WEB3

Web3 sa momentálne nachádza v raných štádiách vývoja a jeho presná definícia ešte nie je ustálená. Avšak prístupné definície sa zhodujú v jednom - že ide o novú verziu internetu, ktorá stojí na princípoch decentralizácie, súkromia a anonymity.[12] V rámci Web3 je decentralizácia dosahovaná využitím technológii akou je peer-to-peer (p2p)[13] a blockchain, ktorá je jeho kľúčovým hnacím motorom. Decentralizácia, anonymita a absencia centrálnej autority môžu mať významné dôsledky pre kriminalitu v kyberpriestore, a to aj pre evidenciu elektronických dôkazov o týchto činnostiach. S decentralizáciou sa môže zvýšiť obťažnosť vyšetrovania a trestania trestnej činnosti v kyberpriestore, keďže neexistuje centrálny orgán, ktorý by mal kontrolu nad týmito sieťami.[14]

---

[10] Rada Európskej únie: Metaverse – virtual world, real challenges. [online]. 2022. [cit. 19. 03. 2023]. Dostupné z: https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf

[11] Ibidem.

[12] FENWICK, Mark, JURCYS, Paulius: The contested meaning of Web3 and why it matters for (IP) Lawyers. In: *Product and services*. [online]. 2022. [cit. 19. 03. 2023]. Dostupné z:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4017790

[13] Sieť so vzájomným sprístupňovaním obsahu medzi užívateľmi.

V súčasnosti existuje niekoľko projektov, ktoré kombinujú technológie blockchainu a peer-to-peer (p2p) na poskytovanie rôznych služieb, ako napr. herný obsah, nezastupiteľné tokeny (NFT)[15] a riešenia na zdieľanie médií. Tieto technológie predstavujú existujúcu infraštruktúru, ktorá môže byť využitá pre rozvoj metaverse a môže byť ďalej prispôsobená a rozvíjaná, aby vyhovovala jeho špecifickým potrebám. Hoci koncept Web3 má potenciál poskytnúť decentralizovaný internet, veľké korporácie začínajú preberať tieto technológie a integrovať ich do svojich platformových riešení. To vedie k vytváraniu centralizovaných služieb a platformových ekosystémov, ktoré môžu konkurovať decentralizovaným projektom. Tento trend vyvoláva diskusiu o rovnováhe medzi decentralizáciou a centralizáciou v rámci metaverse a otázku, ako udržať decentralizované hodnoty v kontexte rastúcej účasti veľkých technologických hráčov.[16]

2.2 AVATAR POUŽÍVATEĽA

Avatar (známy aj ako digitálne dvojča) reprezentuje digitálnu replikáciu objektov a systémov z reálneho do virtuálneho sveta. V súčasnosti je definovaný ako virtuálna entita, ktorá má charakteristiky svojho tvorcu - používateľa. Tento koncept umožňuje zrkadlenie fyzických entít a zároveň predpovedanie a optimalizáciu ich virtuálnych inkarnácií prostredníctvom analýzy senzorických dát, fyzikálnych modelov a historických informácií v reálnom čase.[17]

Avatary slúžia ako nástroje pre získavanie údajov od fyzických entít na následné samoučenie a prispôsobenie v rámci virtuálneho prostredia. Okrem toho majú avatary schopnosť poskytovať presné digitálne modely predpokladaných objektov s požadovanými atribútmi v metaverse. Táto

[14] FENWICK, Mark, JURCYS, Paulius: The contested meaning of Web3 and why it matters for (IP) Lawyers. In: *Product and services*. [online]. 2022. [cit. 19. 03. 2023]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4017790

[15] Non-fungible token

[16] Porovnaj MA Winston, HUANG Ken. *Blockchain and Web3: Building the Cryptocurrency, Privacy, and Security Foundations of the Metaverse.* 1st Edition, Wiley, 2022, s. 56.

[17] BANAEIAN FAR Saeed, RAD IMANI Azadeh. Applying Digital Twins in Metaverse: User Interface, Security and Privacy Challenges. [online]. 2022. [cit. 08. 08. 2023]. Dostupné z: https://arxiv.org/pdf/2204.11343.pdf

presnosť je dosiahnutá simuláciou komplexných fyzikálnych procesov a využitím technológií umelej inteligencie, čo je významné pre rozvoj a renderovanie metaverse na veľkej škále. Ďalej, avatary podporujú prediktívnu údržbu a monitorovanie bezpečnosti fyzického sveta prostredníctvom obojsmerného pripojenia medzi fyzickými entitami a ich virtuálnymi reprezentáciami.[18]

2.3 VIRTUÁLNA, ROZŠÍRENÁ A ZMIEŠANÁ REALITA

Zatiaľ čo niektoré technológie virtuálnej a rozšírenej reality existujú už nejaký čas, ďalšie sa stále intenzívne vyvíjajú a sú podporované mnohými rôznymi technológiami, akými sú priestorové výpočty, senzory, haptika a lokalizačné služby. rozšírený hardvér a softvér na prístup k platforme, ako aj sprievodná technológia na uľahčenie používania platforiem.

Rozšírená realita (AR) je technologický koncept, ktorý umožňuje používateľom interagovať s digitálnym obsahom a virtuálnymi objektmi v reálnom svete prostredníctvom grafiky, videonahrávok a hologramov. Na druhej strane, virtuálna realita (VR) poskytuje používateľom pohlcujúce zážitky v plne digitálnom prostredí, kde sú odtrhnutí od fyzického sveta. MR[19] predstavuje koncept, ktorý umožňuje prechod medzi AR a VR, čím ponúka komplexnejšie a dynamické interakcie medzi digitálnym a reálnym svetom. Tieto technológie spadajú pod rámec rozšírenej reality (XR), čo je zastrešujúci termín, zahŕňajúci VR, AR a MR. XR umožňuje používateľom prežiť rozmanité zážitky v spojení s metaverse, čím im otvára dvere k rôznorodým službám a aktivitám, ktoré sa odohrávajú v rámci fyzického aj digitálneho sveta.[20]

---

[18] Ibidem.

[19] MR - mixed reality, vo voľnom preklade „zmiešaná realita“. Na účely tohto príspevku sa ale „zmiešanou realitou“ rozumie pojem Extended reality (XR).

[20] RASHID, Mamunur, CHOI, Piljoo, KWON, Ki-Ryong. Emergence of the Metaverse: How Blockchain, AI, AR/VR, and Digital Transformation Technologies will change the Future World. [online]. 2022. [cit. 09.08.2023]. Dostupné z: https://www.researchgate.net/publication/
362302545_Emergence_of_the_Metaverse_How_Blockchain_AI_ARVR_and_Digital_Transformation_Technologies_will_change_the_Future_World

S vyspelosťou miniaturizovaných senzorov, vstavanej technológie a technológie zmiešanej reality (XR) sa očakáva, že XR zariadenia, ako sú helmy s montovanými displejmi (HMD[21]), budú hlavným terminálom pre vstup do metaverse. XR začleňuje technológie virtuálnej a rozšírenej reality (VR/AR), aby ponúklo multisenzorické ponorenie, zvýšený zážitok a interakciu v reálnom čase medzi používateľom/avatarom/prostredím prostredníctvom holografického displeja s predným projektorom, HCI[22] (najmä BCI[23]) a rozsiahleho 3D modelovania. Nosiace XR zariadenia vykonávajú vnímanie informácií o ľudských špecifikáciách s vysokým rozlíšením, ako aj všeobecné vnímanie objektov a prostredia s pomocou vnútorných inteligentných zariadení (napr. kamier).[24]

Týmto spôsobom interaktivita medzi používateľom a avatarom už nebude obmedzená na mobilné vstupy (napr. na držanie smartfónov a notebookov), ale na všetky druhy interaktívnych zariadení pripojených k metaverse.

2.4 TECHNOLÓGIA UMELEJ INTELIGENCIE

Technológia umelej inteligencie (AI) slúži ako centrálny systém alebo „mozog“ metaverse, ktorý zabezpečuje personalizované služby pre používateľov v tomto virtuálnom svete. Tieto služby zahŕňajú vytváranie živých a prispôsobených avatarov, renderovanie rozsiahlych scén metaverse a poskytovanie multijazykovej podpory prostredníctvom analýzy multimodálnych vstupov a spracovania dát.

AI v metaverse má schopnosť inteligentných interakcií s používateľmi, ako napr. poskytovanie inteligentných sprievodcov pri nakupovaní alebo predpovedanie pohybu používateľa. Tieto interakcie prebiehajú medzi používateľmi a avatarom alebo NPC[25] prostredníctvom inteligentného roz-

[21] Helmet-mounted display

[22] Human–computer interaction (Interakcia človeka s počítačom)

[23] Brain–computer interface (neuralink)

[24] WANG Yuntao, SU Zhou, ZHANG Ning et. A Survey on Metaverse: Fundamentals, Security, and Privacy. [online]. 2022. [cit. 09. 08. 2023]. Dostupné z: https://arxiv.org/pdf/2203.02662.pdf

[25] Non-player character

hodovania. Jedným z príkladov je kontinuálne učenie sa výrazov tváre, emócií, účesov a iných faktorov zo strany AI algoritmov. Tieto algoritmy následne vytvárajú živé a personalizované avatary, ktoré reagujú na používateľov a sú schopné inteligentne odporúčať produkty alebo informácie, ktoré by mohli byť pre používateľov v rámci metaverse zaujímavé.[26]

2.5 NETWORKING

V poslednom desaťročí bolo predstavených niekoľko inovatívnych technológií na zlepšenie celkového výkonu bezdrôtových komunikačných a sieťových systémov, v ktorých sa AI intenzívne využíva na viacerých vrstvách sieťovej architektúry. Multimediálne služby a aplikácie v reálnom čase zvyčajne vyžadujú spoľahlivé pripojenie s vysokou priepustnosťou a nízkou latenciou, aby bola zaručená aspoň základná používateľská skúsenosť. Podľa požiadaviek sietí piatej generácie (5G) by maximálna rýchlosť prenosu údajov mala byť okolo 10 Gbps (gigabitov za sekundu) a oneskorenie medzi koncovými bodmi nemôže presiahnuť 10 ms (milisekundy). V súčasnosti sú už v testovacej fáze aj 6G siete.[27]

V metaverse je prítomný všeobecný sieťový prístup, ktorý umožňuje prenos veľkého objemu dát v reálnom čase medzi virtuálnym a reálnym svetom, ako aj medzi rôznymi sub-metaversmi. Tento sieťový prístup je podporovaný širokým spektrom sieťových technológií vrátane Internetu vecí (IoT), softvérovo definovanej siete (SDN), B5G a potenciálne aj 6G. V rámci 6G sa rozvíja potenciálna paradigma integrovanej siete Space-Air-Ground (SAGIN), ktorá má za cieľ zabezpečiť všeobecný a plynulý sieťový prístup k aplikáciám metaverse. Okrem toho technológia SDN umožňuje škálovateľné a flexibilné riadenie rozsiahlych sietí metaverse tým, že oddelí dátovú rovinu od riadiacej roviny. Logicky centralizovaný kontrolér využíva štandardizované rozhranie na správu zdrojov a fyzických zariadení

[26] Pozri viac napr. HUYNH-THE Thien, PHAM Quoc-Viet, PHAM Xuan-Qui et. Artificial Intelligence for the Metaverse: A Survey. [online]. 2022. [cit. 11. 08. 2023]. Dostupné z: https://arxiv.org/pdf/2202.10336.pdf

[27] HUYNH-THE Thien, PHAM Quoc-Viet, PHAM Xuan-Qui et. Artificial Intelligence for the Metaverse: A Survey. [online]. 2022. [cit. 11. 08. 2023]. Dostupné z: https://arxiv.org/pdf/2202.10336.pdf

v metaverse a umožňuje dynamické prerozdeľovanie virtualizovanej šírky pásma, úložného priestoru a výpočtových zdrojov v reálnom čase na základe požiadaviek rôznych sub-metaversov. Senzory internetu vecí (IoT) v metaverse slúžia ako rozšírenie ľudských zmyslov, čím pridávajú ďalšie dimenzie interakcie medzi virtuálnym a reálnym svetom. Tieto senzory zlepšujú vnímanie a monitorovanie prostredia v metaverse a umožňujú efektívnejšiu interakciu a komunikáciu medzi používateľmi a prostredím metaverse.[28]

V metaverse založenom na SDN sú fyzické zariadenia a zdroje riadené logicky centralizovaným radičom pomocou štandardizovaného rozhrania, ako je OpenFlow, čím je možné dynamicky prideľovať virtualizované výpočty, úložisko a zdroje šírky pásma podľa požiadaviek rôznych čiastkových metaverse v reálnom čase. Okrem toho je internet vecí sieť mnohých fyzických objektov, do ktorých sú zabudované senzory, softvér, komunikačné komponenty a ďalšie technológie s cieľom spájať, vymieňať si a spracovávať údaje medzi vecami, systémami, cloudmi a používateľmi cez internet. V metaverse sú senzory internetu vecí rozšírením ľudských zmyslov.[29]

2.6 BLOCKCHAIN

V kontexte metaverse sa použitie blockchain technológie navrhuje ako prostriedok, ktorý umožňuje používateľom prenášať svoje avatary a aktíva z jedného virtuálneho sveta do druhého. Blockchain je tiež úzko spojený s konceptom virtuálnych mien, pričom sa predpokladá, že tieto budú zohrávať dôležitú úlohu v ekonomickej činnosti v rámci metaverse. Technológia blockchain ponúka decentralizovaný a bezpečný spôsob zaznamenávania a overovania vlastníctva digitálnych aktív a virtuálnych mien v metaverse. To umožňuje používateľom prenášať svoje digitálne hodnoty

[28] ALI Mansoor, NACEM Faisal, KADDOUM, Georges, HOSSAIN, Ekram. Metaverse Communications, Networking, Security, and Applications: Research Issues, State-of-the-Art, and Future Directions. [online]. 2022. [cit. 18. 08. 2023]. Dostupné z: https://arxiv.org/pdf/2212.13993.pdf

[29] WANG Yuntao, SU Zhou, ZHANG Ning et. A Survey on Metaverse: Fundamentals, Security, and Privacy, [online]. 2022. [cit. 18. 08. 2023]. Dostupné z: https://arxiv.org/pdf/2203.02662.pdf

medzi rôznymi metaversmi bez potreby závislosti na centrálnej autorite alebo entite. Týmto spôsobom môžu používatelia ľahko spravovať svoje aktíva a virtuálne meny v rámci rozmanitých virtuálnych svetov. Virtuálne meny, ktoré sú často považované za kryptomeny vytvorené na blockchaine, môžu byť v metaverse využité na nákup digitálnych aktív, služieb alebo produktov. Predpokladá sa, že tieto virtuálne meny budú mať v metaverse významný vplyv na hospodársku aktivitu, pretože umožnia používateľom vykonávať rôzne transakcie a obchody v digitálnom prostredí. Celkovo vzato, blockchain technológia prispieva k decentralizácii a bezpečnosti vlastníctva digitálnych aktív a virtuálnych mien v metaverse a zohráva dôležitú úlohu v budúcej ekonomike tohto virtuálneho sveta.[30]

Blockchainy sú distribuované digitálne účtovné knihy kryptograficky podpísaných transakcií, ktoré sú zoskupené do blokov. Každý blok je po overení a podstúpení konsenzuálneho rozhodnutia kryptograficky prepojený s predchádzajúcim, čím sa vytvorí reťaz (chain). Tento reťazec znamená, že žiadny jednotlivý záznam nemožno zmeniť bez toho, aby sa zmenili aj všetky nasledujúce záznamy. Implementácia blockchainu ako verejnej distribuovanej účtovnej knihy znamená, že všetky záznamy sú verejné a každá zmena je overená niekoľkými uzlami v sieti, čím sa vytvárajú dodatočné záruky integrity údajov na blockchaine.[31]

Použitie blockchainu v tejto technológii je navrhnuté ako spôsob na uľahčenie interoperability rôznych platforiem metaverse. V tomto prípade by záznamy obsahovali všetky relevantné informácie o používateľskom avatare, ako sú jeho atribúty a vlastníctvo. Nahliadnutím do blockchainu by všetky platformy našli zhodné informácie o používateľovi. Používatelia sa tak môžu na všetkých týchto platformách javiť rovnako (t. j. oblečenie a aktíva,

[30] HUYNH, Thien, REDDY GADEKALLU, Thippa, WANG Weizheng et al. Blockchain for the metaverse: A Review. [online]. 2022. [cit. 18. 08. 2023]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0167739X23000493

[31] KUMAR, Randhir, TRIPATHI, Rakesh. Implementation of distributed file storage and access framework using IPFS and blockchain, *Fifth international conference on image information processing*, 2019. s. 250.

ale aj metadáta o nich) a teda môžu mať jednu identitu na všetkých platformách.[32]

3. HMOTNOPRÁVNE ASPEKTY TRESTNEJ ČINNOSTI SPOJENEJ S METAVERSE

Ako sme si načrtli v úvode, rýchly technologický vývoj v posledných desaťročiach viedol k mnohým pozitívnym zmenám v našich životoch. Avšak tento vývoj priniesol aj nové výzvy, najmä v oblasti trestného práva. S nástupom nových technológií vznikajú nielen nové príležitosti pre trestnú činnosť, ale aj komplexné výzvy v oblasti vyšetrovania a následného trestania. Jedným z kľúčových aspektov, ktorý by mal byť zdôraznený, je rýchly vývoj internetu a mobilných, resp. počítačových zariadení. Podľa viacerých autorov je nárast počítačovej kriminality zapríčinený tým, že tieto technológie a cezhraničná povaha internetu umožňujú páchateľom páchať trestné činy rýchlo, efektívne a anonymne.[33] Orgány činné v trestnom konaní sa častokrát musia vyrovnávať s rozdielnymi právnymi systémami a jurisdikciami, čo komplikuje vyšetrovanie a trestanie trestných činov na globálnej úrovni.[34]

Rovnako ako s nástupom éry internetu aj s nástupom metaverse je pravdepodobné, že dôjde k zneužitiu tejto technológie na účely trestnej činnosti, či už z dôvodu možnej decentralizácie, anonymity alebo aj cezhraničnej povahy tejto technológie.

---

[32] Policing in the metaverse: what law enforcement needs to know. [online]. 2022. [cit. 19.08.2023]. Dostupné z: https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know

[33] Napr. CURTIS, Joanna, OXBURGH, Gavin. Understanding cybercrime in 'real world' policing and law enforcement. [online]. 2022. [cit. 07. 11. 2023]. Dostupné z: https://journals.sagepub.com/doi/10.1177/0032258X221107584

[34] Viac pozri napr. Rozhodnutie Rady, ktorým sa členské štáty poverujú podpísať v záujme Európskej únie Druhý dodatkový protokol k Dohovoru o počítačovej kriminalite o posilnenej spolupráci a sprístupňovaní elektronických dôkazov. [online]. 2022. [cit. 27. 03. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:52021PC0718

3.1 NEOPRÁVNENÉ NAKLADANIE S OSOBNÝMI ÚDAJMI A KRÁDEŽE IDENTITY

V dnešnej dobe sa na internete zhromažďuje obrovské množstvo údajov o jednotlivcoch, ktoré sa využívajú na sledovanie ich správania a preferencií. Táto digitálna stopa môže byť zneužitá na manipuláciu s ľuďmi a dokonca na ich identifikáciu. Avšak, ako sme už uviedli v predchádzajúcej časti, metaverse prináša nové technológie, ktoré umožnia ešte hlbšie a pohlcujúcejšie interakcie medzi používateľmi. Týmto spôsobom sa budú zhromažďovať ešte väčšie objemy údajov, ktoré umožnia presnejšie predikcie správania jednotlivcov a dokonca aj ich jedinečnú identifikáciu na základe týchto interakcií. To môže mať obrovský vplyv na súkromie a bezpečnosť ľudí, pretože tieto údaje môžu byť následne zneužité na neetické a nezákonné účely.

Rastúci vývoj technológií v metaverse prináša nové a závažné výzvy v oblasti ochrany osobných údajov a digitálnych identít. S nárastom možností reálneho a trvalého virtuálneho zobrazovania používateľov v metaverse sa otvárajú nové príležitosti na vytváranie presvedčivých kópií vzhľadu používateľov, známych ako deepfakes. Toto zvyšuje riziko zneužitia digitálnej identity, keďže manipulácia a falzifikácia môžu byť na úrovni metaverse ešte sofistikovanejšie a presvedčivejšie. S rozvojom pokročilých senzorov pre sledovanie očí, tváre a haptiky sa získavajú podrobnejšie biometrické informácie o jednotlivých používateľoch, ktoré môžu byť využité na účely manipulácie a zneužitia digitálnych identít, čo predstavuje ďalšie riziko. Metaverse poskytuje nové a efektívnejšie spôsoby interakcie medzi používateľmi a systémom, čo môže zvýšiť úroveň komplexity a sofistikovanosti manipulácie s digitálnymi identitami. Preto je nevyhnutné zvýšiť úroveň ochrany a bezpečnosti digitálnych identít v rámci metaverse. Toto opatrenie je kľúčové na minimalizovanie rizika zneužitia a manipulácie, ktoré môžu viesť k situáciám, kde používatelia budú komunikovať s falošnými identitami, čo má potenciál značne narúšať dôveru a bezpečnosť v tomto virtuálnom prostredí. Môže tak kľudne dôjsť k situácii, keď si jeden

používateľ bude myslieť, že komunikuje s iným známym, avšak reálne pôjde o cudziu osobu.

V oblasti metaverse vznikajú nové výzvy súvisiace s dôverou v digitálnu identitu. S rastúcou kvalitou virtuálnej reprezentácie používateľov, ako aj s pokročilými senzormi, ktoré monitorujú interakciu používateľov s virtuálnym priestorom, sa zhromažďuje značné množstvo biometrických informácií, ktoré môžu byť zneužité na neoprávnený prístup k citlivým informáciám alebo na manipuláciu s používateľmi. Takisto existuje potenciál na využitie umelej inteligencie na spracovanie informácií o používateľoch, ktoré sa zhromažďujú v rámci metaverse a na následnú manipuláciu s nimi. Je zrejmé, že v oblasti metaverse by mali platiť rovnaké otázky o ochrane osobných údajov a bezpečnosti ako v iných oblastiach digitálneho sveta.

Rovnako dôležité je určenie toho, kto vlastní virtuálnu identitu používateľa. Tento problém vlastníctva virtuálnej identity je kľúčový pre používateľov metaverse a vyvoláva rôzne otázky týkajúce sa práv na ochranu osobných údajov a duševného vlastníctva. Ak platforma nárokuje vlastníctvo nad virtuálnymi identitami používateľov a s nimi súvisiacimi osobnými údajmi, môže to mať zásadné následky pre používateľov v oblasti dôveryhodnosti a súkromia. Navyše, ak používateľ poskytne biometrické informácie na prihlásenie sa do platformy, tieto informácie môžu byť použité na ďalšie účely bez súhlasu používateľa, ak to platforma explicitne nezakáže.

Údaje generované používateľmi v metaverse môžu poskytnúť veľmi podrobný obraz o ich identite a správaní, ktoré môže byť viac definujúce ako vzhľad používateľského avatara. Tieto údaje môžu byť zhromažďované, spracovávané a využívané rôznymi spôsobmi, čo môže mať dôležité následky pre súkromie a bezpečnosť používateľov. Existujú riziká, že tieto údaje môžu byť predané alebo duplikované bez súhlasu používateľov, čo môže spôsobiť potenciálne vážne dôsledky pre ich identitu a súkromie. Je dôležité, aby jednotlivé korporácie chránili tieto údaje a zabezpečili, aby boli používané v súlade s právnymi predpismi a etickými zásadami. Takisto je dôležité, aby používatelia boli informovaní o tom, ktoré ich údaje sú zhromažďované a ako sú následne používané, aby mohli urobiť rozhodnutia o tom, ako sa v metaverse prezentovať a aké údaje poskytovať. Rovnako

ako na internete, aj v metaverse by mali používatelia byť obozretní a chrániť svoje súkromie a bezpečnosť. Uvidí sa, do akej miery bude následná implementácia týchto platforiem v súlade s GDPR v rámci EÚ.

V súčasnosti sa stretávame s predajom digitálnych biometrických údajov na dark webe, čo umožňuje páchateľovi použiť takýto údaj obete na účely obídenia autentifikačných systémov.[35] S veľmi podrobnými informáciami, ktoré by sa mohli získať od používateľov metaverse, by bolo ťažšie bojovať proti takýmto exploitom. Tie by sa dali dokonca použiť na generovanie syntetických identít s celou hĺbkou človeka pridaním behaviorálnej vrstvy k deepfakes čo by vytvorilo dokonalé príležitosti na zneužitie cudzej identity, pričom by z hľadiska trestného práva mohlo ísť o trestný čin podvodu podľa § 221 slovenského zákona č. 300/2005 Z.z. Trestný zákon (ďalej len „Trestný zákon“)[36] alebo podľa § 209 českého zákona č. 40/2009 Sb. Trestní zákoník (ďalej len „Trestní zákoník“)[37] vzhľadom na uvedenie iného do omylu za účelom obohatenia sa. Už teraz sú známe medializované prípady podvodu, keď sa páchateľ vydával za niekoho iného za účelom vylákania finančných prostriedkov od obete.[38] Popísané konania môžu napĺňať aj ďalšiu skutkovú podstatu trestného činu a to poškodzovania cudzích práv podľa § 181 Trestního zákoníka,[39] ktorého objektom sú nemajetkové práva

[35] Genesis marketplace, a digital fingerprint darknet store insights: Into genesis marketplace, a black market trading in digital identity. [online]. [cit. 29. 03. 2023]. Dostupné z: https://www.f5.com/labs/articles/threat-intelligence/genesis-marketplace--a-digital-fingerprint-darknet-store

[36] Podľa § 221 ods. 1 Trestného zákona kto na škodu cudzieho majetku seba alebo iného obohatí tým, že uvedie niekoho do omylu alebo využije niečí omyl, a spôsobí tak na cudzom majetku malú škodu, potrestá sa odňatím slobody až na dva roky.

[37] Podľa § 209 ods. 1 Trestního zákoníka kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

[38] Predstavil sa ako jej vnuk: Seniorku v Bratislave obrali o 14.000 eur. [online]. [cit. 31.03.2023]. Dostupné z: https://www.teraz.sk/regiony/predstavil-sa-ako-jej-vnuk-seniorku-v-b/704934-clanok.html

[39] Podľa § 181 ods. 1 Trestního zákoníka kdo jinému způsobí vážnou újmu na právech tím, že a) uvede někoho v omyl, nebo b) využije něčího omylu, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

fyzickej a právnickej osoby,[40] najmä tie, ktoré vyplývajú z čl. 7 ods. 1 a čl. 10 Listiny základných práv a slobôd.[41]

Okrem toho, ak by podrobné osobné údaje boli presvedčivo použité na napodobňovanie osoby, pre orgány činné v trestnom konaní by bolo náročné identifikovať reálneho používateľa služby a prípadného páchateľa trestného činu. V tejto súvislosti je veľmi dôležitý postup identifikácie známy ako „poznaj svojho klienta“ (KYC - Know Your Customer), ktorý je už v súčasnosti využívaný najmä finančnými inštitúciami. Tento postup je rovnako dôležitý aj pre technológiu metaverse, pretože pomáha predchádzať zneužitiu osobných údajov a podporuje vyšetrovanie trestných činov spáchaných v tejto forme.

3.2 LEGALIZÁCIA VÝNOSU Z TRESTNEJ ČINNOSTI A PODVODY

Finančné prostriedky a ich hodnota môžu mať v metaverse rôzne formy. Zatiaľ čo NFT môžu umožňovať preukázanie vlastníctva digitálneho tovaru, transakcie v metaverse môžu byť uľahčené množstvom rôznych virtuálnych mien (kryptomien) v závislosti od príslušných platforiem, pričom fiat meny[42] pravdepodobne zostanú ako prostriedok vstupu z bežnej ekonomiky do ekonomiky metaverse. Legalizácia príjmov z trestnej činností, môže byť v metaverse pomerne jednoduchá vzhľadom na virtuálne meny a už viackrát spomínanú decentralizáciu systému.

Z ekonomického hľadiska bude v metaverse nevyhnutné, aby používatelia mohli vykonávať platby jednoducho a rýchlo. To znamená, že okrem tradičných fiat mien a známych kryptomien, ktoré poznáme, pravdepodobne uvidíme aj ďalšie implementácie platforiem špecifických pre virtuálne meny a iné decentralizované kryptomeny, ktoré budú vyžadovať nové právne riešenia. Tento nový digitálny priestor pravdepodobne zvýši nároky

[40] ŠÁMAL, Pavel, GŘIVNA, Tomáš, BOHUSLAV, Lukáš a kol. *Trestní právo hmotné.* 9. vydanie. Wolters Kluwer ČR, 2021, s. 698.

[41] Nedotknuteľnosť osoby a súkromia, právo na zachovanie svojej ľudskej dôstojnosti, osobnej cti, dobrej povesti a na ochranu mena, právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života, právo na ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe.

[42] Fiat mena predstavuje bežné peňažné prostriedky, akými sú euro, americký dolár a pod.

na monitorovanie a reguláciu. To znamená, že budú potrebné nové právne a regulačné mechanizmy, ktoré budú musieť riešiť otázky týkajúce sa vlastníctva virtuálnych aktív, zodpovednosti za škody spôsobené virtuálnymi transakciami a iné problémy, ktoré sa môžu objaviť v digitálnej ekonomike. Rovnako to môže otvoriť príležitosti pre cezhraničný prevod peňazí spôsobom, ktorý bude ťažšie monitorovateľný.

Už v súčasnosti sa kryptomeny využívajú na účely legalizácie výnosu z trestnej činnosti a uľahčovania kriminálnych prevodov peňazí. Medzi jednotlivé techniky legalizácie výnosu z trestnej činnosti patrí tzv. peeling a jeho opak tzv. layering. Pri peelingu dochádza k opakovanému posielaní malých čiastok nepresahujúcich istú sumu (napr. 1.000 eur) z celkového množstva kryptomien na rôzne adresy (najčastejšie burzy alebo zmenárne, kde môžu byť kryptomeny zmenené na fiat meny), pričom takýmto konaním dochádza k eliminovaniu jedného z najrizikovejších faktorov pri kontrole transakcií a to vysokých objemov súm. Layering predstavuje pridávanie dodatočných vrstiev (transakcií z rôznych adries kryptomien) k originálnej transakcii, čo v konečnom dôsledku sťažuje identifikáciu majiteľov adries a vykonávateľov transakcií v rámci celého procesu.[43]

Pri uvedenom konaní pri splnení ďalších predpokladov môže dojsť k naplneniu skutkovej podstaty trestného činu legalizácie výnosu z trestnej činnosti v zmysle ust. § 233[44] a § 233a[45] Trestného zákona.[46] Obe uvedené skutkové podstaty trestného činu legalizácie výnosu z trestnej činnosti vo svojej objektívnej stránke postihujú konanie páchateľa, ktorý taxatívne vy-

[43] ŠANTA, Ján, ŠANTA, Ivo, ŠIROKÝ, Tomáš. K niektorej aktuálnej trestnej činnosti spojenej s virtuálnymi menami. *Justičná revue*, 74, 2022, č. 4, s. 480.

[44] Podľa § 233 ods. 1 Trestného zákona kto nadobudne, prechováva alebo užíva vec, ktorá je výnosom z trestnej činnosti spáchanej inou osobou na území Slovenskej republiky alebo v cudzine, potrestá sa odňatím slobody na dva roky až päť rokov.

[45] Podľa § 233a ods. 1 Trestného zákona kto z nedbanlivosti ukryje, na seba alebo iného prevedie, prechováva alebo užíva vec väčšej hodnoty, ktorá je výnosom z trestnej činnosti spáchanej inou osobou na území Slovenskej republiky alebo v cudzine, potrestá sa odňatím slobody až na dva roky.

[46] V Trestním zákoníku sú predmetné trestné činy upravené v § 216 a § 217.

medzenými spôsobmi disponuje s výnosom pochádzajúcim z trestnej činnosti.[47]

Očakáva sa, že tento trend legalizácie výnosu z trestnej činnosti pomocou virtuálnych mien bude rásť s ich ďalším rozvojom. Možnosti anonymného používania kryptomien sťažia orgánom činným v trestnom konaní odhalenie trestných činov spojených s legalizáciou výnosu z trestnej činnosti a podvodmi.[48] Vzhľadom k tomu, že v metaverse budú existovať vlastné digitálne meny a hospodárske systémy, môže dôjsť k výskytu podvodov, kde sa používateľom sľubujú falošné investičné príležitosti, alebo k podvodom pri nákupe falošných digitálnych produktov napĺňajúci skutkovú podstatu už spomínaného trestného činu podvodu.[49]

3.3 OBŤAŽOVANIE A SEXUÁLNE ZNEUŽÍVANIE

Nebezpečné elektronické obťažovanie predstavuje v súčasnosti závažný problém, pričom až 58 % žien v medzinárodnom prieskume v roku 2020 realizovaného neziskovou organizáciou Plan International sa už s takýmto obťažovaním stretlo.[50] Preto je dôvodné očakávať, že takéto správanie bude existovať aj v metaverse, pričom bude mať rastúci potenciál.

Už v roku 2007 došlo k situácii, keď jeden avatar v online videohre Second Life údajne znásilnil druhého. Viacerí kritici odmietli simulovaný útok ako digitálnu fikciu, ale polícia v Belgicku proti páchateľovi reálne začala trestné stíhanie pre trestný čin znásilnenia.[51] Rovnako sme sa mohli stretnúť

---

[47] ŠANTA, Ján, ŠANTA, Ivo, ŠIROKÝ, Tomáš. K niektorej aktuálnej trestnej činnosti spojenej s virtuálnymi menami. *Justičná revue*, 74, 2022, č. 4, s. 490, 484 – 499.

[48] EUROPOL: Cryptocurrencies: tracing the evolution of criminal finances. [online]. 2022. [cit. 01.04.2023]. Dostupné z: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances

[49] Over 80 percent of NFTs minted for free on OpenSea are fake, plagiarized or spam. [online]. [cit. 01. 04. 2023]. Dostupné z: https://www.engadget.com/opensea-freeminting-tool-220008042.html

[50] Online harassment is silencing girls: the EU and its Member States can do more and better. [online]. 2020. [cit. 02. 04. 2023]. Dostupné z: https://plan-international.org/eu/ blog/ 2020/11/25/online-harassment/

[51] Virtual rape is traumatic, but is it a crime? [online]. 2007. [cit. 02. 04. 2023]. Dostupné z: https://www.wired.com/2007/05/sexdrive-0504/

aj s incidentom, ktorý obeť opísala ako „online znásilnenie“ v rámci platformy Horizon Venues.[52]

Tieto druhy virtuálnych konaní vyvolávajú vážne otázky o uplatniteľnosti súčasnej legislatívy. Znásilnenie v zmysle § 185 Trestního zákoníka[53], resp. § 199 Trestného zákona[54] alebo sexuálny nátlak, resp. sexuálne násilie podľa § 186 Trestního zákoníka[55], resp. § 200 Trestného zákona[56] vyžaduje fyzický kontakt, zatiaľ čo kontakt s avatarom v metaverse je podľa definície virtuálny. Avšak z dôvodu napredovania technológii môže byť vymedzenie medzi fyzickým a virtuálnym svetom čoraz problematickejšie. Aj vzhľadom na prvé pokusy s implantovanými čipmi v mozgu opíc sa takéto konania môžu stať realistickejšími, aj keď k priamemu fyzickému kontaktu nemusí dôjsť.[57] Preto bude potrebné z legislatívneho hľadiska takýto technologický pokrok zohľadniť nie len v trestnoprávnych normách v zmysle citovaných ustanovení Trestního zákoníka, ako aj slovenského Trestného zákona, ale aj na úrovni medzinárodných dohovoroch.

V metaverse môžu vzniknúť nové formy znásilnenia a sexuálneho násilia, ktoré pre súčasné trestné právo ešte nie sú známe, pretože všetky interakcie v tomto virtuálnom svete môžu byť zaznamenané na blockchaine pod jednou identitou. Táto skutočnosť môže pomôcť pri vyšetrovaní a od-

---

[52] Reality or Fiction? [online]. 2021. [cit. 02. 04. 2023]. Dostupné z: https://medium.com/kabuni/fiction-vs-non-fiction-98aa0098f3b0

[53] Podľa § 185 ods. 1 Trestního zákoníka kdo jiného násilím nebo pohrůžkou násilí nebo pohrůžkou jiné těžké újmy donutí k pohlavnímu styku, nebo kdo k takovému činu zneužije jeho bezbrannosti, bude potrestán odnětím svobody na šest měsíců až pět let.

[54] Podľa § 199 ods. 1 Trestného zákona kto násilím alebo hrozbou bezprostredného násilia donúti ženu k súloži alebo kto na taký čin zneužije jej bezbrannosť, potrestá sa odňatím slobody na päť rokov až desať rokov.

[55] Podľa § 186 ods. 1 Trestního zákoníka kdo jiného násilím, pohrůžkou násilí nebo pohrůžkou jiné těžké újmy donutí k pohlavnímu sebeukájení, k obnažování nebo jinému srovnatelnému chování, nebo kdo k takovému chování přiměje jiného zneužívaje jeho bezbrannosti, bude potrestán odnětím svobody na šest měsíců až čtyři léta nebo zákazem činnosti.

[56] Podľa § 200 ods. 1 Trestného zákona kto násilím alebo hrozbou bezprostredného násilia donúti iného k orálnemu styku, análnemu styku alebo k iným sexuálnym praktikám alebo kto na taký čin zneužije jeho bezbrannosť, potrestá sa odňatím slobody na päť rokov až desať rokov.

[57] What should be considered a crime in the metaverse. [online]. 2022. [cit. 02. 04. 2023]. Dostupné z: https://www.wired.com/story/crime-metaverse-virtual-reality/

haľovaní páchateľov týchto trestných činov. Informácie zaznamenané v blockchaine môžu byť cenným dôkazom a následne môžu pomôcť pri identifikácii páchateľov. Avšak toto riešenie prináša aj potenciálne nebezpečenstvo pre obete, pretože zaznamenané informácie môžu byť opakovane vyhľadávané a viesť k sekundárnej viktimizácii, ktorá môže spôsobiť, že obete budú vystavené ďalším psychickým a emocionálnym ťažkostiam tak ako je tomu vo fyzickom svete, vzhľadom na podobnosť avatara fyzickej schránky obete a emocionálnemu prepojeniu so zážitkom, čím sa zvyšuje závažnosť tohto problému.

Aj napriek tomu, že používanie takýchto služieb môže požadovať overenie veku užívateľa, takéto overenie sa dá ľahko obísť a neexistuje tak vekový konsenzus pre vyššie popísané možnosti konania. Na platforme sociálnej siete VRChat sa používatelia stretávali so striptízovými klubmi.[58] Medzitým v platforme Roblox ľudia vytvárali sexuálne „byty“, kde dochádzalo medzi avatarmi k vzájomnej súloži.[59] Napriek tomu, že takéto konania nemusia byť v súlade s podmienkami používania jednotlivých platforiem, nie len maloletí užívatelia sú aj napriek tomu s takýmito konaniami konfrontovaní.

Metaverse môže byť ideálnym miestom pre páchateľov mravnostnej kriminality na získanie prístupu k maloletým, nakoľko môže páchateľom umožniť zapojiť sa do interakcie s maloletými a postupne prehĺbiť ich zneužívanie za pomoci vzájomnej komunikácie bez toho, aby sa s nimi stretli vo fyzickom svete. Navyše, pre maloletých môže byť náročné rozlíšiť dospelých od iných maloletých v metaverse, čo vytvára nebezpečné prostredie pre grooming a iné formy sexuálneho zneužívania detí.

Vývoj v oblasti haptiky a podobných technológií prináša nový zmyslový prvok pre interakcie používateľov. Páchatelia môžu využiť tieto technológie na sexuálne zneužívanie maloletých bez fyzického kontaktu. Vzhľadom na realistické vizuálne prezentácie avatarov a možnosti pocitov by mohli

[58] Metaverse app allows kids into virtual strip clubs. [online]. 2022. [cit. 03. 04. 2023]. Dostupné z: https://www.bbc.com/news/technology-60415317

[59] The children’s game with a sex problem. [online]. 2022. [cit. 03. 04. 2023]. Dostupné z: https://www.bbc.com/news/technology-60314572

páchateľom poskytnúť nový fyzický rozmer pri sexuálnom zneužívaní v metaverse.

3.4 TRESTNÉ ČINY TERORIZMU A EXTRÉMIZMU

V minulosti sme videli, ako teroristi využívali internet na komunikáciu a organizáciu svojich aktivít, pričom vhodné prostredie môžu nájsť aj v metaverse, ktorý môžu použiť predovšetkým na propagandu, nábor a výcvik nových členov.[60]

Metaverse môže byť skutočne užitočným prostredím na školenie a vzdelávanie, nielen v oblastiach ako hry a zábava, ale aj v závažnejších oblastiach, akými je aj terorizmus. Využitie metaverse na školenie umožňuje používateľom získať praktické skúsenosti bez potreby fyzickej prítomnosti a bez rizika skutočných nebezpečenstiev. Avšak virtuálna simulácia miesta môže byť zneužitá pre plánovanie a trénovanie teroristických aktivít, kde môžu byť používané virtuálne nástroje na plánovanie a koordináciu útokov vo fyzickom svete. To znamená, že metaverse môže byť využívaný aj ako tréningový nástroj pre teroristické skupiny a umožniť vojenským jednotkám vykonávanie prieskumu a plánovanie cieľov v rámci virtuálneho prostredia. Takéto virtuálne prostredie môže byť veľmi užitočné pre plánovanie misií, ktoré môžu byť použité na testovanie rôznych scenárov a stratégií v rámci teroristických útokov. Z trestnoprávneho hľadiska hovoríme pri takomto konaní o skutkovej podstate trestného činu teroristického útoku podľa § 311 ods. 1 písm. a) Trestního zákoníka[61] v štádiu prípravy podľa § 20 Trestního zákoníka.[62]

Na druhej strane metaverse môže používateľom umožniť vytvoriť taký virtuálny svet, ktorý by si chceli docieliť svojimi aktivitami vo fyzickom svete, napr. vytvoriť virtuálny kalifát alebo virtuálne miesto nadradenosti jednej rasy. Členovia takýchto miest by mohli žiť svoj virtuálny život podľa svojich pravidiel, ktoré môžu byť v rozpore so zákonmi štátov a hodnotami spoločnosti, v ktorej žijú vo fyzickom svete. Pre kontext možno uviesť sku-

[60] Violent extremists could find the metaverse a useful recruiting and organizing tool – and a target-rich environment. [online]. 2022. [cit. 04. 04. 2023]. Dostupné z: https://www.nextgov.com/ideas/2022/01/metaverse-offers-future-full-potential-terrorists-and-extremiststoo/360494/

točnosť, že na platforme Roblox užívatelia vytvárali nacistické plynové komory a vyhladzovacie tábory.[63] Uvedené konania tak môžu napĺňať skutkovú podstatu trestného činu založenia, podpory a propagácie hnutia smerujúceho k potlačeniu základných práv a slobôd podľa § 421 Trestného zákona[64], nakoľko podporou je akékoľvek konanie, ktorým sa poskytuje ideológii alebo jej šíriteľom možnosť šírenia, ako aj možnosť získavania prívržencov. Prostriedky podpory môžu byť materiálne, napr. poskytovaním financií, technických prostriedkov, vytváraním podmienok na založenie hnutia alebo nemateriálne, napr. získavaním priaznivcov, možnosťou publikovať názory, umožnením vydávať letáky a tlačoviny a pod.[65]

Virtuálne svety môžu byť využité aj na vytvorenie paralelného sveta, kde by boli uvalené extrémistické pravidlá na každého, kto by do tohto sveta vstúpil. Títo používatelia by potom mohli žiť a konať podľa scenárov, ktoré by podkopávali akceptovanie právneho štátu. To by mohlo vytvoriť

[61] Podľa § 311 ods. 1 písm. a) Trestního zákoníka kdo v úmyslu poškodit ústavní zřízení nebo obranyschopnost České republiky, narušit nebo zničit základní politickou, hospodářskou nebo sociální strukturu České republiky nebo mezinárodní organizace, závažným způsobem zastrašit obyvatelstvo nebo protiprávně přinutit vládu nebo jiný orgán veřejné moci nebo mezinárodní organizaci, aby něco konala, opominula nebo trpěla, zničí nebo poškodí ve větší míře veřejné prostranství, majetek nebo veřejné zařízení, dopravní nebo telekomunikační systém, pevnou plošinu na pevninské mělčině, energetické, vodárenské, zdravotnické nebo jiné důležité zařízení, včetně počítačového systému, na jehož fungování takové zařízení, systém nebo plošina závisejí, s cílem vydat majetek v nebezpečí škody velkého rozsahu, bude potrestán odnětím svobody na tři až dvanáct let, popřípadě vedle tohoto trestu též propadnutím majetku.

[62] Podľa § 20 Trestního zákoníka jednání, které záleží v úmyslném vytváření podmínek pro spáchání zvlášť závažného zločinu, zejména v jeho organizování, opatřování nebo přizpůsobování prostředků nebo nástrojů k jeho spáchání, ve spolčení, srocení, v návodu nebo pomoci k takovému zločinu, je přípravou jen tehdy, jestliže to trestní zákon u příslušného trestného činu výslovně stanoví a pokud nedošlo k pokusu ani dokonání zvlášť závažného zločinu.

[63] Children's gaming platform removes 'disturbing' nazi concentration camp 'experience' with gas chambers. [online]. 2022. [cit. 04. 04. 2023]. Dostupné z: https://www.algemeiner.com/2022/02/21/childrens-gaming-platform-removes-disturbing-naziconcentration-camp-experience-with-gas-chambers/

[64] Podľa § 421 ods. 1 Trestného zákona kto založí, podporuje alebo propaguje skupinu, hnutie alebo ideológiu, ktorá smeruje k potlačeniu základných práv a slobôd osôb, alebo ktoré hlása rasovú, etnickú, národnostnú alebo náboženskú nenávisť alebo kto propaguje skupinu, hnutie alebo ideológiu, ktorá v minulosti smerovala k potlačeniu základných práv a slobôd osôb, potrestá sa odňatím slobody na jeden rok až päť rokov.

[65] ČENTÉŠ, Jozef a kol. *Trestný zákon - Veľký komentár*. Eurokódex, 2020. s. 941.

nové prostredie pre extrémistov, aby šírili svoju ideológiu a vykonávali nábor nových členov do svojich organizácií.

3.5 ŠÍRENIE POPLAŠNEJ SPRÁVY A DEZINFORMÁCIE

Súčasný Web2.0 viedol k vzniku bezprecedentnej presnosti v schopnostiach zamerať sa na špecifické demografické skupiny s cieľom ovplyvniť ich správanie na účely komerčného alebo politického zisku.[66] Nesmierne zvýšené množstvo údajov, ktoré môžu nové zariadenia získať od používateľov platforiem budú mať väčší vplyv na správanie ľudí, pričom takéto správanie môže destabilizovať jednotlivé komunity, ktoré majú orgány činné v trestnom konaní chrániť, a páchatelia môžu tento vplyv využiť aj na to, aby sa zamerali na svoje obete.

Súčasné technológie už umožňujú personalizované zameranie reklám na základe vyhľadávania a zhromažďovanie informácií o preferenciách a aktivitách používateľov na sociálnych sieťach. Metaverse však poskytuje ešte väčšie možnosti na sledovanie a zameriavanie informácií na konkrétnych používateľov, vzhľadom na ich správanie vo virtuálnom svete.

Na platformách metaverse sa môžu tiež šíriť hoaxy a poplašné správy, podobne ako na sociálnych sieťach, čo môže napĺňať skutkovú podstatu trestného činu šírenia poplašnej správy podľa § 361 ods. 1 Trestného zákona[67], resp. § 357 ods. 1 Trestního zákoníka[68], ktorých objektom je verejný kľud a záujem na ochrane obyvateľstva pred vyvolávaním vážneho znepokojenia na základe rozširovania nepravdivých poplašných správ. Poplašnou správou je taká objektívne nepravdivá správa, ktorá je spôsobila podľa svojho obsahu vyvolať obavy z určitej udalosti u aspoň časti obyva-

[66] BASTICK, Zach Would you notice if fake news changed your behavior? An experiment on the unconscious effects of disinformation, In: *Computers in human behavior*, 2021, Volume 116, s. 33.

[67] Podľa § 361 ods. 1 Trestného zákona kto úmyselne spôsobí nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta tým, že rozširuje poplašnú správu, ktorá je nepravdivá, alebo sa dopustí iného obdobného konania spôsobilého vyvolať také nebezpečenstvo, potrestá sa odňatím slobody až na dva roky.

[68] Podľa § 357 ods. 1 Trestního zákoníka kdo úmyslně způsobí nebezpečí vážného znepokojení alespoň části obyvatelstva nějakého místa tím, že rozšiřuje poplašnou zprávu, která je nepravdivá, bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

teľstva.[69] Avšak v tomto prípade by mohlo byť oveľa ťažšie ich overiť, pretože šírenie informácií by bolo ešte viac decentralizované a mohli by ich šíriť aj fiktívne osoby alebo umelá inteligencia.

V kombinácii s algoritmami a technológiami, ktoré sledujú správanie používateľov, môžu poplašné správy v metaverse mať ešte väčší dopad a vďaka kombinácii technológií, ktoré sledujú správanie používateľov by mohlo dôjsť k ešte väčšiemu šíreniu poplašných správ. Tento dopad môže byť ešte silnejší vďaka možnosti ponoreného zážitku, ktorý sa môže javiť ako reálnejší. Ďalej, decentralizácia šírenia poplašných správ by mohla viesť k situácii, kedy bude nemožné odstrániť nepravdivé informácie, pretože sa budú šíriť cez rôzne platformy a siete, vrátane Web3 technológie.

4. ZÁVER

V tomto príspevku sme si predstavili základne druhy trestnej činnosti, ktoré môžu byť spáchané v metaverse. Aj keď predmetný príspevok môže vyznievať ako sci-fi, netreba zabúdať, že takýmto sci-fi bol na počiatku tohto milénia aj samotný internet. Napriek tomu má metaverse stále ďaleko od vízií inovátorov a technologických spoločnosti. Nie je možné predpokladať, ako sa daný koncept bude vyvíjať, ale technológie napredujú každým dňom, pričom legislatíva na ne nedokáže v dostatočnej miere reagovať, čo sa preukázalo aj pri počítačovej kriminalite.

Vďaka výraznému vývoju vo virtuálnej realite budeme navštevovať obchodné centrá, cestovať, stretávať sa so známymi v kaviarňach a vymieňať si zážitky spôsobom, ktorý bude pôsobiť až prekvapivo autenticky. Metaverse už existuje v štruktúre internetových hier pre viacerých hráčov. Čoskoro však môžeme dosiahnuť éru pohlcujúcich zážitkov na nerozoznanie od nášho skutočného sveta, čo prinesie nové druhy angažovanosti pre hráčov, ale aj bežných používateľov internetu. Decentraland a Somnium Space, dva prototypy produkčných metaverse, už demonštrujú virtuálne začiatky civilizácie s ľuďmi, ktorí osídľujú pôdu, spoločensky sa stýkajú, obchodujú s vecami a presadzujú vlastníctvo občianskych slobôd.

[69] ŠÁMAL, Pavel, GŘIVNA, Tomáš, BOHUSLAV, Lukáš a kol. *Trestní právo hmotné.* 9. vydanie. Wolters Kluwer ČR, 2021. s. 1027.

Dohliadanie na metaverse predstavuje značnú výzvu. Významnú rolu v tomto procese budú mať organizácie, ktoré poskytujú platformy pre monitorovanie a moderovanie obsahu, ktorý sa na nich nachádza. Súčasne budú zodpovedné aj za poskytnutie nástrojov a mechanizmov, ktoré umožnia efektívne presadzovanie práva a ochranu záujmov v rámci týchto platform. Podobne ako v prípade súčasných online aktivít, aj tu sa predpokladajú zložité výzvy, ktoré budú umocnené novými, doposiaľ nepoznanými problémami. Riešenie týchto problémov si vyžaduje zodpovedný prístup a aktívnu spoluprácu medzi všetkými zainteresovanými stranami.

Povaha metaverse predstavuje značnú výzvu z hľadiska kontroly a monitorovania, čiže sledovania a regulácie toho, čo sa na týchto platformách deje. Táto výzva vyplýva z faktu, že očakávaný nárast počtu platforiem zvýši nároky na kontrolu a reguláciu obsahu. Monitorovanie online aktivít v metaverse predstavuje náročnú úlohu, ktorá sa týka nielen moderovania značného množstva obsahu, ale aj sledovania správania používateľov, ktoré je oveľa viac závislé od kontextu než samotný obsah. Interakcie v metaverse môžu byť takmer také efemérne ako v reálnom svete, čo znamená, že po týchto interakciách nemusia zostať žiadne stopy použiteľné na účely trestného konania.

História internetu a ďalších technológií nás naučila, že trestnú činnosť s nimi spojenú nie je možné podceňovať. Pochopenie vývoja technológii predstavuje hlavnú výzvu pre orgány činné v trestnom konaní, aby dokázali na trestnú činnosť reagovať adekvátnym spôsobom. Je preto potrebné získavať skúsenosti s novými technológiami a osvojovať si potrebné informácie, ktoré môžu dopomôcť k úspešnému trestnému stíhaniu páchateľov. Vybudovanie medzinárodnej siete odborníkov a následná medzinárodná spolupráca sa tak javí ako najlepšia možnosti budovania poznatkov nie len v oblasti metaverse.

5. ZOZNAM POUŽITÝCH ZDROJOV

5.1 KNIHY

[1] ČENTÉŠ, Jozef a kol. *Trestný zákon - Veľký komentár*. Eurokódex, 2020. 1024 s. ISBN 978-808-1550-96-6.

[2] MA Winston, HUANG Ken. *Blockchain and Web3: Building the Cryptocurrency, Privacy, and Security Foundations of the Metaverse.* 1st Edition, Wiley, 2022, 400 s. ISBN 978-111-9891-08-6.

[3] ŠÁMAL, Pavel, GŘIVNA, Tomáš, BOHUSLAV, Lukáš a kol. *Trestní právo hmotné.* 9. vydanie. Wolters Kluwer ČR, 2021, s. 698. ISBN 978-807-5987-64-8.

5.2 PRÍSPEVOK V ODBORNOM PERIODIKU

[4] BASTICK, Zach. Would you notice if fake news changed your behavior? An experiment on the unconscious effects of disinformation, *Computers in human behavior*, 2021, Volume 116, s. 25 – 48. ISSN 0747-5632.

[5] KUMAR, Randhir, TRIPATHI, Rakesh. Implementation of distributed file storage and access framework using IPFS and blockchain, *Fifth international conference on image information processing*. Institute of Electrical and Electronics Engineers (IEEE). 2019. s. 241 - 259. ISBN 978-172-8109-00-8.

[6] ŠANTA, Ján, ŠANTA, Ivo, ŠIROKÝ, Tomáš. K niektorej aktuálnej trestnej činnosti spojenej s virtuálnymi menami. *Justičná revue*, 74, 2022, č. 4, s. 484 – 499. ISSN 1335-6461

5.3 ONLINE ZDROJE

[7] ALI Mansoor, NACEM Faisal, KADDOUM, Georges, HOSSAIN, Ekram. Metaverse Communications, Networking, Security, and Applications: Research Issues, State-of-the-Art, and Future Directions. [online]. 2022. [cit. 18.08.2023]. Dostupné z: https://arxiv.org/pdf/2212.13993.pdf

[8] BANAEIAN FAR Saeed, RAD IMANI Azadeh. Applying Digital Twins in Metaverse: User Interface, Security and Privacy Challenges. [online]. 2022. [cit. 08.08.2023]. Dostupné z: https://arxiv.org/pdf/2204.11343.pdf

[9] CURTIS, Joanna, OXBURGH, Gavin. Understanding cybercrime in 'real world' policing and law enforcement. [online]. 2022. [cit. 07.11.2023]. Dostupné z: https://journals.sagepub.com/doi/10.1177/0032258X221107584

[10] Elon Musk má veľké plány: Čochvíľa začne testovať Neuralink aj na ľuďoch! [online]. 2022. [cit. 19.03.2023]. Dostupné z: https://www.techbyte.sk/2022/12/elon-musk-zacne-testovat-neuralink-ludoch/

[11] EUROPOL: Cryptocurrencies: tracing the evolution of criminal finances. [online]. 2022. [cit. 01.04.2023]. Dostupné z: https://www.europol.europa.eu/publications-events/publications/cryptocurrencies-tracing-evolution-of-criminal-finances

[12] Genesis marketplace, a digital fingerprint darknet store insights: Into genesis marketplace, a black market trading in digital identity. [online]. [cit. 29.03.2023]. Dostupné z: https://www.f5.com/labs/articles/threat-intelligence/genesis-marketplace--a-digital-fingerprint-darknet-store

[13] HUYNH, Thien, REDDY GADEKALLU, Thippa, WANG Weizheng et al. Blockchain for the metaverse: A Review. [online]. 2022. [cit. 18.08.2023]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0167739X23000493

[14] HUYNH Thien, PHAM Quoc-Viet, PHAM Xuan-Qui et. Artificial Intelligence for the Metaverse: A Survey. [online]. 2022. [cit. 11.08.2023]. Dostupné z: https://arxiv.org/pdf/2202.10336.pdf

[15] Children's gaming platform removes 'disturbing' nazi concentration camp 'experience' with gas chambers. [online]. 2022. [cit. 04.04.2023]. Dostupné z: https://www.algemeiner.com/2022/02/21/childrens-gaming-platform-removes-disturbing-naziconcentration-camp-experience-with-gas-chambers/

[16] Introducing Meta: A social technology company. [online]. 2021. [18.03.2023]. Dostupné z: https://about.fb.com/news/2021/10/facebook-company-is-now-meta/

[17] Metaverse app allows kids into virtual strip clubs. [online]. 2022. [cit. 03.04.2023]. Dostupné z: https://www.bbc.com/news/technology-60415317

[18] Online harassment is silencing girls: the EU and its Member States can do more and better. [online]. 2020. [cit. 02.04.2023]. Dostupné z: https://plan-international.org/eu/ blog/2020/11/25/online-harassment/

[19] Over 80 percent of NFTs minted for free on OpenSea are fake, plagiarized or spam. [online]. [cit. 01.04.2023]. Dostupné z: https://www.engadget.com/opensea-freeminting-tool-220008042.html

[20] Policing in the metaverse: what law enforcement needs to know. [online]. 2022. [18.03.2023]. Dostupné z: https://www.europol.europa.eu/publications-events/publications/policing-in-metaverse-what-law-enforcement-needs-to-know

[21] HUYNH-THE Thien, PHAM Quoc-Viet, PHAM Xuan-Qui et. Artificial Intelligence for the Metaverse: A Survey. [online]. 2022. [cit. 11.08.2023]. Dostupné z: https://arxiv.org/pdf/2202.10336.pdf

[22] Predstavil sa ako jej vnuk: Seniorku v Bratislave obrali o 14.000 eur. [online]. [cit. 31.03.2023]. Dostupné z: https://www.teraz.sk/regiony/predstavil-sa-ako-jej-vnuk-seniorku-v-b/704934-clanok.html

[23] Rada Európskej únie: Metaverse – virtual world, real challenges. [online]. 2022. [cit. 19.03.2023]. Dostupné z: https://www.consilium.europa.eu/media/54987/metaverse-paper-9-march-2022.pdf

[24] RASHID, Mamunur, CHOI, Piljoo, KWON, Ki-Ryong. Emergence of the Metaverse: How Blockchain, AI, AR/VR, and Digital Transformation Technologies will change the Future World. [online]. 2022. [cit. 09.08.2023]. Dostupné z: https://www.researchgate.net/publication/362302545_Emergence_of_the_Metaverse_How_Blockchain_AI_ARVR_and_Digital_Transformation_Technologies_will_change_the_Future_World

[25] Reality or Fiction? [online]. 2021. [cit. 02.04.2023]. Dostupné z: https://medium.com/kabuni/fiction-vs-non-fiction-98aa0098f3b0

[26] Rozhodnutie Rady, ktorým sa členské štáty poverujú podpísať v záujme Európskej únie Druhý dodatkový protokol k Dohovoru o počítačovej kriminalite o posilnenej spolupráci a sprístupňovaní elektronických dôkazov. [online]. 2022. [cit. 27.03.2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX:52021PC0718

[27] The children's game with a sex problem. [online]. 2022. [cit. 03.04.2023]. Dostupné z: https://www.bbc.com/news/technology-60314572

[28] Violent extremists could find the metaverse a useful recruiting and organizing tool – and a target-rich environment. [online]. 2022. [cit. 04.04.2023]. Dostupné z: https://www.nextgov.com/ideas/2022/01/metaverse-offers-future-full-potential-terrorists-and-extremiststoo/360494/

[29] Virtual rape is traumatic, but is it a crime? [online]. 2007. [cit. 02.04.2023]. Dostupné z: https://www.wired.com/2007/05/sexdrive-0504/

[30] WANG Yuntao, SU Zhou, ZHANG Ning et. A Survey on Metaverse: Fundamentals, Security, and Privacy. [online]. 2022. [cit. 09.08.2023]. Dostupné z: https://arxiv.org/pdf/2203.02662.pdf

[31] What is the metaverse and how will it work? [online]. [18.03.2023]. Dostupné z: https://blog.servermania.com/what-is-metaverse/

[32] What should be considered a crime in the metaverse. [online]. 2022. [cit. 02.04.2023]. Dostupné z: https://www.wired.com/story/crime-metaverse-virtual-reality/

[33] Which companies are investing in the metaverse? 7 stocks to watch. [online]. [18.03.2023]. Dostupné z: https://finance.yahoo.com/news/companies-investing-metaverse-7-stocks

5.4 ONLINE PRÍSPEVOK V ODBORNOM PERIODIKU

[34] FENWICK, Mark, JURCYS, Paulius: The contested meaning of Web3 and why it matters for (IP) Lawyers. In: Product and services. [online]. 2022. [cit. 19.03.2023]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4017790

---

https://doi.org/10.5817/RPT2023-2-2

VYŠETŘOVÁNÍ KYBERNETICKÉ KRIMINALITY A JEJÍ PŘEDPOKLÁDÁNÝ BUDOUCÍ VÝVOJ[1]

PAVLA STANKOVÁ[2]

ABSTRAKT

Článek představuje problematiku jedné z rapidně se vyvíjejících oblastí trestné činnosti – kriminalitu kybernetickou. Pozornost je zaměřena na její odhalování a následné vyšetřování kriminalistickým, ale i trestněprávním prismatem, zejména je poukázáno na nedostatky, se kterými se orgány činné v trestním řízení potýkají. Opomenut není rovněž ani mezinárodní boj s kyberkriminalitou, zejména pak přeshraniční instituty, které vyšetřování napomáhají. Článek pracuje se statistickými údaji, kdy je nastíněn současný, ale i předpokládaný budoucí vývoj kybernetické kriminality v České republice. Závěrem je zmíněna otázka budoucnosti České republiky v oblasti kybernetické bezpečnosti.

KLÍČOVÁ SLOVA:

Kyberkriminalita; vyšetřování kyberkriminality; statistické údaje v oblasti kybernetické kriminality; kyberbezpečnost České republiky; budoucí vývoj; covid-19 a jeho vliv na kyberzločin

---

[1] Tento text vychází z autorčiny diplomové práce s názvem “Kriminalizace útoků na informační systémy” , která byla zveřejněna v rámci digitálního repozitáře UK viz https://dspace.cuni.cz/handle/20.500.11956/179367. Diplomová práce byla zmíněna v sekci "Recenze závěrečných prací I/2023" v Revue pro právo a technologie č. 27, roč. 14, 2023.

[2] Mgr. Pavla Stanková je asistentkou soudce na Městském soudě v Praze. Kontaktní e-mail: padza.s@seznam.cz

ABSTRACT

The article presents the issue of one of the rapidly developing areas of crime - cybercrime. Attention is focused on its detection and subsequent investigation by criminalistic, but also criminal law view, in particular, it is pointed out the shortcomings that law enforcement authorities face. The international fight against cybercrime is also not neglected, in particular the cross-border institutes that facilitate the investigation. The article works with statistical data, outlining the current and projected future development of cybercrime in the Czech Republic. Finally, the question of the future of the Czech Republic in the field of cyber security is mentioned.

KEY WORDS:

Cybercrime; Cybercrime Investigation; Cybercrime Statistics; Cybersecurity of the Czech Republic; Future of Cybercrime, COVID-19 and its Impact on Cybercrime

1. ÚVOD

Kybernetická kriminalita představuje jednu z nejdynamičtěji se rozvíjejících oblastí trestné činnosti. Neustálá expanze kyberprostoru skýtá pachatelům, ať už více či méně technicky zdatným, příhodné prostředí pro páchání nelegálních aktivit, neboť značnou výhodu pro pachatele představuje vysoká míra anonymity, následně jejich ztížená identifikace a taktéž jednoduchý postup směřující k opatření si nástrojů ke spáchání útoků. S ohledem na variabilitu a dynamičnost nelegálních aktivit v kyberprostoru, se musela kriminalistika, ale i trestní právo vypořádat s nedostatečností běžných institutů a vyšetřovacích metod.

Článek přibližuje problematiku vyšetřování kyberkriminality, kdy je pozornost koncentrována na digitální stopy včetně jejich zajišťování a není opomenuta ani nezastupitelná role znalce při zkoumání těchto stop. Je poukázáno na problematické aspekty vyšetřování, načež jsou představeny instituty trestního řádu a mezinárodní justiční spolupráce, které vyšetřování umožňují. Teoretické poznatky jsou podpořeny statistickými údaji. Variabilita kyberprostoru je demonstrována na koronavirové pandemii a rovněž na

probíhajícím ozbrojeném konfliktu na Ukrajině. Závěrem je představena situace České republiky v oblasti kybernetické bezpečnosti a nastíněn možný budoucí vývoj kyberkriminality.

2. DIGITÁLNÍ STOPY A JEJICH ZAJIŠŤOVÁNÍ

Pro vyšetřování kyberkriminality, potažmo pro účely následného trestního řízení, hrají nezastupitelnou roli digitální stopy. Přiléhavou definici nabídla mezinárodní organizace IOCE (International Organization on Computer Evidence), která definovala digitální stopu jako *„jakoukoliv informaci, uloženou nebo přenášenou v binární formě, která může být předložena soudu jako věcný důkaz“*.[3] Digitální stopy jsou charakteristické markantními odlišnostmi od běžných kriminalistických stop, což mimo jiné také determinuje celý proces sběru, manipulace, vyhodnocování a uchovávání takových stop.

Zpravidla se odlišují v tom, že jde o stopy nehmotné, latentní, časově trasovatelné, s velmi nízkou životností, ale na druhou stranu mnohdy obnovitelné. Nevýhodu představuje fakt, že pachatelé disponují nespočtem možností, jak digitální stopy zastřít, čehož dosahují pomocí jejich šifrování a různých anonymizačních metod. Odlišnost lze také nalézt v prostředí, ve kterém se stopy nacházejí. Informační a komunikační systémy jsou tvořeny heterogenním prostředím, které se může poměrně dynamicky v čase měnit. Specifické vlastnosti digitálních stop však většinou budou OČTŘ a znalcům v trestním řízení působit spíše komplikace.

Nezastupitelnou roli při zajišťování digitálních stop plní metody digitální forenzní analýzy (DFA). První metoda, kterou DFA aplikuje, je tzv. tradiční, někdy také klasická digitální forenzní analýza, která předpokládá pořízení identické bitové kopie původního hmotného nosiče dat. Bitové kopie se vytváří na pevné disky Policie ČR, a to po transportu hmotných nosičů na specializované pracoviště, případně výjimečně již v průběhu samotné domovní prohlídky. Praxe vyžaduje, aby byla vytvořena jedna

[3] PORADA, Viktor a Eduard BRUNA. Digitální svět a dokazování obsahu elektronických dokumentů. *Bezpečnostní technologie, systémy a management*. [online]. 2013. [cit. 24. 8. 2023], s. 3.

hlavní kopie a minimálně jedna kopie vedlejší, a to z toho důvodu, že osoba provádějící zajišťování digitálních dat svým zkoumáním data modifikuje. Druhou metodou využívanou u běžících, neodpojitelných zařízeních, která nelze fyzicky zajistit, je metoda forenzní analýzy živých systémů (tzv. Live Forensics). Nevýhodou zajišťování stopy z „živých systémů" je však to, že v systému bude docházet k neustálým tokům dat, a tedy i ke změnám, a proto i kopie, která zde bude pořízena, se bude vztahovat pouze k okamžiku jejího provedení. Co se týče osob oprávněných zajišťovat digitální stopy, půjde o kriminalistického technika, kriminalistického IT specialistu (na rozdíl od technika má oprávnění zajišťovat bitové kopie), znalce nebo policistu bez zvláštních technických znalostí, který je nicméně oprávněn pouze k fyzickému zajištění hmotných nosičů.[4]

Pro účely trestního řízení je vždy nutné na zajištěné digitální stopy pohlížet jako na potenciální důkazy, které budou v řízení předloženy, a proto je klíčové je zabezpečit tak, aby zajištěná data nebyla v průběhu celého procesu nijak upravována a pravost dat nemohla být nikterak zpochybněna. Osobně se přikláním k názoru, že na veškeré stopy a informace přenášené v digitální podobě, sloužící posléze v trestním řízení jako digitální důkazy, by mělo být nahlíženo ve smyslu nepřímých důkazů, a to vzhledem k jejich snadné falzifikaci.

Obecný a fundamentální rámec pro práci s digitálními stopami poskytuje mezinárodní technická norma ISO 27037:2012 (Směrnice pro identifikaci, sběr, akvizici a uchování digitálních důkazů). Jako základní požadavek při sběru stop uvádí spolehlivost, dostatečnost, relevantnost a při práci s digitálními stopami také pak reprodukovatelnost, kontrolovatelnost a ospravedlnitelnost. Norma rovněž klade nároky i na osobu manipulující s digitálními stopami, kterou označuje jako DEFR (Digital Evidence First Responder). DEFR je speciálně vyškolenou osobou, která by měla na místě vyhledávat a zajišťovat digitální důkazy, přičemž by měla dodržovat následující:

[4] ČÁP, Jan, Lukáš BREU a Zdeněk PROKEŠ. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. *Bezpečnostní teorie a praxe*. 2022, č. 1. s. 89.

- „Minimalizovat manipulaci s digitálním zařízením či digitálními daty,
- zdokumentovat veškeré akce a změny provedené s danou digitální stopou tak, aby si mohl nezávislý expert vytvořit názor na spolehlivost předložených důkazů,
- postupovat v souladu se zákony dané země,
- *DEFR by neměl postupovat nad rámec své působnosti“*.[5]

Norma také konkretizuje dílčí procesy při manipulaci s digitálními důkazy, jako je identifikace, zajištění zařízení, zajištění dat a uchování. Důraz je mimo jiné rovněž kladen na řádnou dokumentaci veškerých kroků, které osoba provedla. Přestože norma byla jakýmsi prvotním základním mezinárodním doporučením, setkala se s kritickým pohledem odborníků z praxe. Podle analytiků Vyskočila a Světlíka není daná norma nijak pravidelně aktualizována, a proto ani nemůže přiléhavě reagovat na rapidní vývoj technologií. Jako problém vidí autoři i to, že všechny osoby podílející se na zajišťování stop (například znalci), nedisponují stejnou mírou znalostí základních principů sběru dat. Potíže v praxi působí i to, že sběr často neprovádí ani osoby specializované na digitální stopy, nýbrž osoba zajišťující běžné fyzické stopy.[6]

3. ROLE ZNALCE

Vzhledem k odborným znalostem a zkušenostem zaujímají znalci v oblasti dokazování své nezastupitelné místo. Znalecká činnost je upravena zákonem č. 254/2019 Sb., o znalcích, znaleckých kancelářích a znaleckých ústavech, vyhláškou č. 503/2020 Sb., o výkonu znalecké činnosti, vyhláškou č. 504/2020 Sb., o znalečném, dále vyhláškou č. 505/2020 Sb., kterou se stanoví seznam znaleckých odvětví jednotlivých znaleckých oborů, a v neposlední řadě hlavou pátou zákona č. 141/1961 Sb., o trestním řízení soudním.

---

[5] VEBER, Jaromír, Zdeněk SMUTNÝ a Ladislav VYSKOČIL. Practice of Digital Forensic Investigation in the Czech Republic and ISO/IEC 27037:2012 [in Czech]. *Acta Informatica Pragensia*. 2015, roč. 4. s. 244.

[6] Ibidem, s. 253.

Hlavní činnost znalce spočívá ve vypracování znaleckého posudku, ve kterém prostřednictvím svých odborných znalostí posuzuje skutečnosti mu předložené zadavatelem posudku. Ačkoliv bývají posudky zpracovány zpravidla písemně, není v oblasti kyberkriminality cizí ani elektronická podoba, zejména pokud se k posudku přikládají zajištěná data v elektronické podobě.

Znalce lze dále v trestní řízení využít i jako konzultanta při ohledání, a to v případě, kdy půjde o zajištění počítačového systému nebo nosiče informací. Nutno podotknout, že neodborné zásahy mohou vést ke ztrátě digitálních stop, a proto je účast znalce i v takových případech potřebná. Pakliže nepůjde zajistit celý počítačový systém nebo nosič informací, může znalec vytvořit na místě identickou bitovou kopii nosiče.[7] Znalecký posudek představuje pro trestní řízení významný důkazní prostředek, a je proto zapotřebí dbát na přesnou formulaci otázek a správný výběr osoby znalce. Pozitivní legislativní posun v problematice znaleckého dokazování a znaleckých posudků z oblasti kyberkriminality, lze spatřovat ve vytvoření nového seznamu znaleckých oborů, jako je obor informační a komunikační technologie a kybernetická bezpečnost.[8]

4. PROBLEMATICKÉ ASPEKTY VYŠETŘOVÁNÍ A DOKAZOVÁNÍ KYBERKRIMINALITY

Pro dokazování kybernetické kriminality, stejně jako pro dokazování jakékoliv jiné kriminality, platí ustanovení trestního řádu o dokazování (srov. § 89 a násl. TŘ). Nicméně se v oblasti kybernetické kriminality setkáváme s určitými specifickými aspekty, které dokazování poněkud ztěžují.

Úskalím celého procesu dokazování je bezpochyby čas. Vzhledem k dynamickému charakteru digitálních stop se možnost získání potřebných

[7] KOLOUCH, Jan. *CyberCrime*. 1.vydání. Praha: CZ.NIC, z.s.p.o., 2016, s. 453.

[8] Seznam nových znaleckých oborů a odvětví byl zaveden do právního řádu zákonem č. 254/2019 Sb., resp. vyhláškou č. 505/2020 Sb., kterou se stanoví seznam znaleckých odvětví jednotlivých znaleckých oborů, jiná osvědčení o odborné způsobilosti, osvědčení vydaná profesními komorami a specializační studia pro obory a odvětví, a to s účinností od 1. ledna 2021.

důkazů se zvyšující časovou prodlevou značně omezuje. V souvislosti s tím je také nutné dodat, že s rostoucím časem získává samotný pachatel možnost, aby digitální stopy zastřel, pozměnil, případně i smazal. Dalším problematickým aspektem dokazování je čitelnost dat. Ve světe elektronických důkazů mohou poměrně často OČTŘ narazit na sofistikované formy zabezpečení souborů, které se jim nemusí vždy podařit rozšifrovat. V takovém případě nenabízí trestní řád OČTŘ žádné procesní nástroje, kterými by mohl být obviněný donucen ke zpřístupnění takových souborů.[9] Potíž představuje pro OČTŘ i autentizace. V případě, že OČTŘ získají potřebný soubor, vyvstává otázka, kdo je jeho autorem, případně kdo k němu měl přístup a mohl jej modifikovat. Možné řešení nabízí identifikace prostřednictvím metadat[10]. Někteří autoři nicméně poukazují na možné nedostatky vyvstávající při dokazování skrze přeceňovaná metadata souborů. Ačkoliv jsou metadata užitečná a běžně s nimi není záměrně manipulováno, je třeba mít na paměti, že více či méně sofistikovaní pachatelé je můžou bez problému dle potřeby taktéž pozměnit.[11]

Při vyšetřování kyberkriminality je klíčové postupovat co možná nejrychleji, a to z důvodu nízké životnosti a nestálosti digitálních stop. Způsoby páchání kyberzločinu jsou velmi rozličné, což vyšetřovatelům může působit potíže při sestavování vyšetřovacího plánu, respektive při plánování celé vyšetřovací situace. Praxe vyšetřování a stíhání kyberkriminality se nicméně potýká s jistými problémy i na straně vyšetřovatelů, kdy jde zejména o personální deficit pracovníků specializujících se na IT systémy. Podle autorů Požára a Hníka jde dále o nedostatečné softwarové vybavení a nevhodné organizační uspořádání specializovaných policejních pracovišť.[12]

---

[9] Srov. se zásadou nemo tenetur se ipsum accusare.

[10] Metadata jsou strukturovaná data poskytující informace o datech v digitalizovaných dokumentech.

[11] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. s. 709–710.

[12] POŽÁR, Josef a Václav HNÍK. *Specifické problémy boje s kybernetickou kriminalitou* [online]. Praha: Policejní akademie ČR v Praze – Fakulta bezpečnostního managementu. [cit. 24. 8. 2023]. s. 23–24.

Při určování základního předmětu dokazování vycházíme z § 89 odst. 1 TŘ, nicméně kyberkriminalita vykazuje určité charakteristické atributy ve vztahu k předmětu dokazování. Ve všech formách kyberzločinu je zapotřebí určovat, zda se jedná o jeden či více skutků, zda došlo k zajištění původních souborů, jak byly operace na počítačovém systému provedeny a s jakým časovým odstupem byla technika po trestném činu zajištěna.[13] V souvislosti s tím je také potřeba vždy zkoumat jaká je výše způsobené škody, kolik bylo pachatelů a jaký byl jejich motiv, případně další okolnosti, které danou trestnou činnost umožnily. *„Společnou zvláštností dokazování (…) kybernetické kriminality je dále to, že její charakter nelze dovodit ze skutkové podstaty trestného činu aplikovaného na daný skutek. Charakter kybernetické kriminality je dovozován ze způsobu spáchání (modus operandi).“*[14]

Přestože mívá kybernetická kriminalita povahu pokračujících nebo trvajících trestných činů, zůstává zpravidla velmi dlouho neodhalena, což je způsobeno především tím, že většina trestných činů není ani orgánům činným v trestním řízení oznámena. Typické podněty k vyšetřování kybernetických trestných činů můžeme dle nauky dělit do čtyř kategorií: a) výsledky operativně pátrací činnosti orgánů činných v trestním řízení, b) oznámení kontrolních, inspekčních a revizních orgánů různých institucí, c) ústní, písemná a telefonická oznámení osob, d) ostatní druhy oznámení (např. anonymní oznámení nebo podněty skrze veřejné sdělovací prostředky). Rovněž v neposlední řadě může orgánům činným v trestním řízení při vyšetřování pomoci i institut podpůrných operativně pátracích prostředků, zejména pak osoba informátora (taktéž konfidenta).

[13] PORADA, Viktor a Jiří STRAUS. *Kriminalistika (výzkum, pokroky, perspektivy)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014, s. 525.

[14] Ibidem, s. 523–524.

5. INSTITUTY TRESTNÍHO ŘÁDU NAPOMÁHAJÍCÍ VYŠETŘOVÁNÍ KYBERKRIMINALITY

5.1 DOMOVNÍ PROHLÍDKA

Domovní prohlídky představují významný nástroj z hlediska opatřování elektronických důkazů a stop potřebných pro trestní řízení. Lze je vykonat, je-li důvodné podezření, že v bytě nebo jiné prostoře sloužící k bydlení nebo v prostorách k nim náležejících je věc nebo osoba důležitá pro trestní řízení (srov. § 82 TŘ). Vzhledem k tomu, že se jedná o zásah do ústavně zaručeného práva na nedotknutelnost obydlí (čl. 12 LZPS), je možné ji realizovat pouze za zákonem přísně stanovených podmínek.

Při prohlídkách konaných v souvislosti s podezřením na kyberkriminalitu je zapotřebí předem stanovit, zda na místě prohlídky dojde k zajištění fyzických nosičů informací nebo budou zajištěny pouze otisky počítačových dat. Obecně můžeme říci, že při domovních prohlídkách koncentrují pozornost OČTŘ buď na údaje archivní (magnetická média) a zálohy dat, nebo dennodenně používané informace (nacházející se často na pevném disku).[15] V neposlední řadě je nutné se zaměřit i na připojení počítačového systému k internetu či zaznamenat připojení systémů do místní sítě. Takové úkony je pak vhodné konat za přítomnosti znalce, konzultanta nebo jiné osoby znalé IT systému, aby nedošlo k možnému znehodnocení případných důkazů.

Domovní prohlídku je možné provést i jako neodkladný a neopakovatelný úkon vzhledem k možnosti manipulace s potenciálními důkazy souvisejícími s počítačovou kriminalitou a v důsledku toho pak i k možnému maření účelu trestního řízení. *„I když lze v zásadě připustit, že (…) může mít domovní prohlídka v konkrétní věci charakter neodkladného úkonu (§ 160 odst. 4 TŘ) a že jako taková je ex lege přípustná (§ 83 odst. 1 al. 2 TŘ), jde v takovém případě o zvlášť závažný zásah do ústavně zaručeného základního práva na domovní svobodu, a proto také rozhodnutí, na jehož základě má být takový úkon proveden, musí být i z tohoto hlediska zvláštní závažnosti přimě-*

[15] PORADA, Viktor a kolektiv. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. s. 798–799.

řeně a dostatečně zdůvodněno.“[16] V souvislosti s počítačovou kriminalitou byla rozhodovací praxí neodkladnost a neopakovatelnost specifikována. Nejvyšší soud ve svém rozhodnutí stanovil, že chybějící dostatečně podrobné odůvodnění neodkladnosti a neopakovatelnosti v příkazu nemusí nutně znamenat nezákonnost takové prohlídky.[17] *„Zásah do softwarového či hardwarového vybavení počítače nebo úprava na něm uložených dat před tím, než by byl odborně zjištěn a zadokumentován jeho reálný stav, by znamenal zmaření objasňování skutečností závažných pro trestní stíhání. Toto závažné riziko dostatečně odůvodňuje kvalifikaci napadeného úkonu jako neodkladného a neopakovatelného.“*[18]

5.2 ODPOSLECH A ZÁZNAM TELEKOMUNIKAČNÍHO PROVOZU

Dalším klíčovým institutem pro potírání kriminality, zejména pak kriminality kybernetické, je odposlech a záznam telekomunikačního provozu. Odposlech chápeme jako *„záměrné a utajené a současné vnímání obsahu komunikace zprostředkované telekomunikačními zařízeními nebo sítěmi prostřednictvím k tomu určených zařízení. Záznamem je souběžné zachycení obsahu komunikace na nosičích záznamu (…)“*.[19] Jde o poměrně specifický institut, neboť na rozdíl od ostatních zajišťovacích prostředků, působí pro futuro, tedy směřuje na zajištění toho, co teprve vznikne v budoucnu. Vzhledem k tomu, že se jedná o velmi významný zásah do práva na listovní tajemství a tajemství jiných písemností a záznamů (viz čl. 13 LZPS), vymezuje trestní řád taktéž velmi přísné podmínky pro jeho aplikaci.

Pozitivní úpravu daného institutu nalezneme v § 88 TŘ, kde zákon omezuje využití odposlechů u zločinů, na které je stanoven trest odnětí svobody s horní hranicí trestní sazby nejméně osm let. Dále umožňuje nařídit odposlech pro taxativně vyjmenované trestné činy, jako je například trestný čin pletichy v insolvenčním řízení (§ 226 TZ), pletichy při veřejné dražbě

[16] Nález Ústavního soudu ze dne 22. 5. 1997, sp. zn. III. ÚS 287/96.

[17] Usnesení Nejvyššího soudu ze dne 15. 12. 2010, sp. zn. 5 Tdo 1312/2010.

[18] Usnesení Nejvyššího soudu ze dne 15. 12. 2010, sp. zn. 5 Tdo 1312/2010.

[19] ŠÁMAL, Pavel. Zajišťovací úkony a předběžná opatření. In: ŠÁMAL, Pavel, Jan MUSIL, Josef KUCHTA a kolektiv. *Trestní právo procesní*. 4. přepracované vydání. Praha: C. H. Beck, 2013, s. 325.

(§ 258 TZ) či zneužití pravomoci úřední moci (§ 329 TZ). Jako třetí a poslední uvádí trestní řád možnost využít odposlechy u úmyslného trestného činu, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva. Z výše uvedeného je zcela nepochybně vidět snaha zákonodárce omezit okruh podmínek pro nařizování odposlechů a lze vyvodit, že aplikace tohoto institutu má být v praxi spíše subsidiární.

Je žádoucí zmínit, že naprostá většina počítačových zločinů, nebude subsumována pod trestné činy s trestem odnětí svobody s horní hranicí osmi let a také nepůjde o zákonem vyjmenované trestné činy.[20] Proto je z hlediska kybernetické kriminality významné zaměřit se na podmínku poslední, tj. na trestné činy, které mají podklad v mezinárodních smlouvách nebo na ně navazují. Ze smluv je v daném případě relevantní Úmluva o počítačové kriminalitě, Úmluva o ochraně dětí proti sexuálnímu vykořisťování a pohlavnímu zneužívání či Dodatkový protokol k Úmluvě o počítačové kriminalitě o kriminalizaci činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů.

V souvislosti s vyšetřováním kybernetické kriminality je v poslední době poměrně hojně diskutovaný recentní procesní institut uchování dat (angl. data preservation) dle § 7b TŘ. Ustanovení bylo začleněno do trestního řádu v souvislosti s implementací článku 16 Úmluvy Rady Evropy o počítačové kriminalitě. Osobě, která data drží nebo je má pod svou kontrolou, může být nařízeno, aby je uchovala v nezměněné podobě po stanovenou dobu (až na 90 dnů) a dále aby činila opatření, aby nedošlo k zpřístupnění informací o tom, že jí takové nařízení bylo uloženo. Důvodová zpráva dále upřesňuje, že příkaz se vztahuje na všechny typy uložených počítačových dat, tedy na základě zmíněného by bylo možné institut aplikovat i na obsah komunikace na sociálních sítích, ale taktéž na obsah emailové komunikace.[21] Zajímavé rovněž je i to, že daný institut nikterak nereflektuje zá-

[20] Pro srovnání slovenská právní úprava pojala institut odposlechu poněkud šířeji. Klíčová odlišnost spočívá v tom, že se dá uplatnit již na trestné činy, na které zákon stavuje trest odnětí s horní hranicí trestní sazby převyšující 5 let, což z hlediska počítačové kriminality může mít zásadní význam.

[21] Důvodová zpráva k zákonu, kterým se mění zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, a některé další zákony, sněmovní tisk 79/0.

važnost vyšetřovaného trestného činu, tedy lze jej de facto aplikovat na jakýkoliv trestný čin. Problematická se dle mého názoru taktéž jeví dikce zákona, která uvádí, že příkaz může být vydán policejním orgánem i bez předchozího souhlasu státního zástupce. Ačkoliv se z hlediska vyšetřování kyberkriminality zcela jistě jedná o institut, který má potenciál její vyšetřování urychlit i objasnit, je zapotřebí zamyslet se nad tím, zda aplikací tohoto institutu nedochází k obcházení jiných procesních institutů (jako je například odposlech), u kterých zákonodárce pragmaticky stanovil přísné podmínky jejich aplikace.

5.3 VYŽÁDÁNÍ ÚDAJŮ O USKUTEČNĚNÉM TELEKOMUNIKAČNÍM PROVOZU

Vyjma odposlechu a záznamu na telekomunikačním provozu umožňuje zákon využít obdobného institutu, a to vyžádání údajů o uskutečněném telekomunikačním provozu dle § 88a TŘ. Při vyžadování údajů o uskutečněném telekomunikačním provozu, OČTŘ zajišťují data, na která se aplikuje ochrana osobních a zprostředkovacích dat nebo která jsou předmětem telekomunikačního tajemství. Odposlech a vyžádání údajů se tak od sebe odlišuje v několika směrech.

Hlavní rozdíl mezi § 88 TŘ a § 88a TŘ spočívá v povaze zajišťovaných dat. Nebude zde zajišťován obsah zpráv, nýbrž provozní a lokalizační údaje. Například se bude jednat o údaje ohledně IP adresy, přístupy do e-mailových schránek či informace ohledně webových stránek. Nejednotně vnímaná problematika se také týká otázky, zda údaje dle § 88a TŘ lze vyžadovat pouze zpětně do minulosti nebo je lze vztáhnout i na data nově vzniklá. Z dikce samotného ustanovení § 88a TŘ nikterak nevyplývá, zda by údaje mohly být zajištěny jak do minulosti, tak do budoucnosti. Kolouch tvrdí, že údaje je možné vyžadovat jak do minulosti, tak i do budoucnosti, přičemž argumentuje aplikací jazykového a historického výkladu § 88a TŘ. Upozorňuje, že předchozí právní úprava obsahovala podmínku „o uskutečněném telekomunikačním provozu“, kdežto nyní zákon hovoří pouze o zajištění údajů o telekomunikačním provozu.[22] Opačný názor zastává

[22] KOLOUCH, Jan. *CyberCrime*. 1.vydání. Praha: CZ.NIC, z. s. p. o., 2016, s. 443.

Dostál, který poukazuje na to, že pokud nějaká data mají být zajištěná, musí nejdříve vůbec existovat.[23] Ani judikatura však nezaujala shodný názor. V roce 2011 Nejvyšší soud jednoznačně potvrdil, že § 88 TŘ lze uplatnit do budoucna, kdežto § 88a TŘ nikoliv.[24] O několik let později ale připustil, že v odůvodněných případech lze § 88a TŘ vydat i do budoucna. Půjde tak o *„situaci, kdy se šetřená trestná činnost nachází ve stadiu přípravy a zjišťované údaje mají orgánům činným v trestním řízení poskytnout informace důležité pro odhalení či usvědčení pachatelů, popř. k zabránění dokonání připravované trestné činnosti anebo k zjištění jiných skutečností důležitých pro trestní řízení“*.[25]

Poslední odlišnost spočívá v tom, vůči komu daný institut působí. Vyžádání údajů o uskutečněném telekomunikačním provozu směřuje vůči držiteli lokalizačních a provozních dat. Držitelé takových dat mají pak povinnost je podle zákona uchovávat po dobu šesti měsíců (viz § 96 odst. 3 ZEK), což v praxi často představuje problém. Povinnost retence dat vyplynula ze směrnice 2006/24/ES[26] (dále jen „směrnice o uchovávání dat“), ve které byla členským státům uložena povinnost uchovávat data po dobu minimálně šesti měsíců, nejvýše však po dobu dvou let. Ačkoliv byla Směrnice o uchovávání dat již zrušena, právní řády některých členských států příslušnou povinnost retence stále obsahují.[27] Současnou úpravu uchovávání dat vybraných členských zemí EU přibližuje následující tabulka.

[23] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – odposlech a údaje o komunikaci (2. díl). *Trestněprávní revue*. 2019, č. 4, s. 77–83.

[24] Usnesení Nejvyššího soudu ze dne 29. 11. 2011, sp. zn. 4 Pzo 5/2011.

[25] Usnesení Nejvyššího soudu ze dne 7. 5. 2019, sp. zn. 4 Tdo 1591/2018.

[26] Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. 3. 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí.

[27] Směrnice byla zrušena ex tunc pro rozpor s Chartou základních práv EU.

Země	**Povinnost retence dat**
Belgie	zrušena v roce 2021[28]
Česká republika	6 měsíců
Francie	12 měsíců
Itálie	30 měsíců
Polsko	12 měsíců

Tabulka 1 – Srovnání povinnosti uchovávání dat ve vybraných státech EU[29]

Závěrem je nutné ještě odkázat na možnost policejního orgánu požadovat poskytnutí provozních a lokalizačních údajů na základě zákona č. 273/2008 Sb., o Policii České republiky (dále jen „PolČR“). Policie může za zákonem stanovených specifických podmínek[30] žádat od fyzických a právnických osob zajišťujících veřejnou komunikační síť nebo službu zmíněná data (viz § 66 odst. 3 PolČR). Třebaže lze pozorovat určité obdobné znaky jako u § 88a TŘ, nelze dané instituty nikterak ztotožňovat. Jsem toho názoru, že získávání dat na základě § 66 PolČR by nemělo prvotně sledovat získávání důkazů pro trestní řízení, neboť vzhledem k velmi specifickému okruhu podmínek stanovených dle PolČR bylo nejspíše snahou zákonodárce minimalizovat pokusy obcházení § 88a TŘ.

[28] BERTHÉLÉMY, Chloé. New Belgian data retention law: a European blueprint? In: *EDRi.* [online]. 2021 [cit. 24. 8. 2023] Dostupné z: https://edri.org/our-work/new-belgian-data-retention-law-a-european-blueprint/

[29] ROJSZCZAK, Marcin. The uncertain future of data retention laws in the EU: Is a legislative reset possible? *The computer law and security report*. [online]. 2021, roč. 41, s. 2–12. ISSN 0267-3649. Dostupné z: doi:10.1016/j.clsr.2021.105572

[30] Jde o podmínku zjištění totožnosti neznámé osoby, nebo mrtvoly (§ 68 odst. 2 PolČR). Druhá podmínka svědčí útvaru Policie ČR, který bojuje s terorismem a využije daná data za účelem odhalování teroristických hrozeb (§ 71 PolČR).

5.4 OPERATIVNĚ PÁTRACÍ PROSTŘEDKY

Operativně pátrací prostředky chápeme jako systém činností policejních orgánů uskutečňovaných na základě trestního řádu. Zákon je taxativně vymezuje jako předstíraný převod (§ 158c TŘ), sledování osob a věcí (§ 158d TŘ) a použití agenta (§ 158e TŘ). Z hlediska boje proti kyberzločinu je pro nás stěžejní především institut sledování osob a věcí dle § 158d odst. 3 TŘ. Sledování osob a věcí může být využíváno například ke zjištění kontaktů z adresáře, zjištění obsahu e-mailové schránky či provedení její zálohy. Právě problematika e-mailových schránek, konkrétně zajišťování e-mailových zpráv, byla poněkud roztříštěná a musela být aplikační praxí upřesněna. Nejvyšší státní zastupitelství ve výkladovém stanovisku[31] vymezilo, že dle § 158d odst. 3 TŘ lze zjišťovat pouze aktuální obsah e-mailové schránky, tedy pokud by mělo dojít k zajištění obsahu komunikace budoucí, musel by OČTŘ uplatnit již institut dle § 88 TŘ. Judikatura je v tomto směru prozatím poměrně strohá, nicméně bylo prozatím dovozeno, že použití § 158 odst. 3 TŘ za účelem otisku elektronických dat na sledovaných zařízeních je přípustné.[32] V neposlední řadě lze i v rámci kyberkriminality využít institutu použití agenta dle § 158e TŘ, a to za účelem infiltrace skupin na dark webu.[33]

6. MEZINÁRODNÍ SPOLUPRÁCE PŘI VYŠETŘOVÁNÍ KYBERKRIMINALITY

S ohledem na přeshraniční a mezinárodní charakter kyberkriminality si v dnešní době nelze vystačit pouze s vnitrostátní úpravou. Pro vyšetřování a shromažďování elektronických důkazů je zcela klíčová spolupráce na nadnárodní úrovni. Evropská unie tak v rámci zefektivnění a ucelení

[31] Výkladové stanovisko poř. č. 1/2015 Sb. v. s. Nejvyššího státního zastupitelství ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek ze dne 26. ledna 2015, sp. zn. 1 SL 760/2014.

[32] Usnesení Ústavního soudu ze dne 3. 10. 2013, sp. zn. III. ÚS 3812/2012.

[33] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z. s. p. o., 2016, s. 451.

přeshraničního získávání důkazů nabídla členským státům několik možných nástrojů.

6.1 EVROPSKÝ VYŠETŘOVACÍ PŘÍKAZ (EVP)

Evropský vyšetřovací příkaz je institut, jenž je vydáván za účelem provedení konkrétních vyšetřovacích úkonů s cílem shromáždit elektronické důkazy ve vykonávajícím státě, případně i k získání důkazů, kterými disponují OČTŘ jiné jurisdikce. Byl zaveden směrnicí Evropského parlamentu a Rady 2014/41/EU o evropském vyšetřovacím příkazu v trestních věcech. Česká republika jej implementovala do vnitrostátního práva, a to zákonem č. 178/2018 Sb., kterým novelizovala zákon o mezinárodní justiční spolupráci ve věcech trestních.

Evropský vyšetřovací příkaz je založen na principu vzájemného uznávání, což znamená, že vykonávající orgán má povinnost danou žádost uznat a zajistit její výkon bez dalších formálních postupů. Směrnice dále stanoví, že se příkaz provádí za stejných podmínek a stejným způsobem, jako by jej nařídil vykonávající orgán. Pro zajištění spolupráce mezi státy bylo žádoucí určit i lhůty pro provedení vyšetřovacích úkonů. Bylo vymezeno, že úkony by měly probíhat se stejnou rychlostí a prioritou, jako by se postupovalo v obdobném případě na vnitrostátní úrovni. Nastaveným limitem je zde nejvýše 30 dnů na přijetí rozhodnutí a maximálně 90 dnů pro výkon požadovaného úkonu.

Nespornou výhodou dále je, že se jedná o příkaz formulářového typu s již předem danými formálními náležitostmi. V době svého vzniku byl formulář veřejností vnímán jako krok vpřed z hlediska zjednodušení formalit, zlepšení kvality a snížení nákladů na překlad.[34]

Ačkoliv se nepochybně jedná o průlomový institut ve světě elektronických důkazů, je nutné poukázat na několik možných nedostatků. První otázka se nabízí hned u překladu právní terminologie. Třebaže jde, jak již bylo výše uvedeno, o formulářový typ, vydávající orgán musí uvést a po-

[34] GUERRA, José Eduardo a Christine JANSSENS. Legal and Practical Challenges in the Application of the European Investigation Order. In: *EUCRIM – The European Criminal Law Associations Forum.* [online]. 2019, vol. 1, s. 48–49 [cit. 24. 8. 2023]. Dostupné z: https://eucrim.eu/media/issue/pdf/eucrim_issue_2019-01.pdf

psat jaké úkony mají být provedeny. Při překladu právních textů by měl orgán postupovat co možná nejkomplexněji a snažit se hledat ekvivalentní termíny i například v souvislosti s historickým kontextem. Právě jazyková bariéra a snaha nalézt vhodné ekvivalentní pojmy mezi různými právními řády pak může pro orgány představovat problém. Další nedostatek lze spatřovat v tom, že zmíněné lhůty pro přijetí rozhodnutí a jeho následný výkon, dle mého názoru, ne zcela pružně nereagují na povahu elektronických důkazů, respektive jakýchkoliv dat nacházejících se v kyberprostoru.

6.2 SPOLEČNÉ VYŠETŘOVACÍ TÝMY

Evropský vyšetřovací příkaz není jediným použitelným nástrojem v oblasti přeshraničního zajišťování elektronických důkazů. Společné vyšetřovací týmy jsou tvořeny skupinou soudců a státních zástupců z několika různých členských států, jejichž působení vzniklo za účelem vedení trestního stíhání v jednom nebo více státech. Vyšetřovací týmy se zřizují obvykle na dobu 12 až 24 měsíců, a to na základě písemné dohody. Cílem je vyměňování důkazů a získaných informací, dále efektivní sdílení technických znalostí a zkušeností. Sekundárně je také členům týmů umožněno budovat vzájemné vztahy a důvěru, což vede k efektivnější a rychlejší spolupráci.[35]

6.3 ALTERNATIVNÍ MECHANISMY KE STÁVAJÍCÍM INSTITUTŮM MEZINÁRODNÍ JUSTIČNÍ SPOLUPRÁCE

V souvislosti s usnadněním zajištění a shromažďováním elektronických důkazů nalézajících se v cizí jurisdikci představila Evropská komise legislativní návrh nařízení o evropských předávacích a uchovávacích příkazech.[36] Návrh nařízení reagoval na roztříštěné právní úpravy členských států a na rostoucí aktivitu páchání trestných činů v oblasti kyberprostoru. Nařízení mimo jiné vytváří dva zcela nové instituty, a to evropský předávací příkaz

[35] European Union Agency For Criminal Justice Cooperation. Joint investigation teams. In: *eurojust.europa.eu*. [online]. [cit. 24. 8. 2023]. Dostupné z: https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/joint-investigation-teams.

[36] Dne 25. ledna 2023 potvrdila Rada dohodu s Evropským parlamentem o návrhu nařízení a návrhu směrnice o přeshraničním přístupu k elektronickým důkazům.

a evropský uchovávací příkaz. Oba příkazy by měly opět vycházet ze zásady vzájemného uznávání a lze je užívat pouze v trestním řízení, a to jak v přípravném řízení, tak v řízení před soudem. Oba zmíněné instituty by pak měly zrychlit a zúčelnit přeshraniční přístup k případným elektronickým důkazům.

6.4 EVROPSKÝ PŘEDÁVACÍ PŘÍKAZ (EPP)

EPP je vyšetřovací opatření, které umožní justičním orgánům členského státu požadovat uložená data (např. e-mailovou komunikaci, textové zprávy atd.) přímo od poskytovatelů údajů z jiného členského státu. Lze si ze zmíněného vyvodit, že EPP má fungovat na principu obcházení systému justiční spolupráce, neboť zahraniční justiční orgány budou důkazy požadovat přímo od soukromého subjektu, který má důkazy v danou chvíli dostupné ve své sféře. Důvod vzniku tohoto institutu lze spatřovat v tom, že vnitrostátní justiční orgány mnohdy nedisponují dostačujícími prostředky, které by zajistily rychlé a efektivní zajištění elektronických důkazů. Na druhou stranu vyvstává problém, jak bude řešena situace, kdy po soukromém subjektu budou justičním orgánem cizí země požadovány například údaje, které v dané jurisdikci vyžadovány být vůbec nemohou. Zůstává otázkou, zda by nějakým způsobem neměla být zachována kontrola zákonnosti EPP ze strany příslušného justičního orgánu, v jehož jurisdikci se o důkaz žádá. Jistou výhodu, kterou lze spatřovat, jsou velmi krátké lhůty určené k poskytnutí elektronického důkazu. Poskytovatel údajů, respektive případných důkazů, bude vázán standardní lhůtou deseti dnů, aby na EPP zareagoval. Návrh rovněž počítá i s naléhavými případy, kdy lhůta může být zkrácena na šest hodin. Tyto poměrně krátké lhůty lze z hlediska kybernetické kriminality více než kvitovat a oproti lhůtám uvedeným v evropském vyšetřovacím příkazu (30 dnů na přijetí rozhodnutí + 90 dnů na jeho výkon), je lze hodnotit jako adekvátní vzhledem k nestálému charakteru kyberprostoru.

6.5 EVROPSKÝ UCHOVÁVACÍ PŘÍKAZ (EUP)

EUP je adresován členskému státu, respektive poskytovateli údajů a služeb mimo jurisdikci vydávajícího státu, a to za účelem uchování určitých údajů. Je potřeba zmínit, že EUP se vztahuje pouze na údaje, které jsou již uloženy u poskytovatele v době vydání příkazu, tedy nepůjde o údaje zachycené teprve v budoucnu, tj. po obdržení EUP. Zatímco EPP lze vydat v souvislosti s jakýmkoliv trestným činem, EUP lze vydat jen u trestných činů, na které ve vydávajícím státě zákon stanoví trest odnětí svobody s horní hranicí sazby nejméně tři roky.

Závěrem lze poznamenat, že přijetím zmíněného nařízení, evropský předávací příkaz ani evropský uchovávací příkaz nenahradí stávající evropský vyšetřovací příkaz, ale budou jen dalším alternativním řešením problematického přeshraničního zajišťování elektronických údajů.

7. KYBERKRIMINALITA – PROBLÉM MODERNÍ DOBY?

Dle statistických údajů lze pozorovat, že nápad trestné činnosti kybernetické kriminality a kriminality páchané na internetu má v České republice od roku 2011 tendenci progresivního růstu. Výjimkou byl rok 2020, který přinesl mírný pokles oproti předchozímu roku, což bylo odůvodňováno narůstajícími případy koronavirového onemocnění COVID-19, ale především spíše legislativní změnou trestního zákoníku[37], která mimo jiné posunula hranice škody nikoliv nepatrné z původních pěti tisíc na deset tisíc korun. Rok 2022 byl z hlediska nárůstu kyberkriminality zlomový, neboť bylo zaznamenáno 18 554 skutků, což je oproti roku 2021 nárůst o téměř 95 %. K nejčastěji páchaným trestným činům prostřednictvím kyberprostoru řadíme majetkovou trestnou činnost, zejména podvodná jednání, kdy signifikantní nárůst byl zaznamenán u inzertních podvodů (zejména podvody reverzní) a v neposlední řadě jsou ve větším množství páchány trestné činy podle § 230 TZ (neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací), § 231 TZ (opatření a přechovávání přístupového zařízení a hesla k počítačovému

[37] Novela účinná od 1.10. 2020, provedená zákonem č. 333/2020 Sb., kterým se mění zákon č. 40/2009 Sb., trestní zákoník, zákon č. 141/1961 Sb., ve znění pozdějších předpisů.

systému a jiných takových dat) a § 232 TZ (neoprávněný zásah do počítačového systému nebo nosiče informací z nedbalosti).

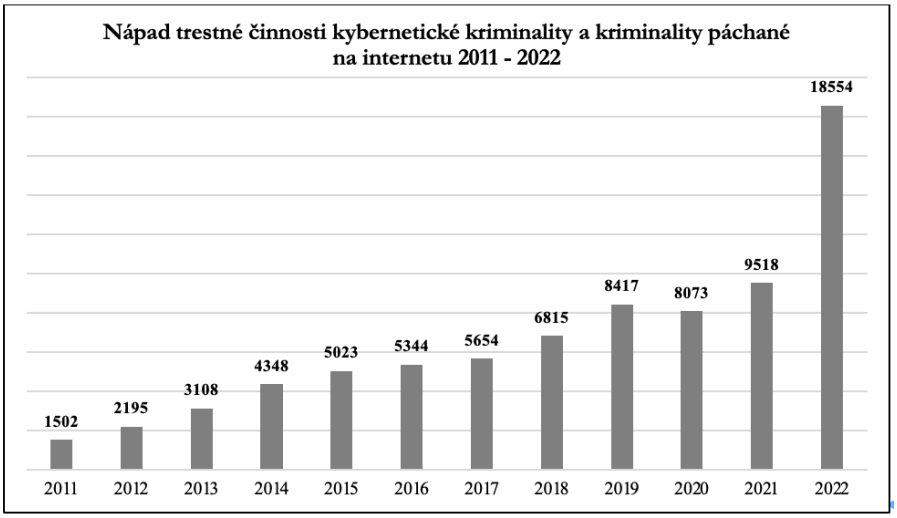
Mezi nejčastěji páchaným typem útoku za rok 2022 byl phishing a jeho různé podoby, kdy tyto útoky byly v České republice zpravidla realizovány zasíláním podvodných e-mailů. V menším měřítku útočníci využívali i podvodných telefonátů (tzv. vishing) či zasílání podvodných sms zpráv (tzv. SMiShing). Minulý rok byla na území České republiky zpozorována rovněž i nová phishingová technika s názvem Browser in the Browser (BitB).[38] Takový útok pak uživateli otevřel podvodné přihlašovací okno, které se zobrazilo jako součást běžného internetového prohlížeče a vybídlo uživatele k zadání přihlašovacích údajů.[39]

Podle oficiálních údajů z minulého roku tvoří nápad trestné činnosti kybernetické kriminality 10 % z celkové registrované trestné činnosti, z čehož by se dalo vyvozovat, že se jedná o problematiku ne tak důležitou. Je potřeba ovšem poznamenat, že na statistické údaje se nelze bezmezně spoléhat, neboť kyberkriminalita se vyznačuje vysokou mírou latence a celkový počet trestných činů s největší pravděpodobností mnohonásobně převyšuje získané údaje. Statistiky také zkresluje skutečnost, že převážná část trestných činů, která by byla podřaditelná ke kyberkriminalitě, je subsumována pod jiné skutkové podstaty.

Nápad trestné činnosti kybernetické kriminality a kriminality páchané na internetu v České republice mezi lety 2011 až 2022 přibližuje následující graf.

[38] NÚKIB. Kybernetické incidenty pohledem NÚKIB [online]. 2022 [cit. 29.10.2023]. Dostupné z: https://nukib.cz/download/publikace/vyzkum/03-2022-Novinky.pdf

[39] GRUSTNIY, Leonid. Browser-in-the-browser attack: a new phishing technique. In: kaspersky.com. [online]. 25.5.2022. [29.10.2023]. Dostupné z: https://www.kaspersky.com/blog/browser-in-the-browser-attack/44163/



*Graf **1** – Nápad trestné činnosti kybernetické kriminality a kriminality páchané na internetu v letech 2011-2022*[40]

7.1 COVID-19 A KYBERKRIMINALITA

Česká republika, podobně jako ostatní státy, byla v roce 2020 a 2021 podstatně poznamenána vlivem pandemie onemocnění COVID-19. Hrozba kybernetických útoků v souvislosti s vypuknutím infekční nemoci zesílila, neboť koronavirová pandemie zcela nepopíratelně vedla k rapidnímu přesunu veškerých běžných aktivit do virtuálního světa. V souvislosti s tím došlo k nárůstu domén s názvy spojených s koronavirem, přičemž tyto domény byly posléze využívány převážně k podvodným jednáním na internetu a k šíření poplašných zpráv. V neposlední řadě bylo zpozorováno, že i obsah dark webu reflektoval koronavirovou situaci. Objevily se zde nabídky různých neidentifikovatelných látek, které byly vydávány za látky očkovací, nicméně u nich nebylo možné ověřit, zda mají potřebnou certifikaci nebo zda se jedná o čistě podvodná jednání. Pachatele v kyberprostoru po-

[40] Ministerstvo vnitra České republiky. *Statistiky kriminality – dokumenty (hodnocení bezpečnostní situace, statistiky kriminality)*. Zpráva o situaci v oblasti veřejného pořádku a vnitřní bezpečnosti na území České republiky. [online]. Poslední změna 17. 7. 2023. [cit. 24. 8. 2023]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx

vzbudil též fakt, že se souvisejícími karanténami a prací z domova, došlo mezi zaměstnavateli k nárůstu přístupu BYOD *(Bring Your Own Device)*[41]. BYOD umožnil zaměstnancům používat svá osobní zařízení, jako jsou mobilní telefony a notebooky, k přístupu k firemním informacím a souborům. Výsledkem tak bylo, že zaměstnavatelé byli více vystaveni hrozbám kybernetických útoků, neboť práce z domova ve většině případů nezaručila stejnou kybernetickou bezpečnost jako zaručuje práce na pracovišti. Taktéž cíle kybernetických útoků velmi přiléhavě reagovaly na koronavirovou situaci, neboť touto dobou byl i největší nárůst útoků zaznamenán u nemocnic a jiných zdravotnických zařízení (příkladmo lze uvést útok na Fakultní nemocnici Brno či Psychiatrickou nemocnici Kosmonosy).

7.2 PŘEDPOKLÁDANÝ BUDOUCÍ VÝVOJ KYBERKRIMINALITY

S neustálým zdokonalováním komunikačních a informačních technologií a nárůstem sofistikovanosti pachatelů lze důvodně předpokládat, že kyberzločin bude i nadále pronikat do všech možných aspektů našich každodenních životů, což mimo jiné potvrdila i výše zmíněná pandemie koronaviru. Zcela s jistotou lze konstatovat, že cíle útočníků budou nadále převážně sledovat zištné motivy. V současné době se v souvislosti s probíhajícím ozbrojeným konfliktem mezi Ruskou federací a Ukrajinou dá obdobně usuzovat, že i nadále budou narůstat útoky na kritické informační a komunikační systémy. Vliv ozbrojeného konfliktu na český kyberprostor potvrzují i data poskytnutá NÚKIB za rok 2022, kdy byl zaznamenán zvýšený počet útoků (zejména DDoS) stran ruských hackerů převážně na české subjekty veřejného sektoru, což velmi pravděpodobně souviselo s podporou, kterou Česká republika vyjádřila Ukrajině.[42] Obecně byl taktéž

[41] BYOD je novým trendem na poli pracovněprávních vztahů, kdy zaměstnancům je ze strany zaměstnavatele umožněno přinést si do práce vlastní výpočetní techniku, kterou na pracovišti využívají pro výkon práce.

[42] NÚKIB. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022. [online] 2023, s. 15. [cit. 28.10.2023]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf

zaznamenán zvýšený počet kyberútoků od počátku války na cíle v členských zemí NATO až o 300 %.[43]

S ohledem na připravovanou digitalizaci veřejné správy lze mít za to, že kybernetická trestná činnost bude v budoucnu cílit na nejzranitelnější strategický cíl, jakým je veřejný sektor. Tuto domněnku rovněž podporuje i zpráva Agentury EU pro kybernetickou bezpečnost za rok 2022, která vyhodnotila, že sektor veřejné správy zaznamenal nejvyšší procento kybernetických incidentů.[44]

Možným řešením je posílení kybernetické bezpečnosti v kritických oblastech, jako je energetika, průmysl a zdravotnictví. Osobně se domnívám, že by pozornost měla být koncentrována na spolupráci mezi orgány působícími v oblasti kybernetické bezpečnosti, jako je PČR a NÚKIB (Národní úřad pro kybernetickou a informační bezpečnost), přičemž opomenuta by rovněž neměla zůstat spolupráce se soukromým sektorem. Je nutné zmínit, že jedním z nejdůležitějších prostředků v boji proti potenciální kriminalitě je bezpochyby posilování mezinárodní spolupráce mezi státy.

7.3 BUDOUCNOST ČESKÉ REPUBLIKY NA POLI KYBERNETICKÉ BEZPEČNOSTI

NÚKIB zpracovává minimálně jednou za pět let národní strategii kybernetické bezpečnosti a k tomu přidružený akční plán. Činí tak na základě § 22 písm. q) zákona č. 181/2014 Sb., o kybernetické bezpečnosti, který transponuje požadavky směrnice Evropského parlamentu a Rady EU 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Národní strategie kybernetické bezpečnosti ČR obsahuje cíle a vize republiky v oblasti kybernetické

[43] Google Threat Analysis Group (TAG). Fog of War – How the Ukraine Conflict Transformed the Cyber Threat Landscape. In: services.google. [online]. 16. 2. 2023. [cit. 29. 10. 2023]. Dostupné z: https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

[44] European Parliament. Cybersecurity: main and emerging threats. In: euparl.europa.eu. [online]. 21. 3. 2023. [cit. 30. 10. 2023]. Dostupné z: https://www.europarl.europa.eu/pdfs/news/expert/2022/1/story/20220120STO21428/20220120STO21428_en.pdf

bezpečnosti, které pak následně konkretizuje v úkolech obsažených v rámci Akčního plánu.

Dle Národní strategie pro rok 2021-2025 je *„základním předpokladem pro účinnou obranyschopnost ČR ucelený systém detekce kybernetických hrozeb, závislý na schopnostech a kapacitách jednotlivých bezpečnostních složek, stejně jako na účinném fungování modelu národní spolupráce mezi bezpečnostními a dalšími složkami a koordinovaném, efektivním a včasném sdílení informací. Vzhledem k faktu, že narůstá riziko ohrožení státu prostřednictvím kyberprostoru, musí ČR reagovat na celé spektrum nových výzev“*.[45]

Druhým dokumentem, určujícím aktuální směřování České republiky v oblasti kybernetické bezpečnosti, je Strategie prevence kriminality v České republice na léta 2022-2027. Strategie je vypracována Ministerstvem vnitra v součinnosti s Republikovým výborem pro prevenci kriminality. Rozvíjí již existující cíle a poznatky a promítají se zde i doporučení z mezinárodních dokumentů. Kromě obecné kriminality se zaměřuje na specifické druhy kriminality, jako je právě kromě jiného také kybernetická kriminalita a její prevence. Strategie poukazuje, že kybernetická kriminalita má za trend cílit na nejzranitelnější skupinu, a to děti, které nejenom, že se stávají často oběťmi, ještě častěji se ale stávají jejími pachateli. Jako celorepublikový problém vidí zvyšující se počty kriminálních jednání páchaných skrze sociální sítě. Hlavní boj proti tomuto trendu má představovat prevence a osvěta, zejména pak různá školení pro rizikové cílové skupiny.

Srovnání vybraných cílů strategických dokumentů představuje následující tabulka.

[45] Národní úřad pro kybernetickou a informační bezpečnost. Národní strategie kybernetické bezpečnosti České republiky na období let 2021-2025. In: *NUKIB.cz*. [online]. 2. 12. 2020. [cit. 24. 8. 2023]. Dostupné z: Národní úřad pro kybernetickou a informační bezpečnost - Strategie / Akční plán (nukib.cz)

Dokument	**Vybrané cíle**				
Národní strategie kybernetické kriminality	prevence a potírání kybernetické kriminality	zabezpečení digitální veřejné správy	efektivní mezinárodní spolupráce	sdílení schopností expertizy/ export know-how	důraz na sdílení informací, koordinaci a spolupráci
Strategie prevence kriminality	podpora obětí kybernetické kriminality	prevence a osvěta s důrazem na skupiny zvlášť zranitelné	spolupráce a vzdělávání na národní úrovni	zohlednění problematiky genderově podmíněnéh o kybernásilí	podpora policejní spolupráce v oblasti řešení kyberkriminality

Tabulka 2 – Srovnání vybraných cílů strategických dokumentů v oblasti kybernetické bezpečnosti

Vyjma výše uvedených dokumentů determinují budoucnost České republiky na poli kybernetické bezpečnosti i legislativní akty EU, jmenovitě stojí za zmínku recentně přijatá NIS2 směrnie[46] (Network and Information Systems), jejíž požadavky mají být implementovány do českého právního řádu v druhé polovině roku 2024. Směrnice koncentruje pozornost zejména na oblasti jako je zdravotnictví, energetika, veřejný sektor, bankovnictví, poskytovatelé digitálních služeb, tedy ta odvětví, která jsou v současné době velmi náchylná ke kybernetickým incidentům a rozšiřuje tak okruh subjektů, které jsou povinny zabezpečovat své systémy. Povinné subjekty v daných odvětvích budou podrobeny přísnější regulaci z hlediska bezpečnostních opatření, kdy budou zajišťovat míru kybernetické bezpečnosti, identifikovat, vyhodnocovat rizika a zajišťovat bezpečnost IT infrastruktury. Požadavky směrnice představují takové stěžejní změny v oblasti kybernetické bezpečnosti, pročež bylo přistoupeno k vytvoření zcela nového návrhu zákona o kybernetické bezpečnosti.

[46] Směrnice Evropského parlamentu a Rady 2022/2555 ze dne 14. 12. 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii.

Bezpečnost v oblasti kyberprostoru je rovněž každoročně posilována účastí České republiky na mezinárodních bezpečnostních cvičeních s názvem Locked Shields, která jsou pořádána ve spolupráci s NATO, kdy primárním cílem je testovat obranu národních kritických infrastruktur fiktivních zemí v reálném čase, přičemž tyto útoky odpovídají závažným a sofistikovaným kybernetickým incidentům.[47]

Z výše zmíněného lze zpozorovat, že kybernetická bezpečnost v České republice postupně směřuje k vybudování pevné základny, která v budoucnu zajistí potřebnou míru takového zabezpečení, čímž bude zajištěna schopnost čelit nejrůznějším kybernetickým útokům.

8. ZÁVĚR

Kybernetická kriminalita je problematika nesporně nadmíru důležitá, neboť lze důvodně očekávat, že bude čím dál tím intenzivněji docházet k přesunu tradiční kriminality do virtuálního prostředí. Svědčí tomu zejména rapidní technologický pokrok, uživatelská neznalost kyberprostředí, lhostejnost uživatelů k možnostem digitálního zabezpečení a rostoucí technické dovednosti pachatelů. Dále tomu nasvědčuje fakt, že většina každodenních aktivit se pomalu, ale jistě přesouvá do kyberprostoru, což potvrdila mimo jiné i pandemie onemocnění COVID-19. Vše zmíněné je navíc taktéž umocněno bázlivou reakcí právního řádu, který se se specifickými atributy kybernetické trestné činnosti vypořádává vždy s určitým zpožděním.

Nutno dodat, že ani orgány činné v trestním řízení nejsou v jednoduché situaci, neboť odhalování a vyšetřování kybernetických útoků je náročné z toho důvodu, že vyžaduje kvalifikované lidské zdroje, moderní technické vybavení a sdílení získaných znalostí a postupů. Nadto je nutné disponovat efektivní procesní úpravou, která by jim práci usnadňovala. Boj s kyberkriminalitou nikterak neulehčuje ani fakt, že velká část kybernetických útoků, není orgánům činným v trestním řízení vůbec oznámena. Trestní řád disponuje řadou procesních institutů, které vyšetřování kybernetické kriminality usnadňují, kdy se specificky jde jmenovat institut domovních prohlídek, od-

[47] CCDCOE. Locked Shields. Tallinn: CCDCOE. In: ccdcoe.org. [online]. [cit. 29. 10. 2023]. Dostupné z: https://ccdcoe.org/exercises/locked-shields/

poslechů a záznamů telekomunikačního provozu, vyžádání údajů o uskutečněném telekomunikačním provozu a operativně pátrací prostředky. Procesní nedostatek lze spatřovat v poměrně dlouhých lhůtách, se kterými trestní řád, potažmo zákon o mezinárodní justiční spolupráci, pracuje, což se z hlediska vyšetřování kybernetické trestné činnosti nemusí jevit vždy jako dostačující. Extrémní dynamičnost digitálních stop může zapříčinit, že po určité době již stopy nebudou existovat, případně dojde k jejich modifikaci. Nelehká situace se jeví i v případě prokazování viny za pomocí digitálních stop, potažmo elektronických důkazů, u kterých zpravidla nelze jednoznačně a bez důvodných pochybností dovodit, že daná osoba čin skutečně spáchala, a to vzhledem k možnosti jejich snadné manipulace.

Kyberkriminalita klade nároky nejen na zákonodárce a orgány činné v trestním řízení, nýbrž na každého uživatele internetu. Kromě problematiky týkající se potrestání samotného pachatele je stěžejní i otázka prevence, která by měla směřovat vůči každému koncovému uživateli internetu, neboť právě ten bývá velmi často terčem útoku. Prevence by měla především měla cílit na rizikové skupiny, jako jsou děti a mládež. Nejen, že tyto skupiny bývají kvůli své důvěřivosti velmi často oběťmi útoků, ale stávají se mnohdy jejich samotnými pachateli. Klíčové pro boj s touto trestnou činností je rovněž posilování mezinárodní spolupráce, neboť kyberkriminalita se zřídka omezuje na hranice jednoho státu.

Třebaže ze statistických údajů vyplývá, že kybernetická trestná činnost tvoří poměrně nepodstatnou výseč veškeré páchané trestné činnosti, nelze z těchto důvodů danou problematiku opomíjet. Jak bylo již zmíněno, jde o činnost nadmíru latentní a ve většině případů neregistrovanou. Vzhledem k její dynamické proměnlivosti a zdlouhavé reakci zákonodárce, lze tvrdit, že pachatelé budou vždy při páchání kyberzločinu o krok před zákonem. Z těchto důvodů je stěžejní vytvořit takový obecný legislativní základ, který bude připraven vypořádat se s budoucím technologickým vývojem, a tudíž i novými způsoby páchání trestné činnosti. Klíčové pro objasňování kyberkriminality je rovněž zajištění proškolených odborníků na straně vyšetřovatelů. Zvyšující se nároky jsou mimo to kladeny i na samotný stát, který bude muset do budoucna být schopen zabezpečit kritické informační sys-

témy a infrastrukturu, neboť lze očekávat, kupříkladu z důvodu probíhající digitalizace veřejné správy, že bude docházet k nárůstu kybernetických útoků směřujících vůči státu. Závěrem je nutné dodat, že nicméně ty největší nároky v boji proti kyberkriminalitě leží na každém z nás.

9. SEZNAM POUŽITÝCH ZDROJŮ

[1] BERTHÉLÉMY, Chloé. New Belgian data retention law: a European blueprint? In: *EDRi*. [online]. 2021 [cit. 24. 8. 2023] Dostupné z: https://edri.org/our-work/new-belgian-data-retention-law-a-european-blueprint/

[2] CCDCOE. Locked Shields. Tallinn: CCDCOE. In: ccdcoe.org. [online]. [cit. 29. 10. 2023]. Dostupné z: https://ccdcoe.org/exercises/locked-shields/

[3] ČÁP, Jan, Lukáš BREU a Zdeněk PROKEŠ. Zajišťování, zpřístupňování a vyhodnocování digitálních stop. *Bezpečnostní teorie a praxe*. 2022. ISSN: 1801-8211.

[4] DOSTÁL, Otto. Zajišťování důkazů u počítačové kriminality – odposlech a údaje o komunikaci (2. díl). *Trestněprávní revue*. 2019, č. 4, s. 77–83. ISSN 1213-5313.

[5] European Parliament. Cybersecurity: main and emerging threats. In: euparl.europa.eu. [online]. 21.3.2023. [cit. 30.10.2023]. Dostupné z: https://www.europarl.europa.eu/pdfs/news/expert/2022/1/story/20220120STO21428/20220120STO21428_en.pdf

[6] European Union Agency For Criminal Justice Cooperation. Joint investigation teams. In: *eurojust.europa.eu*. [online]. [cit. 24. 8. 2023]. Dostupné z: https://www.eurojust.europa.eu/judicial-cooperation/eurojust-role-facilitating-judicial-cooperation-instruments/joint-investigation-teams.

[7] Google Threat Analysis Group (TAG). Fog of War – How the Ukraine Conflict Transformed the Cyber Threat Landscape. In: services.google. [online]. 16. 2. 2023. [cit. 29. 10. 2023]. Dostupné z: https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

[8] GRUSTNIY, Leonid. Browser-in-the-browser attack: a new phishing technique. In: kaspersky.com. [online]. 25. 5. 2022. [29. 10. 2023]. Dostupné z: https://www.kaspersky.com/blog/browser-in-the-browser-attack/44163/

[9] GUERRA, José Eduardo a Christine JANSSENS. Legal and Practical Challenges in the Application of the European Investigation Order. In: *EUCRIM – The European Criminal Law Associations Forum*. [online]. 2019, vol. 1, s. 48–49 [cit. 24. 8. 2023]. Dostupné z: https://eucrim.eu/media/issue/pdf/eucrim_issue_2019-01.pdf

[10] HEJDUK, Marek. Kriminalistické aspekty odhalování, prověřování a vyšetřování počítačové mravnostní kriminality. *Bezpečnostní teorie a praxe*. 2021, č. 1. ISSN: 1801-8211.

[11] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z.s.p.o., 2016, 524 s. ISBN 978-80-88168-18-8.

[12] Ministerstvo vnitra České republiky. *Statistiky kriminality – dokumenty (hodnocení bezpečnostní situace, statistiky kriminality)*. Zpráva o situaci v oblasti veřejného pořádku a vnitřní bezpečnosti na území České republiky [online]. Poslední změna 17. 7. 2023. [cit. 24. 8. 2023]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx.

[13] Nález Ústavního soudu ze dne 22. 5. 1997, sp. zn. III. ÚS 287/96.

[14] Národní úřad pro kybernetickou a informační bezpečnost. Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025. In: *NUKIB.cz*. [online]. 26. 7. 2021. [cit. 24. 8. 2023]. Dostupné z: Národní úřad pro kybernetickou a informační bezpečnost - Strategie / Akční plán (nukib.cz).

[15] Národní úřad pro kybernetickou a informační bezpečnost. Národní strategie kybernetické bezpečnosti České republiky na období let 2021-2025. In: *NUKIB.cz*. [online]. 2. 12. 2020. [cit. 24. 8. 2023]. Dostupné z: Národní úřad pro kybernetickou a informační bezpečnost - Strategie / Akční plán (nukib.cz).

[16] NÚKIB. Kybernetické incidenty pohledem NÚKIB [online]. 2022 [cit. 29. 10. 2023]. Dostupné z: https://nukib.cz/download/publikace/vyzkum/03-2022-Novinky.pdf

[17] NÚKIB. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2022. [online] 2023, s. 15. [cit. 28. 10. 2023]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf

[18] POLČÁK, Radim a kol. *Elektronické důkazy v trestním řízení*. 1. vydání. 2015. Brno: Masyrykova univerzita, Právnická fakulta, 2015. 253 s. Spisy Právnické fakulty Masarykovy univerzity, řada teoretická, Edice Scientia č. 542. ISBN 978-80-210-8073-7.

[19] PORADA, Viktor a Eduard BRUNA. Digitální svět a dokazování obsahu elektronických dokumentů. *Bezpečnostní technologie, systémy a management*. [online]. 2013. [cit. 24. 8. 2023]. Dostupné z: http://trilobit.fai.utb.cz/Data/Articles/PDF/37bacb88-3602-4ea7-b9c8-7864970f89e7.pdf

[20] PORADA, Viktor a Jiří STRAUS. *Kriminalistika (výzkum, pokroky, perspektivy)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2014, 704 s. ISBN 978-80-7380-477-0.

[21] PORADA, Viktor a kolektiv. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016, 1024 s. ISBN 978-80-7380-589-0.

[22] POŽÁR, Josef a Václav HNÍK. *Specifické problémy boje s kybernetickou kriminalitou* [online]. Praha: Policejní akademie ČR v Praze - Fakulta bezpečnostního managementu. [cit. 24. 8. 2023]. Dostupné z: http://www.mvcr.cz/soubor/policejni-akademie.aspx

[23] ROJSZCZAK, Marcin. The uncertain future of data retention laws in the EU: Is a legislative reset possible? *The computer law and security report*. [online]. 2021, roč. 41. ISSN 0267-3649. Dostupné z: https://doi.org/10.1016/j.clsr.2021.105572.

[24] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018, 936 s. ISBN 978-80-7380-720-7.

[25] Směrnice Evropského parlamentu a Rady 2022/2555 ze dne 14. 12. 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii.

[26] ŠÁMAL, Pavel, Jan MUSIL, Josef KUCHTA a kolektiv. *Trestní právo procesní*. 4. přepracované vydání. Praha: C. H. Beck, 2013, 1065 s. ISBN 978-80-7400-496-4.

[27] Usnesení Nejvyššího soudu ze dne 15. 12. 2010, sp. zn. 5 Tdo 1312/2010.

[28] Usnesení Nejvyššího soudu ze dne 29. 11. 2011, sp. zn. 4 Pzo 5/2011.

[29] Usnesení Nejvyššího soudu ze dne 7. 5. 2019, sp. zn. 4 Tdo 1591/2018.

[30] Usnesení Ústavního soudu ze dne 3. 10. 2013, sp. zn. III. ÚS 3812/2012.

[31] VEBER, Jaromír, Zdeněk SMUTNÝ a Ladislav VYSKOČIL. Practice of Digital Forensic Investigation in the Czech Republic and ISO/IEC 27037:2012 [in Czech]. *Acta Informatica Pragensia*. 2015, roč. 4. s. 244-257. ISSN: 1805-4951.

[32] Výkladové stanovisko poř. č. 1/2015 Sb. v. s. Nejvyššího státního zastupitelství ke sjednocení výkladu zákonů a jiných právních předpisů k problematice zjišťování obsahu mobilních telefonů a jiných datových nosičů, včetně obsahu e-mailových schránek ze dne 26. ledna 2015, sp. zn. 1 SL 760/2014.

---

https://doi.org/10.5817/RPT2023-2-3

PŘEHLED AKTUÁLNÍ JUDIKATURY II/2023

ANNA BLECHOVÁ, KRISTÝNA BÓNOVÁ, MARTIN ERLEBACH, ŠIMON CHVOJKA, ANEŽKA KARPJÁKOVÁ, ANDREJ KRIŠTOFÍK, PAVEL LOUTOCKÝ, TINA MIZEROVÁ, KRISTÝNA MLČÁKOVÁ, JAKUB STOJAN, JAKUB VOSTOUPAL

1. PRÁVO DUŠEVNÍHO VLASTNICTVÍ A AUTORSKÉ PRÁVO

VÝJIMKA SOUKROMÉ KOPIE A SDĚLOVÁNÍ DÍLA VEŘEJNOSTI V KONTEXTU IPTV SLUŽEB

Soud: Soudní dvůr Evropské unie
Věc: C-426/21
Datum: 13. 7. 2023
Dostupnost: curia.europa.eu

Společnost Ocilion[1] poskytuje svým zákazníkům[2] službu IPTV, jejímž prostřednictvím vysílá obsah televizních programů ve prospěch koncových uživatelů. Práva spojená s obsahem drží společnost Seven.One a další.[3,4] Služba má formu *on premises*[5] nebo cloudového řešení a umožňuje sledovat programy s časovým odstupem díky online videorekordéru. Podnět k záznamu dává uživatel aktivací funkce a zvolením obsahu k zaznamenání. Je vy-

[1] Ocilion IPTV Technologies GmbH.

[2] Např. provozovatelé sítě nebo zařízení jako hotely, stadiony apod.

[3] Seven.One Entertainment Group GmbH a Puls 4 TV GmbH und Co.KG.

[4] Bod 2 anotovaného rozhodnutí.

[5] V takovém případě poskytuje provozovatelům sítě hardware i software, který je spravován těmito provozovateli a Ocilion pro ně zajišťuje technickou podporu.

užívána technika deduplikace, která zabraňuje vytváření kopií[6] obsahově shodných záznamů.[7]

Seven.One a další podaly návrh na předběžné opatření, které směřovalo k zákazu společnosti Ocilion zpřístupňovat obsahy programů nebo je rozmnožovat či umožnit rozmnožení bez jejich souhlasu. Návrhu bylo v prvním stupni vyhověno, v odvolacím řízení bylo rozhodnutí potvrzeno. Ocilion tedy podala kasační opravný prostředek k Nejvyššímu soudu.[8]

Nejvyšší soud položil Soudnímu dvoru dvě předběžné otázky:

1. Je aplikovatelná výjimka „soukromé kopie“ v případě služby online videorekordéru poskytované společností Ocilion?[9]
2. Jedná se o sdělování veřejnosti v případě *on premises* řešení?[10]

Předběžná otázka se týkala výkladu čl. 3 odst. 1[11] a čl. 5 odst. 2 písm. b)[12] ve spojení s čl. 2 směrnice InfoSoc.[13]

Soudní dvůr v případě první otázky zejména akcentoval cíle Směrnice.[14] Dále upozornil na dvojí charakter předmětné služby – přenos televizního vysílání a nástroj pro online nahrávání, přičemž služba online nahrávání se týká vysílání přenášených v rámci IPTV, není tedy autonomní a představuje přidanou hodnotu služby.[15] Technika deduplikace umožňuje zpřístupnění

---

[6] Kopie je pak zpřístupněna i dalším uživatelům, kteří chtějí sledovat tentýž obsah.

[7] Body 12-14 anotovaného rozhodnutí.

[8] Body 16-18 anotovaného rozhodnutí.

[9] Body 20 a 24.

[10] Body 22 a 24.

[11] Čl. 3 odst. 1 směrnice InfoSoc upravuje povinnost členských států poskytnout autorům výlučné právo udělit souhlas nebo zakázat jakékoliv sdělení jejich děl veřejnosti.

[12] Čl. 5 odst. 2 písm. b) směrnice InfoSoc se týká možnosti členských států stanovit výjimky a omezení práva na rozmnožování, konkrétně tzv. výjimky soukromé kopie, tj. rozmnoženiny vytvořené fyzickou osobou pro soukromé užití a pro účely, které nemají komerční charakter za podmínky, že nositelé práv získají spravedlivou odměnu. Rakouská republika využila možnosti, kterou ji toto ustanovení přiznává viz § 42 odst. 4 a § 76 odst. 3 UrhG.

[13] Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti.

[14] Konkrétně zajištění rovnováhy mezi zájmy nositelů práv a zájmy uživatelů a ochranu zájmu autorů.

[15] Body 42 a 43 anotovaného rozhodnutí.

kopie předem neurčenému počtu příjemců.[16] Soudní dvůr tak dovodil, že uplatnění výjimky by v předmětné věci mohlo ohrozit zmíněné cíle Směrnice.[17]

K zodpovězení druhé otázky bylo nutné zapojit tzv. doplňující kritéria, a to nepominutelnou úlohu poskytovatele a vědomou povahu jeho zásahu. Ocilion neposkytuje uživatelům přístup k dílům, poskytuje pouze hardware a software provozovatelům sítě. Soud tak dovodil, že mezi poskytnutým hardwarem a softwarem a koncovými uživateli neexistuje přímá vazba a předmětná služba nemůže být považována za sdělování veřejnosti.[18] Zároveň pouhá skutečnost, že Ocilion ví, že daná služba může být využita pro přístup k chráněným dílům bez souhlasu nositelů práv, nenaplňuje pojem sdělování veřejnosti.[19]

Soudní dvůr stanovil, že v předmětné věci nelze na službu online nahrávání uplatnit výjimku „soukromé kopie“ a v případě *on premises* řešení se nejedná o sdělování veřejnosti.[20]

Autorka: KM

2. SOUKROMÍ A OSOBNÍ ÚDAJE

POUŽITÍ TECHNOLOGIÍ NA ROZPOZNÁNÍ OBLIČEJE PRO IDENTIFIKACI PROTESTUJÍCÍHO V RUSKU

Soud: Evropský soud pro lidská práva
Věc: Glukhin v Russia (stížnost č. 11519/20)
Datum: 26. 4. 2023
Dostupnost: hudoc.echr.coe.int

Stěžovatel protestoval proti zatčení jiného aktivisty, Konstantina Kotova tak, že cestoval moskevským metrem s kartonovou postavou Kotova s nápisem „I *am facing five years in prison for peacefull protests*.“ V moskevském

[16] Bod 46 anotovaného rozhodnutí.

[17] Bod 49 anotovaného rozhodnutí.

[18] Body 60-64 anotovaného rozhodnutí.

[19] Bod 65 anotovaného rozhodnutí.

[20] Bod 68 anotovaného rozhodnutí.

metru byly nainstalovány bezpečnostní kamery vybavené technologií na rozpoznávání obličeje, které dle stěžovatele policie použila k jeho identifikaci. Stěžovatel byl shledán vinným ze spáchání přestupku protestování bez předchozího oznámení příslušným autoritám a musel zaplatit pokutu 20 000 rublů (asi 283 eur).[21] S odvoláním stěžovatel neuspěl, a proto se obrátil na Evropský soud pro lidská práva.

Ve své stížnosti namítal porušení svého práva na svobodu projevu a shromažďování,[22] a také svého práva na ochranu soukromého a rodinného života, do kterého měly ruské správní orgány zasáhnout nepřiměřeným užitím technologie na rozpoznání obličeje ve správním řízení.

ESLP řešil, zda využití technologií na rozpoznávání obličeje v přestupkovém řízení představuje zásah do soukromí stěžovatele. Dle Úmluvy musí být jakýkoliv zásah do soukromí (1) v souladu se zákonem, (2) nezbytný v demokratické společnosti, (3) sledovat některý z legitimních cílů. Dále ESLP připomněl, že stěžejní součástí práva na soukromí je ochrana osobních údajů, kdy právo musí zajistit, aby jakékoliv použití osobních údajů bylo v souladu s výše uvedenými limity. Údaje o politickém smýšlení osob navíc patří mezi obzvlášť citlivá data, kterým přísluší vyšší stupeň ochrany.[23]

ESLP se zde zabýval zejména otázkou, zda bylo použití technologie pro rozpoznávání obličeje zásahem do soukromí, který je nezbytný v demokratické společnosti. Při posuzování této otázky je třeba vzít v úvahu závažnost trestných činů, které lze s jejich pomocí odhalit.[24] Zde byl navíc stěžovatel shledán vinný za přestupek, který podle ESLP představoval zásah i do jeho práv na svobodu projevu a shromažďování. ESLP proto stěžovateli vyhověl, a konstatoval, že využití technologie k rozpoznávání obličejů v tomto případě není nezbytným opatřením v demokratické společnosti a představuje zásah do práva na soukromý a rodinný život stěžovatele.[25]

---

[21] Bod 15 anotovaného rozhodnutí.

[22] Článek 10 a 11 Evropské úmluvy o ochraně lidských práv.

[23] Bod 75 a 76 anotovaného rozhodnutí.

[24] Bod 87 anotovaného rozhodnutí.

[25] Bod 90 a 91 anotovaného rozhodnutí.

Autorka: TM

PRÁVNÍ ZÁJEM NA POSKYTNUTÍ INFORMACÍ Z REGISTRU SILNIČNÍCH VOZIDEL

Soud: Krajský soud v Hradci Králové
Věc: 30 a 31/2023-44
Datum: 15. 6. 2023
Dostupnost: vyhledavac.nssoud.cz

Žalobce, který zastupuje správce parkování ve městě Pula, požadoval od správních orgánů sdělení identifikačních údajů 20 majitelů vozidel z registru silničních vozidel. Tato vozidla totiž stála ve městě Pula bez uhrazení poplatku za parkování, což dokládala přiložená fotodokumentace, a údaje měly sloužit k jeho dodatečnému vymožení.[26]

Hlavní otázkou v soudním řízení byl výklad pojmu „právní zájem“, který musí žadatel pro poskytnutí informací z registru vozidel prokázat.[27]

Krajský soud navázal na judikaturu Nejvyššího správního soudu[28] a shledal, že právní zájem může spočívat i v odpovědnostním vztahu mezi žadatelem o informace a majitelem vozu. Existenci tohoto vztahu přitom měl z přiložených fotografií za dostatečně prokázanou.[29] Ačkoliv krajský soud shledal elementární procesní pochybení správních orgánů – konkrétně, že právní předpisy aplikované prvoinstančním orgánem (týkající se přeshraniční spolupráce veřejných orgánů v trestních věcech) jsou nepřiléhavé,[30] což sice odvolací orgán napravil, nicméně nepřezkoumatelně, jelikož neuvedl jakoukoliv hlubší úvahu o neprokázání právního zájmu[31] –

[26] Body 2 a 19 anotovaného rozhodnutí.

[27] § 5 odst. 7 písm. a) zákona č. 56/2001 Sb. o podmínkách provozu vozidel na pozemních komunikacích.

[28] Konkrétně rozsudek Nejvyššího správního soudu ze dne 13. 8. 2020, č. j. 1 As 387/2019-56, č. 4064/2020 Sb. NSS.

[29] Body 28 a 29 anotovaného rozhodnutí.

[30] Bod 24 anotovaného rozhodnutí.

[31] Bod 26 anotovaného rozhodnutí.

zároveň uzavřel, že pokud se v dalším řízení zásadně nezmění skutkové okolnosti, je na místě informace z registru vozidel poskytnout.[32]

Autor: ŠCh

OSOBNÍ ÚDAJE SUBJEKTU ÚDAJŮ VS. OSOBNÍ ÚDAJE ZAMĚSTNANCE SPRÁVCE

Soud: Soudní dvůr Evropské unie
Věc: C-579/21
Datum: 22. 6. 2023
Dostupnost: curia.europa.eu

Bývalý zaměstnanec společnosti Pankki S podal této bance žádost o informace, kteří zaměstnanci, kdy a za jakým účelem nahlíželi v době, kdy byl zaměstnancem, do jeho údajů jakožto klienta této banky. Informace mu nebyly poskytnuty s odůvodněním, že se zároveň jedná o osobní údaje daných zaměstnanců.[33] Žádost zamítl i Úřad pověřence pro ochranu osobních údajů.[34] Proti rozhodnutí Úřadu podal bývalý zaměstnanec žalobu k soudu, který SDEU položil následující předběžné otázky:

1. Zda má podle čl. 15 odst. 1 GDPR subjekt údajů právo na poskytnutí informace shromažďované správcem, z níž vyplývá, kdo osobní údaje subjektu údajů, kdy a k jakému účelu zpracovával i přesto, že se jedná o údaje, které se týkají zaměstnanců správce;
2. zda účel zpracování zakládá právo na přístup k protokolovým souborům uživatele, které shromáždil správce, jako jsou například informace o osobních údajích osob provádějících zpracování osobních údajů subjektu údajů, době a účelu tohoto zpracování.[35]

[32] Bod 30 anotovaného rozhodnutí.

[33] Bod 22 rozhodnutí.

[34] Bod 25 rozhodnutí.

[35] Bod 28 rozhodnutí.

Prvně SDEU vyjasnil, že pro časovou působnost GDPR postačuje, že žádost byla podána po nabytí účinnosti nařízení a že na její posouzení nemá vliv skutečnost, že společnost vykonává regulovanou činnost.[36]

SDEU pokládal za podstatné, že žadatel nepožadoval informace o totožnosti zaměstnanců z důvodu, že ve skutečnosti nejednali z pověření a v souladu s pokyny správce, ale protože pochyboval o pravdivosti, resp. dostatečnosti informací týkajících se účelu těchto nahlížení.[37]

SDEU rozhodl, že informace o operacích nahlížení do osobních údajů subjektu, které se týkají dat a účelů těchto operací, jsou informacemi, které má tento subjekt právo získat od správce podle tohoto ustanovení. GDPR naopak toto právo neupravuje, pokud jde o informace o totožnosti zaměstnanců uvedeného správce, kteří prováděli tyto operace z jeho pověření a v souladu s jeho pokyny, ledaže jsou tyto informace nezbytné k tomu, aby subjekt údajů mohl účinně vykonávat práva, která mu toto nařízení přiznává, a za podmínky, že jsou zohledněna práva a svobody těchto zaměstnanců.[38]

Autorka: KB

POSOUZENÍ PORUŠENÍ GDPR ORGÁNEM OCHRANY HOSPODÁŘSKÉ SOUTĚŽE

Soud: Soudní dvůr Evropské unie
Věc: C-252/21
Datum: 4. 7. 2023
Dostupnost: curia.europa.eu

Německý spolkový úřad pro hospodářskou soutěž v únoru 2019 zakázal společnosti Meta Platforms Ireland (Meta) provozující Facebook, aby podmiňovala, na základě všeobecných podmínek, užívání služby Facebook soukromými uživateli z Německa zpracováním jejich údajů získaných mimo

[36] Body 36 a 89 rozhodnutí.

[37] Bod 81 rozhodnutí.

[38] Bod 84 rozhodnutí.

Facebook. Údaji získanými mimo Facebook jsou ty, které Meta získala buď z ostatních poskytovaných služeb (Instagram, WhatsApp…) nebo jiným způsobem.[39] Současně přikázal společnosti Meta změnit tyto podmínky tak, aby bylo možné shromažďovat údaje mimo Facebook pouze na základě informovaného souhlasu soukromého uživatele.[40]

Rozhodnutí bylo podloženo nejen tím, že takové chování je zneužíváním dominantního postavení, ale také, že chování společnosti Meta je v rozporu s GDPR (konkrétně čl. 6 odst. 1 a čl. 9 odst. 2). Proti tomuto rozhodnutí Meta podala žalobu.

Z následujícího soudního řízení pak vzešlo velké množství předběžných otázek jejichž jádrem je:

1. Je slučitelné s čl. 51 GDPR, že o porušení GDPR rozhoduje orgán ochrany hospodářské soutěže, přestože není dozorovým úřadem ve smyslu čl. 51 GDPR a nesídlí ve státě, kde má provozovatel služby hlavní provozovnu?
2. Je získání citlivých údajů prostřednictvím údajů získaných mimo Facebook (např. při zobrazení stránky pro seznamování homosexuálů a jeho zaznamenání pomocí souborů cookies) zpracováním citlivých údajů? a pokud ano, je kliknutím na tlačítko „To se mi líbí“ nebo obdobné tlačítko umístěné na této internetové stránce mimo Facebook zjevným zveřejněním ve smyslu čl. 9 odst. 2 e) GDPR?
3. Jsou oprávněné zájmy a nutnost pro splnění smlouvy uváděné společností Meta jako právní důvod zpracování osobních údajů dostatečné pro všechna zpracování, která provádí?[41]

Soudní dvůr odpověděl, že pokud je pro posouzení zneužití dominantního postavení třeba zhodnotit i soulad s jinými právními předpisy než jen s předpisy ochrany hospodářské soutěže, je možné v takovém kontextu taktéž konstatovat jejich porušení. To ovšem pouze pokud je to nutné k pod-

[39] Bod 28 anotovaného rozhodnutí.

[40] Bod 29 anotovaného rozhodnutí.

[41] Bod 35 anotovaného rozhodnutí.

ložení zjištění, že dochází ke zneužití dominantního postavení.[42] Při takovém rozhodnutí se úřad pro hospodářskou soutěž nemůže odchýlit od rozhodovací praxe svých národních soudů a dozorového orgánu podle GDPR.

Dále pak, že získání citlivých údajů pomocí nástrojů umístěných mimo Facebook je také zpracování citlivých údajů. Samotná návštěva stránek s integrovaným nástrojem Facebooku pak není zjevným zveřejněním tohoto údaje, ovšem právě uváděné kliknutí na tlačítko „To se mi líbí" jím je.[43]

Ke třetí otázce se Soudní dvůr vyjádřil tak, že zpracování, která společnost Meta uvedla jako nutná ke splnění smlouvy nejspíše nebude možné provádět pod tímto právním základem, konkrétní řešení ovšem leží na národních soudech. Ve spojení s tímto závěrem pak Soudní dvůr také doplnil, že v případě neexistujícího souhlasu ke zpracování osobních údajů za účelem poskytování personalizované reklamy, nemůže společnost Meta založit toto zpracování na oprávněném zájmu, a to i přesto, že touto aktivitou financuje svou činnost.[44]

Autor: ME

SÚKROMIE AKO ANONYMIZÁCIA DIGITÁLNEHO ARCHÍVU NOVÍN A SLOBODA PREJAVU

Soud: Európsky súd pre ľudské práva
Věc: Hurbain proti Belgicku (sťažnosť č. 57292/16)
Datum: 04.07.2023
Dostupnost: hudoc.echr.coe.int

Predmetný prípad sa zaoberá konfliktom práva na ochranu súkromného a rodinného života, resp. práva na to byť zabudnutý a práva na slobodu prejavu, resp. šírenie informácií. Konkrétne sa jedná o prípad belgického občana „G" (v tomto rozhodnutí ako vedľajší účastník), ktorý v roku 1994

[42] Body 62 a 63 anotovaného rozhodnutí.

[43] Body 84 a 85 anotovaného rozhodnutí.

[44] Body 125 a 126 anotovaného rozhodnutí.

pri dopravnej nehode pod vplyvom alkoholu usmrtil niekoľko osôb, za čo bol odsúdený. Po vykonaní trestu bolo jeho odsúdenie zahladené. O predmetnej nehode informovalo periodikum Le Soir (vydavateľ, ktorého je sťažovateľom) v rámci článku o narastajúcom počte nehôd v roku 1994.[45] Periodikum v roku 2008 spustilo voľne dostupný online archív, v ktorom bol aj článok o dopravnej nehode z roku 1994 a uvádzal plné meno účastníka „G".[46]

„G" sa domáhal odstránenia článku z archívu sťažovateľa, alebo aspoň jeho anonymizácie, nakoľko bol tento článok prvým výsledkom po zadaní jeho mena do vyhľadávača Google, zároveň poukázal na to, že to pre neho ako pre lekára znamená stratu klientov, ktorí ho takto vyhľadávajú.[47] Prvé senátne rozhodnutie ESĽP v tejto veci bolo vydané v roku 2021. To na základe testu predstaveného v prípade Axel Springer AG proti Nemecku[48] rozhodlo v prospech G,[49] pričom upozornil na skutočnosť, že sťažovateľ udržuje 3 archívy – pôvodnej papierovej tlače, verejný digitálny archív a neverejný digitálny „master file", rozhodnutie súdu ponechalo 2 z nich bez zásahu, čím bola podľa súdu naplnená proporcionalita obmedzenia.[50] V teste založenom v prípade Axel Springer rozhodlo najmä, že G nie je verejne činná či známa osoba a publikácia neprispieva k verejnej diskusii, význam má nanajvýš štatisticky a preto nie je potrebné uvádzať celé meno G.[51] Súd sa tiež stotožnil s názorom, že výsledok tohoto testu, má byť citlivý k plynutiu času, teda že aj ak bola prvotná publikácia oprávnená, neznamená to že jej udržiavanie v podobe digitálneho archívu po určitom čase je legitímna rovnakým spôsobom.[52]

Sťažovateľ sa s týmto názorom nestotožnil a nakoľko namietal, že sa jedná o novú, doposiaľ nerozhodnutú otázku – udržovania digitálneho

[45] Bod 13 anotovaného rozhodnutia.

[46] Bod 14 anotovaného rozhodnutia.

[47] Body 15 a 17 anotovaného rozhodnutia.

[48] Bod 135 anotovaného rozhodnutia.

[49] Bod 134 anotovaného rozhodnutia.

[50] Bod 136 anotovaného rozhodnutia.

[51] Bod 225 anotovaného rozhodnutia.

[52] Body 154, 141, 151 anotovaného rozhodnutia.

archívu, vec sa dostala pre veľký senát ESĽP.[53] Ten prakticky hneď v úvode rovnako poukázal na otázku plynutia času, ako aj rozdielne kritéria pre posudzovanie udržiavania (integrity) digitálneho archívu, k čomu stanovuje nový zvláštny test.[54] V rámci toho sa má posudzovať súčasný záujem na verejnosti informácie, činnosť osoby od zverejnenia informácie ako aj doba, ktorá od jej zverejnenia uplynula.[55] Zároveň však súd upozorňuje, že nie je nutné v každom prípade aplikovať všetky stanovené kritériá.[56] Súd sa ďalej zaoberal otázkou delistingu a deindexácie,[57] ktoré vníma ako dva rozdielne prístupy k ochrane súkromia vo vzťahu k digitálnej informácii. Preto podľa súdu nie je predmetné, či sa osoba domáhajúca sa odstránenia informácie zo stránky vydavateľa domáhala deindexingu u prevádzkovateľa internetového vyhľadávača.[58]

V nadväznosti na stanovenie tohto testu si súd uvedomuje vznik možného chilling efektu, kedy by médiá prestali plniť rolu digitálneho archívu z dôvodu nutnosti vykonávať tento test kontinuálne aby zabezpečili anonymizáciu po dostatočne dlhej dobe od publikácie. Súd k tomu preto uvádza, že udržiavateľ digitálneho archívu je povinný vykonať tento test, a prípadne publikáciu anonymizovať, len v dôsledku žiadosti osoby, do ktorej práva na súkromný život publikácia zasahuje.[59] Zároveň súd aplikáciu testu sprísňuje stanovením dôkazného bremena, kedy osoba žiadajúca o anonymizáciu musí preukázať závažný dopad na osobný život, vyplývajúci z kontinuálnej dostupnosti danej informácie.[60]

Súd po opise všetkých stanovených kritérií pristúpil k ich identifikácii v rozhodnutí národného súdu, a dospel k záver, že v rozsahu akom ich stanovuje toto rozhodnutie boli naplnené aj národným súdom a preto dospel k záveru, že anonymizácia uverejneného článku, ktorý fakticky

[53] Bod 203 anotovaného rozhodnutia.

[54] Bod 205 anotovaného rozhodnutia.

[55] Tamtiež.

[56] Body 206, 241 anotovaného rozhodnutia.

[57] Bod 175 anotovaného rozhodnutia.

[58] Bod 208 anotovaného rozhodnutia.

[59] Bod 209 anotovaného rozhodnutia.

[60] Bod 210 anotovaného rozhodnutia.

vytváral „virtuálny záznam v trestnom registri“ G nebola neprimeraným zásahom do práv sťažovateľa.[61]

Autor: AK

SPISOVÁ ZNAČKA JAKO JEDNOZNAČNÝ IDENTIFIKÁTOR SUBJEKTU

Soud: Nejvyšší správní soud
Věc: 3 As 76/2022
Datum: 24. 8. 2023
Dostupnost: nssoud.cz

Žalovanému Krajskému soudu v Ostravě byla dle zákona 106/1999 Sb. doručena žádost o informace týkající se počtu nahlédnutí do spisu k věci vedené pod sp. zn. 81 T 2017. Žalovaný dané žádosti vyhověl a odpověděl, že*“ ve věci 81 T 1/2017 nebyla ode dne 11.4. 2017 nalezena ani jedna žádost obžalovaného o nahlížení do spisu. Do trestního spisu nahlížel dne 4. 7. 2017 obhájce obžalovaného – Mgr. R. F“.*[62] V návaznosti na tuto skutečnost se žalobce, P. N.,[63] domáhal u žalovaného určení, že poskytnutí předmětné informace je nezákonným zásahem do jeho práv, jelikož se jedná o nepravdivou informaci.[64] Zároveň žalobce v odpovědi Krajského soudu v Ostravě spatřoval zásah do svého práva na informační sebeurčení.[65]

Krajský soud žalobu usnesením ze dne 17. 2. 2022 odmítl.[66] Zamítavé stanovisko soudu bylo založeno na skutečnosti, že v návaznosti na absenci jména, příjmení či jiného jednoznačného identifikátoru samotná spisová značka nemůže vést k identifikaci jednotlivce. Proti rozhodnutí krajského soudu pak žalobce podává kasační stížnost ve které namítá, že z veřejně

[61] Bod 255 anotovaného rozhodnutia.

[62] Bod 1 anotovaného rozhodnutí.

[63] Ačkoli se žalobce, Pavel Nárožný, který byl odsouzený za dvojnásobnou vraždu, brání proti jeho možné identifikaci v odpovědi soudu na žádost dle zákona 106/1999 Sb., dle autorky této anotace se žalobci podařilo svými kroky vytvořit tzv. efekt Streisandové.

[64] Bod 2 anotovaného rozhodnutí.

[65] Bod 4 anotovaného rozhodnutí.

[66] Bod 3 anotovaného rozhodnutí.

přístupných informací je možné identifikovat, že v řízení pod předmětnou spisovou značkou byl obžalovaným on. Toto své tvrzení opírá o „specifičnost" svého případu a fakt, že případ byl medializován.[67,68]

Právním problémem, který se v daném sporu řešil tedy je, zda poskytnuté informace, konkrétně spisová značka, umožňují přímou identifikaci fyzické osoby.[69]

Při zkoumání, zda je spisová značka jednoznačným identifikátorem fyzické osoby, a tedy osobním údajem dle čl. 4 odst. 1 GDPR,[70] je nutné vycházet z výkladu daného ustanovení a zároveň z relevantní judikatury. Tou je v tomto případě především rozsudek NSS ve věci EUROVIA[71] a rozsudek SDEU ze dne 19. 10. 2016, C-582/14, ve věci P. B.[72]

Pro zodpovězení otázky, zda je spisová značka osobním údajem je třeba dle NSS a SDEU postupovat v souladu s tzv. objektivním pojetím osobních údajů. V tomto pojetí se zjišťuje, zda někde existuje další informace, který by ve spojení s původní informací mohla vést k identifikaci subjektu.[73] Dle NSS by *„[T]akovými dalšími informacemi mohly být například jiné údaje týkající se totožného řízení zveřejněné podle informačního zákona, rozhodnutí týkající se řízení zveřejněná na webových stránkách soudů, nedostatečná pseudonymizace obžalovaného, mediální zprávy apod."*[74]

Na základě výše uvedeného NSS tedy došel k závěru, že i spisová značka, v kombinaci s dalšími informacemi, může vést k identifikaci osoby.[75] Ji-

---

[67] Konkrétně žalobce poukazoval na článek zveřejněný na www.ceskenoviny.cz dne 26.1.2021 pod názvem „Žalobce žádá pro N. doživotí, obžalovaný vinu odmítá", článek zveřejněný na www.rozhlas.cz dne 5. 2. 2021 pod názvem „Soud poslal N. na 25 let do vězení za dvojnásobnou vraždu. Těla obětí se nikdy nenašla", a článek uveřejněný na webu www.blesk.cz dne 28. 1. 2016 pod názvem „Olomoucký krajský soud definitivně prohlásil M. N. za mrtvého".

[68] Body 5 a 8 anotovaného rozhodnutí.

[69] Bod 14 anotovaného rozhodnutí.

[70] Bod 16 anotovaného rozhodnutí.

[71] Rozsudek rozšířeného senátu Nejvyššího správního soudu ze dne 21. 11. 2017, č. j. 7 As 155/2015–160, č. 3687/2018 Sb. NSS známý jako rozsudek NSS ve věci EUROVIA.

[72] Bod 17 anotovaného rozhodnutí.

[73] Bod 17 anotovaného rozhodnutí.

[74] Bod 18 anotovaného rozhodnutí.

[75] Bod 19 anotovaného rozhodnutí.

nými slovy, stejně jako např. dynamická IP adresa nebo registrační značka vozidla může být spisová značka osobním údajem.[76]

Autorka: AB

TRESTNĚPRÁVNÍ NÁSLEDKY UŽÍVÁNÍ MOBILNÍ APLIKACE

Soud:	Evropský soud pro lidská práva
Věc:	Yüskel Yalçinkaya v. Türkiye (stížnost č. 15669/20)
Datum:	26. 9. 2023
Dostupnost:	hudoc.echr.coe.int

Pan YY byl učitelem na státní škole v Kayseri. V návaznosti na neúspěšný pokus teroristické organizace FETÖ/PDY o ozbrojený převrat v červenci 2016 však byl výkon jeho funkce pozastaven a nedlouho poté byl propuštěn na základě Nařízení č. 672.[77] Z důvodu podezření pana YY z trestného činu členství v FETÖ/PDY místní státní zastupitelství a orgány činné v trestním řízení získaly povolení k prohlídce a zabavení digitálních důkazů na jeho adrese, během které došlo k jeho zatčení.[78] Hlavním důkazem, na základě kterého započalo trestní stíhání pana YY, bylo jeho údajné používání aplikace s koncovým šifrováním ByLock, která měla sloužit výhradně pro potřeby FETÖ/PDY. Dále se jednalo o jeho členství ve dvou organizacích, které byly s teroristickou skupinou spjaty, a existenci jeho bankovního účtu u společnosti Bank Asya, kterou tato skupina taktéž používala.[79]

Turecké vnitrostátní soudy přezkoumaly dostupné důkazy, vyjádřily se k několika expertním posudkům vydaným tureckými správními a bezpečnostními orgány a ve všech instancích uznaly pana YY vinným.[80]

Soud se nejprve zabýval údajným porušením čl. 7 Úmluvy, kterého se vnitrostátní soudy měly dopustit mimo jiné tím, že považovaly užívání

[76] Bod 17 anotovaného rozhodnutí.

[77] Bod 24 anotovaného rozhodnutí.

[78] Body 27-30 anotovaného rozhodnutí.

[79] Body 27 a 34-35 anotovaného rozhodnutí.

[80] Body 70, 88, 98 a 106 anotovaného rozhodnutí. YY v jednotlivých instancích vznášel různé procedurální námitky a požadoval přístup k důkazům, ve většině případů mu však nebylo vyhověno.

aplikace ByLock jako důkaz členství v FETÖ/PDY.[81] Soud po důkladném posouzení všech informací jedenácti hlasy proti šesti rozhodl, že došlo k porušení čl. 7 Úmluvy, neboť turecké soudy „[aniž] by se snažily zjistit, zda byly v konkrétním případě přítomny vědomosti a úmyslu vyžadované zákonnou definicí, [spojily] s užíváním aplikace ByLock objektivní odpovědnost".[82]

Dále Soud projednával porušení čl. 6 Úmluvy zajišťující právo na spravedlivý proces. Toto právo mělo být v daném případě porušeno tím, že obžalovaný neměl k dispozici veškeré informace spojené s případem, zejména data a metadata o uživatelích aplikace ByLock získaná bezpečnostními složkami, a to navíc nezákonným způsobem neumožňujícím přezkum a aplikaci dalších procesních zásad.[83] Soud seznal, že čl. 15 Úmluvy umožňuje omezení některých práv vyvěrajících z čl. 6, avšak upozornil, že tato omezení musí stále respektovat základní principy právního státu.[84] Vzhledem k nedostatku procesních záruk zejména z hlediska přístupnosti informací o důkazech vedených proti YY a jejich původu, a konstatoval proto šestnácti hlasy proti jednomu porušení čl. 6 Úmluvy.[85] Soud se zabýval taktéž domnělým porušením čl. 8 Úmluvy, resp. porušením práva YY na soukromý a rodinný život, které však posoudil společně s porušením čl. 6 a rozhodl se k němu blíže nevyjadřovat.[86]

V neposlední řadě se Soud blíže zabýval domnělým porušením čl. 11. Toho se turecké soudy měly dopustit (a dle jednohlasného rozhodnutí Soudu dopustily) tím, že považovaly členství v dobrovolné organizaci, která se nijak nevyznačovala protidemokratickými či násilnými myšlenkami a činy, za důkaz členství stěžovatele v teroristické organizaci.[87]

Soud tak poskytl jasný návod k tomu, kdy a za jakých podmínek je používání internetových a mobilních aplikací, které jsou spojovaný s organizací

[81] Body 68, 87-88, 98 a 106 anotovaného rozhodnutí.

[82] Bod 271 anotovaného rozhodnutí.

[83] Body 278 a 282 anotovaného rozhodnutí.

[84] Body 347 anotovaného rozhodnutí.

[85] Body 341 a 356 anotovaného rozhodnutí.

[86] Bod 373 anotovaného rozhodnutí. Toto bylo způsobeno též tím, že sám YY k tomuto bodu stížnosti neposkytl dostatek specifických informací.

[87] Bod 396 anotovaného rozhodnutí.

vykonávající trestnou činnost, možné považovat za důkaz členství uživatele v této organizaci.

Autor: JSt

AUTOMATIZOVANÉ ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PŘI KONTROLE COVID-19 CERTIFIKÁTŮ

Soud: Soudní dvůr Evropské Unie
Věc: C-659/22
Datum: 5. 10. 2023
Dostupnost: curia.europa.eu

Ministerstvo zdravotnictví stanovilo kvůli probíhající pandemii COVID-19 od začátku roku 2023 povinnost prokázat svoji bezinfekčnost při vstupu na různé akce. Tu kontrolovali pořadatelé akcí prostřednictvím aplikace čTečka tak, že načetli QR kód certifikátu účastníka akce, čímž se jim zobrazily údaje o identitě účastníka, platnosti certifikátu a případně i podobnosti o očkování.[88] Mimořádné opatření,[89] které tuto povinnost stanovilo, napadl navrhovatel s argumentací ohledně nedostatečně stanovených pravidel pro zpracování zvláštní kategorie osobních údajů.

Nejvyšší správní soud měl pochyby o tom, zda při ověřování platnosti certifikátu dochází k automatizovanému zpracování podle čl. 4 odst. 2 GDPR, a tedy zda je tento předpis aplikovatelný.

Soudní dvůr velmi rychle došel k závěru, že GDPR je aplikovatelné. Nejdříve konstatoval, že informace, ke kterým má pořadatel akce přístup při kontrole certifikátu jsou osobními údaji,[90] ostatně nařízení zavádějící certifikáty na evropské úrovni[91] požadovalo, aby součástí certifikátu byla

[88] Body 13–14 a 16 anotovaného rozhodnutí.

[89] Vydané podle zákona č. 94/2021 Sb., o mimořádných opatřeních při epidemii onemocnění COVID-19.

[90] Bod 25 anotovaného rozhodnutí.

[91] Nařízení Evropského parlamentu a Rady (EU) 2021/953 ze dne 14. června 2021 o rámci pro vydávání, ověřování a uznávání interoperabilních certifikátů o očkování, o testu a o zotavení v souvislosti s onemocněním COVID-19 (digitální certifikát EU COVID) za účelem usnadnění volného pohybu během pandemie COVID-19.

i totožnost držitele.[92] Pojem „zpracování“ je pak nutné vykládat široce, a to pro zajištění účinnosti ochrany základních práv.[93] Naskenování QR kódu certifikátu – tedy postup, kdy jsou informace v něm obsažené převedeny pro kontrolující osobu do čitelné podoby – umožňuje prostřednictvím automatizovaného postupu (skenování) náhled do osobních údajů a následně rozhodnout o vpuštění na danou akci.[94] Takový postup představuje „zpracování“ podle GDPR a spadá do jeho věcné působnosti. To je navíc podpořeno i výkladem nařízení týkající se certifikátů, jelikož z jeho odůvodnění a různých článků explicitně aplikovatelnost GDPR vyplývá.[95]

Nejvyššímu správnímu soudu tak přísluší ověřit, zda toto zpracování probíhalo v souladu se zásadami stanovenými GDPR.

Autor: ŠCh

PRÁVA OSOB NÁHODNĚ DOTČENÝCH POLICEJNÍM ODPOSLECHEM

Soud:	Evropský soud pro lidská práva
Věc:	Plechlo v. Slovensko (stížnost č. 18593/19)
Datum:	26. 10. 2023
Dostupnost:	hudoc.echr.coe.int

V roce 2006 vydal slovenský Zvláštní soud příkaz k odposlechu ve věci podezření z korupce v Národní privatizační agentuře.[96] Policie tento příkaz zdárně implementovala, přičemž při pořizování záznamů došlo též k zachycení komunikace žadatele, který ale nebyl cílem odposlouchávání (toliko s těmito cíli komunikoval).[97] Přestože na základě pořízených materiálů nedošlo k žádnému obvinění, orgány činné v trestním řízení záznamy uchovaly, přičemž pak došlo k jejich zahrnutí do separátního vyšetřování

[92] Bod 26 anotovaného rozhodnutí.

[93] Body 27–28 anotovaného rozhodnutí.

[94] Bod 29 anotovaného rozhodnutí.

[95] Bod 31 anotovaného rozhodnutí.

[96] Bod 6 anotovaného rozhodnutí.

[97] Body 7 a 8 anotovaného rozhodnutí.

(v kontextu zneužití pravomoci úřední osoby, kde už žadatel figuroval jako jeden z primárních podezřelých), které bylo otevřeno v souvislosti s kauzou Gorila.[98] V roce 2016 byl žadatel na základě tohoto vyšetřování obžalován.[99]

Žadatel opakovaně namítal proti použití daných odposlechů v rámci trestního řízení proti němu, ale byl vždy ujištěn (mj. i slovenským Ministerstvem vnitra), že daný materiál nemůže být použit jako důkazní materiál a je součástí spisu pouze jako příloha k žádosti o zahájení trestního stíhání.[100] Protože žadatel nebyl cílem daného odposlechu, nemohl se ani seznámit s příkazem k odposlechu jako takovým, ani vůči němu namítat.[101] Pokusil se uplatnit své námitky vůči nakládání s odposlechy a samotnému příkazu i u Nejvyššího soudu a následně Ústavního soudu (mj. kvůli způsobu používání získaných odposlechů a jejich pokračující retenci).[102] Všechny tyto pokusy byly neúspěšné, přičemž Ústavní soud jej odkázal na možnost rozporovat důkazy v rámci trestního řízení či dožadovat se náhrady skrze civilní soudnictví.[103] V roce 2022 žadatel zemřel a trestní stíhání bylo zastaveno. Došlo ovšem k zahájení trestního stíhání proti dalším osobám, mj. na základě zmíněných odposlechů, a to s odůvodněním, že jejich použitelnost jakožto důkazu se mezitím vyvinula.[104] Syn žadatele se tak obrátil na Evropský soud pro lidská práva.

Žadatel primárně namítal porušení článků 8 a 13 Úmluvy, přičemž s přihlédnutím k faktům případu Soud podřadil tento případ čistě pod materii článku 8, a náležitostí právního zásahu do práva na soukromí.[105]

V prvé řadě se Soud zabýval otázkou, zda je možné, aby žadatelův syn pokračoval v reprezentaci nároku, a přestože vyloučil část podání pro zjevnou nekompatibilitu nároků (konkrétně v kontextu čl. 34 Úmluvy), zby-

[98] Body 9 a 10 anotovaného rozhodnutí.

[99] Bod 11 anotovaného rozhodnutí.

[100] Bod 12 anotovaného rozhodnutí.

[101] Body 15-19 a 44 anotovaného rozhodnutí.

[102] Tamtéž.

[103] Tamtéž.

[104] Bod 14 anotovaného rozhodnutí.

[105] Bod 32 anotovaného rozhodnutí.

tek podání připustil.[106] Následně se zabýval námitkou Slovenska, že nedošlo k vyčerpání všech možných nástrojů nápravy, mj. v rámci již zmíněného civilního soudnictví, tento argument ale Soud odmítl s poukazem na další případy kauzy Gorila (civilní soudnictví sice umožňuje nahradit škodu, ale nikoliv dovolat se zničení odposlechového materiálu).[107] Ve věci samé se pak Soud zaměřil na náležitosti legálního zásahu do práva na soukromí, přičemž připomněl, že nestačí, aby byl zásah postaven na právním základu, ale že je též nutná určitá kvalita těchto právních nástrojů a musí obsahovat sérii záruk, aby „*pod záštitou ochrany národa nedošlo k postupnému zničení demokracie.*“[108] S ohledem na to, že žadatel nebyl úspěšný v žádném ze svých dílčích pokusů a nebylo mu ani umožněno, aby se seznámil s konkrétním příkazem k odposlechu, došel Soud k názoru, že právní rámec (či jeho absence v konkrétním případě), sice poskytuje určité záruky osobám, jichž se odposlouchávání přímo týká, ale nenabízí osobám náhodně dotčeným při odposlechu jiných téměř žádnou právní ochranu a možnost dožádat se nápravy.[109]

Soud tak konstatoval porušení čl. 8 Úmluvy a uzavřel, že ochrana práva na soukromí se v kontextu policejních odposlechů vztahuje i na osoby tímto odposlechem náhodně dotčené, přičemž je nutné, aby tyto osoby měly k dispozici nástroje a záruky proti netransparentnímu užívání (a potenciálnímu zneužívání) získaných odposlechů.[110]

Autor: JV

[106] Body 28-31 anotovaného rozhodnutí.

[107] Jednalo se o případy *Zoltán Varga proti Slovensku* a *Haščák proti Slovensku*. Více viz bod 36 anotovaného rozhodnutí.

[108] Body 42-44 anotovaného rozhodnutí.

[109] Body 44-49 anotovaného rozhodnutí.

[110] Body 44-49 a výrok anotovaného rozhodnutí.

PUBLIKACE ZÁZNAMU Z POLICEJNÍHO ZÁSAHU A PRÁVO NA SOUKROMÍ ZASAHUJÍCÍCH POLICISTŮ

Soud: Evropský soud pro lidská práva
Věc: Bild GMBH v Germany (stížnost č. 9602/18)
Datum: 31. 10. 2023
Dostupnost: hudoc.echr.coe.int

Policie v roce 2013 zasáhla v brémském nočním klubu proti agresivnímu muži. Zásah, který zachytily bezpečnostní kamery, byl publikován deníkem Bild. Ze zveřejněného okomentovaného záznamu je zřejmé, jak několik policistů zpacifikuje muže silou a jak jeden z nich následně na muže nehybně ležícího na zemi použije obušek a kope jej.[111] Následně Bild vydal ještě jeden článek s videem, které ukazuje i chování agresivního muže před zásahem policie.[112] Jeden ze zasahujících policistů, jehož tvář byla krátce na záznamu zřejmá a který neužil nepřiměřené síly, požadoval u národních soudů zákaz publikace záznamu bez rozmazání jeho obličeje. Tomu soud vyhověl, na rozdíl od požadavku náhrady škody.[113] Odvolací soud se s tím ztotožnil a Ústavní soud stížnost deníku Bild bez dalšího odmítl.[114]

ESLP se zabýval otázkou, zda zákaz publikace záběrů bez rozmazání obličeje jednoho ze zasahujících policistů byl nezbytný v demokratické společnosti. a dospěl k závěru, že z části nikoliv.

ESLP začal analýzu tím, že veřejný zájem na publikování videa se týkal policie jako celku, a nikoliv konkrétně stěžovatele, který nezneužil svého postavení a nezapojil se do nelegální činnosti.[115] Ačkoliv i příslušníci státu musí snést vyšší míru kritiky, například při údajných pochybeních,[116] nejsou takové osoby (včetně policistů) v případě absence podezření zbave-

[111] Body 5–6 anotovaného rozhodnutí.
[112] Bod 7 anotovaného rozhodnutí.
[113] Body 9–11 anotovaného rozhodnutí.
[114] Body 13 a 14 anotovaného rozhodnutí.
[115] Bod 31 anotovaného rozhodnutí.
[116] Bod 33 anotovaného rozhodnutí.

ny ochrany před nepravdivým vyobrazováním jako zneužívajících své postavení.[117]

Problém soud shledal v rozsahu zákazu zveřejňování, který se vztahoval jak na videa v obou článcích, tak jakoukoliv budoucí publikaci. V rozsahu zveřejnění prvního videa, ze kterého může kvůli nezobrazení předchozího chování agresivního muže a doprovodného komentáře vyplývat zneužití pravomoci i ze strany žalujícího policisty, se ESLP se zákazem ztotožnil.[118] U druhého delšího videa a jakékoliv budoucí publikace to už ovšem neplatí – v tomto rozsahu neprovedly národní soudy vyvažování práv dostatečně, jelikož vyšly ze stejných argumentů jako u prvního videa.[119] Nebylo ani zřejmé, jaké negativní dopady má pro policistu budoucí zveřejňování neupraveného záznamu.[120] Jakkoliv tedy deníku Bild nebylo znemožněno o incidentu informovat a uložená povinnost rozmazat obličej není zvláště závažným omezením, ESLP dospěl k závěru, že rozhodnutí národních soudů nemohou pro absenci balancování ve vztahu k druhému videu a jakékoliv budoucí publikaci obstát.[121] Fakticky tak došlo k porušení čl. 10 Úmluvy pro nepřezkoumatelnost.

Autor: ŠCh

ZVEŘEJŇOVÁNÍ NEANONYMIZOVANÝCH ZNĚNÍ ROZSUDKŮ NA ÚŘEDNÍ DESCE NEJVYŠŠÍHO SPRÁVNÍHO SOUDU

Soud: Nejvyšší správní soud
Věc: 6 As 48/2023-52
Datum: 9. 10. 2023
Dostupnost: vyhledavac.nssoud.cz

Žalobce brojil deklaratorní zásahovou žalobou proti zveřejnění úplných znění rozhodnutí v jeho předcházejících věcech Nejvyšším správním sou-

[117] Bod 35 anotovaného rozhodnutí.

[118] Bod 39 anotovaného rozhodnutí.

[119] Body 40 a 41 anotovaného rozhodnutí.

[120] Bod 43 anotovaného rozhodnutí.

[121] Bod 44 anotovaného rozhodnutí.

dem na úřední desce soudu, jelikož součástí vyvěšeného rozhodnutí byly jeho identifikační údaje, což považoval za zbytečné a neoprávněné zpřístupňování osobních údajů.[122]

Vzhledem k tomu, že krajský soud nepovažoval Nejvyšší správní soud při vyvěšování rozhodnutí na úřední desce za správní orgán ale za orgán moci soudní,[123] bylo hlavní otázkou v řízení postavení Nejvyššího správního soudu.

Nejvyšší správní soud, po odmítnutí možnosti úspěšně uplatit námitku systémové podjatosti všech soudců a soudkyň tohoto soudu[124] a vypořádání dalších nedůležitých procesních námitek,[125] se s hodnocením krajského soudu ztotožnil. Výkon soudní moci je pojem širší, než pouze samotná rozhodovací činnost soudu a zahrnuje i činnosti s tím bezprostředně spojené.[126] Jednou z nich je i vyhlášení rozhodnutí, které má kromě zveřejnění i procesní důsledek vázanosti soudu rozhodnutím. V souladu s názorem Ústavního soudu sice není nutné zveřejňovat úplné znění rozhodnutí a postačí nosné důvody, nicméně zveřejnění anonymizované verze není dostatečné.[127] Relevantním argumentem pak nebyla ani úprava zveřejňování v interních předpisech soudu, jelikož soudci a soudkyně jsou vázány pouze Ústavou a zákonem.[128] Z odůvodnění pak i implicitně vyplývá, že Nejvyšší správní soud souhlasí s názorem krajského soudu v jeho jiném rozhodnutí, kterým žalobce taktéž argumentoval, že v případě zveřejňování anonymizovaných znění rozhodnutí v elektronické databázi postupuje jako správní orgán a nikoliv jako orgán moci soudní. Tyto dva způsoby zveřejňování rozhodnutí je nutné odlišovat.[129]

Autor: ŠCh

[122] Body 2 a 3 anotovaného rozhodnutí.

[123] Bod 34 anotovaného rozhodnutí.

[124] Bod 18 anotovaného rozhodnutí.

[125] Body 23 a 28–30 anotovaného rozhodnutí.

[126] Bod 35 anotovaného rozhodnutí.

[127] Bod 36 anotovaného rozhodnutí a tam odkazovaný nález Ústavního soudu ze dne 18. 6. 2019, sp. zn. Pl. ÚS 38/18.

[128] Bod 39 anotovaného rozhodnutí.

[129] Bod 40 anotovaného rozhodnutí, kde soud reaguje na závěry rozsudku Krajského soudu v Brně ze dne 7. 11. 2018, č. j. 31 a 68/2018-177.

3. SOCIÁLNÍ SÍTĚ A SVOBODA ŘEČI

VÝHRUŽKY POLITIKŮM NA SOCIÁLNÍCH SÍTÍCH

Soud: Nejvyšší soud
Věc: 4 Tdo 304/2023
Datum: 26. 4. 2023
Dostupnost: nsoud.cz

Dovolatel byl obecnými soudy odsouzen za zločin vydírání,[130] kterého se měl dopustit tím, že na sociálních sítích psal ministru vnitra Vítu Rakušanovi[131] zprávy ve znění: „*DEMISI TY SVINĚ FAŠISTICKÁ*;“ „*Když do 48 hodin neodstoupíš, odstraníme Tě sami, Občanská partyzánská brigáda!!!!*;“ „*Takže už jen 24 hodin!!!!*“ a „*No jak chceš, sepisuj závěť!!!!*“. Proto, že výhružky směřovaly vůči Rakušanovi, vyhodnotily nižší soudy jednání dovolatele jako vydírání spáchané pro politické přesvědčení poškozeného, a podřadily je proto pod kvalifikovanou skutkovou podstatu.

Dovolatel v dovolání namítal, že skutková zjištění jsou v rozporu s obsahem důkazů,[132] a dále poukazoval na absenci subjektivní stránky,[133] protože zločin nespáchal kvůli politickému přesvědčení Rakušana. Obecné soudy dle dovolatele nesprávně daly do souvislosti politické přesvědčení a jednotlivé kroky vlády, s nimiž nesouhlasil.

Nejvyšší soud se tak zabýval správností dokazování obecného soudu a zda dovolatel spáchal zločin kvůli politickému přesvědčení ministra Rakušana. Vzhledem k provedenému dokazovaní neshledal, že by obecné soudy pochybily.[134] Dovolání ale vyhověl proto, že dle jeho názoru dovolatel zločin nespáchal kvůli politickému přesvědčení ministra Rakušana. Dle NS k naplnění speciální skutkové podstaty vyhrožování kvůli skutečnému nebo

[130] Dle § 175 odst. 2 písm. g) zákona č. 40/2009 Sb., trestní zákoník.

[131] Navzdory anonymizaci rozhodnutí lze poškozeného identifikovat z výpovědi obžalovaného před obecnými soudy, zejména z věty: „*na svůj strach z osoby poškozeného jak tento řídi policii ČR*,“ viz bod 40 anotovaného rozhodnutí.

[132] Dovolací důvod dle § 265b odst. 1 písm. g) zákona č. 141/ 1961 Sb., trestního řádu.

[133] Dovolací důvod dle § 265b odst. 1 písm. h) zákona č. 141/ 1961 Sb., trestního řádu.

[134] Bod 33 a 36 anotovaného rozhodnutí.

domnělému politickému přesvědčení poškozeného[135] nestačí, že je poškozený členem politické strany nebo politickým funkcionářem. Je třeba, aby bylo nepochybné, že byly výhružky motivovány nesouhlasem s politickým přesvědčením poškozeného. NS závěry obecných soudů označil za předčasné a upozornil, že pokud by se všechny výhružky adresované politicky aktivním osobám považovaly za výhružky spáchané z důvodu jejich politického přesvědčení, šlo by o nepřiměřeně široký výklad této speciální skutkové podstaty.[136]

Autorka: TM

4. BOJ PROTI DEZINFORMACÍM

BLOKOVÁNÍ DEZINFORMAČNÍCH WEBŮ PO INVAZI RUSKA NA UKRAJINU

Soudy:	Městský soud v Praze a Nejvyšší správní soud
Věci:	11 a 25/2022-63 a 7 As 22/2023
Data:	11. 5. 2023 a 9. 8. 2023
Dostupnost:	justice.cz a nssoud.cz

Bezprostředně po invazi Ruských vojsk na Ukrajinu v únoru 2022 zablokovaly spolek CZ.NIC z.s.p.o. a Asociace provozovatelů mobilních sítí (APMS) přístup ke dvaceti třem dezinformačním webům. O dva měsíce později vyšlo najevo, že tak učinily na základě výzvy ze strany Národního centra kybernetických operací (NCKO) ze dne 25. 2. 2022.[137] Daný dopis nebyl veřejně publikován.[138]

Na základě tohoto postupu podaly neziskové organizace Institutte H21, z.ú. a Otevřená společnost, o.p.s., které se mimo jiné věnují ochraně svobody projevu na internetu (dále jen „žalobci“ či „stěžovatelé“), žalobu proti Ministerstvu obrany ČR (dále jen „žalovaný“) na ochranu před nezákonným zásahem podle § 82 z. č. 150/2002 Sb., soudního řádu správního (dále jen

[135] Ustanovení § 175 odst. 2 písm. g) zákona č. 40/2009 Sb., trestní zákoník.

[136] Bod 40 anotovaného rozhodnutí.

[137] Bod 1 a 4 anotovaného usnesení MS.

[138] Tamtéž.

„SŘS“).[139] K tomu mělo dojít dle žalobců tím, že žalovanému chybělo zákonné zmocnění k nařízení blokace daných webů, kterýmžto jednáním zkrátil žalobce na jejich základních právech, zejména svobodě projevu a právu vyhledávat a přijímat informace.[140] Tím, že žalovaný daný dopis nezveřejnil, se mimo jiné dopustil dle žalobců porušení principu publicity veřejné správy.[141]

Žalovaný tvrzení žalobců popřel, jelikož se dle něj nejednalo o závazný pokyn, ale pouze o nezávaznou žádost.[142] Toto tvrzení také podložil skutečností, že několik adresátů, vůči nimž dopis směřoval, žádosti nevyhovělo, přičemž žádný z nich za to nebyl jakkoliv následně postižen.[143]

Městský soud v Praze žalobu odmítl s odůvodněním, že daný dopis žalovaného skutečně představoval pouze nezávazné doporučení blokovat dané webové stránky adresované správcům konkrétních webů a mobilním operátorům a nejednalo se tedy o správní úkon.[144] Z tohoto důvodu nemůže jít o nezákonný zásah ve smyslu § 82 SŘS, jelikož jednou z obligatorních podmínek aplikace daného ustanovení je, že porušení musí být způsobeno zásahem, pokynem nebo donucením správního orgánu.[145] Soud dále konstatoval, že pokud žalobci pochopili daný dopis jako závazný příkaz, jednalo se dle soudu o nesprávnou interpretaci, kterou nelze přičítat k tíži žalovaného.[146]

Stěžovatelé tak odmítavý rozsudek Městského soudu v Praze dále napadli kasační stížností.

Nejvyšší správní soud již zamítl jednu kasační stížnost, v níž se otázkou této blokace dezinformačních webů zabýval,[147] dle stěžovatelů je ale pro

[139] Bod 2 a 3 anotovaného usnesení MS.

[140] Bod 7 anotovaného usnesení MS.

[141] Tamtéž.

[142] Bod 13 anotovaného usnesení MS.

[143] Bod 14 anotovaného usnesení MS.

[144] Bod 33 anotovaného usnesení MS.

[145] Bod 29 anotovaného usnesení MS.

[146] Bod 40 anotovaného usnesení MS.

[147] Rozsudek Nejvyššího správního soudu ze dne 9. 12. 2023, č.j. 5 As 230/2022-66.

jejich případ stěžejní zveřejnění výzvy NCKO, kterou soudy v předchozím rozhodnutí nezohlednily, protože se o její existenci ještě nevědělo.[148]

NSS zde tak posuzoval, zda je výzva NCKO nezákonným zásahem. Z judikatury NSS vyplývá, že nezákonný zásah, musí splňovat tři kritéria: (1) Jde o úkon veřejné moci, (2) který je namířen vůči jednotlivci, (3) přímo zasahuje do jeho subjektivních práv.

NSS ve shodě s Městským soudem došel k závěru, že výzva NCKO není úkonem veřejné moci, ale představuje pouze nezávazné doporučení, které není ze strany státních orgánů vynutitelné. Výzva navíc nesměřuje vůči jednotlivci, ale vůči jiným soukromým osobám, a nejedná se o zásah do subjektivních práv stěžovatelů i přesto, že se dovolávali nemožnosti přijímat z blokovaných stránek informace. Výzva NCKO tak nesplnila ani jedno ze tří výše uvedených kritérii a nepředstavuje nezákonný zásah.[149] NSS ji označil za nezávaznou politickou proklamaci doporučujícího charakteru[150] a kasační stížnost zamítl jako nedůvodnou.

Autorky: AKar a TM

5. ELEKTRONICKÉ PODPISY

ELEKTRONICKÝ PODPIS A JEHO SPECIFIKA DLE SDEU

Soud: Soudní dvůr Evropské unie
Věc: C-362/21
Datum: 20. 10. 2022
Dostupnost: curia.europa.eu

Společnost Ekofrukt (žalobkyně) je bulharskou obchodní společností s předmětem podnikání, kterým je prodej ovoce a zeleniny. U této společnosti byla provedena daňová kontrola týkající se DPH. Všechny relevantní dokumenty vydané v souvislosti s kontrolou byly daňovou správou vydány v podobě elektronických dokumentů podepsaných elektronickými

[148] Bod 4 anotovaného rozhodnutí NSS.

[149] Bod 12 anotovaného rozhodnutí NSS.

[150] Bod 13 anotovaného rozhodnutí NSS.

podpisy. Společnost Ekofrukt v rámci souvisejícího soudního řízení zpochybnila platnost vydaných dokumentů a tvrdila, že dané dokumenty nebyly podepsány kvalifikovaným elektronickým podpisem dle požadavků národní právní úpravy a nařízení eIDAS. Dokumenty byly po zjištění znalcem totiž podepsány tzv. profesionálním elektronickým podpisem (podobu tohoto podpisu rozebíráme dále).

Předkládací soud (bulharský správní soud) tak primárně řešil otázku, jaký charakter má tamní profesionální elektronický podpis. Dále pak pracoval se zásadou uvedenou v čl. 25 nařízení eIDAS, které obecně zakazuje nediskriminaci elektronického podpisu jen na základě toho, že se jedná o podpis v elektronické podobě.

Bulharský soud formuloval předběžné otázky, které se týkaly především vymezení požadavků kladených na kvalifikovaný elektronický podpis, rovněž pak formuloval dotaz, za jakých podmínek lze (a jestli) považovat profesionální elektronický podpis za kvalifikovaný přičemž zdůraznil v případě formalistického pojetí vymezení požadavků kladených na podpis rovněž potenciální „*následek vytvoření nerovnováhy mezi dokumentem v papírové podobě s vlastnoručním podpisem na jedné straně a elektronickým dokumentem s elektronickým podpisem na druhé straně*“.[151] Mj. se pak rovněž dotázal, jestli fakt, že jména v certifikátu jsou uvedena v cyrilici a následně jsou přepsána do latinky, představuje překážku pro to, aby byly naplněny požadavky kladené na kvalifikovaný elektronický podpis.

SDEU se nejprve zabýval požadavkem nediskriminace elektronického podpisu dle č. 25 nařízení eIDAS. Zdůraznil, že čl. 25 „*nezakazuje vnitrostátním soudům zneplatnit elektronické podpisy, které nesplňují požadavky tohoto nařízení k tomu, aby mohly být považovány za „kvalifikovaný elektronický podpis*“”,[152] což byl i tento konkrétní případ, jelikož profesionální elektronický podpis stanovené požadavky nenaplňoval. V daném SDEU navázal v tom, že profesionální elektronický podpis je sice založen na kvalifikovaném certifikátu, nenaplnil ovšem další požadavky kladené nařízením eIDAS na kvalifikovaný elektronický podpis (především nebyl vytvořen

[151] Bod 21 odůvodnění.

[152] Bod 40 odůvodnění.

kvalifikovaným prostředkem pro vytváření elektronických podpisů).[153] Nelze jej tedy za takový podpis považovat a pokud právní úprava požadavek na podepsání takovým podpisem stanovuje, nelze ji naplnit využitím podpisu jiného. V souvislosti s přepisem cyrilicí uvedených jmen do latinky SDEU konstatoval, že dané nemusí být na překážku naplnění vymezení a požadavků kladených na kvalifikovaný elektronický podpis, pokud lze posoudit, že „*tento podpis jednoznačně spojen s podepisující osobou a umožňuje její identifikaci*“.[154] Dané ale musí ověřit vnitrostátní soud.

Rozhodnutí nelze vnímat jako nějak zásadně revoluční, *de facto* shrnulo základní limity a chápání toho, co lze (a za jaké situace) považovat za kvalifikovaný elektronický podpis. Jedná se ale o první rozhodnutí SDEU týkající se nařízení eIDAS a poskytuje vhodná vodítka k tomu, jak nejen na problematiku elektronických podpisů, ale obecně i elektronických dokumentů nahlížet.

Autor: PL

[153] Jedná se tedy vlastně o podobný podpis, který v rámci české právní úpravy známe jako elektronický podpis založený na kvalifikovaném certifikátu.

[154] Bod 59 odůvodnění.

ESSAYS II/2023

CONTENTS

PRIVACY SELF MANAGEMENT: CAN I DO IT ALONE?[1]

KRYŠTOF DVOŘÁČEK[2]

1. INTRODUCTION

In our increasingly digitalized society, personal information has become a currency of unprecedented value. The concept of privacy self-management has been a long-prevailing ideal, that operates under the assumption that individuals possess both the capacity and the agency to make informed decisions about their personal data and that they have meaningful control over its fate. Yet, as we delve deeper into the intricacies of personal data management in the digital era, it becomes increasingly evident that this ideal harbours fundamentally flawed assumptions. By examining the limitations of individual control over personal data, the essay aims to shed light on the reasons behind the inevitable shift towards a more collective approach to privacy protection in our evolving digital landscape, current attempts, their success and future challenges and considerations.

2. CRITICAL TERMS

First of all, it is necessary to define the terms that will be freely used throughout the paper. Unfortunately, the term *privacy* does not have a universal nor definitive legal definition as its interpretation varies by country. However, various human rights instruments recognize the right to privacy as a fundamental human right, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

[1] Esej byla zpracována v semestru podzim 2023 v rámci předmětu MVV1368K Privacy and Personal Data Law. / The essay was written in the autumn 2023 semester for the course MVV1368K Privacy and Personal Data.

[2] Bc. Kryštof Dvořáček is a student at the Faculty of Law, Masaryk university, contact e-mail: 480376@mail.muni.cz

Privacy laws are therefore considered within the context of one's privacy rights or within reasonable expectation of privacy. On the other hand, *privacy self-management* is a principle that enables each individual to manage their privacy through notice and choice[3] or, in other words, allow them to consider all costs as well as benefits under sharing, providing and allowing for collection and storage of their data.[4] Finally, the *privacy paradox* is a phenomenon where people claim to value privacy highly but do not act accordingly. Occasionally it is called a myth because some scholars argue that it is created by faulty logic and that people's attitudes about their privacy concerns or how much they value privacy are much more general in nature than the specific behaviours studied in privacy paradox studies.[5]

3. CURRENT ASSUMPTIONS FOR PRIVACY SELF-MANAGEMENT

Establishing an individual as the leading actor in privacy self-management rises and falls on the ability of a given individual to make informed and rational decisions about their personal data as well as having meaningful control over their data granted by law.

Nevertheless, empirical and social science investigations have demonstrated that people's actual capacity to make these informed and logical choices falls far short of the ideal envisioned by privacy self-management.[6] Among the most common causes of irrational behaviour researchers cite time constraints, lack of knowledge, the nature of human decision making

---

[3] KRÖGER, Jacob Leon, Otto Hans-Martin LUTZ a Stefan ULLRICH. The *Myth of Individual Control: Mapping the Limitations of Privacy Self-management*. [online]. Rochester, NY, 2021. [cit. 15. 11. 2023]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881776

[4] SOLOVE, Daniel J. *Privacy Self-Management and the Consent Dilemma* [online]. Rochester, NY, 2012 [cit. 15. 11. 2023]. Available at: https://papers.ssrn.com/abstract=2171018

[5] SOLOVE, Daniel J. The *Myth of the Privacy Paradox*. [online] Rochester, NY, 2021. [cit. 15. 11. 2023]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265

[6] DWIVEDI, Yogesh K. et al. Opinion Paper: "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*. [online]. 2023, vol. 71. [cit. 15. 11. 2023]. Available at: https://www.sciencedirect.com/science/article/pii/S0268401223000233?via%3Dihub

and information overload.[7] To be put differently cognitive demands play a critical role in privacy self-management.[8] However, these face sequential limitations, while usually, individuals tend to lack adequate information about the choices they make, primarily because they often neglect to peruse privacy policies. Even if they do take the time to read them, they frequently encounter challenges in comprehending the content. Even when comprehension is achieved, they often lack the requisite knowledge to make a genuinely informed decision. Furthermore, even when well-informed, their capacity for decision-making is constrained by the typical complexities inherent in human decision-making.[9]

Similarly, to the failure to demonstrate the presumed rationality in privacy self-management, having meaningful control over an individual's data is often an illusion. Data collectors are still able to manipulate individuals into making unfavourable choices from an individual's point of view while keeping in line with the law. As these external limitations to one's ability to privacy self-management it is possible to note consciously creating obstacles to presenting privacy information and usage of dark patterns, nudging and coercion, financial incentives, uniformity of privacy practises, social norms, dependence on services provided,[10] non-negotiability of usage terms, timing and duration of the consent, scale, data aggregation, downstream uses,[11] legal loopholes and complexities of data processing.[12] Additionally, creating technology that focuses primarily on privacy while stay-

[7] KRÖGER, Jacob Leon, Otto Hans-Martin LUTZ a Stefan ULLRICH. The *Myth of Individual Control: Mapping the Limitations of Privacy Self-management*. [online]. Rochester, NY, 2021. [cit. 15. 11. 2023]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881776

[8] LEHTINIEMI, Tuukka a Yki KORTESNIEMI. Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach. *Big Data & Society*. [online]. SAGE Publications Ltd, 2017, vol. 4, issue no. 2. [cit. 15. 11. 2023]. Available at: https://journals.sagepub.com/doi/10.1177/2053951717721935

[9] SOLOVE, Daniel J. *Privacy Self-Management and the Consent Dilemma* [online]. Rochester, NY, 2012 [cit. 15. 11. 2023]. Available at: https://papers.ssrn.com/abstract=2171018

[10] KRÖGER, Jacob Leon, Otto Hans-Martin LUTZ a Stefan ULLRICH. The *Myth of Individual Control: Mapping the Limitations of Privacy Self-management*. [online]. Rochester, NY, 2021. [cit. 15. 11. 2023]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881776

ing competitive with non-privacy-focused competitors serves as yet unsolved challenge. Likewise, legal and other regulations for privacy are always "just catching up" to the latest technological advances – the latest generative AI tool serving as an excellent example, since not only national but also corporate regulations have been on the defensive and reactionary state since ChatGPT became widely popular.[13]

Therefore, neither of the initially defined assumptions stand their ground in the face of research and thus raises the question of whether privacy self-management is the correct way to go. In case the privacy of individuals is in the best interest of society and intrinsically of regulators and potential changemakers, then it is not a question of "if" but "when and how".

4. INEVITABLE SHIFT

A transition away from exclusively relying on individual control is inevitable because privacy self-management requires responsibilities that go beyond the inherent capabilities of most if not all, individuals. At the same time, it fails to provide substantial control over personal data, and it becomes exceedingly challenging for individuals to assess the trade-offs involved in disclosing information or permitting its use and transfer without a comprehensive understanding of the potential downstream consequences. This limitation further hampers the effectiveness of the privacy self-management framework. Moreover, privacy self-management tends to address privacy concerns as a series of isolated transactions driven by specific indi-

[11] LEHTINIEMI, Tuukka a Yki KORTESNIEMI. Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach. *Big Data & Society*. [online]. SAGE Publications Ltd, 2017, vol. 4, issue no. 2. [cit. 15. 11. 2023]. Available at: https://journals.sagepub.com/doi/10.1177/2053951717721935

[12] KRÖGER, Jacob Leon, Otto Hans-Martin LUTZ a Stefan ULLRICH. The *Myth of Individual Control: Mapping the Limitations of Privacy Self-management*. [online]. Rochester, NY, 2021. [cit. 15. 11. 2023]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881776

[13] BETTINI, Claudio a Daniele RIBONI. Privacy protection in pervasive systems: State of the art and technical challenges. *Pervasive and Mobile Computing*. [online]. 2015, vol. 17. [cit. 15. 11. 2023]. p. 170. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1574119214001631?via%3Dihub

viduals, often overlooking the broader impact of individual privacy choices on both other individuals and society as a whole. Consequently, there is a compelling need to shift toward a more collective approach to safeguarding privacy, one that considers the broader societal implications of personal data processing and the power dynamics involving individuals, corporations, and governments.[14, 15,16]

Attempts to shift from privacy self-management are already happening, the evidence being the growing adoption of privacy regulations and laws globally. On one hand, initiatives like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) serve as exemplary illustrations. These measures are designed to safeguard individual's privacy by placing greater accountability on companies and similar collecting entities to protect personal data and giving individuals more control over their data by providing stronger legal ground to individuals and thus empowering the individuals at the expense of companies and possibly the state.[17] On the other hand, China cultivates the social credit system (SCS), which is hailed as its most substantial reform of the economic and social environment to ensure China's continuous development in the digital age, which takes a completely different approach by strengthening the state by monitoring and assessing the trustworthiness of individual, companies and governmental entities.[18]

---

[14] KRÖGER, Jacob Leon, Otto Hans-Martin LUTZ a Stefan ULLRICH. The *Myth of Individual Control: Mapping the Limitations of Privacy Self-management*. [online]. Rochester, NY, 2021. [cit. 15. 11. 2023]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881776

[15] SOLOVE, Daniel J. *Privacy Self-Management and the Consent Dilemma* [online]. Rochester, NY, 2012 [cit. 15. 11. 2023]. Available at: https://papers.ssrn.com/abstract=2171018

[16] BROUWER, Simeon de. Privacy self-management and the issue of privacy externalities: of thwarted expectations, and harmful exploitation. *Internet Policy Review* [online]. 2020, vol. 9, issue no. 4 [cit. 16. 11. 2023].Available at: https://policyreview.info/articles/analysis/privacy-self-management-and-issue-privacy-externalities-thwarted-expectations-and

[17] VOGELS, Janna Anderson, Lee Rainie and Emily A. *Experts Say the 'New Normal' in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges* [online]. 2021 [cit. 15. 11. 2023]. Available at: https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges/

While all of the aforementioned initiatives account for limitations of privacy self-management and its assumptions, and instead take a collective approach as a step towards better data privacy (at least in the case of GDPR and CCPA), it is worth noting that all of them have their fair share of criticism. For GDPR it is mostly vague and undefined legal terminology, scope limitations,[19] questionable enforcement, compliance challenges and negative impact on services (companies) itself, while still providing only limited impact on privacy. CCPA is likewise criticized for limited application, potential functional uselessness, insufficient protection and unclear enforcement rules.[20] Finally, for SCS beyond lack of transparency, accuracy and standardization, the most pressing criticism is actually the limited rights of individuals and privacy concerns, which would go completely against the initial goal of privacy protection.[21,22]

5. FIXING PRIVACY MANAGEMENT

As a reaction to the aforementioned failures of assumptions for privacy self-management as well as heavy criticism for collective initiatives, it is necessary to explore possible fixes to privacy management. Since we are looking at a complex issue requiring a multifaceted approach, some possibilities include simplification of privacy policies by means such as plainer language

[18] AHO, Brett a Roberta DUFFIELD. Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*. [online]. Routledge, 2020, vol. 49, issue no. 2. [cit. 15. 11. 2023]. p. 188. Available at: https://www.tandfonline.com/doi/full/10.1080/03085147.2019.1690275

[19] KRÖGER, Jacob Leon, Otto Hans-Martin LUTZ a Stefan ULLRICH. The *Myth of Individual Control: Mapping the Limitations of Privacy Self-management*. [online]. Rochester, NY, 2021. [cit. 15. 11. 2023]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881776

[20] VILJOEN, Salomé. The Promise and Pitfalls of the California Consumer Privacy Act. In: *DLI Cornell tech* [online]. 11. 4. 2020 [cit. 15. 11. 2023]. Available at: https://www.dli.tech.cornell.edu/post/the-promise-and-pitfalls-of-the-california-consumer-privacy-act

[21] AHO, Brett a Roberta DUFFIELD. Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*. [online]. Routledge, 2020, vol. 49, issue no. 2 [cit. 15. 11. 2023]. p. 205. Available at: https://www.tandfonline.com/doi/full/10.1080/03085147.2019.1690275

[22] KOBIE, Nicole. The complicated truth about China's social credit system. *Wired UK* [online] [cit. 15. 11. 2023]. ISSN 1357-0978. Available at: https://www.wired.co.uk/article/china-social-credit-system-explained

and shortening text, intuitive presentation, explanatory videos, Q&A chatbots,[23] increasing public awareness to nudge individuals towards more rational decisions, further development of various software tools for privacy protection on the one hand and overcoming technology challenges in creating products with privacy at its core. Finally, collaboration between all stakeholders will be elementary, that is including individuals, companies, governments and educators.[24]

In the end, even if the challenges connected to the possible fixes were overcome, we get to the implications of the privacy paradox and its status as a myth. Given the limitations of privacy self-management laid out before, it would be tempting to label the privacy paradox as a myth, since they would imply that even if individuals cared enough about their privacy, it would not be possible to fully adhere to these values unless living without digital world, its tools and away from urbanized public areas not to be subjected to surveillance capitalism. At the same time, seeing data collection as a business interest (either for marketing and advertisement purposes or for product development), it would be interesting to experiment with the idea of a "direct pricing" system of data provided to the data collector from an individual's point of view. That is assigning monetary value to each package of data provided or collected and thus allowing all individuals to see data of what worth has he provided, building on an idea that there is no such thing as a free lunch and potentially serving as a counterbalance to using current services seemingly for free. However, this would require a centralized, yet simple enough UX, strong and precise legal regulation and collaboration of all parties involved, creating a challenge not only from the technical and legal side of things but from the moral and ethical as well, especially if the system were to be designed as a voluntary trade of personal information from individual to companies, creating a dis-

[23] KRÖGER, Jacob Leon, Otto Hans-Martin LUTZ a Stefan ULLRICH. The *Myth of Individual Control: Mapping the Limitations of Privacy Self-management*. [online]. Rochester, NY, 2021. [cit. 15. 11. 2023]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881776

[24] OFFICE OF EDUCATIONAL TECHNOLOGY. Barriers & Strategies. [online] 2021. [cit. 15. 11. 2023]. Available at: https://tech.ed.gov/advancing-digital-equity-for-all/barriers-and-strategies/

crepancy between privacy as a fundamental human right and privacy as a commercial estate. Some are already pointing out this idea and its complexity;[25, 26] however, it seems as a best possible step in order to create a well-functioning privacy management system, fair to both individuals and businesses alike.

6. CONCLUSION

In conclusion, the examination of the fundamentally wrong assumptions underpinning the concept of privacy self-management underscores the critical need for re-evaluation in our approach to safeguarding personal data. As the digital age evolves, we are faced with a growing understanding of the intricate challenges that individuals encounter in managing their own privacy. The evidence of individuals' struggles to make informed decisions, the inability to grasp the complexities of data policies, and the consequences of their choices on a broader societal scale is undeniable. A more collective approach to privacy protection is necessary, one that takes into account the societal implications of personal data processing and the power dynamics between individuals, corporations, and governments. This shift is already happening, as evidenced by the increasing number of privacy regulations and laws being enacted around the world. With their questionable success however, we may sooner or later face a question, whether we shall allow individuals to freely trade their personal information as a commercial estate, creating a mechanism for counter-balancing the data collection benefits for companies, and if so, how to protect them from making irreversible faulty decisions.

---

[25] MALGIERI, Gianclaudio a Bart CUSTERS. Pricing privacy – the right to know the value of your personal data. *Computer Law & Security Review*. [online]. 2018, vol. 34, issue no. 2. [cit. 15. 11. 2023]. p. 299. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0267364917302819?via%3Dihub

[26] PURTOVA, Nadya a Gijs VAN MAANEN. Data as an economic good, data as a commons, and data governance. *Law, Innovation and Technology*. [online]. Routledge, 2023. [cit. 15. 11. 2023]. s. 41. Available at: https://www.tandfonline.com/doi/full/10.1080/17579961.2023.2265270

7. BIBLIOGRAPHY

[1] AHO, Brett a Roberta DUFFIELD. Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*. [online]. Routledge, 2020, vol. 49, issue no. 2. [cit. 15. 11. 2023]. p. 187–212. ISSN 0308-5147. Available at: https://www.tandfonline.com/doi/full/10.1080/03085147.2019.1690275

[2] BETTINI, Claudio a Daniele RIBONI. Privacy protection in pervasive systems: State of the art and technical challenges. *Pervasive and Mobile Computing*. [online]. 2015, vol. 17. [cit. 15. 11. 2023]. p. 159–174. ISSN 1574-1192. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1574119214001631?via%3Dihub

[3] DWIVEDI, Yogesh K. et al. Opinion Paper: "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*. [online]. 2023, vol. 71. [cit. 15. 11. 2023]. p. 102642. ISSN 0268-4012. Available at: https://www.sciencedirect.com/science/article/pii/S0268401223000233?via%3Dihub

[4] KRÖGER, Jacob Leon, Otto Hans-Martin LUTZ a Stefan ULLRICH. The *Myth of Individual Control: Mapping the Limitations of Privacy Self-management*. [online]. Rochester, NY, 2021. [cit. 15. 11. 2023]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881776

[5] LEHTINIEMI, Tuukka a Yki KORTESNIEMI. Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach. *Big Data & Society*. [online]. SAGE Publications Ltd, 2017, vol. 4, issue no. 2. [cit. 15. 11. 2023]. ISSN 2053-9517. Available at: https://journals.sagepub.com/doi/10.1177/2053951717721935

[6] MALGIERI, Gianclaudio a Bart CUSTERS. Pricing privacy – the right to know the value of your personal data. *Computer Law & Security Review*. [online]. 2018, vol. 34, issue no. 2. [cit. 15. 11. 2023]. p. 289–303. ISSN 0267-3649. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0267364917302819?via%3Dihub

[7] KOBIE, Nicole. The complicated truth about China's social credit system. *Wired UK* [online] [cit. 15. 11. 2023]. ISSN 1357-0978. Available at: https://www.wired.co.uk/article/china-social-credit-system-explained

[8] OFFICE OF EDUCATIONAL TECHNOLOGY. Barriers & Strategies. [online] 2021. [cit. 15. 11. 2023]. Available at: https://tech.ed.gov/advancing-digital-equity-for-all/barriers-and-strategies/

[9] PURTOVA, Nadya a Gijs VAN MAANEN. Data as an economic good, data as a commons, and data governance. *Law, Innovation and Technology*. [online]. Routledge, 2023. [cit. 15. 11. 2023]. p. 1–42. ISSN 1757-9961. Available at: https://www.tandfonline.com/doi/full/10.1080/17579961.2023.2265270

[10] SOLOVE, Daniel J. *Privacy Self-Management and the Consent Dilemma* [online]. Rochester, NY, 2012 [cit. 15.11.2023]. Available at: https://papers.ssrn.com/abstract=2171018

[11] SOLOVE, Daniel J. The *Myth of the Privacy Paradox*. [obline] Rochester, NY, 2021. [cit. 15. 11. 2023]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3536265

[12] VILJOEN, Salomé. The Promise and Pitfalls of the California Consumer Privacy Act. In: *DLI Cornell tech* [online]. 11. 4. 2020 [cit. 15.11.2023]. Available at: https://www.dli.tech.cornell.edu/post/the-promise-and-pitfalls-of-the-california-consumer-privacy-act

[13] VOGELS, Janna Anderson, Lee Rainie and Emily A. *Experts Say the 'New Normal' in 2025 Will Be Far More Tech-Driven, Presenting More Big Challenges* [online]. 2021 [cit. 15. 11. 2023].Available at: https://www.pewresearch.org/internet/2021/02/18/experts-say-the-new-normal-in-2025-will-be-far-more-tech-driven-presenting-more-big-challenges/

[14] BROUWER, Simeon de. Privacy self-management and the issue of privacy externalities: of thwarted expectations, and harmful exploitation. *Internet Policy Review* [online]. 2020, vol. 9, issue no. 4 [cit. 16. 11. 2023]. ISSN 2197-6775. Available at:: https://policyreview.info/articles/analysis/privacy-self-management-and-issue-privacy-externalities-thwarted-expectations-and

---

PROTECTING FREE SPEECH AGAINST FREE SPEECH[27]

H. CAN ÖZDEMIR[28]

1. INTRODUCTION

Undoubtedly, freedom of speech is essential for human rights and democracy. Since the establishment of the internet in the information age, the importance of freedom of speech is highly felt by internet users because now every individual can represent their ideas on social media platforms. The main difference between traditional media and social media is every individual can share their ideas on social media platforms but in traditional media, the percentage of participation in speech is meagre and that leads to some changes in communication.

The accessibility and popularity of the internet have made the reach of free speech cheaper, faster, and easier to access, causing concern among some governments. Governments are pressuring social media platforms to ban ideas that are considered harmful to democracy and society.[29] Although certain philosophers have discussed limiting freedom of speech to protect it, the restrictions of content on social media platforms raised questions among people about freedom of speech and whether it is justifiable to limit ideas that may harm society or a country's democratic order. To answer

[27] Esej byla zpracována v semestru podzim 2023 v rámci předmětu MVV1368K Privacy and Personal Data Law. / The essay was written in the autumn 2023 semester for the course MVV1368K Privacy and Personal Data.

[28] Hasan Can Özdemir is a student at the Faculty of Law, Izmir University of Economics, contact e-mail: can.ozdemir@std.izmirekonomi.edu.tr

[29] CHOTINER, Isaac. The Evolving Free-Speech Battle Between Social Media and the Government. The *New Yorker* [online]. 2023. [cit. Cit. 23. 10. 2023]. Available at: https://www.newyorker.com/news/q-and-a/the-evolving-free-speech-battle-between-social-media-and-the-government

this question, this essay first examines the three major theories of free speech to determine their justifications for the freedom of speech. Next, it attempts to determine whether it is possible to limit political speech under the reasoning of each theory. This essay is focused on anti-democratic and extremist political speech because it is the type of speech that is considered to be potentially harmful to the democratic organization of a society and, eventually, to free speech.

2. THREE MAJOR THEORIES OF FREE SPEECH

2.1 MARKETPLACE OF IDEAS

The oldest and most known theory for justification of free speech is the acquisition of truth in the marketplace of ideas. The theory was first mentioned by John Milton in the seventeenth century and developed systematically by John Stuart Mill. The main idea of the theory is that in a platform of free debate truth will prevail over falsehood.[30]

In a platform of free debate, wrong ideas will be freely criticized and eliminated because their falsehood will be pointed out. Truth, on the other hand, can be criticized. But it will not be eliminated because it has no weaknesses, or through debate, people may realize that the idea is wrong. Justice Oliver Wendell Holmes wrote that "the ultimate good desired is better reached by free trade in ideas."[31]

Some may argue against allowing criticism of the truth, but even truth should be criticized. If people stop thinking, talking, or debating about the ideas we hold to be true, then truth will be held as a dead dogma, not a living truth.[32]

In my opinion "truth" in this theory should be understood as the most logical outcome for political speech because the issues of politics are all ab-

[30] MILTON, John. *Areopagitica: A Defense of Free Speech - Includes Reproduction of the First Page of the Original 1644 Edition*. ARC Manor, 2008. p. 55.

[31] ABRAMS et al. v. UNITED STATES. In: *LII / Legal Information Institute* [online]. 10. 11. 1919. [cit. 15. 11. 2023]. Available at: https://www.law.cornell.edu/supreme-court/text/250/616

[32] MILL, John Stuart. *On Liberty and Other Essays.* 1st edition. Oxford: Oxford Paperbacks, 2008. p. 40.

stract; we cannot falsify a political idea by testing it. For example, we cannot do an experiment and decide that country X should be run under a communist regime for 10 years to see if it is a good political regime or not. Because politics are abstract, the most logical outcome from political debates may change from person to person because the interests of individuals differ from their personal experiences and preferences.

The way science works is in line with the theory of the marketplace of ideas. Karl Popper differentiates science from non-science by using the falsification principle, which states that if there is no way to falsify a theory by testing or criticizing it, then the theory is not scientific.[33] Popper's idea focuses on the falsification principle because scientific theories need to be tested to see if the theory is working or not. Also, scientific theories improve through critiques from other scientific theories. In order to get closer to a better theory, scientists focus on eliminating incorrect theories. The marketplace of ideas theory works in a similar way; ideas need to be criticized to test them to determine if they are true or false. Without freedom of speech, the process of criticizing ideas will not happen in a healthy way, because people may fear getting punished for their ideas.

2.2 DEMOCRATIC SELF-GOVERNANCE

This theory understands free speech as a tool for achieving core democratic values.[34] Abraham Lincoln said, "Democracy is a rule of the people, for the people and by the people".[35] In a democratic form of government, leaders are representatives of the people and democracy is grounded on equal participation of the public in the government of public affairs.[36] Freedom of

[33] POPPER, Karl. The *Logic of Scientific Discovery*. [online]. 2nd edition. London: Routledge, 2002. [cit. 23. 10. 2023]. p. 72. Available at: https://philotextes.info/spip/IMG/pdf/popper-logic-scientific-discovery.pdf

[34] BARENDT, Eric. *Freedom of Speech*. [online]. 2nd edition. Oxford, New York: Oxford University Press, 2007. [cit. 23. 10. 2023]. p. 19. Available at: https://www.jstor.org/stable/840191

[35] LINCOLN, Abraham. *Gettysburg Address.* [online]. 19. 11. 1863. [cit. 23. 10. 2023]. Available at: https://voicesofdemocracy.umd.edu/lincoln-gettysburg-address-speech-text/

[36] TSESIS, Alexander. Balancing Free Speech. *Faculty Publications & Other Works* [online]. 2016. [cit. 23. 10. 2023]. p. 11. Available at: https://lawecommons.luc.edu/facpubs/580

speech is essential to the existence of democracy because, without it, core democratic values such as the rule of the people and the principle of equal participation cannot be achieved.

Without freedom of speech core democratic values cannot be achieved because democracy is more than voting. It is true that elections allow people to choose their representatives, but political debate is essential to shaping voters' ideas before an election.[37] If there is no public debate and people don't have any ideas about political issues, what's the point of holding an election? Such an election would not accurately reflect the views of voters, since they may have no opinion on political matters because political debate informs citizens on political matters. Even though voters may have opinions about political issues, public debate may have an influence that leads to changes in their ideas.

Political debate is crucial both for informing and shaping voters' ideas and also for finding solutions to our minor and major problems. At the end of all these discussions, people may have different ideas or different solutions for their problems, and they will vote for the politicians who represent ideas similar to their own. Politicians present themselves at rallies, in interviews, or even in public places like parks to participate in political debate. All those political discussions cannot be held in a healthy way without freedom of speech, and because political debate is essential to the running of a democracy, freedom of speech should be protected.

2.3 SELF-FULFILLMENT

This theory understands freedom of speech as a human right which comes from our dignity and what we say, write, hear and read affects our personality and our growth as intellectual human beings.[38]

Humans do not have sharp teeth like sharks, sharp claws like bears, and the strength of a gorilla. Instead, we have our superior communication

[37] MEIKLEJOHN, Alexander. *Free Speech and its Relation to Self-Government*. Union, N.J: The Lawbook Exchange, Ltd., 2011. pp. 105-107.

[38] BARENDT, Eric. *Freedom of Speech*. [online]. 2nd edition. Oxford, New York: Oxford University Press, 2007. [cit. 23. 10. 2023]. ISBN 978-0-19-922581-1. p. 13. Available at: https://www.jstor.org/stable/840191

skills to cooperate and survive in the wild. Our ability to communicate was instrumental in our survival during humanity's early ages as every individual inherently adopted the ability to communicate. Every person has the inherent dignity to speak freely, it is intrinsic to our nature.[39]

Self-fulfilment theory suggests that individuals fulfil themselves by communicating. Engaging in conversation with others allows individuals to test their thoughts, maybe realize that their ideas are wrong, or realize that their ideas need to be improved. They may also learn from others. All these situations help individuals develop themselves. Although this theory does not focus on the consequences of freedom of speech to society, the right to freedom of speech leads to the development of more self-aware and mature individuals, which eventually benefits society.[40] The development of our intellectual existence through communication is perhaps the most important feature that differentiates humans from animals.

The theory also focuses on the autonomy of individual human beings. It suggests that autonomy and freedom of speech have an intense relationship because individuals develop and fulfil their intellectual existence through speech, which affects their autonomy.[41] According to Thomas Scanlon, "an autonomous person cannot accept without independent consideration the judgement of others as to what he should believe or what he should do."[42]

The autonomy of human beings leads both to the ability to act and speak freely and to receive other people's ideas. Being able to act and speak freely because of our autonomy leads to freedom of speech, and being able to receive others' ideas leads to independently criticizing and understand-

[39] SHIFFRIN, Seana Valentine. A *thinker-based approach to freedom of speech*. [online]. University of Minnesota Law School, 2011. [cit. 23. 10. 2023], pp. 302-303. Available at: http://conservancy.umn.edu/handle/11299/163435

[40] CAMPBELL, Tom a Wojciech SADURSKI. *Freedom of Communication*. Dartmouth Publishing Company, 1994, pp. 33-34.

[41] TSESIS, Alexander. Balancing Free Speech. *Faculty Publications & Other Works* [online]. 2016. [cit. 23. 10. 2023], p. 15. Available at: https://lawecommons.luc.edu/facpubs/580

[42] SCANLON, Thomas. A Theory of Freedom of Expression. *Philosophy and Public Affairs*. [online]. Wiley-Blackwell, 1972, vol. 1, issue no. 2. [cit. 23. 10. 2023], p. 163. Available at: https://www.jstor.org/stable/2264971

ing those ideas, which gives us the autonomy to develop our intellectual existence. Autonomy leads to freedom of speech; freedom of speech leads to autonomy.

3. THE JUSTIFIABILITY OF LIMITING FREEDOM OF SPEECH FOR ITS PROTECTION

It is crucial to understand the concept of limiting freedom of speech in order to secure it. What types of speech can be dangerous to the existence of freedom of speech? Can defamation, libel, disinformation, or blasphemy threaten freedom of speech? Such forms of speech do not necessarily target the existence of free speech; however, they may cause disorder in society, which may be harmful to free speech. Nevertheless, this paper focuses on theoretical issues about restriction on political speech that is considered anti-democratic and extremist.

Speech that directly targets the existence of free expression or indirectly aims to disrupt it may be harmful to the existence of freedom of speech. For example, extremist ideologies, like fascism, ethnonationalism, and totalitarianism, all support restrictions on free speech. In a democratic society, where freedom of speech is highly valued, is it justifiable to restrict the freedom of speech of people who defend or talk about these kinds of extremist ideologies because such ideologies can change the structure of society and distort freedom of speech? To find an answer to this question, let's examine it under three major theories of freedom of speech.

3.1 MARKETPLACE OF IDEAS

Finding the truth for this theory is more important than everything. The theory justifies freedom of speech because it is a tool for humans to get the most logical outcome. Limiting political speech because it may lead to harm to the freedom of speech is not justifiable for this theory because the theory focuses on finding the truth; freedom of speech is just a tool for it.

Theory suggests that the best way to reach truth is to put our thoughts on the marketplace of ideas and debate about them to test if it is the most

logical outcome or not. Even if the idea may be dangerous, we should put it in the marketplace of ideas and debate about it because it may be the most logical outcome.

Some argue that debating issues that contradict the truth is pointless. Mill supposes that even truth should be open to criticism, otherwise, it may turn out to be a dead dogma.[43] Dead dogma refers to an unquestionable idea that is accepted by society as a whole. Such an idea is inevitably going to lose its meaning because no one will question it because everyone automatically accepts it. By criticizing the ideas that we take as truth, we may be able to improve that idea because we may find some weaknesses in it, or we may realize that it is actually wrong. Even if neither scenario arises, criticizing and thinking about the truth will make it alive, and people will remember why they've accepted the idea as truth.

3.2 DEMOCRATIC SELF GOVERNANCE

As I mentioned, this theory uses freedom of speech as a tool for achieving core democratic values. Freedom of speech is essential for achieving equal participation in the governance of public affairs and healthy public debate. Both of those things are considered core values of democracy. Even though freedom of speech is essential for democracy, we can interpret that it is just a tool for democracy. If the political speech of certain groups, such as people who defend extremist ideologies, will be harmful to democracy, that group's freedom of speech may be restricted to protect the democratic form of government. Limiting freedom of speech to protect democracy is possible for this theory but the government should be extremely careful about it because it may lead to a totalitarian regime which is also dangerous to the core values of democracy.

3.3 SELF-FULFILLMENT

This theory assumes that freedom of speech is essential for self-fulfilment, intellectual development, and autonomy. I believe for this theory, it is

[43] MILL, John Stuart. *On Liberty and Other Essays.* 1st edition. Oxford: Oxford Paperbacks, 2008, p. 100.

unacceptable to allow governments to restrict some political ideas because they may be harmful to society. Theory suggests that the right to free speech is inherent in every individual and that each person has the autonomy to evaluate ideas in his or her own mind. Individuals have the autonomy to evaluate ideas in their own minds, when the government acts in a paternalistic way and restricts the idea, it is disregarding our autonomy. As Dworkin stated:

"[*M]orally responsible people insist on making up their own minds about what is good and bad in life or in politics, or what is true and false in matters of justice or faith. Government insults its citizens, and denies their moral responsibility when it decrees that they cannot be trusted to hear opinions that might persuade them to dangerous or offensive convictions. We retain our dignity, as individuals, only by insisting that no one no official and no majority has the right to withhold opinion from us on the ground that we are not fit to hear and consider it."*[44]

4. INSIGHTS ON RESTRICTING POLITICAL SPEECH

In my opinion, it seems clear that freedom of speech should not be restricted to the marketplace of ideas and self-fulfilment theories, but it is controversial for the theory of democratic self-governance. I believe that, for the theory of democratic self-governance, restricting freedom of speech to protect democracy is more harmful to democracy because it does not solve the problem of the existence of dangerous ideas, it may turn democracy into a dead dogma, and it gives a basis of justification for totalitarian regimes to restrict freedom of their opponents.

4.1 IT DOES NOT WORK

Censorship of news that might affect political discourse or political ideas does not make them disappear from society, especially in the age of the internet. Instead, censorship might draw more attention to what is censored,

[44] DWORKIN, Ronald. The Coming Battles over Free Speech. The *New York Review of Books* [online]. 1992, vol. 39, issue no. 11. [cit. cit. 23. 10. 2023]. Available at: https://www.nybooks.com/articles/1992/06/11/the-coming-battles-over-free-speech/

and people might be more curious about something after knowing that it is banned. To give an example, Barbra Streisand sued a photographer and a website because the photographer took a photo of her mansion and published it online, before the lawsuit the photo was downloaded six times, after the lawsuit it was downloaded 420,000 times in just one month.[45]

4.2 DANGER OF TURNING DEMOCRACY INTO A DEAD DOGMA

When we face criticism of an idea we support, defending it has an important benefit: it reminds us why we support that idea. While making a counterargument, we test our idea and remember why we decided to support it. If governments ban speech that is considered anti-democratic and extremist, there will be no opportunity to defend democracy against those ideas. This could result in democracy becoming a dead dogma that everyone supports, but no one remembers why they support it, and eventually loses its meaning in society.

4.3 POTENTIAL FOR ABUSE BY TOTALITARIAN REGIMES

If a democratic government limits the freedom of speech of a group based on their political ideas, it might provide an opportunity for totalitarian governments to limit the freedom of speech of their opponents. For example, if a democratic government bans speech about dangerous politics, which is justifiable under democratic self-government theory, totalitarian governments can restrict the free speech of their opposition, and they can try to justify it by claiming that it is a justifiable act for other democratic countries in the world.

5. CONCLUSION

In conclusion, although there are similarities among theories, the primary justifications for free speech are different, acquisition of the truth, achieving democratic values and self-fulfillment of the individual.

[45] JANSEN, Sue Curry a Brian MARTIN. The Streisand Effect and Censorship Backfire. *International Journal of Communication*. [online]. 2015, vol. 9. [cit. 23. 11. 2023], p. 656. Available at: https://www.researchgate.net/publication/273947761_The_Streisand_Effect_and_Censorship_Backfire

The question of whether to limit free speech to protect it is a complex one, and for some theories, it is justifiable, for others it is not.

First, if we consider freedom of speech to be a tool for humanity to find the truth, then it cannot be restricted because the idea that wanted to be restricted may be the truth.

Second, if we understand freedom of speech as an inherited right that comes from our dignity and leads to the development of an autonomous individual, then it cannot be limited because it could prevent the self-development of that individual, and every autonomous individual has the right to evaluate ideas in his own mind and act in accordance with his own thoughts.

Finally, if we acknowledge freedom of speech as a tool for achieving core values of democracy then it could be restricted in order to secure democracy because freedom of speech is just a tool that serves democracy.

I believe that freedom of speech should not be restricted to protect itself, even when the speech in question is considered anti-democratic and extremist. Restrictions on political speech can prevent individuals from improving their political opinions and achieving personal fulfilment. Furthermore, it can turn democracy into a dead dogma and prevent the chance of improving our knowledge through discussion.

6. BIBLIOGRAPHY

[15] SCANLON, Thomas. A Theory of Freedom of Expression. *Philosophy and Public Affairs*. [online]. Wiley-Blackwell, 1972, vol. 1, issue no. 2. [cit. 23. 10. 2023], pp. 204–226. Available at: https://www.jstor.org/stable/2264971

[16] SHIFFRIN, Seana Valentine. A *thinker-based approach to freedom of speech*. [online]. University of Minnesota Law School, 2011. [cit. 23.10.2023], pp. 283-307. ISSN 0742-7115. Available at: http://conservancy.umn.edu/handle/11299/163435

[17] ABRAMS et al. v. UNITED STATES. In: *LII / Legal Information Institute* [online]. 10. 11. 1919. [cit. 15. 11. 2023]. Available at: https://www.law.cornell.edu/supremecourt/text/250/616

[18] MILTON, John. *Areopagitica: A Defense of Free Speech - Includes Reproduction of the First Page of the Original 1644 Edition*. ARC Manor, 2008. 85 p. ISBN 978-1-60450-151-3.

[19] TSESIS, Alexander. Balancing Free Speech. *Faculty Publications & Other Works* [online]. 2016. [cit. 23. 10. 2023]. 225 p. Available at: https://lawecommons.luc.edu/facpubs/580

[20] MEIKLEJOHN, Alexander. *Free Speech and its Relation to Self-Government*. Union, N.J: The Lawbook Exchange, Ltd., 2011. 126 p. ISBN 978-1-58477-087-9.

[21] CAMPBELL, Tom a Wojciech SADURSKI. *Freedom of Communication*. Dartmouth Publishing Company, 1994. 320 p. ISBN: 978-1-85521-542-9

[22] BARENDT, Eric. *Freedom of Speech*. [online]. 2nd edition. Oxford, New York: Oxford University Press, 2007. [cit. 23. 10. 2023]. 526 p. ISBN 978-0-19-922581-1. Available at: https://www.jstor.org/stable/840191

[23] LINCOLN, Abraham. *Gettysburg Address*. [online]. 19. 11. 1863. [cit. 23. 10. 2023]. Available at: https://voicesofdemocracy.umd.edu/lincoln-gettysburg-address-speech-text/

[24] MILL, John Stuart. *On Liberty and Other Essays*. 1st edition. Oxford: Oxford Paperbacks, 2008. 632 p. ISBN 978-0-19-953573-6.

[25] DWORKIN, Ronald. The Coming Battles over Free Speech. The *New York Review of Books* [online]. 1992, vol. 39, issue no. 11. [cit. Cit. 23. 10. 2023]. ISSN 0028-7504. Available at: https://www.nybooks.com/articles/1992/06/11/the-coming-battles-over-free-speech/

[26] CHOTINER, Isaac. The Evolving Free-Speech Battle Between Social Media and the Government. The *New Yorker* [online]. 2023. [cit. cit. 23. 10. 2023]. ISSN 0028-792X. Available at: https://www.newyorker.com/news/q-and-a/the-evolving-free-speech-battle-between-social-media-and-the-government

[27] POPPER, Karl. The *Logic of Scientific Discovery*. [online]. 2nd edition. London: Routledge, 2002. [cit. 23. 10. 2023]. 544 p. ISBN 978-0-415-27844-7. Available at: https://philotextes.info/spip/IMG/pdf/popper-logic-scientific-discovery.pdf

[28] JANSEN, Sue Curry a Brian MARTIN. The Streisand Effect and Censorship Backfire. *International Journal of Communication*. [online]. 2015, vol. 9. [cit. 23. 11. 2023]. p. 656-671. ISSN 1932-8036. Available at: https://www.researchgate.net/publication/273947761_The_Streisand_Effect_and_Censorship_Backfire

CLOUD GAMING: TECHNICAL AND COPYRIGHT ASPECTS OF CLOUD VIDEO GAME STREAMING[46]

JAKUB RAŠE[47]

1. INTRODUCTION

The future of cloud gaming is only limited by our imagination. "[48]

Phil Eisler [49]

With this sentence, Phil Eisler concluded his answer to the question about the future and direction of cloud gaming. Eisler more than hinted that cloud gaming as such has great potential and that the possibilities for its use in the video game industry are, poetically speaking, endless. In today's fast-paced era, cloud gaming, or the actual playing of video games via PCs, consoles and mobile phones, has become a popular leisure activity not only for Generation Z, and gaming has long since ceased to be essentially a hobby for a closed group of video game enthusiasts. Today, games are simply an essential part of our lives. And Nvidia has a big part to play in that.

This company started in 1993 as a manufacturer of graphics cards for the gaming and multimedia markets. Today, however, its portfolio is far more extensive. Nvidia provides hardware products such as powerful RTX graphics cards and G-Sync gaming monitors. It also provides software services like various application frameworks (for developing artificial intelli-

[46] Esej byla zpracována v semestru jaro 2023 v rámci předmětu MVV93K Videoherní právo. / The essay was written in the spring 2023 semester for the course MVV93K Videogames Law.

[47] Jakub Raše is a student at Faculty of Law, Masaryk university, contact e-mail 495639@mail.muni.cz

[48] VJESTICA. Adam. Nvidia GeForce Now interview: 'the future of cloud gaming is only limited by our imagination'. In: *Tech radar* [online]. 2022. [cit. 10. 3. 2023]. Available at: https://www.techradar.com/features/nvidia-geforce-now-interview-the-future-of-cloud-gaming-is-only-limited-by-our-imagination

[49] Phil Eisler is a General Manager of NVIDIA's GeForce NOW cloud gaming service.

gence for autonomous vehicles and healthcare, or for multimedia content analysis), various applications (for data engineering), AI-based data infrastructure (NVIDIA AI Enterprise, Cloud Native), and last but not least, the cloud gaming service Nvidia GeForce Now (hereafter referred to as "GFN").[50] This service was first known as Nvidia Grid when it was introduced in 2013 as a limited beta version for Nvidia Shield gaming consoles. Later in 2015, the beta version of Nvidia Shield was officially launched as the full version, allowing gamers to play games supported and offered by Nvidia on those consoles.[51] Subsequently, in March 2017, Nvidia GFN was revealed for Windows and Mac computers, where its functionality was based on the Nvidia Grid model, with the service only being available in beta testing.

Nonetheless, it brought the novelty of being able to link a Steam account and its game library to the service, i.e., the ability to run primarily a game that the player *already owned*.[52] In 2019, the Nvidia Grid service was discontinued and rebranded to GFN. Finally, on February 4, 2020, the full version of the GFN service was officially launched to the public, supporting a wide range of operating systems such as Windows, macOS, Android, Chromebook, and Nvidia's multimedia device, the Nvidia Shield TV.[53] But it has gradually grown again and now supports Android and iOS mobile phones as well.[54]

---

[50] More information about Nvidia and it is body of work can be found in the official document Nvidia Story available at: https://images.nvidia.com/aemdam/Solutions/homepage/pdf/NVIDIA-Story.pdf

[51] MAG UHG, Gordon. Nvidia GeForce Now aims to be the 'Netflix of games' for just 8 bucks a month. In: *PC world* [online]. 2015. [cit. 10. 3. 2023]. Available at: https://www.pcworld.com/article/423733/nvidia-geforce-now-aims-to-be-the-netflix-of-games-for-just-8bucks.html#:~:text=Nvidia%20GeForce%20Now%20aims%20to%20be%20the%20%E2%80%98Netflix,after%20purchase.%20...%204%204K%20gaming%20too%20

[52] CLOVER, Juli. Nvidia's Free GeForce NOW Beta Lets You Play System Intensive PC Games on Your Mac. In: *Macrumors* [online]. 2017. [cit. 10. 3. 2023]. Available at: https://www.macrumors.com/2017/10/13/nvidia-geforce-now-beta-for-mac/

[53] CRANZ, Alex. Nvidia's Game-Streaming Service Is Finally Live. In: *Gizmodo* [online]. 2020. [cit. 10. 3. 2023]. Available at: https://gizmodo.com/after-7-years-in-beta-nvidias-game-streaming-service-i-1841449313

[54] More detailed information about the GFN video game service system requirements available at: https://www.nvidia.com/en-us/geforce-now/system-reqs/

Since that date, video game players have experienced a revolution in gaming. The service joined other cloud-based services already in existence at the time, namely Google Stadia, PsNow and Xcloud (nowadays Microsoft Xbox Game Pass Ultimate), but brought a few innovations over the competition. Firstly, the service allowed players to link their existing game libraries to the GFN service, meaning players didn't have to buy new game titles to be able to run and play a given video game through the service. Secondly, the GFN service also introduced a free-to-play model, whereby players could use the service for free for a limited time each day, in addition to various subscription tiers.

This paper will therefore focus on cloud gaming, namely gaming through the aforementioned cloud gaming service Nvidia GFN, where it will try to answer the question "*How does the transmission of audiovisual content work with Nvidia GFN, and how does the service affect copyright law in terms of publication and reproduction of works?*" In the first part, the paper will focus on the technical functioning of GFN, more specifically on its network and cloud aspects in streaming. In the second part, the paper will focus on copyright in the context of making copyrighted works available to the public and the reproduction of copyrighted works.

2. TECHNICAL ASPECTS OF NVIDIA GFN

This chapter's primary objective is to explore the description of the technical functioning of a given GFN video game service. The first part will try to analyze the network protocol that GFN uses, focusing on audio and video data transmission during streaming. It will also focus on image resolution options and network load for a given stream. The second part of the chapter will break down the cloud tool that GFN uses.

2.1 ANALYSIS OF GFN NETWORK OPERATION WITH FOCUS ON STREAMING DATA TRANSFER

The GFN video game service uses and operates on the basis of the *Real Time Protocol* (hereinafter referred to as the "RTP protocol")[55], which is built on top of other protocols such as the *UDP Protocol* and the *IP Protocol*. However, this paper will focus mainly on the RTP protocol. This RTP protocol is a network protocol that ensures audio and video transmission over an Internet connection. The given protocol is mainly used widely in communication and entertainment applications, which include streaming music and video media, organizing video conferences, operating television services and using push-to-talk web functions. Applications such as Microsoft Team or Zoom for calls and video conferences can be mentioned, but its use is wide, and it can even be used for cloud gaming. The RTP protocol is often found simultaneously with the RTP Control Protocol (RTCP) where the task of this RTCP protocol is to monitor the quality of transmission services and to transmit information about session participants[56]. However, we do not observe the given presence of the RTCP protocol here in GFN[57]. The RTP protocol was designed for both multicast transmissions (network communication between one device that sends data and several selected receiving devices) and unicast transmissions (communication occurs only between the sending device and the receiving device), both for one-way and two-

[55] DI DOMENICO, Andrea. PERNA, Gianluca. TREVISAN, Martino. VASSIO, Luca. GIORDANO, Danilo. A *Network Analysis on Cloud Gaming: Stadia, GeForce Now and PSNow*. Network [online]. 2021. [cit. 16. 3. 2023], p. 3. Available at: https://www.mdpi.com/2673-8732/1/3/15

[56] KOISTINEN, Tommi. *Protocol overview: RTP and RTCP*. *Research Gate,* [online]. 1999. [cit. 24. 3. 2023], p. 2. Available at: https://www.researchgate.net/publication/251203018_Protocol_overview_RTP_and_RTCP

[57] DI DOMENICO, Andrea. PERNA, Gianluca. TREVISAN, Martino. VASSIO, Luca. GIORDANO, Danilo. A *Network Analysis on Cloud Gaming: Stadia, GeForce Now and PSNow*. Network [online]. 2021. [cit. 16. 3. 2023], p. 8. Available at: https://www.mdpi.com/2673-8732/1/3/15

way transmission[58]. GFN uses unicast communication, which occurs between one device and the server.

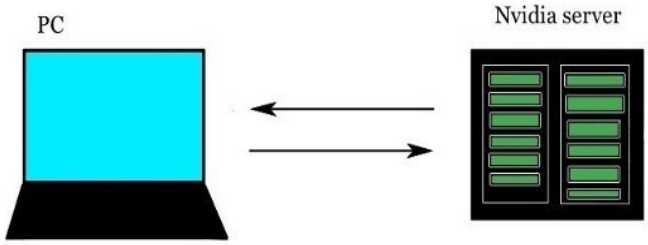


Figure 1 Example of unicast

It is also necessary to mention the characteristics of the RTP protocol during data transmission. Unfortunately, the RTP protocol does not guarantee data delivery as such during transmission. It does not even guarantee the correct order of delivery of individual packets (i.e. blocks of data). So if data are evaporated at the time of transfer, these data will not be transferred and it is the main reason why there is sometimes a loss of data quality when streaming. However, on the other hand, the protocol defines the sequence numbers of these packets, according to which the multimedia receiving applications can subsequently recognize whether an error has occurred and whether a packet is missing.[59]

A given protocol RTP packet in the form in which it is used by the GFN service when moving in the network is used in its most common form, i.e. an RTP packet transmitted based on the IP and UDP protocols and which adheres to the conventions defined by RFC 3551 (RTP Profile for Audio and Video Conferences with Minimal Control). An RTP packet consists of four

[58] SCHULZRINNE, Hennig at al. *RFC3550: RTP: A Transport Protocol for Real-Time Applications*. [online]. 2003. [cit. 20. 3. 2023]. Available at: https://dl.acm.org/doi/book/10.17487/RFC3550

[59] KOISTINEN, Tommi. *Protocol overview: RTP and RTCP*. In: *Research Gate* [online]. 1999. [cit. 24. 3. 2023], pp. 2-3 Available at: https://www.researchgate.net/publication/251203018_Protocol_overview_RTP_and_RTCP

parts. These are IP and UDP protocol headers and parts identifying the RTP protocol, RTP header and RTP payload.[60] Each given header thus has a certain function within the RTP packet. The first in order is the IP header, which identifies the source and destination IP addresses where the packet will travel within the network. The second is the UDP header, which is part of the UDP protocol (i.e. the transfer protocol) and which uses the port contained in the header to identify the target device. The third is the RTP header, which, in its essence, was already mentioned above. The RTP protocol creates sequence numbers according to which the missing packet is detected. It is this sequence number of the packet (i.e. sequence number) used to detect possible loss or duplication of packets. For each delivered RTP packet, the sequence number is increased by one, and the receiving device can use it for identification. The last one is the RTP payload, which contains an indication of the primary type of content, i.e. information about the format of the multimedia file that makes up the content of the packet (e.g. JPEG). The format of the RTP protocol packet is very general, so it suits a wide range of applications working in real-time.[61]

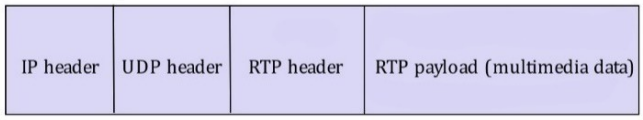


Figure 2 protocol packet

For these real-time data transfers, it is therefore necessary to ensure the uniformity of the flow of RTP packets, which means that the time delay between these individual packets should be constant. Suppose the time intervals between individual received packets change significantly. In that case, the given streaming application working in real-time may have a low-qual-

[60] PUŽMANOVÁ, Rita. *Streaming media (4): transportní protokoly RTP/RTCP*. [online]. 2004. [cit. 25. 3. 2023]. Available at: https://www.dsl.cz/clanky/60-streaming-media-4-transportni-protokoly-rtprtcp

[61] KOISTINEN, Tommi. *Protocol overview: RTP and RTCP*. In: *Research Gate* [online]. 1999. [cit. 24. 3. 2023], pp. 2-3. Available at: https://www.researchgate.net/publication/251203018_Protocol_overview_RTP_and_RTCP

ity image and sound output and may even fail. Maintaining the same time intervals between individual packets is a fundamental requirement for real-time multimedia transmission so that this failure does not occur. On the other hand, a certain tolerance of possible movements is allowed. If there are "reasonable" packet losses during the transmission of the given packets, the interpreted information (i.e. sound and image) will appear to the user as being of lower quality on the receiving side. The said packet loss can be influenced by many external factors, such as an outdated modem and router, damaged network card driver, faulty software and overloaded network equipment.[62] However, if there is a complete violation of the time sequence of the packets, the mentioned sound and image may completely disappear or "tear", i.e. stop transmitting.[63]

Figure 3 Example of degradation of image quality when streaming due to packet loss (the left one) on the case of the game Shadow of the Tomb Raider

The theoretical principles of audio and video transmission operation in connection with RTP protocol packets have been explained above. There-

[62] PARRISH, Kevin. What is packet loss, and how do you fix it? In: *Digital trends* [online]. 2021. [cit. 28. 3. 2023]. Available at: https://www.digitaltrends.com/computing/what-is-packet-loss-and-how-to-fix/

[63] KOISTINEN, Tommi. *Protocol overview: RTP and RTCP*. In: *Research Gate* [online]. 1999. [cit. 24. 3. 2023], pp. 2-3. Available at: https://www.researchgate.net/publication/251203018_Protocol_overview_RTP_and_RTCP

fore, we will now focus on the technical parameters and aspects of the network load when streaming video with the GFN service. First of all, it should be noted that streaming quality directly depends on the level of subscription that the user has purchased. There is a difference between the given free version and the other priority and ultimate versions. It is true that the service allows several video resolutions, in aspect ratios 16:9, 16:10, but also 4:3. According to the settings of the GFN application, the basic and recommended resolution setting is 16:9 aspect ratio. In this setting, the lowest resolution is 1280x720p, and the highest is 1920x1080p, but GFN also supports 1600x900p. According to system requirements, GFN consumes 15 Mbit/s for image transmission in 1280x720p quality and 25 Mbit/s for 1920x1080p quality transmission. With both of these transfers, GFN guarantees a frame rate of 60 FPS.[64] When streaming, the data rate can sometimes reach values of more than 30 Mbit/s for 720p and 40 Mbit/s for 1080p. Nevertheless, GFN can, for example, maintain a video stream with a resolution of 1080p even with an available bandwidth of less than 15 Mbit/s without a drop in the frame rate, probably by adjusting the compression parameters using H.264.[65] H.264 is a video compression standard that is used to effectively reduce video file size and data rate when video is transmitted over a network. Its task is to transmit a higher-quality image at a lower bit rate, whereas H.264 uses a wide range of techniques to reduce video size. These techniques include, for example, motion prediction or entropic coding.[66]

What is more, compared to a higher level of subscription, for example, the requirements are more demanding on the ultimate level. This is the highest level of subscription, where GFN offers a resolution of up to 3840x2160p at a frame rate of at least 120 FPS for streaming. In return,

[64] More detailed information about the GFN video game service system requirements available at: https://www.nvidia.com/en-us/geforce-now/system-reqs/

[65] DI DOMENICO, Andrea. PERNA, Gianluca. TREVISAN, Martino. VASSIO, Luca. GIORDANO, Danilo. A *Network Analysis on Cloud Gaming: Stadia, GeForce Now and PSNow*. Network [online]. 2021. [cit. 25. 3. 2023], p 12. Available at: https://www.mdpi.com/2673-8732/1/3/15

[66] More information about what is H.264 available here: https://techterms.com/definition/h264

however, the service requires a connection speed of at least 45 Mbit/s or at least 35 Mbit/s for streaming up to 3440x1440p, 2560x1440p or 2560x1600p at 120 FPS. For this level, it is also recommended to use a fixed Ethernet connection or a wireless router with a 5 GHz parameter instead of a WiFi connection.

2.2 GFN CLOUD PERFORMANCE ANALYSIS

A Czech proverb says that as you make your bed, so you must lie in it. From today's point of view and the fact that modern technologies surround us at every step, we could, with a bit of exaggeration, harmlessly change this saying to "what cloud tool you use, such a service you get". There are several cloud tools that can be divided according to what computing and technical resources are actually shared or what service is provided.[67] There are many such tools, for example, SaaS (Software as a service), PaaS (Platform as a service), and AIaaS (AI as a service)[68], but only one tool is essential for GFN.

The GFN video game service uses the IaaS cloud tool or the so-called Infrastructure as a Service.[69] IaaS is a type of cloud utility that allows users to rent virtual hardware represented by server, storage and computing capacity. Users then use this virtual hardware as a service instead of actually having to own it physically. The hosting of computing resources and the provided server infrastructure is the most essential feature of an IaaS tool for cloud gaming. In addition to providing server resources, some IaaS providers also offer compatible additional (non-IaaS) services. These can be

---

[67] LICHNOVSKÝ, Bohuslav. NONNEMANN, František. Clouds and the law - Part 1: Why to think about them and what to prepare for. In: *Epravo.cz* [online]. 2022. [cit. 10. 4. 2023]. Available at: https://www.epravo.cz/top/clanky/cloudy-a-pravo-1-dil-proc-o-nich-uvazovat-a-na-co-se-pripravit-115077.html

[68] Annex no. 1 in Strategic analysis of cloud services-Č. j.: 7226/2022-NÚKIB E/310 • BRNO. In: *NÚKIB* [online]. 2022. [cit 11. 4. 2023]. Available at: https://www.nukib.cz/download/publikace/analyzy/Strategicka%20analyza%20cloudovych%20sluzeb.pdf

[69] LONGAN, Mitchell. DIMITA, Geatano. MICHELS, Johan. MILLARD, Christopher. Cloud Gaming Demystified: *An Introduction to the Legal Implications of Cloud-Based Video Games.* In: *SSRN* [online]. 2021. [cit. 12. 4. 2023]. p. 14. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3949611

in the form of game analytics, matchmaking software, game leaderboards and can even provide machine learning technologies.[70]

Regarding the IaaS and GFN tools, one more consideration needs to be added. This is the fact that the arrival and use of these cloud tools in the world of gaming apparently gave rise to its own GaaS (gaming as a service) cloud model. This GaaS cloud model can then be divided according to the combination of cloud tools used during gaming.[71] In connection with the GFN service, the service thus provides a remote computing resource for users to play games without offering specific video game content. We could, therefore, refer to such a fact as the so-called "IaaS consumer model".[72] In essence, it is that the GFN service provides a remote computing resource, and the player can use this computing resource, even if the GFN does not offer the related video game content. It is then up to the player to purchase the video game content themselves. The GFN then only contains a list of supported game titles.

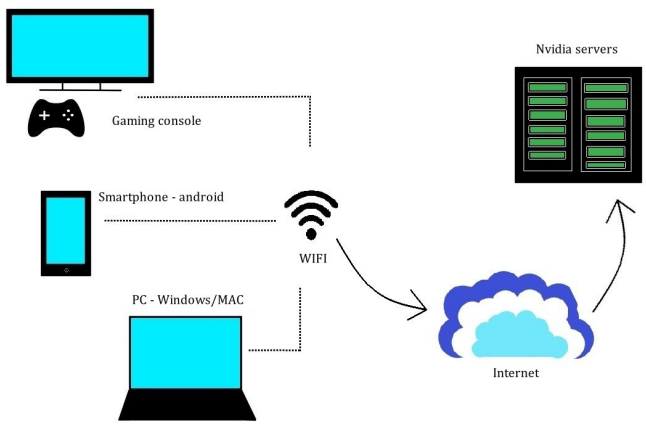


Figure 4 An example of connecting an input device to an Nvidia

[70] LONGAN, Mitchell. DIMITA, Geatano. MICHELS, Johan. MILLARD, Christopher. *Cloud Gaming Demystified: An Introduction to the Legal Implications of Cloud-Based Video Games.* In: *SSRN* [online]. 2021. [cit. 12. 4. 2023], p. 14. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3949611

[71] Ibidem, p. 18.

[72] Ibidem.

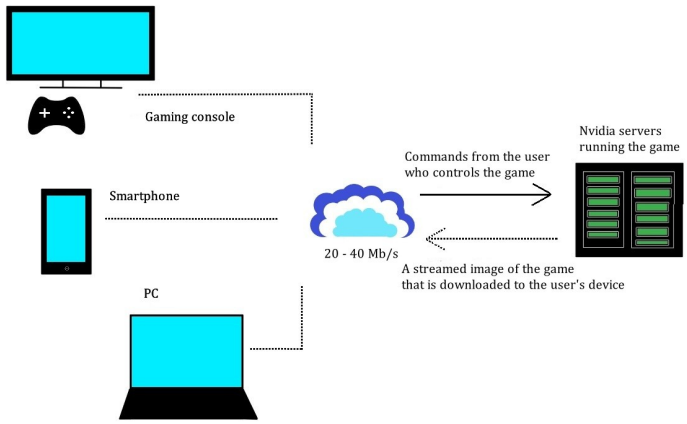


Figure 5 An example of GFN cloud streaming

3. COPYRIGHT ASPECTS OF NVIDIA GFN

The second part of this paper will focus on the legal aspects of cloud streaming, mainly through the prism of copyright. It is important to remember that a computer game is a collective work of authorship and is therefore covered by the copyright regime. By purchasing it, there is no actual acquisition of the ownership right to this game, but in essence, the given player only buys the given license agreement, which determines his possibilities of using the game. These affiliations are due to the very nature of copyright, namely the fact that copyright is non-transferable and only the right to exercise copyright is transferred through contractual licensing arrangements.

In this chapter, the paper will focus on two rights contained in copyright law that are very closely related to video game streaming. This is the right to make the work available to the public and the right to reproduce the work, where the work will try to compare these two rights in the context of the GFN service and the streaming functionality in connection with the licensing conditions of video game studios or video games themselves and shed light on cloud streaming from the perspective of EU copyright law.

3.1 MAKING COPYRIGHT WORK AVAILABLE TO THE PUBLIC AND CLOUD STREAMING

The basic EU regulation in the field of copyright is contained in Directive 2001/29/EC of the European Parliament and of the Council on the harmonization of certain aspects of copyright and related rights in the information society (hereinafter referred to as the "Infosoc Directive"). According to the wording of the text of Article 3 of this Directive, communication to the public is understood as any communication of a work to the public by wire or wireless, including making the works available to the public in such a way that every individual member of the public has access to these works from a place and at a time of their choosing.[73] Subsequently, recital 23 of the directive states that this right must be understood in a broad sense, including all communication to the public that is not present at the place where the communication originates. This right should apply to any communication of the work to the public by wire or wireless, including broadcasting.[74] We can thus say that communication to the public in the wording of Article 3 and Recital 23 of the Directive includes all dissemination of works by means of remote communication, where this right includes all methods of dissemination of works on the Internet, including all methods of streaming, as well as dissemination of works by other means, such as radio and television broadcasting.[75]

The issue of communicating a work to the public, in the form of making it available, was dealt with by two court decisions that are pivotal for this topic. The first decision is that of the United States Supreme Court in the

[73] Article 3 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society.

[74] Recital 23 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society.

[75] For instance: Judgment of the CJEU (fourth chambre) from day 13. February 2014 in case C-466/12 Swonson or Judgment of the CJEU (third chambre) from day 15. March 2012 in case C-135/10 Societá Consortile Fonografici (SCF) v Marco Del Carso.

case of *American Broadcasting Companies, Inc. v. Aereo, Inc.*.[76] In that lawsuit, ABC claimed that Aereo was infringing copyright by allowing its subscribers to watch television programs over the Internet (or watch them later from a recording) around the same time that the programs were broadcast live on television. At the same time, Aereo did not have a license that would allow it to carry out the given transmission. The court ultimately ruled 6 to 3 that Aereo was making a public disclosure. The main conclusions of the court were that, firstly, the company carries out the transmission of programs. It is not simply a matter of providing the infrastructure to ensure the transmission. Secondly, that the relationship between the recipients and the transmitted work is important in determining whether the recipients represent the public, and thus, communication to the public occurs. The court stated that an entity that broadcasts a work to individuals as owners or licensees is not making a communication to the public, while an entity such as Aereo that broadcasts to a large number of paying subscribers, when they are individuals, but those individuals are not connected to each other and therefore form the public, and at the same time have no prior licensing relationship to the broadcast works, is in its sense making a communication to the public.[77]

The previous decision concerned the question of whether there was any communication to the public at all. The second decision is a decision regarding the question of who makes the communication and thereby makes the work available, the user of the service or the provider? In this matter, the Court of Justice of the European Union ruled in the case of *Youtube vs. Cyando*.[78] The basis of the dispute was YouTube's claim that some users of

[76] LONGAN, Mitchell. DIMITA, Geatano. MICHELS, Johan. MILLARD, Christopher. *Cloud Gaming Demystified: An Introduction to the Legal Implications of Cloud-Based Video Games*. In: *SSRN* [online]. 2021. [cit. 27. 4. 2023], p. 32. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3949611

[77] ABC, Inc. v. Aereo, Inc. In: *Harward law review* [online]. 2014. [cit. 25. 4. 2023]. Available at: https://harvardlawreview.org/print/vol-128/abc-inc-v-aereo-inc/

[78] LONGAN, Mitchell. DIMITA, Geatano. MICHELS, Johan. MILLARD, Christopher. *Cloud Gaming Demystified: An Introduction to the Legal Implications of Cloud-Based Video Games.* In: *SSRN* [online]. 2021. [cit. 26. 4. 2023], p. 30. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3949611

MEGA (cloud storage operated by Cyando AG) store and share pirated content (e.g. movies, music, etc.) and that Cyando AG does nothing to prevent this content from being shared. YouTube believed that Cyando AG was infringing copyright by not adequately monitoring and restricting the distribution of these pirated files. The CJEU answered the question by stating that, under normal circumstances, it is users who perform the act of public communication, but hosting platforms acting as intermediaries for making content available can only perform public communication depending on how they interfere with users' activities.[79] To determine the role of cloud storage, the Court stated that "*if the very fact that the use of the platform is necessary for the public to actually enjoy the work, or if it only facilitates this use, would automatically lead to the intervention of the operator of this platform being qualified as "communication", any "provision of a physical device to enable or carry out communication" would indeed constitute such communication, which, however, is point 27 of the rationale of the Copyright Directive, which essentially takes the joint statement on Article 8 of the WCT, expressly excludes.*"[80] The court thus concluded that if the platform serves only as a tool and its use is necessary for the use of the work or facilitates that use, in accordance with Recital 27 of the Infosoc directive, this use of the platform cannot be considered as communication to the public and therefore making the work available.

Compared to both rulings, it cannot be said, that Nvidia and its GFN service are sharing copyrighted works in the form of video games with the public. If we compare GFN with the case of *ABC vs Aereo*, both services allow remote transmission; however, where they differ from each other is the business model of GFN service. This is based on the fact that the player has already purchased the given game (license) and, therefore, only pays for the server infrastructure and computing power. In relation to the user,

[79] REDA, Felix. SELINGER, Joschka. YouTube/Cyando – an Important Ruling for Platform Liability – Part 1. In: *Kluwer Copyright Blog* [online]. 2021. [cit. 28. 4. 2023]. Available at: https://copyrightblog.kluweriplaw.com/2021/07/01/youtube-cyando-an-important-ruling-for-platform-liability-part-1/

[80] Judgment CJEU (Grand chambre) from 22. June 2021 in joined cases C-682/18 and C-683/18, Youtube and Cyano, point 79.

there is thus a relationship between the user of the service and the work itself. The comparison of the second case of *Youtube vs Cyando* in relation to GFN brings the conclusion that if the GFN service serves and facilitates the use of video games, it is also not the communication of a work to the public within the meaning of Article 3 of the Infosoc Directive. Therefore, if the streaming takes place to the device of only one player who is related to this game based on the purchased license (the game files and the game are already pre-installed on the Nvidia servers, so it is just a matter of linking the player account data) from the selected game library to the game data and the GFN service only serves as an intermediary providing remote computing resources, where it facilitates the use of the video game by the player in the sense that the player does not have to install the games on his device or invest in expensive hardware, thereby saving the player's resources and thus making the games generally more accessible to use, we cannot consider the cloud streaming technology as communication to the public. The author of this work thus agrees with the opinion of Longan, Dimiti, Michels and Millard in their (already quoted) published work *Cloud Gaming Demystified: An Introduction to the Legal Implications of Cloud-Based Video Games*, that streaming via GFN cannot be considered as publishing a work to the public.

Given these facts, that streaming via GFN cannot be considered as publishing a work to the public, Nvidia would probably not need a license to communicate to the public with its GFN service. However, since its full release, Nvidia has been doing so, probably out of caution, as this view is not yet firmly anchored in doctrine, and the question is whether there will ever be a lawsuit in the future that will answer this exact question. Nvidia thus often has secured consent and is allowed to stream from the property rights holder based on extensive partnership agreements. Withal, the permission to stream a game with GFN technology can also be based on the end-user license terms (EULA) of the game publishing studios, the EULA of the games themselves, and last but not least, just a simple measure of consent from the given developer or publisher that Nvidia can place the game in its offer and it can be streamed.

Unfortunately, Nvidia did not take this step at first, and during the beta version, Nvidia placed games in its offer without these consents or consents based on license agreements. After the launch of the full-fledged version, the GFN service decided to start using the opt-in consent mode for the placement of the given video game in its offer. Game publishing companies, due to the first failure to secure consent and then the introduction of the opt-in regime, therefore took different positions on GFN. Some companies such as Activision Blizzard Bethesda, Capcom, Crytek, Konami, Xbox Game Studios, Rockstar, Sega, and Square Enix have left the service or terminated their cooperation with the service. Other companies such as Bandai Namco, Bungie, CCP Games, Electronic Arts, Epic, Riot, Ubisoft, and Valve remained.[81]

After some studios left this gaming platform, they spoke out against it (and similar services on the same principle) in their end-user license agreements. For example, Blizzard's current EULA license terms are quite reserved in relation to cloud streaming and the use of cloud computing technologies. The terms and conditions include section C, dealing with license restrictions in relation to users. Blizzard "*hereby*" declares that the Company may suspend or even terminate the user's license to use the Platform or any part, component or feature thereof (*the word Platform Blizzard means (1) the Battle.net computer application software, (2) the Battle.net Game Service, (3) each of the Games, (4) the authorized mobile applications relating to the Battle.net Games and Services, and (5) all features and components of each, whether installed or used on a computer, console or mobile device*), if the User violates the license restrictions below or if the user will assist other users in violating the license terms. According to these license agreements, the user therefore agrees that he will not subsequently, according to point V, which directly stipulates restrictions regarding cloud computing, "*use the platform in connection with any third-party cloud computing service, cloud gaming service or any software or service intended to enable unauthorized streaming or*

[81] STATT, Nick. Nvidia says developers must now opt in to include games on GeForce Now. In: *The Verge* [online]. 2020. [cit. 28. 4. 2023]. Available at: https://www.theverge.com/2020/5/27/21272558/nvidia-geforce-now-opt-in-agreement-game-developers-publishers-licensing-cloud-gaming

transmission of game content from a third-party server to any device." [82] The company thus stipulates in the conditions and is quite specific that it does not want users of its platforms to use cloud services that enable streaming.

However, as for Konami's EULA license terms, they only prohibit using the game as part of a "*remote access arrangement*"[83]. The ban is drafted more generally than the prohibition in Blizzard's license terms. But although the ban is built on the general wording of the prohibition on the use of the game in the context of a remote access arrangement, the prohibition, unfortunately, stands in relation to cloud gaming services, and Konami's license therefore also does not permit the use of cloud streaming technologies.

In contrast, Electronic Arts' license terms do not prohibit cloud technologies and in fact, do not mention them at all.[84] However, what Electronic Arts has done is to enter into a partnership with Nvidia and the EA's games are on the service's offer. [85] It is clear that Nvidia's model is controversial, as its business model does not include game publishers who lose revenue because there is no separate purchase of a game license for cloud access (as with competing cloud gaming services such as PlayStation Now). Nevertheless, Electronic Arts, as well as other companies that support GFN, understand that this is a unique opportunity to get, for example, some of their most popular game series into the hands of a rapidly growing global gaming audience as GFN extends the reach of the gaming experience to millions of gamers who do not have sufficiently powerful devices.

In relation to the mentioned company, Activision Blizzard, a new fact appeared that changed its direction and decision-making possibilities. In 2022, the largest video game deal in history took place in the form of Mi-

---

[82] Part C, Section V of the Blizzard End User License Terms. [online]. Last revised 9/19/2022. [cit. 15. 4. 2023]. Available at: https://www.blizzard.com/en-us/legal/08b946df-660a-40e4-a072-1fbde65173b1/blizzard-end-user-license-agreement

[83] Section 6 of the Konami End User License Terms. [online]. [cit. 16. 4. 2023]. Available at: http://simpleeulas.weebly.com/konami-eula.html

[84] Electronic Arts End User License Terms. [online]. [cit. 16. 4. 2023]. Available at: https://www.ea.com/cs-cz/legal/user-agreement

[85] HAGEDOORN, Hilbert. Nvidia Partners With Electronic Arts to Bring Hit Games to GeForce NOW. In: *Guru 3D* [online]. 2021. [cit. 29. 4. 2023]. Available at: https://www.guru3d.com/story/nvidia-partners-with-electronic-arts-to-bring-hit-games-to-geforce-now/

crosoft's purchase of Activision Blizzard. In addition to this, Microsoft and Activision Blizzard took a 180-degree turn when Microsoft announced on February 21, 2023, a newly formed ten-year partnership with Nvidia and its GFN service. Microsoft thus apparently realized the huge potential of cloud gaming and the potential of the GFN business model in terms of the possibility of reaching the masses of gamers.[86] So far, however, GFN does not include Microsoft's game offerings. Therefore, we can probably expect their addition to the menu in the near future, as well as a change in the license terms, when streaming or transferring game content from Nvidia servers to any device for games under the Microsoft roof, will be allowed in the licenses. Nvidia and its GFN service will probably not be granted license exclusivity as the only cloud gaming platform, given that Microsoft itself operates the cloud gaming platform Xbox Game Pass Ultimate, yet we cannot say with certainty what development awaits us in the future, after all, in the words of Phil Eisler as mentioned in introduction, the future of cloud gaming is limited only by our imagination.

3.2 COPYRIGHT REPRODUCTION AND CLOUD STREAMING

If we start again from the Infosoc directive, the reproduction of the author's work according to the second article of the directive is understood as "*direct or indirect, temporary or permanent reproduction by any means and in any form, in whole or in parts*"[87], while permission or prohibition to reproduce the work is available to the author of the work according to the same article. It is thus within the author's sphere of influence to decide the fate of the work. EU law (as well as the Czech Copyright Act, into which the Union regulation was transposed) distinguishes several types of reproductions of the author's work related precisely to the method of reproduction of the work. At first, these are direct, indirect, permanent, and temporary repro-

[86] Microsoft News Center. Microsoft and Nvidia announce expansive new gaming deal. In: *Microsoft news* [online]. 2023. [cit. 30. 4. 2023]. Available at: https://news.microsoft.com/2023/02/21/microsoft-and-nvidia-announce-expansive-new-gaming-deal/

[87] Article 2 Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society.

ductions. However, it is also necessary to mention that from the point of view of copyright and the reproduction of an author's work, there are other types of reproductions. For example, it is possible to mention intentional and accidental reproductions, identical and non-identical reproductions, with or without economic significance. However, these do not make relevant sense for the work as the first four mentioned above.

As for direct reproduction, according to Telec and Tůma, this reproduction consists of the reproduction of the work by directly reproducing its original expression.[88] Simply put, it is a copy of the original work. Indirect reproductions, on the other hand, consist of the expression of the work in a way other than its immediate reproduction and are often related in particular to a change in the form of the reproduction compared to its model or the natural nature of the work. For example, we could consider its musical notation to be an indirect reproduction of a performed musical work, or its construction to be an indirect reproduction of an architectural work expressed in construction documentation, and its photograph to be an indirect reproduction of a visual work. An indirect reproduction of a work must be distinguished from a mere description of the work or instructions for its production, which is not a reproduction of the work (e.g. the production of a confectionery product according to a recipe that meets the characteristics of a literary work is not a reproduction of this recipe).[89] Permanent reproduction or, better said, the property of its permanence is related to the existential permanence of the material on which it is captured.[90] For example, if a reproduction is captured on paper and on an external HDD again in image form, both reproductions are permanent, but the external HDD is a more permanent reproduction than the reproduction on paper. However, existentially, all reproductions, although permanent, are also temporary, as they cease to exist by their destruction. This brings us to the temporal reproduction, where temporality must be judged from the point of view of

[88] TELEC, Ivo, TŮMA, Pavel. § 13 [Reproduction]. In: TELEC, I., TŮMA, P. *Copyright Act*. 2nd. edition. Praha: C. H. Beck, 2019, p. 179.

[89] Ibidem pp. 179 – 180.

[90] Ibidem, p. 179.

their independence from the mentioned durability of their carrier and from the point of view of their purpose. These are therefore reproductions whose duration, by the very nature of the capture of the work, is not unconditionally linked to the existence of the carrier or whose existence is predetermined and limited only by the duration of the specified purpose for which they were made.[91]

In the first part of the work, the technical functioning of cloud streaming was explained. It is a process of transferring data packets, in which the packets are arranged in a consecutive sequence while travelling through the network (although the delivery of the packets as such or in the correct order is not guaranteed) and this sequence is subsequently downloaded from the server in the form of a data file and made available to the stream user on his end device in the form of an audiovisual file. At the same time, the fundamental question here is who reproduces the given content, whether the user of the service or the provider of the cloud service?

Earlier in the past, the reproduction of a game would mean simply making a copy of the original game itself, when players made copies of the games on their own computers and thus reproduced these games among themselves, but unfortunately with the advent of cloud technologies and especially the GFN service, the situation regarding the reproduction of copyrighted works is a little more complicated, and the reproduction does not have to occur only by making a copy of the game software on one device, but also by cloud streaming itself.

As mentioned again in the first part of the thesis, GFN uses the IaaS cloud tool, a tool generally built on the fact that it provides the user with a remote computing and server infrastructure that the user can use at his discretion. In the context of GFN, it is subsequently an IaaS consumer model, where the user uses remote access to computing and server (cloud) infrastructure for playing video games, with the specifics that the user may only use supported software based on BYOL (bring your own license), i.e.

[91] TELEC, Ivo, TŮMA, Pavel. § 13 [Reproduction]. In: TELEC, I., TŮMA, P. *Copyright Act.* 2nd. edition. Praha: C. H. Beck, 2019, p. 179.

that the user uses a game for which he has already acquired a license.[92] The user of the service also does not install the game software on his device, but the installation of the software takes place on a remote server belonging to the cloud infrastructure, where the whole process is functionally the same as if it were an installation on "*his*" physical device.[93] It is therefore necessary to ask the already mentioned fundamental question, namely, who creates the reproduction, the user or the provider? With the aforementioned GFN specifications and the fact that the overall initiative is developed by the user, it is the user of the service who is probably involved in the game reproduction process, since it is the user who installs the reproductions on the given server in connection with his specific previously purchased game license. This would be a direct temporary reproduction. The given directness consists in the direct derivation from the original of the given game work and the temporality in the fact that the reproduction of the game (copy) is placed on the server for the purpose of playing the given video game via cloud servers by the user.

But what about the service provider? Longa, Dimiti, Michels and Millard state that in this respect a quite logical argument is offered, related to the conclusion made in the previous chapter dedicated to making the work available to the public, that the cloud service provider again only passively provides its services to ensure streaming functionality using its server infrastructure and does not participate in the process of reproduction of the game work, however, they also add that this issue is unclear.[94] However, there is an argument to support the opposite view, that there is duplication of work by the service provider because cloud service providers often add a clause to their terms of use (TOU) that provides compensation for the cloud service operator in the event that a lawsuit is filed and there is a lawsuit by the third person affected by the violation of intellectual property

[92] LONGAN, Mitchell. DIMITA, Geatano. MICHELS, Johan. MILLARD, Christopher. *Cloud Gaming Demystified: An Introduction to the Legal Implications of Cloud-Based Video Games*. In: *SSRN* [online]. 2021. [cit. 2. 6. 2023], p. 59. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3949611

[93] Ibidem.

[94] Ibidem.

rights related to the service user's content.[95] These indemnification clauses indicate that cloud service providers are aware that they can reproduce works[96] and therefore try to minimize the risk of harm caused by the user's actions. However, with respect to the GFN service and its TOU, there is no such indemnification clause in the terms[97]. According to this knowledge and again based on the facts mentioned above, we could say that there is no reproduction of the work.

In addition, if we consider that cloud gaming works in the same way as a classic live stream, in the sense that the streamed content is temporarily stored in the buffer of the user's end device and the streamed data is overwritten during listening or viewing by the user, and after the end of the stream the data is no longer stored in the end device and is no longer available[98], then according to the judgment of the CJEU in the case of *Public Relations Consultants Association Ltd v Newspaper Licensing Agency Ltd and others*, this streamed data meets the conditions and falls under the exception to the rights to reproduction according to Article 5, paragraph 1 of the Infosoc directive and it is not a reproduction of the work as such.[99] Namely, these conditions are met if, firstly, they are temporary copies of data or data packets necessary for the purpose for which the content is available in streaming mode, in the sense that their duration is limited to the time dur-

---

[95] For example, in the terms of use of AMAZON WEB SERVICES and its cloud computing service, there is a provision that represents this given indemnification clause. In section number 53.9.1. contains a provision that states "…[…] *You will defend and indemnify AWS against all damages, liabilities, fines, penalties, costs and expenses (including reasonable attorneys' fees) arising out of or in any way related to your direct or indirect failure to comply with the requirements of this Section*…[…]."

[96] LONGAN, Mitchell. DIMITA, Geatano. MICHELS, Johan. MILLARD, Christopher. *Cloud Gaming Demystified: An Introduction to the Legal Implications of Cloud-Based Video Games*. In: *SSRN* [online]. 2021. [cit. 2. 6. 2023], p. 61. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3949611

[97] See the GeForce Now Terms of Use, available at: https://www.nvidia.com/en-us/geforce-now/terms-of-use/

[98] STROWEL, Alain. *'Private Copying Levies do not Apply in the Case of Streaming'*. [online]. 2020. [cit. 6. 7. 2023], p. 13. Available at: https://cdn.digitaleurope.org/uploads/2021/04/Expert-Opinion_Streaming-and-Private-Copying-Levies_Strowel.pdf

[99] Judgment CJEU (fourth chambre) from 5. June 2014 in joined case C-360/13, Public Relations Consultants Association Ltd v Newspaper Licensing Agency Ltd and others, point 65.

ing which the content is available in streaming mode, secondly, that these data are necessary for the proper completion of the entire technological process of streaming, and thirdly, that the deletion of this data comes automatically at the end of the process and takes place without human intervention.[100] All these conditions in relation to downloaded data packets within the ongoing cloud stream via the GFN service should probably be met, therefore these data packets should also fall under the exception to reproduction rights according to Article 5(1) of the Infosoc Directive.

All in all, the answer to the question is that in the context of cloud streaming via GFN, the user of the service, rather than its provider, is responsible for the reproduction of the work.

4. CONCLUSION

The aim of this paper was to disentangle both the technical and copyright implications of cloud streaming. The paper tried to answer the question of *how the transmission of audiovisual content works with Nvidia GFN and how the service affects copyright law in terms of the publication and reproduction of works.* As far as the technical conclusions are concerned, GFN works based on the RTP protocol, when the transmission of audiovisual content takes place in real time with the help of and in a sequence of data packets. Moreover, the GFN service is a service using the IaaS cloud tool, providing remote computing and technical infrastructure to the user. In relation to conclusions about copyright law and cloud streaming, it is not a matter of making the work available in the sense of communicating to the public, since there is already a previous contractual relationship between the user of the service and the work itself, as well as the fact that GFN serves as a tool to use the work. However, the answer to whether this is a reproduction of the work comes with a split in the form of two possible answers. First, the user of the service is responsible for the reproduction, since it is he who initiates the whole process and the installation takes place on the

[100] STROWEL, Alain. *'Private Copying Levies do not Apply in the Case of Streaming'*. [online]. 2020. [cit. 6. 7. 2023], p. 14. Available at: https://cdn.digitaleurope.org/uploads/2021/04/Expert-Opinion_Streaming-and-Private-Copying-Levies_Strowel.pdf

remote virtual device in relation to his "brought" license. Secondly, the provider should not be responsible, as it passively ensures the functionality of the cloud stream, as well as the fact that the data created during the stream is only a technical part of the entire process.

5. BIBLIOGRAPHY

[1] ABC, Inc. v. Aereo, Inc. [online]. *Harward law review*. 2014. [cit. 25. 4. 2023]. Available at: https://harvardlawreview.org/print/vol-128/abc-inc-v-aereo-inc/

[2] Annex no. 1 in Strategic analysis of cloud services-Č. j.: 7226/2022-NÚKIB-E/310 • BRNO. [online]. 2022. [cit 11. 4. 2023]. Available at: https://www.nukib.cz/download/publikace/analyzy/Strategicka%20analyza%20cloudovych%20sluzeb.pdf

[3] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society

[4] Blizzard End User License Terms. [online]. Last revised 9/19/2022. [cit. 15. 4. 2023]. Available at: https://www.blizzard.com/en-us/legal/08b946df-660a-40e4-a072-1fbde65173b1/blizzard-end-user-license-agreement

[5] CLOVER, Juli. Nvidia's Free GeForce NOW Beta Lets You Play System Intensive PC Games on Your Mac. In: *Macrumors* [online]. 2017. [cit. 10. 3. 2023]. Available at: https://www.-macrumors.com/2017/10/13/nvidia-geforce-now-beta-for-mac/

[6] CRANZ, Alex. Nvidia's Game-Streaming Service Is Finally Live. In: *Gizmodo* [online]. 2020. [cit. 10. 3. 2023]. Available at: https://gizmodo.com/after-7-years-in-beta-nvidias-game-streaming-service-i-1841449313

[7] DI DOMENICO, Andrea. PERNA, Gianluca. TREVISAN, Martino. VASSIO, Luca. GIORDANO, Danilo. A *Network Analysis on Cloud Gaming: Stadia, GeForce Now and PSNow*. Network, [online]. 2021. [cit. 16. 3. 2023]. p 3. Available at: https://www.mdpi.com/2673-8732/1/3/15

[8] Electronic Arts End User License Terms. [online]. [cit. 16. 4. 2023]. Available at: https://www.ea.com/cs-cz/legal/user-agreement

[9] HAGEDOORN, Hilbert. Nvidia Partners With Electronic Arts to Bring Hit Games to GeForce NOW. In: *Guru 3D* [online]. 2021. [cit. 29. 4. 2023]. Available at: https://www.guru3d.com/story/nvidia-partners-with-electronic-arts-to-bring-hit-games-to-geforce-now/

[10] Judgment CJEU (Grand Chambre) from 22. June 2021 in joined cases C-682/18 and C-683/18, Youtube and Cyano

[11] Judgment CJEU (fourth chambre) from 5. June 2014 in joined case C-360/13, Public Relations Consultants Association Ltd v Newspaper Licensing Agency Ltd and others

[12] LICHNOVSKÝ, Bohuslav. NONNEMANN, František. Clouds and the law - Part 1: Why to think about them and what to prepare for. In: *Epravo.cz*[online]. 2022. [cit. 10. 4. 2023]. Available at: https://www.epravo.cz/top/clanky/cloudy-a-pravo-1-dil-proc-o-nich-uvazovat-a-na-co-se-pripravit-115077.html

[13] KOISTINEN, Tommi. *Protocol overview: RTP and RTCP*. In: *Research Gate*[online]. 1999. [cit. 24. 3. 2023], p. 2. Available at: https://www.researchgate.net/publication/251203018_Protocol_overview_RTP_and_RTCP

[14] Konami End User License Terms. [online]. [cit. 16. 4. 2023]. Available at: http://simpleeulas.weebly.com/konami-eula.html

[15] MAG UHG, Gordon. Nvidia GeForce Now aims to be the 'Netflix of games' for just 8 bucks a month. In: *PCWorld* [online]. 2015. [cit. 10. 3. 2023]. Available at: https://www.pcworld.com/article/423733/nvidia-geforce-now-aims-to-be-the-netflix-of-games-for-just-8 bucks.html#:~:text=Nvidia%20GeForce%20Now%20aims%20to%20be%20the%20%E2%80%98Netflix,after%20purchase.%20...%204%204K%20gaming%20too%20

[16] Microsoft News Center. Microsoft and Nvidia announce expansive new gaming deal. In: *Microsoft news* [online]. 2023. [cit. 30. 4. 2023]. Available at: https://news.microsoft.com/2023/02/21/microsoft-and-nvidia-announce-expansive-new-gaming-deal/

[17] PARRISH, Kevin. What is packet loss, and how do you fix it? In: *Digital trends* [online]. 2021. [cit. 28. 3. 2023]. Available at: https://www.digitaltrends.com/computing/what-is-packet-loss-and-how-to-fix/

[18] PUŽMANOVÁ, Rita. *Streaming media (4): transportní protokoly RTP/RTCP*. [online]. 2004. [cit. 25. 3. 2023]. Available at: https://www.dsl.cz/clanky/60-streaming-media-4-transportni-protokoly-rtprtcp

[19] REDA, Felix. SELINGER, Joschka. YouTube/Cyando – an Important Ruling for Platform Liability – Part 1. In: *Kluwer Copyright Blog* [online]. 2021. [cit. 28. 4. 2023]. Available at: https://copyrightblog.kluweriplaw.com/2021/07/01/youtube-cyando-an-important-ruling-for-platform-liability-part-1/

[20] SCHULZRINNE, Hennig at al. *RFC3550: RTP: A Transport Protocol for Real-Time Applications*. [online]. 2003. [cit. 20. 3. 2023]. Available at: https://dl.acm.org/doi/book/10.17487/RFC3550

[21] STATT, Nick. Nvidia says developers must now opt-in to include games on GeForce Now. In: *The Verge* [online]. 2020. [cit. 28. 4. 2023]. Available at: https://www.theverge.com/2020/5/27/21272558/nvidia-geforce-now-opt-in-agreement-game-developers-publishers-licensing-cloud-gaming

[22] STROWEL, Alain. *'Private Copying Levies do not Apply in the Case of Streaming'*. [online]. 2020. [cit. 6. 7. 2023] p. 13. Available at: https://cdn.digitaleurope.org/uploads/2021/04/Expert-Opinion_Streaming-and-Private-Copying-Levies_Strowel.pdf

[23] TELEC, Ivo, TŮMA, Pavel. § 13 [Reproduction]. In: TELEC, I., TŮMA, P. *Copyright Act*. 2nd. edition. Praha: C. H. Beck, 2019

[24] VJESTICA. Adam. Nvidia GeForce Now interview: 'the future of cloud gaming is only limited by our imagination'. In: *Tech radar* [online]. 2022. [cit. 10. 3. 2023]. Available at: https://www.techradar.com/features/nvidia-geforce-now-interview-the-future-of-cloud-gaming-is-only-limited-by-our-imagination

---

RECENZE ZÁVĚREČNÝCH PRACÍ I/2023

OBSAH SEKCE

MAŠKA, J.: NENÁVISTNÉ PROJEVY NA INTERNETU

LUKÁŠ BOHUSLAV[1]

MAŠKA, J.: Nenávistné projevy na internetu. 2023, diplomová práce, Univerzita Karlova, Právnická fakulta, 253 s.

ANOTACE

Téma předkládané diplomové práce Nenávistné projevy na internetu se zabývá aktuálním a dynamickým fenoménem především počítačové a internetové kriminality. V první části práce jsou představeny základní pojmy jako počítačová a internetová kriminalita, nenávistné projevy, předsudečná kriminalita, extremismus či svoboda projevu. Pojem nenávistných projevů je rovněž vyložen v kontextu lidských práv. Práce se dále zabývá základním pojmoslovím, principy fungování internetu a počítačových sítí, mapuje jejich vývoj a zabývá se jejich přiléhavými vlastnostmi. Druhá část práce se věnuje přehledu právní úpravy České republiky ve vztahu k nenávistným trestným činům, a to zejména z hlediska trestního práva, ale i ústavního práva či správního práva, ale i instrumentů na hranici faktických úkonů a politiky uplatňované vůči nenávistným projevům. V třetí části práce je pozornost dedikována otázce omezování svobody projevy za účelem ochrany před nenávistnými projevy. Nejprve jsou vyloženy základy ochrany svobody projevu a možnosti jejího omezení, následně je představen přehled relevantní judikatury jak Ústavního soudu, tak obecných soudů. Tato část práce je zakončena statistickým shrnutím případů nenávistných projevů. Čtvrtá část práce předkládá vhled do názorů odborné veřejnosti stran nenávistných projevů na internetu a diskutuje významné otázky spojené se zkoumanou problematikou. Zprvu autor předkládá právně-filozofické úvahy sdílené v rámci evropského právního prostoru. Ty jsou doprovázeny kritickým hodnocením konceptu ver-

[1] doc. JUDr. Lukáš Bohuslav, Ph.D. působí na katedře trestního práva Právnické fakulty Univerzity Karlovy. Kontaktní e-mail: bohuslav@prf.cuni.cz

bální nenávistné kriminality z pohledu trestního práva. Po něm jsou představeny názory významných představitelů systému trestní justice. Práci uzavírá úvaha nad vlivem extrémů na lidskou společnost.

KLÍČOVÁ SLOVA

Počítačová a internetová kriminalita; nenávistné projevy na internetu; omezování svobody projevu

ABSTRACT

The topic of the thesis Hate speeches on the Internet deals with the current and dynamic phenomenon of computer and Internet crime. The first part of the thesis introduces basic concepts such as cyber and internet crime, hate speech, bias crime, extremism, and freedom of expression. The concept of hate speech is also explained in the context of human rights. The thesis also discusses basic terminology, the principles of the Internet and computer networks, charts their evolution and discusses their adjacencies. The second part of the thesis is devoted to an overview of the legal regulation of the Czech Republic in relation to hate crimes, especially from the point of view of criminal law, but also constitutional law or administrative law, as well as instruments on the border of factual acts and policies applied to hate speech. In the third part of the thesis, attention is devoted to the issue of restricting freedom of expression to protect against hate speech. First, the basics of the protection of freedom of expression and the possibilities of its limitation are laid out, followed by an overview of the relevant case law of both the Constitutional Court and the general courts. This part of the work is concluded with a statistical summary of hate speech cases. The fourth part of the thesis provides an insight into the opinions of the professional public regarding hate speech on the Internet and discusses important issues related to the examined problem. Initially, the author presents legal-philosophical considerations shared within the European legal area. These are accompanied by a critical assessment of the concept of verbal hate crime from the perspective of criminal law. After that, the views of prominent representatives of the criminal justice system are presented. The work concludes with a reflection on the impact of extremes on human society.

KEYWORDS

Computer and Internet Crime; Hate Speech on the Internet; Restriction of Freedom of Expression

Plná verze práce je dostupná z: https://dspace.cuni.cz/handle/20.500.11956/181203

Téma práce je naprosto aktuální, závažné a je třeba mu věnovat zvýšenou pozornost, a to z pohledu *de lege lata* i *de lege ferenda*. Nenávistné projevy na internetu jsou fenoménem, jehož bude přibývat na intenzitě a každé další zkoumání je potřebné a žádoucí. A to nejen zdrojů z literatury, ale i soudních rozhodnutí.

Stran teoretických znalostí autor čerpal znalosti zejména z trestního práva hmotného, ale i trestního práva procesního a ústavního práva. Diplomant vyhledal vzhledem k tématu nadstandardní množství informací, které následně zpracoval sice přiléhavě, ale značně překonal obvyklý rozsah diplomové práce. Autor v práci aplikoval především deskriptivní a analyticko-syntetickou metodu výzkumu.

Předložená práce představuje z hlediska obsahu kvalitní zpracování zvoleného tématu. Je vidět pečlivá, promyšlená práce autora s literaturou a kvalitní excerpce poznatků. Lze ocenit prezentaci vlastního odůvodněného názoru. Velmi pěkná konkluze načerpaných poznatků je reflektována v závěru práce. Autor užil nadstandardní množství zdrojů včetně zdrojů ze zahraniční literatury. Práce obsahuje rovněž zdroje elektronické povahy. Práci s judikaturou byla věnována značná pozornost. Poznámkový aparát je bohatý, autor si na něm dal velmi záležet.

Práce je interdisciplinární povahy. Autor podstatným způsobem respektuje základní ústavní principy a staví je do kontrastu s možností postihu nenávistných projevů prostředky trestního práva. To dokládá např. pojednání o silné demokracii (s. 205 práce).

Diplomant předložil vhodně strukturovanou práci, která je systematicky dobře členěna. Autor postupuje od obecného ke konkrétnímu. Úvodní kapi-

toly jsou pěkným deskriptivním, ale v zásadě dosti komplexním přiblížením problematiky, nicméně meritum práce lze shledávat v kapitole druhé (východiska plynoucí z ústavního a trestního práva), kapitole třetí (především svoboda projevu, ochrana Ústavním soudem), ale rovněž kapitole čtvrté, která se zaměřuje na právní, filozofické, ale rovněž do jisté míry politické úvahy. Poslední kapitolou předložené diplomové práce je závěr.

Práce je graficky přehledná, obsahuje množství zajímavých statistických dat, přičemž ta by v některých pasážích zasluhovaly hlubší komentář. Z hlediska jazykového je práce na velmi dobré úrovni a je psána čtivým jazykem.

Lze shrnout, že diplomant předložil práci, ve které mnohdy prezentuje vlastní odůvodněný názor založený na pečlivém studiu problematiky. Lze ocenit interdisciplinární vhled a analýzu mimo oblast práva, která má přirozené dopady do kriminologie a právní úpravy.

Závěrem doporučuji uchazečům o hlubší vhled do zkoumané problematiky, aby si předkládanou diplomovou práci přečetli, neboť se nebude jednat o promarněný čas. To mohu slíbit.

BORÁKOVÁ, R.: OCHRANA SOUKROMÉHO A RODINNÉHO ŽIVOTA PŘI UKLÁDÁNÍ TRESTU – REFLEXE NÁLEZU II. ÚS 2027/17 V PRAXI OBECNÝCH SOUDŮ

ZDENĚK ČERVÍNEK[2]

BORÁKOVÁ, R.: Ochrana soukromého a rodinného života při ukládání trestu – reflexe nálezu II. ÚS 2027/17 v praxi obecných soudů, 2023, diplomová práce, Univerzita Palackého v Olomouci, Právnická fakulta, 75 s.

ANOTACE

Diplomová práce mapuje přístup obecných soudů České republiky k povinnosti zohlednit nejlepší zájem dítěte při ukládání nepodmíněného trestu odnětí svobody jeho rodiči. Tato povinnost plyne z Úmluvy o právech dítěte, jejíž smluvní stranou je také Česká republika. Nutnost dodržování této povinnosti již zdůraznil také Ústavní soud České republiky ve svém nálezu ze dne 7. srpna 2017, sp. zn. II. ÚS 2027/17. V popředí uvedené práce tedy stojí problematika nejlepšího zájmu dítěte a reflexe nálezu Ústavního soudu České republiky ze dne 7. 8. 2017, sp. zn. II. ÚS 2027/17. Proto mezi další výchozí prameny patří Listina základních práv a svobod, Úmluva o ochraně lidských práv a základních svobod, Listina základních práv EU ale také judikatura Ústavního soudu České republiky či Evropského soudu pro lidská práva. Skutečný přístup obecných soudů k dodržování mezinárodních závazků vyplývá z praktické analýzy 250 prvostupňových rozsudků jimiž byl uložen nepodmíněný trest odnětí svobody, 6

[2] JUDr. Zdeněk Červínek, Ph.D. je odborný asistent na Katedře ústavního práva, Právnické fakulty Univerzity Palackého v Olomouci. Kontaktní e-mail: zdenek.cervinek@upol.cz.

prvostupňových rozsudků, v nichž byl posuzován nejlepší zájem dítěte, ale nedošlo k uložení nepodmíněného trestu odnětí svobody a 49 odpovědí obecných soudů týkajících se posuzování nejlepšího zájmu dítěte. Analýza pracuje s výzkumnými kritérii, jež mají odrazit způsob posuzování nejlepšího zájmu dětí, případné vlivy na výsledek tohoto posuzování a kvalitu odůvodnění zmíněných rozsudků. Přínos této analýzy tudíž spočívá v odhalení reality v oblasti trestání pachatelů rodičů v České republice a nedostatků právní úpravy a praxe s ohledem na lidskoprávní požadavky vnitrostátního a mezinárodního práva. V tomto směru práce nabízí doporučení k systémové změně tak, aby došlo ke zvýšení ochrany zájmů dětí při trestání jejich rodičů.

KLÍČOVÁ SLOVA

Alternativní trest; anonymní rozhovor; empirický výzkum; dítě; nález Ústavního soudu sp.zn. II. ÚS 2027/17; nejlepší zájem dítěte; nepodmíněný trest odnětí svobody; mezinárodní závazky; ohrožení pod vlivem návykové látky; péče poskytovaná rodičem; právo na informace; rodič; rodina; sociálně-právní ochrana dětí; spravedlivý trest; test proporcionality; Úmluva o právech dítěte; Výbor pro práva dítěte

ABSTRACT

This thesis maps the approach of the general courts of the Czech Republic to the obligation to take into account the best interests of the child when imposing an unconditional prison sentence on his/her parents. This obligation stems from the Convention on the Rights of the Child, of which the Czech Republic is a member. The necessity to comply with this obligation has also been emphasised by the Constitutional Court of the Czech Republic in its decision of 7 August 2017, No. II ÚS 2027/17. In the foreground of this thesis is the issue of the best interests of the child and the reflection of the decision of the Constitutional Court of the Czech Republic of 7 August 2017, No. II. ÚS 2027/17. The main sources consist of the Charter of Fundamental Rights and Freedoms, the Convention for the Protection of Human Rights and Fundamental Freedoms, the EU Charter of Fundamental Rights, and the case law of the Constitutional Court of the Czech Republic and the European Court of Human Rights.

The actual approach of the general courts to the compliance with international obligations is shown by a practical analysis of 250 first instance court judgments, that imposed unconditional imprisonment, 6 first instance court judgments in which the best interests of the child were considered but no unconditional imprisonment was imposed, and 49 responses of the general courts regarding the assessment of the best interests of the child. The analysis works with research criteria to reflect the way in which the best interests of children are assessed, the possible influences on the outcome of this assessment and the quality of the reasoning of these judgments. Therefore, the contribution of this analysis lies in revealing the reality of punishment of parents-offenders in the Czech Republic and the shortcomings of legislation and practice with regard to human rights requirements of national and international law. In this respect, the thesis offers recommendations for systemic change in order to increase the protection of children's interests in the punishment of their parents.

KEY WORDS

Alternative Sentence; Anonymous Interview; Empirical Research; Child; Decision of Constitutional Court No. II 2027/17; The Best Interests of the Child; Unconditional Imprisonment; International Commitments; Endangerment Under the Influence of an Addictive Substance; Care Provided by the Parent; Right to Information; Parent; Family; Social and Legal Protection of Children; Fair Punishment; Proportionality Test; Convention on the Rights of the Child; Committee on the Rights of the Child.

Plná verze práce je dostupná z: https://theses.cz/id/bipmk3/

Tato diplomová práce rozebírá pilotní nález Ústavního soudu sp. zn. II. ÚS 2027/17, který se týkal povinnosti trestních soudů zohlednit nejlepší zájem dítěte při ukládání trestních sankcí. Toto rozhodnutí mělo velký ohlas i mimo právnickou komunitu a diplomantka se rozhodla prozkoumat, jakým způsobem je toto rozhodnutí následováno v rozhodovací praxi obecných soudů. Pokud jde tedy čistě o volbu tématu diplomové práce, považuji ji za velmi dobrou a zajímavou, leč ambiciózní a náročnou.

Současně musím konstatovat, že autorka se tohoto tématu zhostila také na výbornou a standardy obecně kladené na diplomové práce naplňuje měrou vrchovatou. Výsledná práce je tak cenným příspěvkem do odborné debaty o ukládání trestních sankcí. Neměla by tudíž uniknout nikomu se zájmem o tuto problematiku a já věřím, že bude též autorkou ještě vhodným způsobem publikována na stránkách odborného tisku.

Co konkrétně přitom v práci najdete? Jak jsem již nastínil, autorka začíná svou analýzu normativním hodnocením pilotního nálezu Ústavního soudu sp. zn. II. ÚS 2027/17, jenž konkretizoval povinnost obecných soudů zohlednit nejlepší zájem dítěte při ukládání nepodmíněného trestu odnětí svobody jeho rodiči. Z něj následně abstrahuje relevantní faktory, jež jí slouží za základ pro empirickou analýzu rozhodovací praxe obecných soudů. V rámci této analýzy zkoumá, jakým způsobem se zmíněný pilotní nález Ústavního soudu a jím proponovaná povinnost vzít při ukládání trestu do úvahy nejlepší zájem dětí pachatelů trestných činů propsaly do rozhodovací praxe obecných soudů (asi nebudu příliš „spoilovat“, když řeknu, že pouze minimálně). Konečně, pro zasazení výsledků normativní i empirické části své práce do kontextu reality české justice autorka také provádí strukturované rozhovory se zástupci relevantních právnických profesí (advokáti, státní zástupci a soudci). A v kontextu odpovědí respondentů se snaží hledat cesty pro řešení zjištěného neutěšeného stavu (minimální reflexe nálezové judikatury Ústavního soudu a principu nejlepšího zájmu dítěte ze strany obecných soudů).

S ohledem na uvedené je třeba autorku pochválit, protože si stanovila ambiciózní cíle a současně se jí podařilo je také naplnit. Nevidí se příliš často, aby se na právnických fakultách zpracovávaly empirické studie. Dokonce by se s trochou nadsázky dalo říci, že je jen málo věcí, které jsou právníkům tak cizí jako právě zpracovávání empirických studií. Nejsme totiž nijak trénováni v metodologii takového druhu (resp. jakéhokoli) výzkumu. Navíc časová náročnost a mravenčí práce, které jejich zpracování provází, má taktéž často na studenty i akademiky odrazující efekt.

Už jsem naťukl otázku metodologie. V tomto směru opět nemám pro autorku nic jiného než pochvalu, neboť postup práce, sběr dat i limity po-

znání, které jí data přináší, jsou transparentně předestřena a dávají dobrý logický smysl. Podporují tak racionalitu závěrů, k nimž autorka ve své práci dospívá. Pokud bych měl být důsledný a zmínit také slabší místo recenzované práce, bylo by jím jen malé množství respondentů výše zmíněných rozhovorů a lepší vysvětlení kritérií svědčících pro jejich relevanci. Nicméně, ohlédnu-li se zpětně za prací, mám pocit, že i přes zmíněnou výhradu dílčí informace získané rozhovory s odborníky z praxe dobře doplňují informační pestrost diplomové práce. Konečně, oceňuji také velmi dobré zakotvení studie v existující odborné literatuře, stejně jako obrovské množství primárních zdrojů (judikatury), které byla diplomantka nucena zpracovat.

Závěrem bych chtěl také konstatovat, že kromě velmi kvalitního obsahu je práce také velmi dobře zvládnutá po formální a jazykové stránce. Má logickou strukturu, je přehledně členěná a moc dobře se čte.

HEROUTOVÁ, A.: KYBERKRIMINALITA NA SOCIÁLNÍCH SÍTÍCH

JAN CHMELÍK[3]

HEROUTOVÁ, A.: Kyberkriminalita na sociálních sítích. 2023, diplomová práce, Západočeská univerzita v Plzni, Fakulta právnická, 98 s.

ANOTACE

Diplomová práce je zaměřena na patologické jevy na sociálních sítích, konkrétně na kyberšikanu, sexting, kybergrooming, kyberstalking a krádež identity. Cílem této práce bylo objasnit, co je obsahem těchto jevů, jaké jsou jejich projevy, a pod které skutkové podstaty trestných činů je lze subsumovat. Současně byla ve vztahu ke každému z těchto škodlivých jevů uvedena odpovídající judikatura, jež umožňuje komplexní pohled na tuto problematiku. Součástí této práce je rovněž kvantitativní výzkum, který si kladl za cíl zjistit úroveň výskytu těchto patologických jevů ve společnosti, a to prostřednictvím dotazníkového šetření s heterogenním souborem respondentů. Na závěr se práce zabývala trestněprocesním postupem orgánů činných v trestním řízením při odhalování a vyšetřování trestné činnosti páchané v tomto prostředí. Tato část vznikla po odborné konzultaci s Oddělením analytiky a kybernetické kriminality Městského ředitelství Policie České republiky v Plzni, s jejichž pomocí bylo možné uvést, jak probíhá tento trestněprocesní postup v praxi.

KLÍČOVÁ SLOVA

Kyberkriminalita; kyberšikana; sexting; kybergrooming; kyberstalking; krádež identity

[3] doc. JUDr. Jan Chmelík, Ph.D. je docentem Západočeské univerzity, Fakulty práva, katedry trestního práva, Plzeň. Kontaktní e-mail: chmelikj@ktr.zcu.cz

ABSTRACT

The thesis focuses on pathological phenomena on social media, namely cyberbullying, sexting, cybergrooming, cyberstalking and identity theft. The aim of this thesis was to clarify what is the content of these phenomena, what are their manifestations, and under which criminal offences they can be subsumed. At the same time, relevant case law has been presented in relation to each of these harmful phenomena, which allows for a comprehensive view of the issue. This thesis also includes quantitative research, which aimed to determine the level of occurrence of these pathological phenomena in society through a questionnaire survey with a heterogeneous set of respondents. Finally, the thesis examined the criminal procedure of law enforcement agencies in the detection and investigation of crimes committed in this environment. This part was written after expert consultation with the Department of Analytics and Cybercrime of the Municipal Police Directorate of the Czech Republic in Plzeň, with whose help it was possible to indicate how this criminal procedure takes place in practice.

KEY WORDS

Cybercrime; Cyberbullying; Sexting; Cybergrooming; Cyberstalking; Identity Theft

Plná verze práce je dostupná z: https://theses.cz/id/pifyhy/

Kyberkriminalita se stala patologickým jevem ve společnosti. Její nárůst a intenzita se stává alarmující pro celou společnost. Její negativní dopady na společnost jsou o to závažnější, že není lehké nalézt cestu k její eliminaci nebo alespoň snížení následků, které ji provází. Odborných publikací zabývajících se touto problematikou je stále zoufale málo, a proto je vítána jakákoli publikace, která se snaží nalézt cesty předcházení, odhalování a následného vyšetřování trestných činů souvisejících s kyberkriminalitou. Ještě větší efekt pak mají ty publikace, které jsou napsány vysoce erudovaně a poskytují vědecký základ pro posuzování tohoto fenoménu. To vše splňuje tato práce.

Diplomová práce je zaměřena na kyberšikanu, sexting, kybergrooming, kyberstalking a krádež virtuální identity, přičemž cílem této práce je objasnit tyto pojmy, poskytnout jejich trestněprávní kvalifikaci a tomu odpovídající judikaturu.

Jako metody práce použité při zpracování lze vydedukovat metodu analýzy, syntézy, výzkumnou metodu. Bohužel v práci nejsou uvedeny.

Pouze jednu diplomovou práci v tomto roce jsem vyzdvihnul a označil za perfektně zpracovanou (DP Konvičková), tuto práci ve všech směrech však předčila tato diplomová práce jejímž tématem je kyberkriminalita, jejíž zpracování co do obsahu, způsobu zpracování a exaktnosti je bezkonkurenční a pokud bych ji měl výslovně hodnotit pak bych musel použít jenom superlativy. Je vynikající svým „nápadem“, strukturou a vlastním zpracováním. Bez zbytečného balastu, uměle tvořenému obsahu řeší od samotného počátku jenom zásadní otázky způsobem, se kterým jsem se ještě nesetkal. Je zaměřena na kyberšikanu, sexting, kybergrooming, kyberstalking a krádež virtuální identity, které analyzuje na vysoké odborné úrovni.

Praktický význam práce koresponduje s vědeckým významem a také je možné jej nalézt při obecném posuzování základní právní úpravy trestných činů páchaných organizovaným zločinem. Praktický význam práce spočívá také v její komplexnosti úpravy, včetně trestněprávní úpravy trestných činů aplikovatelných na organizovaný zločin. Práce je plně využitelná jak při dalším vědeckém zkoumání, tak také v praktické aplikaci.

Argumentace v práci je odborně i věcně správná. Práce používá příléhavou odbornou terminologii, se kterou výstižně pracuje.

Po vymezení základního pojmosloví a rozboru základních otázek kyberprostoru, kybernetické kriminality a kybernetického útoku jsou analyzovány sociální sítě. Poté je obšírně pojednáno o vlastním tématu práce – kyberšikaně, která je rozebírána velmi podrobně, na vysoké odborné úrovni. Obdobně jsou zpracovány i další stěžejní formy kybernetické kriminality a to sexting, kybergrooming, kyberstalking a krádež identity. Každá z těchto forem protiprávního jednání je pak doplněna o bohatou a výstižnou judikaturu, včetně výsledků speciálního výzkumu, který bylv rámci

psaní diplomové práce proveden. Poslední kapitol pojednává o vlastním odhalování a vyšetřování tohoto druhu kriminality se zaměřením zejména na procesní postup při dokování trestné činnosti.

Ke zpracování práce studentka použila dostupnou českou ale i zahraniční literaturu, se kterou dobře pracuje, v přiměřené míře správně cituje. Po formální stránce je práce zpracována na požadované úrovni. Závěrem si dovolím shrnout, že jde o výjimečnou práci po všech stránkách.

PETROVÁ, S.: SDĚLOVÁNÍ AUTORSKÝCH DĚL VEŘEJNOSTI PROSTŘEDNICTVÍM ODKAZU

PETR KALENSKÝ[4]

PETROVÁ, S.: Sdělování autorských děl veřejnosti prostřednictvím odkazu. 2023, diplomová práce, Masarykova univerzita, Právnická fakulta, 86 s.

ANOTACE

Autorka v práci rozebírá pojem odkazů z technického pohledu, včetně možných právně relevantních podob a modifikací způsobu jejich užití v rámci internetového prostředí, představuje institut sdělování díla ve-řejnosti a jeho užití v rámci kvalifikace zásahu odkazů do autorského práva. Na základě porovnání současné rozhodovací praxe SDEU s její reflexí před českými soudy pak práce identifikuje problematické otázky kvalifikace odkazování na internetu jako sdělování díla veřejnosti.

KLÍČOVÁ SLOVA

Autorské právo; sdělování díla veřejnosti; zpřístupňování díla; internetový odkaz; embedding

ABSTRACT

The author analyses the hyperlinks from a technical point of view, including possible legally relevant forms and modifications of their use within the Internet environment, introduces the institute of communication to the public and its use

[4] Mgr. Petr Kalenský je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy Univerzity (*Intellectual Property Law*) a advokátním koncipientem zaměřeným na právo duševního vlastnictví. Kontaktní e-mail: 405146@mail.muni.cz

in the context of the qualification of the interference of hyperlinks with copyright. On the basis of a comparison of the current CJEU decision-making practice with its reflection in front of the Czech courts, the thesis then identifies problematic issues of qualification of linking as communication of a work to the public.

KEYWORDS

Copyright; Communication to the Public; Making the Work Available; Hyperlink; Embedded Link

Plná verze práce je dostupná z: https://is.muni.cz/auth/th/a1fio/

Téma sdělování děl veřejnosti je, zejména v kontextu evropského práva, tématem velmi komplexním, do značné míry kontroverzním, a náročným. Ale také stále aktuálním – a to i díky velmi aktivnímu přístupu Soudního Dvora v této oblasti a přístupu českých soudů spočívajícím v neaplikaci závěrů Soudního Dvora.

Vzhledem k rozsáhlosti judikatury v této oblasti bylo pro účely závěrečné práce nutné vhodně vymezit její cíl. To autorka učinila, když hlavní cíl práce vymezila velmi prakticky. Totiž, že cílem je odpovědět na otázku, za jakých podmínek a při dodržení jakých postupů je pro uživatele internetu legální užívání odkazů na jednotlivé webové stránky a potažmo na autorská díla na nich se nacházející, a to bez souhlasu autora.

A právě ve splnění tohoto hlavního cíle shledávám největší přínos závěrečné práce autorky. Autorka svoji analýzou poskytuje přehledné, byť (adekvátně) obsáhlé shrnutí judikatorní praxe Soudního Dvora EU a českých soudů, které závěry této rozhodovací praxe často nereflektují, či je reflektují pouze omezeně. A to včetně přehledných grafických znázornění, které mohou čtenářům méně zasvěceným do problematiky významně pomoci pochopit komplexní rozhodovací praxi Soudního Dvora EU. Autorka popisuje nikoli pouze právní stránku odkazů, ale poskytuje také vysvětlení toho, co vůbec je podstatou odkazu a s jakými druhy odkazů se lze setkat. I to je

velmi relevantní pro správné pochopení (ale i utváření) rozhodovací praxe soudů.

Ačkoli by samotný popis rozhodovací praxe Soudního Dvora vystačil na samostatnou práci (resp. vícero samostatných prací), autorka se rovněž zaměřila i na judikaturu českých soudů, kterou zkoumala zejména z perspektivy rozhodovací praxe Soudního Dvora – tedy, nakolik je judikatura českých soudů konzistentní s judikaturou Soudního Dvora. Autorka rovněž pracovala se soudními rozhodnutími, které na základě žádosti o poskytnutí informací obdržela od okresních a krajských soudů, z nichž vytvořila přehlednou statistiku uvedenou na straně 65 práce.

Ze strany autorky lze tak ocenit (úspěšnou) snahu o to, některé své dílčí závěry podložit empirickými informacemi a tyto empirické poznatky systematizovat.

Po obsahové stránce práci opravdu nelze vytknout takřka nic. Jedná se o vysoce kvalitní analýzu příslušné právní úpravy, která je přehledná, ale zároveň kvůli této přehlednosti neslevuje na kvalitě poskytnutých informací.

Mou jedinou „výhradou“ vůči závěrečné práci a její struktuře je snad jen zahrnutí samostatné podkapitoly o NFTs. Ačkoli tato tématika nepochybně souvisí se sdělováním děl veřejnosti (což autorka rovněž vysvětluje), působí tato sub-kapitola mírně nesystematicky a jako systematičtější v kontextu práce by mohlo být, kdyby prostor věnovaný NFTs byl věnován k dalšímu „dokrášlení“ hlavního cíle práce, tedy vytvoření jakési „mapy“ pro orientaci v judikatuře ke sdělování děl veřejnosti prostřednictvím odkazu.

Práce autorky dle mého názoru zdaleka přesahuje kvality, které lze očekávat od diplomové práce a povzbuzuji tímto autorku k tomu, aby téma případně rozpracovala formou rigorozní či jiné rozsáhlejší práce, pro kterou práce autorky tvoří více než kvalitní základ.

MIZEROVÁ, T.: PRÁVNÍ NÁSTROJE BOJE PROTI DEZINFORMACÍM NA INTERNETU

FRANTIŠEK KASL[5]

MIZEROVÁ, T.: Právní nástroje boje proti dezinformacím na internetu. 2023, diplomová práce, Masarykova univerzita, Právnická fakulta, 126 s.

ANOTACE

Dezinformace šířené v kyberprostoru představují výzvu pro demokratický právní stát. Cílem této diplomové práce je najít a posoudit existující právní nástroje, které je možné v boji proti dezinformacím použít. V práci jsou rozebrány ústavněprávní východiska existujících i budoucích právních nástrojů určených k omezení šíření dezinformací. Další kapitoly se věnují nástrojům, které nabízí právo občanské, trestní a dílčím aspektům odpovědnosti ISP. V závěrečných kapitolách je provedena případová studie blokování dezinformačních webů po invazi ruských vojsk na Ukrajinu a jsou představeny vládní aktivity v oblasti boje proti dezinformacím.

KLÍČOVÁ SLOVA

Dezinformace; blokování dezinformačních webů; fake news; ochrana osobnosti; verbální trestné činy; internet; svoboda projevu; omezení svobody projevu; akt o digitálních službách

[5] JUDr. Ing. František Kasl, Ph.D. je odborným pracovníkem Centra vzdělávání, výzkumu a inovací v informačních a komunikačních technologiích Fakulty informatiky a Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontaktní e-mail: frantisek.kasl@muni.cz

ABSTRACT

Disinformation spread in cyberspace poses a challenge to the democratic rule of law. The aim of this thesis is to find and assess existing legal instruments that can be used in the fight against disinformation. The thesis analyzes the constitutional legal basis of existing and future legal instruments designed to limit the spread of disinformation. Other chapters are devoted to the tools offered by the law for the civil, criminal and partial aspects of ISP liability. In the final part of the thesis, case study of the blocking of disinformation websites after the invasion of Ukraine by Russian troops is conducted, and government activities in the field of combating disinformation are presented.

KEYWORDS

Disinformation; Disinformation Content Restriction; Fake News; Personality Rights Protection; Verbal Crimes; Freedom of Speech; Freedom of Speech Restrictions; Digital Services Act

Plná verze práce je dostupná z: https://is.muni.cz/th/c8yvj/

Zvolené téma práce je aktuální a řešená perspektiva reflektuje rostoucí potřebu řešit dopady spojené s nárůstem frekvence a dopadu dezinformací na společnost skrze právní nástroje. Za relativní slabinu zvoleného tématu ovšem pokládám omezení se na národní právo a upozadění unijních aktivit v této oblasti. Dezinformace nejsou problémem národním, ale jsou jim vystaveny ve srovnatelné či větší míře i sousední státy. S ohledem na charakter šíření informací po internetu je pak tendence k hledání národních řešení nutně nedostatečná. I vzhledem k roli nadnárodních platforem je pak stěžejní mezinárodní, resp. unijní aktivita a koordinace.

Tato rovina byla v tématu práce cíleně upozaděna, není to ovšem z důvodu, že by jeho významnost autorka pomíjela. Této oblasti se autorka spolu s vedoucím práce věnovala v samostatném publikačním výstupu, kte-

rý vyšel v časopise Právník,[6] a bylo tudíž na místě jej ze zaměření a obsahu práce vydělit. Pokud je tedy na práci nahlíženo společně s tímto dodatečným "dílem skládačky", jedná se o komplexní a velmi zdařilý zdroj k předmětné problematice, který je přínosným příspěvkem do aktuálního diskurzu.

Cílem práce bylo prozkoumat národní právní nástroje pro boj proti dezinformacím, zhodnotit jejich účinnost a diskutovat vhodná budoucí legislativní opatření a iniciativy, které by mohly přispět k omezení šíření dezinformací. Tyto cíle práce v zásadě naplňuje, byť autorka nevěnuje tolik prostoru doporučením *de lege ferenda*, kolik by dle mého názoru mohla.

Práce je po obsahové stránce kvalitní, autorka se problematice věnuje dlouhodobě (srov. *disclaimer* na s. 17) a má tudíž dobrou orientaci v českém prostředí boje proti dezinformacím. Převážná část práce je deskriptivního charakteru, autorka důsledně rozebírá jednotlivé nástroje a instituty platné a účinné národní právní úpravy. Představené poznatky jsou velmi důsledně odzdrojovány a autorka prokázala schopnost shromáždit a zanalyzovat nejen odborné zdroje, ale i relevantní judikaturu (přičemž přístup k části vyžadovala dodatečnou aktivitu, srov. s. 21). Práce je primárně pojata jako hodnotící, tedy důsledné popsání současného stavu je doplněno o komentář ohledně účinnosti, resp. limitů a faktických překážek při uplatnění sledovaných nástrojů. Autorka však do velké míry končí v práci hodnocením, resp. zpravidla konstatováním o nízké účinnosti daného nástroje. Nevěnuje se tedy významněji diskuzi nad možnostmi, jak tento stav zvrátit *de lege ferenda a* nepřináší tak mnoho návrhů a podnětů, jaké právní nástroje by bylo vhodné zavést, resp. neotevírá ani hlubší diskuzi nad ústředním problémem, a to jsou limity, kterým je vystaveno právní zakotvení preemptivních a filtračních nástrojů. To vnímám jako nevyužitou příležitost.

V kapitole 3 se autorka obšírně věnuje pojmu dezinformace, ale problematika časté neuchopitelnosti dezinformace jako nelegálního obsahu pro potřeby právní definice, tzn. nevyhnutelná potřeba hodnotit sdělení případ

[6] Viz MIZEROVÁ, Tina a Jakub HARAŠTA. Dostupnost mediálního obsahu: blokování dezinformačních webů. Právník. Praha: Ústav státu a práva AV ČR, 2023, roč. 162, č. 5, s. 415-430. ISSN 0231-6625.

od případu a obtížnost stanovení obecně platných kritérií pro méně zjevné, ale zpravidla převažující typy dezinformací (hybridní sdělení, manipulativní obsah, který nenaplňuje charakter trestného činu atd.), však není dále rozvinuta do úvah nad překážkou, kterou to vytváří pro právní zakotvení pre-emptivních a filtračních nástrojů.

Analýza manipulativních technik a jejich frekvence na českých zpravodajských serverech přitom byla představena v monografii,[7] na které jsem měl možnost se spolupodílet a se kterou autorka v práci opakovaně pracuje, příslušné informace o datasetu, představené v kapitole 5 této monografie však pro svou práci bohužel pomíjí.

Stejně tak v kapitole 4 je poskytnut kvalitní přehled ústavněprávní dimenze tématu, resp. mantinely vycházející z EÚLP a judikatury ESLP na ochranu svobody projevu, které stojí proti zákonem zřízeným filtračním a blokačním nástrojům, které by dopadaly na dezinformace, které nemají zjevnou trestněprávní kvalifikaci (např. podpora a propagace terorismu - zde přitom autorka pomíjí alespoň zmínku o existenci Nařízení (EU) 2021/784 o potírání šíření teroristického obsahu online), ovšem není s těmito poznatky dále příliš pracováno. Autorka tedy nediskutuje, zda je zavedení účinných filtračních a blokačních nástrojů ze strany státu ve světle těchto mantinelů vůbec možné, resp. na jaké druhy dezinformací je lze vztáhnout, což je ústřední otázkou.

Výsledně je poněkud upozaděna diskuze nad významem soft-law nástrojů, které umožňují zprostředkovaně využít pro zájmy států na boji proti dezinformacím monitorovací kapacity a blokační a filtrační nástroje platforem jakožto definičních autorit. Zde je ústřední aktivita jako nový posílený Code of Practice on Disinformation ve verzi z roku 2022,[8] který autorka

[7] GREGOR, Miloš, Petra MLEJNKOVÁ, Miroslava PAVLÍKOVÁ, Barbora ŠENKÝŘOVÁ, Jakub DRMOLA, Miroslav MAREŠ, František KASL, Aleš HORÁK, Vít BAISA, Radim POLČÁK, Jan HANZELKA, Jonáš SYROVÁTKA a Ondřej HERMAN. Challenging Online Propaganda and Disinformation in the 21st Century. Cham: Palgrave Macmillan, 2021. 273 s. Political Campaigning and Communication. ISBN 978-3-030-58623-2. doi:10.1007/978-3-030-58624-9.

[8] Viz The 2022 Code of Practice on Disinformation. *European Commission* [online]. 2022 [cit. 2023-10-30]. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

zmiňuje jen letmo (např. s. 68, resp. není zřejmé, zda autorka vůbec referuje na tuto posílenou verzi), což souvisí s omezením tématu, ke kterému jsem se vyjádřil výše. Část textu věnující se Nařízení (EU) 2022/2065 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (DSA) v kap. 6 tím však nutně ztrácí na přínosu pro čtenáře, protože pro kontext boje proti dezinformacím je ústřední právě posílení Code of Practice on Disinformation skrze některá ustanovení DSA, která mají posílit vynutitelnost závazků platforem v rámci soft-law nástrojů jako je tento.

Kapitola 5 je převážně věnována *ex post* soudní ochraně osobnosti, která je popsána kvalitně a podrobně, ale i autorka na s. 60 dochází k závěru, že se nejedná o příliš užitečný nástroj pro boj proti dezinformacím. Přitom jsem názoru, že autorka je ve svém hodnocení ještě velmi mírná, a s ohledem na hlavní podobu a rychlost a charakter šíření dezinformací (jak bylo podrobně přiblíženo v kapitole 3), je možnost soudní ochrany, která vyústí v případné smazání jednotlivé dezinformace od konkrétně identifikovaného autora a případné zveřejnění omluvy z hlediska společnosti zcela marginální nástroj.

V kapitole 7 jsou představeny trestněprávní nástroje, přičemž text má převážně charakter deskripce ve stylu komentářového katalogu. Vítám, že je pracováno s dostupnou judikaturou a že kapitola obsahuje podkapitolu 7.4, ve které je poskytnuto zhodnocení. I zde ovšem platí, že je i laickému čtenáři poměrně záhy zjevné, že trestněprávní nástroje se svým významem pro včasné a účinné omezení šíření dezinformací příliš využít nedají, resp. zřejmě nejúčinnější využití skutkových podstat relevantních trestných činů v tomto směru lze pozorovat v německém Netzwerkdurchsetzungsgesetz,[9] kde jsou použity pro vymezení rozsahu monitorovacích povinností provozovatele platformy a tedy zprostředkovaně k charakterizování nelegálního obsahu, který má být soukromoprávními filtrovacími a blokovacími nástroji tohoto provozovatele v rámci jeho platformy omezován. Autorka se ovšem u svého zhodnocení omezuje pouze na přímé využití trestního řízení při

[9] Viz Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG). *Bundesamt für Justiz* [online]. 2017 [cit. 2023-10-30]. Dostupné z: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html

boji proti dezinformacím, odkazuje na strategické koncepce, nepřináší však významnější vlastní komentář ohledně vhodného postupu *de lege ferenda*.

Kapitola 8 popisuje případ blokování dezinformačních webů ze strany CZ.NIC v první polovině roku 2022. Je poskytnuta podrobná deskripce jak vývoje situace, tak právního kontextu a legislativního záměru s tím spojeného a jeho dosavadního osudu. Autorka nevěnuje přílišnou pozornost otázce, zda bylo blokování účinné (resp. zda bylo dlouhodobě účinné) a tudíž zda se jedná o přínosný nástroj pro boj proti dezinformacím. Dále pak přes zmínku o slovenské novele nevede významnější diskuzi nad vhodným právním zakotvením tohoto nástroje, případně možnými alternativami.

V podobném duchu je koncipována kapitola 9, kde je autorkou podrobně popsána vládní inciativa s cílem omezit šíření dezinformací, tedy především Analýza připravenosti České republiky čelit vážné dezinformační vlně (což je také jeden ze stěžejních zdrojů, ze kterých autorka v práci čerpá). Komentáře v této části by ovšem mohly být více kriticky diskuzní.

Práce je zpracována důsledně, práce se zdroji je nadstandardní, představení řešené problematiky a jednotlivých národních právních nástrojů je odborně zdařilé. Je ovšem škoda, že autorka plně nevyužila svou hloubku znalostí a neposkytla doporučení vhodnějších či lépe koncipovaných právních nástrojů v rámci úvahy *de lege ferenda*. Jedná se tedy přínosný podkladový text pro diskuzi nad tématem, vlastní příspěvek do této diskuze však autorka zřejmě plánuje přinést až v navazujících publikačních výstupech, které lze s ohledem na její probíhající doktorské studium zaměřené na problematiku právních nástrojů pro omezení šíření dezinformací v Evropě očekávat a osobně se na ně již těším.

PIVODA, R: PRAKTICKÉ PROBLÉMY VÝVOJE SOFTWARE NA ZAKÁZKU

PAVEL KOUKAL[10]

PIVODA, R.: Praktické problémy vývoje software na zakázku. 2023, závěrečná práce programu LL.M. v právu informačních a komunikačních technologií, Masarykova univerzita, Právnická fakulta, 72 s.

ANOTACE

Vývoj software na zakázku představuje z pohledu práva komplexní problematiku, která vyžaduje individuální přístup v každém samostatném projektu. Nesprávně nastavené smluvní vztahy mohou zásadním způsobem negativně ovlivnit jak výsledek spolupráce zúčastněných stran, tak i možnost plného využití zhotoveného software a jeho životního cyklu. Tato práce mapuje na základě praktických zkušeností a provedené rešerše běžně se objevující problémy, které mohou nastat mezi objednatelem a dodavatelem od začátku vyjednávání smluvní dokumentace až po ukončení spolupráce.

KLÍČOVÁ SLOVA

Software; vývoj software; zakázkový vývoj; licence; cloud

ABSTRACT

Custom software development is a complex legal issue that requires an individual approach in each separate project. Insufficient setup of contractual relations can have a significant negative impact on the outcome of cooperation between the parties involved, as well as on the possibility of full use of the software

[10] doc. JUDr. Pavel Koukal, Ph.D. je vedoucím Katedry občanského práva Právnické fakulty Masarykovy univerzity. Kontaktní e-mail: pavel.koukal@law.muni.cz

and its life cycle. Based on practical experience and research, this paper maps commonly occurring problems that can arise from beginning of the negotiation of contractual documentation to the end of cooperation between the customer and the supplier.

KEYWORDS

Software; Software Development; Custom Development; Licensing; Cloud

Plná verze práce je dostupná z: https://is.muni.cz/th/yq89s/

Autor se v práci detailně zabývá problematikou vývoje software na objednávku a snaží se identifikovat časté právní problémy a jejich řešení. Autor se věnuje různým aspektům, jako jsou licence, zdrojový kód, servisní podpora, cloudové služby a další relevantní témata. Celkově je práce dobře strukturovaná a zabývá se v zásadě všemi důležitými aspekty dané problematiky.

Autor v práci prokazuje solidní znalosti problematiky vývoje software na objednávku (zakázku) a souvisejících relevantních právních aspektů. Jistou slabinou práce je, že by autor by mohl více intenzivně pracovat s judikaturou a odbornými komentáři, zejména komentáři k občanskému zákoníku a k autorskému zákonu, což by mohlo práci informačně a argumentačně posílit a přinést větší analytickou hloubku. Práce je totiž na několika místech deskriptivní, což snižuje její přidannou analytickou hodnotu.

Teoretická a obsahová část práce se zabývá několika klíčovými tématy, která jsou relevantní pro vývoj softwaru na objednávku (zakázku). V kapitole 2.1 je představena základní terminologie, následně se zaměřuje na subjekty zapojené ve vývoji software na objednávku (zakázku). Objednatel a dodavatel jsou v práci představeni jako klíčové postavy, které určují základní parametry nově vznikajícího produktu, přičemž je zdůrazněno, že dodavatel není zodpovědný pouze za samotný software, ale také za následné poskytování licencí, a servisní podpory. Následující podkapitola je věnována metodám vývoje software. Zde jsou detailně popsány tzv. vodopádová metoda a agilní přístup. Autor prezentuje výhody a nevýhody obou

metod a ukazuje, jakým způsobem mohou ovlivnit specifikaci a vývoj software na objednávku (zakázku). Posléze se autor zaměřuje na specifikaci jednotlivých dílčích závazkových vztahů, které v komplexu vývoje software na objednávku (zakázku) vznikají.

Teoretická část je pečlivě strukturovaná a obsahuje relevantní informace o specifikaci a dokumentaci vývoje softwaru. Autor zdůrazňuje důležitost správné specifikace předmětu závazku. Obsahová část se potom zaměřuje na rozlišování mezi předmětem závazku a specifikací díla, což má klíčový význam pro jasnou definici smluvních povinností zhotovitele (dodavatele) a objednatele. Jsou zde zmíněny i konkrétní metody vývoje software a jejich vztah k specifikaci.

Následně se autor zabývá problematikou licencování software (počítačového programu). Autor ukazuje, jak důležité je správně nastavit licenční podmínky, aby nedošlo k omezením v používání software. V práci jsou následně diskutovány různé druhy, včetně otázek jejich rozsahu, řetězení, Open Source licencí a copyleft přístupu. Kapitola 5 zkoumá zpřístupňování zdrojového kódu. Autor prezentuje různé možnosti a podmínky, za kterých může být zdrojový kód zpřístupněn. Důraz je kladen na to, že samotné zpřístupnění kódu nemusí automaticky znamenat schopnost objednatele pokračovat v jeho vývoji. Kapitola 6 se zabývá servisní podporou. Autor se zaměřuje na klíčové aspekty, jako jsou určení parametrů servisu, určitost odměn, klasifikace vad a reakční časy. Detailně zkoumá různé aspekty servisních zásahů a zdůrazňuje důležitost obvyklé dostupnosti služby. V následujících kapitolách potom autor analyzuje efekt „Závislosti na dodavateli“ a ukazuje, jak může omezit možnosti objednatele přecházet k jiným dodavatelům (zhotovitelům).

Posléze se práce soustředí na využití umělé inteligence (AI) a nástrojů třetích stran při vývoji softwaru na zakázku. Autor diskutuje různá rizika spojená s tímto jevem, včetně propojení s AI platformami, závislosti na externích nástrojích, problémů s akceptací díla a dalších témat.

Celkově lze konstatovat, že teoretická a obsahová část práce poskytuje čtenáři relativně ucelený pohled na problematiku vývoje softwaru na zakáz-

ku. Autor prezentuje relevantní informace, podporované příklady (které by nicméně mohly být i četnější) a odkazy na literaturu a právní předpisy.

Přestože teoretická a obsahová část práce přináší užitečné informace týkající se vývoje softwaru na zakázku, lze identifikovat několik oblastí, které mohly být do větší hloubky rozebrány. Například analýza využívání AI při vývoji software mohla být hlubší. Bylo by také užitečné, kdyby autor provedl rozsáhlejší zkoumání konkrétních případů, ve kterých se rizika materializovala, a jakým způsobem byla (resp. měla být) řešena. Zdá se také, že v práci chybí některé aktuální trendy v oblasti vývoje softwaru (hybridní Cloud a Multi-Cloud Strategie; explainable AI (XAI); remote collaboration tools; automatizace a DevOps; Low-Code/No-Code platformy). Zaměření na novější informace a technologické trendy by poskytlo čtenářům lepší pohled na současnou situaci a možná rizika spojená s novými technologiemi (rozbor využití AI se v práci jeví jako velmi obecný).

Co se týče dalších právních aspektů, potom se autor také mohl více zaměřit na problematiku odpovědnosti za vady.

Přes výše uvedené kritické komentáře lze konstatovat, že tato závěrečná práce je hodnotným příspěvkem do oblasti právních aspektů vývoje software na zakázku. Autor identifikuje klíčové problémy a na půdorysu omezeného rozsahu prací LLM nabízí jejich řešení. Práce je čtivá a informačně nosná.

BAROCHOVÁ, P.: OCHRANNÁ ZNÁMKA V POJETÍ EVROPSKÉHO PRÁVA

TOMÁŠ KŘIVKA[11]

BAROCHOVÁ, P.: Ochranná známka v pojetí Evropského práva. 2023, diplomová práce, Západočeská univerzita v Plzni, Fakulta právnická, 109 s.

ANOTACE

Tato diplomová práce se zabývá ochrannými známkami v kontextu evropského práva. Jejím cílem je přiblížit reakci evropského právního systému na vývoj institutu ochranných známek jak na úrovni vnitrostátní, tak i evropské, navíc i s prolnutím mezinárodní známkoprávní ochrany. Zároveň cílí na to čtenáře blíže seznámit s principy fungování systému ochranné známky EU, který se jeví ve vztahu k ostatním systémům co do teritoriálního rozsahu poskytnuté ochrany a vynaložených nákladů na registraci za nejvýhodnější. Celkově je práce členěna do čtyř hlavních kapitol doplněných o úvod, závěr a cizojazyčné resumé. První kapitola se zaměřuje především na definici a význam pojmu ochranná známka. Druhá kapitola se soustředí na právní úpravu ochranných známek a vzájemný vztah mezi evropskou právní úpravou a národním, mezinárodním a evropským systémem ochranných známek. Poslední dvě kapitoly se zaměřují výhradně na pojem, základní principy, zápisné řízení a na způsoby zániku ochranné známky EU, která je ostatně i ústřední analyzovanou problematikou celé práce.

[11] Mgr. Tomáš Křivka, Ph.D. je odborným asistentem na Katedře ústavního a evropského práva Fakulty právnické Západočeské univerzity v Plzni. Kontaktní e-mail: . krivka@kup.zcu.cz

KLÍČOVÁ SLOVA

Ochranná známka; ochranná známka EU; evropské právo; systém evropské ochranné známky; známkoprávní ochrana

ABSTRACT

This thesis deals with trade marks in context of European law. Its aim is to present the reaction of the European legal system to the development of trade marks at both national and European level, with an intertwining of international trademark protection. At the same time, the reader will be introduced to the principles of the EU trade mark system, which appears to be the most advantageous in relation to other systems in terms of the territorial scope of protection granted and the costs incurred for registration. Overall, the thesis is divided into four main chapters, supplemented by an introduction, a conclusion and a foreign-language summary. The first chapter focuses primarily on the definition and meaning of the term trademark. The second chapter deals with the legal regulation of trademarks and the interrelationship between European legislation and national, international and European trademark systems. The last two chapters focus exclusively on the concept, the basic principles, the registration procedure and the methods of extinction of the EU trademark, which is, by the way, the central issue analysed throughout this thesis.

KEYWORDS

Trademark; EU Trademark; European Law; European Trademark System; Trademark Protection

Plná verze práce je dostupná z: https://theses.cz/id/cqv1m2/

Diplomová práce se zaměřuje na ryze specifické téma ochranných známek v rámci unijního práva. Na Katedře ústavního a evropského práva FPR ZČU jde o volbu velmi netypickou, zjevně vedenou osobním zájmem autorky, což se odráží i v jejím pečlivém a soustředěném přístupu k tématu. Zvolené téma je možné považovat v dnešním globalizovaném světě založeném na

stále větším využívání moderních technologií za velmi aktuální a výborně využitelné v právní praxi. Známkové právo lze vnímat jako jednu z částí širší úpravy obchodně právních vztahů, přičemž právě jeho evropský rozměr je spíše podceňovaným tématem kvalifikačních prací. Ačkoli hodnocené dílo není výsledkem žádného hlubšího autentického a originálního výzkumu dané oblasti, zcela nepochybně jde o kvalitní syntetizující práci, která je užitečným příspěvkem k rozšíření povědomí o dané problematice, navíc doplněným o řadu samostatných autorčiných postřehů a závěrů.

Samotná práce o rozsahu 96 stran je fakticky rozdělena na úvod, čtyři číslované kapitoly a závěr. Autorka práce se v úvodu věnuje definici pojmu ochranná známka a historické genezi vzniku ochranných známek. Následně se podrobuje analýze platnou právní úpravu ochranných známek jak v rámci EU, tak v mezinárodním právu. Poté se podrobně zabývá jednotlivými funkcemi a druhy ochranných známek, přičemž důraz klade na ochrannou známku Evropské unie a její povahu. V poslední čtvrté kapitole pak diplomantka rozebírá procesní aspekty řízení o zápisu ochranné známky EU, přičemž postupně analyzuje samotné podání přihlášky, vypořádání případných námitek, ale také podmínky eventuálního zániku ochranné známky. Osnova práce je strukturovaná, přehledná a zjevně vychází z kvalitní rešerše stávající české i zahraniční literatury i veškerých aktuálních právních předpisů. Autorka práce si ve svém díle klade např. otázku, jako jsou dopady Brexitu na ochrannou známku Evropské unie a institucionální rámec řízení ochranných známek v EU, což potvrzuje, že celá práce je zpracována s důrazem na reflexi současné situace v oblasti ochranných známek.

Diplomantka se podle vlastních slov snažila ve své práci analyzovat „reakci evropského právního systému na vývoj ochranných známek jak na úrovni vnitrostátní, tak i evropské s prolnutím mezinárodní známkoprávní ochrany“ a současně bylo jejím cílem „podchytit a vyzdvihnout sbližovací tendence evropských legislativních orgánů ohledně evropských sekundárních aktů přímo se dotýkajících vnitrostátních známkoprávních úprav členských států s koexistujícím systémem ochranné známky EU“. Tyto cíle je možné považovat za splněné, přestože nejsou formulovány ve formě

konkrétní hypotézy, jež je pro podobné kvalifikační práce nejvíce doporučována.

Z formálního pohledu je přitom posuzované dílo napsáno odborně správným a srozumitelným jazykem, používá korektně citační a poznámkový aparát, který přitom značně rozsahem přesahuje úroveň obvyklou pro diplomové práce. Celé dílo je rovněž logicky strukturováno, jednotlivé části na sebe vhodně navazují a rovněž i ze stylistického hlediska jde o čtivou formou sepsané právní pojednání. Pokud jde o teoretickou úroveň, velmi oceňuji schopnost nastudovat, analyzovat a následně srozumitelně vysvětlit podobně komplikované téma, jako si zvolila právě autorka. Celkově proto považuji její zpracování za pečlivé, poctivé a nadprůměrně kvalitní. Jedinou výtku směřuji k absentujícím hypotézám, které by ze stávajícího přehledného, srozumitelného a kvalitního odborného právnického pojednání z oblasti evropského známkového práva mohly vytvořit dílo skutečně vědeckého charakteru, neboť podstatou vědeckého odborného textu nemůže být pouze podrobný a přehledný popis tématu, ani jen izolovaný právní rozbor určité problematiky, ale vědecké dílo by mělo v principu směřovat k ověření určitých teoretických předpokladů formou analýzy konkrétních dat. Na druhou stranu je však nutné připomenout, že se v případě diplomové práce jedná v českém právnickém akademickém prostředí o spíše atypickou volbu individuálního tématu zaměřeného na složitou problematiku, čemuž je vhodné přizpůsobit i konečné hodnocení.

Závěrem si dovoluji celé posuzované dílo zhodnotit tak, že diplomová práce podle mého názoru jednoznačně splňuje obsahové, formální i odborné požadavky kladené na diplomové práce, a to navíc nadprůměrným způsobem.

BENEŠ, P.: KONTRAKTACE V ESPORTU

PAVEL LOUTOCKÝ[12]

BENEŠ, P.: Kontraktace v esportu. 2023, diplomová práce, Masarykova univerzita, Právnická fakulta, 96 s.

ANOTACE

Diplomová práce se bude zabývat kontraktací smlouvami oblasti esportu, jejich vymezením, představením specifik, to včetně mezinárodního přesahu. Teoretická část práce bude identifikovat úvodu relevantní subjekty, které těchto vztazích figurují dále je rozebírat. Na základě identifikovaných subjektů se práce bude dále věnovat analýze smluvních specifik hlediska účinné české právní úpravy. Ve zvláštní části práce budou rozebrána specifika jednotlivých esportových smluv, mj. pracovních smluv tzv. sportovních smluv, práce se ale také zaměří na další smluvní typy podmínky. Cílem práce tak bude analýza charakteristik esportových smluv, jejich právních specifik dále vzhledem často přítomnému mezinárodní-mu prvku dopady rámci mezinárodního práva soukromého, včetně případných doporučení vyplývajících ze zjištěného. Při psaní práce bude diplomant vycházet ze souvisejících unijních národních právních předpisů, českých zahraničních odborných publikací, prioritně komentářové literatury, akademických článků případně dostupné judikatury. Práce je aktuální datu 30. 6. 2023.

KLÍČOVÁ SLOVA

Esport; právo; smlouvy; sport; autorské právo; soutěže

[12] JUDr. Pavel Loutocký, Ph.D., BA (Hons) je odborným pracovníkem na Ústavu práva technologií Právnické fakulty Masarykovy Univerzity. Kontaktní e-mail: loutocky@muni.cz

ABSTRACT

The thesis will deal with contracting and contracts in the field of esports, their definition, introduction of specifics, including international overlap. The theoretical part of the thesis will identify in the introduction the relevant sub-entities that figure in these relationships and further analyse them. On the basis of the identified subjects, the thesis will further analyse the contractual specifics in terms of the effective Czech legislation. In separate part of the thesis, the specifics of individual esport contracts will be analysed, including employment contracts and so-called sports contracts, but the thesis will also focus on other contractual types and sub conditions. The aim of the work will be to analyse the characteristics of esport contracts, their legal specifics and, given the often-present international element, the implications for private international law, including possible recommendations arising from the findings. In writing the thesis, the graduate will draw on relevant EU and national legislation, Czech and foreign publications, primarily commentary literature, academic articles and, where appropriate, available ca-se law. The thesis is current as of 30th June 2023.

KEY WORDS

Esports; Law; Contracts; Copyright Law; Competitions

Plná verze práce je dostupná z: https://is.muni.cz/th/y0aa2/

Práce se zaměřuje na velmi aktuální odborně minimálně řešenou problematiku kontraktačních specifik esportu. Práce nejen, že se věnuje relevantním specifickým otázkám, autor rovněž využívá svých zkušeností, které působením v dané oblasti nabral prezentuje tak praktické příklady dílčí poznatky, které činí práci hodnotnou. Využil také svých možností v získání materiálů, ke kterým by osoba nezapojená do hráčské komunity získávala přístup jen těžko (pokud vůbec). Téma práce tak představuje zajímavou oblast v rámci rostoucího esportového průmyslu, který se stává stále více profesionálním komerčním, popularitou se v některých západních či asijských zemích pohybuje na předních příčkách celkové divácké sledovanosti.

Práce obsahuje velmi zajímavé poznatky doporučení. Autor si za hlavní cíl práce zvolil identifikovat jednotlivé subjekty kontraktaci rámci esportu vystupující. Tato část je velmi důležitá, jelikož velmi dobře prezentuje, že daná problematika není jen hráči týmových organizacích, zapojeny jsou další subjekty, jako jsou mezinárodní organizace, sponzoři, streamovací platformy či organizátoři turnajů.

Dále autor rozebírá specifický vliv zúčastněných subjektů jejich postavení rámci kontraktace posléze se zaměřuje na specifické smluvní vztahy jejich konkretizaci. Autorovi se podařilo obsáhnout celý proces kontraktace včetně předsmluvní fáze. Rozebírá specificky smlouvy mezi vývojářskou společností zúčastněnými subjekty, smlouvy mezi týmovou organizací vývojářskou společností věnuje se dále například specifickým pravidlům ve hře League of Legends, s čímž má praktické zkušenosti. Tato část práce, která se věnuje specifikům smluvních vztahů je pak přínosná právě vzhledem výše uvedeným zkušenostem zapojení autora do hráčské komunity, jeho konkrétních postřezích rovněž znalostech, které jsou mimo komunitu jen obtížně získatelné dostupné.

Závěrečná část práce se pak nad to věnuje možnostem úvahám řešení sporů, to jak soudně, tak zejména mimosoudně. V současnosti jsou totiž spory vyplývající z esportu soudy řešeny jen marginálně (pokud vůbec) potenciál zavedení uceleného řešení sporů online (ODR) je v rámci dané oblasti značný, prozatím ale stále neuchopený.

Lze shrnout, že se jedná práci velmi kvalitní praktickým přínosem svým rozsahem obsahem se jedná práci nadstandardní.

PELIKÁN, K.: PRÁVNÍ ÚPRAVA DIGITÁLNÍ IDENTITY A JEJÍ SOUČASNÝ VÝVOJ

JAKUB MÍŠEK[13]

PELIKÁN, K.: Právní úprava digitální identity a její současný vývoj. 2023, diplomová práce, Masarykova univerzita, Právnická fakulta, 106 s.

ANOTACE

Práce se zabývá právní úpravou digitální identity a jejím současným vývojem. Základní cíle práce spočívají v popsání současné právní úpravy digitální identity, v provedení analýzy současného stavu digitální identity v České republice a v nastínění jejího vývoje včetně případných doporučení. Cílům práce odpovídá i struktura práce, kdy v úvodu bude představena základní právní úprava digitální identity, dále bude popsán její stav v České republice a provedena analýza. Závěr práce se bude věnovat vývoji právní úpravy digitální identity.

KLÍČOVÁ SLOVA

Digitální identita; nařízení eIDAS; analýza; prostředky elektronické identifikace; zákon o elektronické identifikaci; revize nařízení eIDAS

ABSTRACT

The thesis deals with the legal regulation of digital identity and its current development. The main objectives of the thesis are to describe the current legal regulations of digital identity, to analyse the current state of digital identity in the Czechia and to outline its development including possible recommen-

[13] JUDr. MgA. Jakub Míšek, Ph.D. je odborným asistentem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontaktní e-mail: Jakub.Misek@law.muni.cz

dations. The structure of the thesis corresponds to the objectives of the thesis. The basic legal regulations of digital identity will be presented in the introduction, secondly its legal status in Czechia will be described and lastly an analysis will be made. The conclusion part of the thesis will be devoted to the development of the legal regulation of digital identity.

KEY WORDS

Digital Identity; eIDAS Regulation; Analysis; Electronic Identification Means; Electronic Identification Act; Revision of the eIDAS Regulation

Plná verze práce je dostupná z: https://is.muni.cz/th/wfo54/

Diplomová práce se zabývá tématem právní úpravy digitální identity. Autorův přístup je poměrně komplexní, kdy si dal za obecný cíl prozkoumat tento fenomén jako celek. Nejde o téma vyloženě nové, protože této otázce se v českém prostředí již řada textů věnovala, jak ostatně dokládá i autorův přehled literatury. Na druhou stranu, práce bez pochyby přináší nové aspekty, ať již v podobě vlastní analýzy existujících řešení nebo představení chystané úpravy. Kvalitní zpracování práce pak vyžadovalo autorovu dobrou orientaci v daném tématu, včetně přehledu o evropském legislativním procesu. Celkově tak jde o téma spíše náročné.

Autor vymezil cíle své práce takto: „*Základní cíle práce v návaznosti na výše uvedené jsou tedy představit základní vhled do současné právní úpravy digitální identity. Dalším cílem práce je provedení a vyhodnocení analýzy současného stavu digitální identity v České republice. Posledním cílem je nastínit možný vývoj digitální identity pro Českou republiku a navrhnout případné doporučení pro futoro.*“ Tyto cíle, byť jsou samy o sobě poměrně neurčité a široké, odpovídají oficiálnímu zadání práce. Je možné konstatovat, že byly beze zbytku naplněny. Mám za to, že by práci nicméně bývalo prospělo, aby cíle byly formulovány konkrétněji a jasněji. Rovněž celá práce by pak mohla být více konzistentní.

Z obsahového a teoretického hlediska je hodnocená práce zpracována celkově kvalitně. Práci je možné rozdělit na tři základní části. První je tvo-

řena kapitolami 3 a 4 a představuje aktuální stav právní úpravy a praxe digitální identity v ČR. Druhá část je tvořena kapitolou 5 a nabízí detailní praktickou analýzu existujících používaných prostředků pro zajištění digitální identity v ČR. Tato část rovněž představuje hlavní autorův osobní přínos v rámci hodnocené diplomové práce. Konečně třetí část, která je tvořena kapitolami 6 a 7, přináší výhled do budoucího vývoje v podobě chystané revize nařízení eIDAS a jejích dopadů do českého právního prostředí. V kontextu struktury musím uvést dva hlavní problémy hodnocené práce. První spočívá v tom, že uvedené tři části na sebe vlastně moc nenavazují. Bez pochyby spolu souvisí tematicky, ale postrádají vnitřní provázání. Části tak stojí samostatně a budí otázku, proč jsou přítomné v jednom textu. Text práce je navíc velmi obsáhlý a v některých svých pasážích nejde nad rámec prostého převyprávění právní úpravy (zejm. první část). Mám za to, že větší střídmost by diplomové práci prospěla. S uvedenou celkovou obsáhlostí jsou pak naopak velmi kontrastní kapitoly 4 a 7 (a v rámci vnitřního dělení rovněž např. podkapitola 3.5), které jsou oproti ostatním disproporčně krátké.

Z metodologického hlediska je třeba pochválit autorovo využívání metatextu, kterým ozřejmuje proč a jak postupuje. Nedostatek v této oblasti pak spočívá ve volbě kategorií zkoumaných v rámci kapitoly 5. Autor nikde přesvědčivě nevysvětluje, proč zvolil právě tyto kategorie a jaký je přínos v jejich analýze. Závěry z analýzy pak mohou místy působit lehce banálně, byť mají svůj nepopiratelný přínos. I přes uvedené výhrady jde o velice dobrou prakticky orientovanou přehledovou práci, která nabízí na jednom místě komplexní balíček relevantních informací vztahujících se k digitální identitě. Vzhledem k tomu bych autorovi doporučil, aby zvážil publikaci textu práce (po náležitých úpravách) vhodným způsobem, který bude reflektovat praktické zaměření práce.

SNÁŠEL, A.: SVOBODNÝ PŘÍSTUP K INFORMACÍM VE VĚCECH PLATU ZAMĚSTNANCŮ PLACENÝCH Z VEŘEJNÝCH PROSTŘEDKŮ

SOŇA POSPÍŠILOVÁ[14]

SNÁŠEL, A.: Svobodný přístup k informacím ve věcech platu zaměstnanců placených z veřejných prostředků. 2023, diplomová práce, Univerzita Palackého v Olomouci, Právnická fakulta, 61 s.

ANOTACE

Diplomová práce se zabývá otázkami práva na svobodný přístup k informacím ve věcech zaměstnanců placených z veřejných prostředků. Práce obsahuje analýzu tohoto institutu jak ve smyslu zákona, tak ve světle vyvíjející se judikatury. První kapitola vymezuje základní pojmy informačního práva. Druhá kapitola obsahuje vývoj informačního práva. Třetí kapitola popisuje podobu řádné žádosti o poskytnutí informací. Čtvrtá kapitola je zhodnocením podaných žádostí vybraným povinným subjektům a dále je věnována otázce, kdy je namístě žádosti odmítnout.

KLÍČOVÁ SLOVA

Svobodný přístup k informacím; právo na svobodný přístup k informacím; veřejné prostředky; příjemci veřejných prostředků; povinný subjekt; "platový nález"

[14] JUDr. Soňa Pospíšilová, Ph.D. je odbornou asistentkou na Katedře správního práva a finančního práva Právnické fakulty Univerzity Palackého. Kontaktní e-mail: sona.pospisilova@upol.cz

ABSTRACT

This Master's Thesis deals with the topic of the right to access public information regarding salaries of employees paid from public funds. The thesis is an analysis of the right to access from the point of view of both the law and the judgements. The first chapter sums up the basic terms of the information law. The second chapter is about the evolution of the regulation. The third chapter describes how the proper request should be written. The fourth chapter is an evaluation of submitted requests and also is dedicated to the question when the request should be rejected.

KEYWORDS

Free Access to Information; The Right to Free Access to Information; Public Funds; Recipients of Public Funds; Obliged Entity; "Salary Decision"

Plná verze práce je dostupná z: https://theses.cz/id/r9r7js/

V úvodu diplomant přibližuje důvody, které ho vedly k výběru tématu práce, dále se věnuje obecné charakteristice práva na informace a představuje téma práce a její systematiku. Poté si stanovuje hypotézu, kterou hodlá v rámci práce ověřovat a čtyři podrobnější výzkumné otázky. Jako „podstatu“ (a zřejmě i cíl) práce autor uvádí objasnění teoretického uchopení institutu a zjištění aplikačního postupu povinných subjektů. Diplomant uvádí také metody práce, které použije při zpracování tématu, a to metodu analytickou, normativní a empirickou a jako argumentační a logické postupy uvádí indukci, analogii a komparaci.

První kapitola představuje úvod do problematiky svobodného přístupu k informacím a je zaměřena na objasnění základních pojmů práce. Autor se zde věnuje nejprve obecnému vymezení pojmů v právní úpravě, a to pojmu žadatel, informace a povinné subjekty s plnou a částečnou informační povinností. Dále se pozornost autora zaměřuje na vymezení dalších klíčových pojmů, a to zaměstnanec, plat a veřejné prostředky.

Ve druhé kapitole se diplomant zaměřuje na popis vývoje právní úpravy přístupu k informacím, přičemž sleduje novodobý vývoj tohoto institutu, novelizace zákonné právní úpravy se zaměřením na platové otázky. Podobně poté přistupuje k analýze judikatury, která je pro výklad právní úpravy a aplikační praxi klíčová.

Třetí kapitola je věnována objasnění náležitostí žádosti o poskytnutí informace a postupu při její formulaci tak, aby žadatel o informace o platu zaměstnanců placených z veřejných rozpočtů mohl být s žádostí úspěšný. Autor přitom rozlišuje obecné náležitosti žádosti stanovené zákonem a náležitosti „zvláštní“, které jsou dovozovány judikaturou Ústavního soudu. Dále se zamýšlí nad otázkou faktické realizace práva na „platové“ informace ze strany veřejnosti.

Ve čtvrté kapitole diplomant obrací svou pozornost k vlastnímu výzkumu a následnému ověření v úvodu stanovené hypotézy, přičemž se rozhodl zjistit, jak v práci popsaný institut platové žádosti bude vyřízen v konkrétních případech. Pro výzkum si jako povinné subjekty vybral krajské úřady, jimž adresoval svou žádost o informaci a poté provedl zhodnocení postupu jednotlivých krajských úřadů při jejich vyřizování. Nejprve přibližuje postup při formulaci své žádosti a upřesňuje její obsah, poté rozebírá následné postupy krajských úřadů při vyřizování žádosti, a to z hlediska meritorního vyřízení žádosti, z hlediska dodržení lhůty pro její vyřízení a rovněž z hlediska toho, zda postup při vyřízení žádosti lze hodnotit jako zákonný a v souladu s relevantní judikaturou.

V závěru práce diplomant nejprve uvádí cíl své práce, praktické zaměření její výzkumné části a stručně rekapituluje obsah práce. Pokud jde o hypotézu, že krajské úřady plní své povinnosti stanovené recentní judikaturou, tuto se mu v práci podařilo potvrdit. Dále se diplomant vyjadřuje k výzkumným otázkám, přičemž odpovědi na ně vztahuje k závěrům, jež učinil v rámci výzkumné části své práce a zamýšlí se nad možnostmi dalšího výzkumu ve vztahu k jiným povinným subjektům. Předkládá též své úvahy k budoucímu vývoji právní úpravy zkoumané problematiky a opět uvádí postupy a upřesňuje použitou metodologii práce.

Téma práce je aktuální, autor k jeho zpracování přistoupil originálně, teoretické vymezení tématu propojil s poznatky z vlastního výzkumu, v němž nabídl praktický vhled do aplikační praxe. Vedle obecného cíle se rozhodl ověřit v práci hypotézu, upřesněnou čtyřmi výzkumnými otázkami.

Z hlediska teoreticko-metodologického zakotvení práce mohu konstatovat, že autor zdařile usiloval o propojení teoretických východisek práce s poznatky o uplatnění zkoumané problematiky v právní praxi. Stanovil si vhodný cíl práce, jež konkretizoval vymezením relevantní hypotézy. Cíl práce, který si autor vytyčil v Úvodu a v Závěru se však liší v tom, že v Závěru uvedený cíl a záměr autora je ve srovnání s obecně formulovaným cílem v Úvodu formulován přesněji a lépe. U formulace hypotézy pak autor namísto tvrzení, které by ověřoval, tuto formuloval jako otázku (Znění hypotézy obsahuje slovo „zda“ namísto správného slova „že“). Stanovení hypotézy mělo být, s ohledem na text práce, také širší, neboť autor v práci sledoval aplikační praxi krajských úřadů nejen z hlediska respektování recentní judikatury, ale zejména zákonné právní úpravy. V návaznosti na hypotézu se věnoval čtyřem výzkumným otázkám, které lze, až na třetí otázku, poměrně dobře zodpovědět. Metody práce, které zvolil, diplomant dokázal při zpracování práce adekvátně využít.

Diplomová práce je logicky strukturovaná, autor postupuje od obecného ke zvláštnímu, kapitoly na sebe logicky navazují. V Úvodu autor opomenul charakterizovat základní zdroje práce, zejména odbornou literaturu a vyjádřit se k dosavadnímu zpracování tématu. Kapitoly jsou, až na kapitolu druhou, dostatečně představeny, většinou jsou obsahově vyvážené. Kapitola druhá je obsáhlejší, neboť autor zde předložil podrobnou analýzu judikatury, vztahující se k tématu.

Práci se zdroji hodnotím pozitivně, autor v práci prokázal schopnost interpretace, kritické analýzy a hodnocení zdrojů. Vycházel nejen z odborné literatury a časopiseckých článků, ale s ohledem na téma práce bylo klíčové i zpracování relevantní soudní judikatury, zejména Nejvyššího správního soudu a Ústavního soudu. Oceňuji přitom, že autor sledoval a popsal také vývoj judikatury a její vliv na právní úpravu a správní praxi.

Po obsahové stránce lze říci, že autor v práci prokázal schopnost uplatnění zásad vědecké práce. Zdařile identifikoval relevantní problémy zkoumané právní úpravy, průběžně se vyjadřoval k jednotlivým otázkám a kriticky analyzoval právní úpravu ve světle relevantní judikatury, v čemž spatřuji hlavní přínos práce. Podle názoru autora by de lege ferenda bylo vhodné zahrnout „platový test“, formulovaný judikaturou, do textu zákona. V tomto s autorem nemohu souhlasit, zákonodárce by neměl přejímat judikatorně dovozené závěry, byť chápu, že z pohledu žadatele o informace by to aplikační praxi mohlo usnadnit.

Jako vhodnou dalšího rozpracování vnímám autorem zmiňovanou změnu právní úpravy, spočívající v nové možnosti odmítnutí žádosti v případě zneužití práva na informaci, právě ve vztahu k platovým informacím.

VOZANKOVÁ, A.: GENETICKÉ DATABÁZE A OCHRANA GENETICKÝCH ÚDAJŮ

MARTIN ŠOLC[15]

VOZANKOVÁ, A. Genetické databáze a ochrana genetických údajů. 2023, magisterská práce, Univerzita Karlova, Právnická fakulta, 79 s.

ANOTACE

Tato diplomová práce se zaobírá problematikou zpracování genetických údajů, které jsou získávány metodou sekvenování DNA. Získaná data o lidském genomu představují revoluční podklad pro vědecké výzkumy a otevírají cestu pro léčbu některých doposud nevyléčitelných nemocí jako např. rakovina, AIDS či Alzheimerova choroba.

Práce se zabývá především právní úpravou ochrany genetických údajů. Popisuje zpracování genetických údajů, včetně jejich využívání a šíření, a to zejména prostřednictvím pořizovatelů genetických databází a genome browserů pro účely vědeckého výzkumu. Z pohledu platné právní úpravy České republiky a Evropské unie práce analyzuje dosavadní stupeň ochrany genetických dat a v tomto kontextu poukazuje na zjevné nedostatky. Práce se však neomezuje pouze na popis právních předpisů, ale danou problematiku důkladně hodnotí de lege ferenda. Cílem této diplomové práce je zhodnotit aktuální praxi zpracování genetických údajů, zejména jejich zpřístupňování, ukládání, možností anonymizace či způsobů jejich zneužití. Práce se věnuje otázce uplatnění a důsledkům současné právní regulace stanovené především Nařízením Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů (GDPR), nevynechává však ani zhodnocení možných dopadů

[15] JUDr. Mgr. Martin Šolc, Ph.D. je odborným asistentem na Katedře zdravotnického práva a Katedře občanského práva Právnické fakulty Univerzity Karlovy. Kontaktní e-mail: solcma@prf.cuni.cz.

navrhované budoucí právní úpravy. Zvláštní pozornost je přitom věnována rizikům v souvislosti se zneužitím genetických údajů zejména v kontextu ochrany osobnosti a možné reidentifikace subjektu údajů.

Poslední část práce je věnována zpracování zdravotních dat v souvislosti s návrhem Nařízení Evropského parlamentu a Rady (EU) o evropském prostoru pro zdravotní data, European Helath Data Space a sekundárnímu využití těchto dat pro výzkumné účely.

KLÍČOVÁ SLOVA

Genetická databáze; genetické údaje; ochrana osobních údajů

ABSTRACT

This thesis deals with the processing of genetic data obtained by DNA sequencing. The data obtained from the human genome represents a revolutionary basis for scientific research and open the way for the treatment of some so far incurable diseases such as cancer, AIDS, and Alzheimer's disease.

The thesis primarily focuses on the legal regulation of the protection of genetic data. The thesis describes the processing of genetic data, including its use and dissemination, mainly through providers of genetic databases and genome browsers for scientific research purposes. From the perspective of the current legal framework in the Czech Republic and the European Union, the thesis analyzes the existing level of protection of genetic data and points out evident shortcomings. However, the thesis is not limited to a description of legal regulations but thoroughly evaluates the issue de lege ferenda.

The aim of this thesis is to evaluate the current practice of processing genetic data, particularly its accessibility, storage, the possibility of its anonymization, and ways of its misuse. The thesis focuses on the issue of the implementation and consequences of the current legal regulation mainly established by the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons regarding the processing of personal data (GDPR), but also assesses the possible impacts of the proposed future legal regulation. Special attention is given to the risks associated with the misuse

of genetic data, especially in the context of the protection of personality and possible re-identification of the data subjects.
The last part of the thesis is devoted to the processing of healthcare data in connection with the Proposal of the European Parliament and Council Regulation (EU) on the European Health Data Space and the secondary use of the data for research purposes.

KEY WORDS
Genetic Database; Genetic Data; Personal Data Protection

Plná verze je dostupná z: https://dspace.cuni.cz/handle/20.500.11956/183545

Setkávání moderních technologií a ochrany osobních údajů v současnosti připomíná funkci dvou souběžně probíhajících trendů. Na jedné straně stále narůstá význam nových technologií prakticky ve všech oblastech života. Na straně druhé je pak – mimo jiné právě i v reakci na technický rozmach – kladen stále silnější důraz na ochranu osobních údajů jednotlivce. Mezi typické oblasti, kde k naznačené kolizi dochází, dnes patří rozsáhlé genetické databáze, které začínají být i s využitím genome browserů (programů pro vyhledávání dat v uvedených databázích) ve větším měřítku využívány pro vědecký výzkum i klinickou praxi v medicíně. Způsoby řešení nastíněného konfliktu budou mít do budoucna kruciální význam praktický i teoretický. Téma diplomové práce je tak vrcholně aktuální a relevantní.

Nutno přitom konstatovat, že jde zároveň o téma náročné. Podobně jako jiné oblasti na pomezí práva a nových technologií, také aplikace práva na problematiku genetických databází a genome browserů vyžaduje multidisciplinární přístup, schopnost porozumět právním, technickým i praktickým aspektům problematiky, tyto různorodé (avšak neoddělitelné) perspektivy funkčně propojit, a to vše srozumitelně prezentovat. Nadto jsou specifika zvoleného tématu dosud v právní literatuře spíše opomíjena, což se netýká jen doktríny české, ale pohříchu do velké míry i zahraniční. Jde o oblast s enormním potenciálem pro rozvoj vědy i zdravotnictví, která je ovšem re-

lativně nová, rychle se rozvíjí a její pochopení není zcela snadné. Autorka se tedy nemohla opřít o již hotové souhrny právní argumentace a musela se s relevantními otázkami vypořádat do značné míry sama. Recenzovaná práce těmto nesnadným požadavkům vyhovuje.

Sama stavba práce nejen odpovídá formálním náležitostem struktury diplomové práce, ale především je velmi logická. Autorka postupuje od obecného k zvláštnímu. Nejprve představuje základní stavební kameny problematiky – právo ochrany osobnosti a problematiku sekvenování lidského genomu –, aby dále přistoupila k analýze právní úpravy genetických databází a ochrany genetických údajů, jako i k zamyšlení nad vlivem projektu Evropského prostoru pro zdravotní data (European Health Data Space) včetně velmi diskutované otázky sekundárního využití zdravotních dat.

V úvodu práce si diplomantka klade dvojí cíl. Zaprvé jde o přiblížení současného způsobu zpracování genetických údajů a upozornění na problematiku spojenou především s jejich sdílením. Souvisejícím cílem autorky pak je „poukázat na nutnost zaručení vyšší ochrany genetických dat a přispět tak do předpokládané budoucí debaty ohledně regulace genetických údajů“. Práce tedy neusiluje o nalezení hotových řešení a jednoznačných odpovědí, jako spíše o samotné upozornění širší odborné veřejnosti na problematiku, jejíž význam může v blízké budoucnosti strmět narůstat, o identifikaci souvisejících problémů a o naznačení možností jejich řešení. Současně se autorka nevyhýbá formulaci vlastních názorů (např. týkajících se použitelnosti některých právních důvodů zpracování osobních údajů, tzv. širokého souhlasu se zpracováním osobních údajů nebo rozsahu zpřístupňování genetických údajů veřejnosti). Na úrovni diplomové práce jsou takto vymezené cíle přiměřeně ambiciózní a současně realistické. Z provedení práce je zřejmé, že cíle byly autorkou naplněny.

Rovněž z formálního hlediska je práce zdařilá. Autorka čerpala z velice rozsáhlé odborné literatury, právních předpisů (včetně evropských a mezinárodních) i judikatury. Velmi reprezentativně jsou zastoupeny prameny anglofonní. S ohledem na specifickou povahu tématu je přitom pochopitelné, že většina pramenů nemá čistě právní povahu, jde ovšem o zdroje

jednoznačně relevantní. Převaha mimoprávních pramenů je ostatně typickým rysem prací zabývajících se novými technologiemi nebo šířeji novými jevy, na něž právo (zatím ještě) nestihlo reagovat mohutnější diskusí. V této perspektivě se pak využití rozsáhlé mimoprávní literatury nejeví jako nedostatek práce, ale daleko spíše jako její přednost svědčící o poctivě provedené rešerši. Citace jsou v práci používány rozsáhle a za konzistentního použití citační normy. Také jazyková a stylistická úroveň práce odpovídá kvalitě, kterou lze od diplomové práce žádat.

V souhrnu lze konstatovat, že autorka předložila kvalitní pojednání o výsostně aktuálním, náročném a dosud často přehlíženém tématu. Již z podstaty zvolené problematiky je nutný multidisciplinární přístup, v němž diplomantka s přehledem obstála. Práce je nejen zajímavým vhledem do tématu, ale současně jeho kritickou analýzou, kdy diplomantka materii originálně hodnotí a předkládá vlastní argumentačně podložené názory.

GAVENDOVÁ, M.: KYBERNETICKÁ ŠPIONÁŽ

JAKUB VOSTOUPAL[16]

GAVENDOVÁ, M.: Kybernetická špionáž. 2023, diplomová práce, Masarykova univerzita, Právnická fakulta, 112 s.

ANOTACE

Diplomová práce popisuje, jakým způsobem lze vytvořit bezpečné prostředí, ve kterém je nižší pravděpodobnost, že dojde k průmyslové kybernetické špionáži. Obecná část se zabývá vymezením kybernetické špionáže a původci kybernetických útoků. Zvláštní část se zaměřuje na průmyslovou kybernetickou špionáž. Po objasnění technických otázek práce analyzuje, jak stát odrazuje potenciální útočníky a jak přispívá k tomu, aby se organizace nestaly obětí průmyslové kybernetické špionáže. Dále práce rozebírá, jaká opatření mohou přijmout samy organizace, aby zabránily této praktice. Poslední část se věnuje mezinárodnímu právu veřejnému, které může mít významný vliv na další vývoj v této oblasti.

KLÍČOVÁ SLOVA

Kybernetická špionáž; průmyslová špionáž; ekonomická špionáž; kybernetická bezpečnost; kybernetická kriminalita; útok na dodavatelský řetězec; sledování zaměstnanců

ABSTRACT

The thesis describes how to create a secure environment in which industrial cyber espionage is less likely to occur. The general part defines cyber espionage and characterizes cyber threat actors. The specific part focuses on industrial

[16] Mgr. Jakub Vostoupal je doktorandem na Ústavu práva a technologií na Právnické fakultě Masarykovy univerzity a správcem kybernetické bezpečnosti na Nejvyšším soudě a Nejvyšším správním soudě. Kontaktní e-mail: jakub.vostoupal@law.muni.cz

cyber espionage. After clarifying technical issues, the thesis analyses how the state deters potential perpetrators from industrial cyber espionage and how it contributes to preventing organisations from falling victim to this practice. Afterwards, the thesis explains what measures organizations can take to prevent it. The final part of the thesis discusses public international law as it may significantly influence future development in this area.

KEYWORDS

Cyber Espionage; Industrial Espionage; Economic Espionage; Cybersecurity; Cybercriminality; Supply-chain Attack; Employee Monitoring

Plná verze práce je dostupná z: https://is.muni.cz/th/xt7lq/

Autorka si zvolila téma kybernetické špionáže, a to s důrazem na průmyslovou špionáž a jak snížit rizika s ní spojená, což je téma komplexní, rozsáhlé a náročné, ve kterém je nutné kombinovat poznatky nejen několika odvětví právních, ale též aspekty kyberbezpečnostní, technické či např. psychologické. Náročnost tématu je pak dále umocněna tím, že dané téma nebylo v ČR dosud detailně rozebráno, což negativně ovlivňuje dostupnost zdrojů. I kvůli tomu je s takovým tématem spojen velký potenciál, aby kvalitně napsaná práce byla hodnotným přínosem pro praxi. Tento potenciál dle mého názoru autorka dokázala naplnit.

Autorka si v úvodu práce jasně a přehledně definuje výzkumné otázky, se kterými velice vhodně pracuje napříč celou prací. V jednotlivých kapitolách i podkapitolách vysvětluje, jak daná část přispívá k naplňování cílů práce a výzkumných otázek, což značně usnadňuje čtenářovu orientaci v textu i „příběhu" práce, a zároveň toto zacílení využívá k limitaci „rozptylu" svého výkladu. V závěru autorka přehledně sumarizuje splnění cílů práce a vypořádává výzkumné otázky. U některých podkapitol bych ještě ocenil alespoň krátké shrnutí, co z daného textu dle autorky vyplývá, a u představovaných řešení a nástrojů pak důslednější pojednání o tom, jak by měla být navrhovaná řešení konkrétně implementována, proč by měla řešení zafungovat, či co by měl být kýžený vliv daných prezentovaných ná-

strojů. Ovšem přestože mám k některým aspektům čtvrté kapitoly své výhrady, považuji cíle práce za naplněné.

Po teoretické a obsahové stránce je práce velice kvalitní, přičemž zvláště musím ocenit schopnost autorky se držet (až na výjimky) jedné „příběhové linie" v souladu s výzkumnými otázkami, a to zvláště v úvodních kapitolách. Příkladem může být její výklad k rozšíření práva na soukromí na právnické osoby ve druhé kapitole. Práce pak svědčí o nadprůměrné orientaci, kterou autorka v tématu získala, a to je, zvláště s přihlédnutím ke komplexitě tématu a mnoha technickým aspektům, obdivuhodné. Soudím, že pro praxi budou hodnotné nejen závěry a doporučení, které autorka představuje ve čtvrté kapitole, ale také velice kvalitní a přehledná analýza kapitoly druhé a třetí (což může ilustrovat kapitola 3.4.1, ve které se autorka zabývá právní klasifikací relevantních aktiv). Musím pak ocenit účinné propojení hned několika právních odvětví včetně relevantní judikatury a komentářové literatury.

Kapitola čtvrtá, která je nosnou kapitolou celé práce, však trpí určitými problémy. V první řadě by jí jistě prospělo větší provázání s kapitolami předchozími. Podkapitola 4.3 je pak velice popisná, přičemž sledovat veškeré závěry autorky je v této části již trochu náročné (trochu jsem postrádal nějaké jednodušší uspořádání daných doporučení, což se ostatně vztahuje na celou čtvrtou kapitolu), ale to do značné míry přisuzuji rozsahu tématu a potřebě podat zevrubný výklad před jednotlivými doporučeními. Navzdory tomu, že některá doporučení lze označit za lehce idealistická a nereflektující plně stav praxe (např. častý případ vendor lock-inu v kontextu kritérií pro výběr dodavatelů či kapacitní náročnost dostatečného prověření dodavatelů či zájemců o zaměstnání), většinu doporučení považuji za vhodnou a hodnotnou pro praxi.

Mám však určité výhrady k obsahu závěru čtvrté kapitoly, konkrétně k podkapitole 4.5, kde se autorka zaměřila na mezinárodněprávní problematiku. V prvé řadě by si tato část zasloužila poněkud důslednější rozpracování, což je bohužel v limitech diplomové práce problematické, nicméně v současné chvíli se jedná spíše o takové „zabrouzdání" na povrch problému a tato podkapitola kvalitativně „klopýtá" za zbytkem práce. Autorka

pak několik aspektů notně zjednodušila, což může způsobit až jejich dezinterpretaci či faktickou nesprávnost. Konkrétním příkladem je věta „*Jednání hackerských skupin podporovaných státem je státu přičitatelné*". V daném kontextu je nutné zdůraznit, že kybernetické ekonomické špionáže se sice může jednoduše dopouštět i státní orgán či subjekt nadán výkonem státní moci, přičemž přičtení by bylo v takových případech zásadně jednodušší, ale přičtení jednání nestátních aktérů (např. tedy hackerských skupin) podle podmínek článku 8 ARSIWA je podstatně náročnější, a to jak z právního (míra kontroly a podpory ze strany státu), tak z důkazního hlediska. Ostatně Mačák upozorňuje, že takové přičtení, které by uspokojilo právní požadavky testu efektivní kontroly, je za stávající situace i u normálních kybernetických útoků spíše nepravděpodobné (více viz Mačák, K. *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*). Tato skutečnost pak pochopitelně ovlivňuje vyznění zbytku podkapitoly.

Formální úroveň práce je povšechně na velmi vysoké úrovni. Snad jediné povzdechnutí je nad používáním *wir* formy, ke kterému autorka sklouzává zvláště v první polovině práce (toto používání je navíc nejednotné, neb jej autorka střídá s *ich* formou - např. na str. 84). Co bych ale vyzdvihl, je jednoduchost a čtivost textu zvláště druhé a třetí kapitoly, ve kterých se obdivuhodně snoubí s vysokou odbornou úrovní daného pojednání. Tato čtivost ve čtvrté kapitole poněkud upadá na úkor větší popisnosti, kdy text začíná být komplikovanější a čtenář se v něm hůře orientuje, ale to se netýká v zásadě celé kapitoly 4, ale spíše jen některých podkapitol, např. podkapitoly 4.3 a 4.4.3.2.

Ve většině práce pak autorka text strukturuje přehledně, upraveně a logicky. Zvláště jsem ocenil obsahovou strukturu práce, kdy se autorka před samotným návrhem opatření zaměřuje na konkrétní útočníky a útoky, kteří jsou pro téma kybernetické špionáže relevantní, což jí umožnilo navrhovaná řešení daleko konkrétněji a vhodněji zacílit, díky čemuž jsou taková doporučení pro praxi zásadně hodnotnější.

Práci tak ve výsledku, i navzdory výše uvedeným výtkám, považuji za velice kvalitní a hodnotný počin, který jsem si s chutí přečetl.

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

ADAM JAREŠ[1]

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

1. ÚVOD

Oblastem úpravy nařízení eIDAS[2], tedy elektronické identifikace a služby vytvářející důvěru, není dlouhodobě v české právnické literatuře věnována náležitá pozornost. To samé platí pro české právní předpisy upravující elektronické právní jednání, ať již jde o elektronické podepisování, identifikaci nebo doručování. S ohledem na probíhající digitální transformaci zrychlenou katalyzátorem v podobě různých lockdownů a omezení osobního styku či nutnými úsporami na straně státu i soukromého sektoru se tato situace začíná pomalu měnit a téma virtualizace právního jednání se dostává v právnické literatuře větší pozornosti. Kniha Tomáše Lechnera tak do jisté míry splácí dluh spočívající buď ve zcela absentující literatuře či v doplnění k existujícím publikacím jako aktuální a velmi vítaný další zdroj poznání této oblasti.

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

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

2. HODNOCENÍ A PŘÍNOS KNIHY

Význam knihy pro diskurz k tématu elektronického právního jednání je patrný již z jejího samotného názvu. Autor se totiž nezastavil pouze u nařízení eIDAS[3], ale v návaznosti na předchozí výklad k tomuto nařízení komentuje také české adaptační předpisy – zákon o službách vytvářejících důvěru[4] a zákon o elektronické identifikaci[5]. Velmi vhodně se autor věnuje také komentáři evropských prováděcích předpisů.[6]

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

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

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

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

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

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

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

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

3. KNIHA A AKTUÁLNÍ VÝVOJ NA ÚROVNI EVROPSKÉ UNIE

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

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

4. ÚVAHA KE DVĚMA ČÁSTEM NAŘÍZENÍ

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

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

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

Kladu si v této souvislosti otázku, zda tyto dvě oblasti, které mohlo být do jisté míry možné vnímat jako oddělené v době přijetí nařízení eIDAS, je možné vnímat stejným způsobem i v roce 2023. Oddělenost obou oblastí lze sice zdůvodnit nejen autorem odkazovanou prací Vojtěcha Kmenta nebo přijetím dvou různých zákonů v České republice[9]. Odpověď na tuto otázku však není podle mého názoru tak jednoznačná a obě oblasti se postupně začínají stále více prolínat či se vzájemně alternovat.

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

> 1. Zákon o právu na digitální služby[10] dává na stejnou úroveň elektronicky podepsaná podání a podání učiněná po provedení elektronické identifikace. Uživatel digitální služby má podle tohoto zákona právo činit digitální úkon vůči orgánu veřejné moci prostřednictvím sítě elektronických komunikací dokumentem podepsaným uznávaným elektronickým podpisem či v některých případech uznávanou elektronickou pečetí. Stejně tak má uživatel právo digitální úkon vykonat za stanovených podmínek i prostřednictvím informačního systému veřejné správy umožňujícího prokázání totožnosti uživatele služby s využitím elektronické identifikace.[11]
>
> 2. Podle zákona o informačních systémech veřejné správy se úkon, jehož náležitostí má být podpis, považuje za podepsaný, pokud byl učiněný prostřednictvím informačního systému veřejné správy, který umožňuje prokázání totožnosti s využitím elektronické identifikace.[12]

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

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

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

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

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

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

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

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

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

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

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

[14] Srov. čl. 24 nařízení eIDAS.

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

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

5. DISKUZE A ZÁVĚR K ÚVAZE

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

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

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

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

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

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

https://doi.org/10.5817/RPT2023-2-4

NON-FUNGIBLE TOKENS A OCHRANA SPOTŘEBITELE[1]

JAROSLAV KONEČNÝ[2]

ABSTRAKT:

Článek má za cíl analyzovat právní povahu Non-Fungible Tokens neboli NFT a související otázky ochrany spotřebitele. Pro úplné pochopení technologie NFT je nutné nejdříve osvětlit vztah NFT k podkladovému aktivu, použitému k jeho vytvoření. Diferenciace NFT od podkladového aktiva a jejich vzájemný vztah umožní pochopení funkcionalit a následných právních dopadů jednotlivých kategorií NFT a zjištění, jaká práva se vztahují k vlastnictví konkrétního NFT. Vzhledem k faktu, že NFT je virtuálním statkem s určitou hodnotou, je na místě zkoumat aplikaci spotřebitelského práva, které je při prodeji těchto aktiv stále hojně přehlíženo. Článek proto uvádí jednotlivé prvky informační povinnosti podnikatele prodávajícího NFT a blíže se věnuje otázce odstoupení od smlouvy o koupi NFT. Se spotřebitelským právem úzce souvisí ochrana uživatelů digitálního obsahu, je proto poskytnuto teoretické posouzení uplatnění tohoto právního institutu na fenomén NFT.

KLÍČOVÁ SLOVA:

Blockchain; Non-Fungible Token; Ochrana spotřebitele; Poskytování digitálního obsahu; Právo na odstoupení od smlouvy; Tokenizace.

---

[1] Tento článek vychází z autorovy diplomové práce (dostupná z: https://is.muni.cz/th/fpcdl/).

[2] Mgr. Jaroslav Konečný je absolventem Právnické fakulty Masarykovy univerzity v Brně. Kontaktní e-mail: 480534@muni.cz.

ABSTRACT:

The article aims to analyse the legal nature of Non-Fungible Tokens (NFT) and related consumer protection issues. To fully understand NFT technology, it is necessary to first clarify the relationship of the NFT to the underlying asset used in the minting process. Differentiating NFTs from the underlying asset and their relationship will allow for an understanding of the functionalities and subsequent legal implications of respective NFT categories and to determine what rights apply to the ownership of a particular NFT. Given the fact that an NFT is a virtual asset with a value, it is appropriate to examine the application of consumer law, which is still widely overlooked when selling these assets. The article therefore sets out the various elements of the information obligation of the entrepreneur selling NFTs and further explores the issue of right of withdrawal when purchasing an NFT. Consumer law is closely related to the protection of users of digital content; therefore the article provides a theoretical assessment of the application of this legal institute to the phenomenon of NFTs.

KEY WORDS:

Blockchain; Non-Fungible Token; Consumer Protection; Provision of Digital Content; Right of Withdrawal; Tokenization.

1. ÚVOD

Pokrok v oblasti informačních technologií má dopad na všechny oblasti našeho života, ať už se jedná o základní potřeby člověka, nebo lidské záliby. Příkladem takového pokroku je technologie zvaná blockchain,[3] fungující formou distribuované účetní knihy. Její název vznikl spojením anglických slov „block“ (blok) a „chain“ (řetězec), což odráží fungování tohoto systému, využívajícího počítačové zdroje k vytváření vzájemně propojených řetězů bloků k zápisu nezměnitelných a nesmazatelných informací.[4]

[3] Blockchain je druh distribuované decentralizované databáze uchovávající data v rámci šifrovaného protokolu na základě mechanismu konsenzu.

[4] NOFER, Michael, Peter GOMBER, Oliver HINZ a Dirk SCHIERECK. Blockchain. In: *Business & Information Systems Engineering.* 2017, r. 59, č. 3, s. 183-184.

Jedním ze způsobů využití této technologie, který v posledních letech rezonoval nejen mezi nadšenci technologie blockchain, jsou tzv. Non-Fungible Tokens, zkráceně NFT. Pod pojmem *Non-Fungible* si můžeme představit nemožnost změny, nahrazení či záměny za podobný prvek, tedy vytvoření jedinečnosti. Slovo *Token* vychází z konceptu tokenizace, tedy možnosti konkretizace práv v tokenech – záznamech propsaných v digitální databázi blockchainu.[5]

Klíčem k rozšíření povědomí o technologii NFT byla mimo jiné právě schopnost vytvářet jedinečnost a s ní pojící se hodnotu ve virtuálním světě. Této nové příležitosti přinášející novou třídu aktiv schopných komercializace ve virtuálním prostoru se chopily mnohé společnosti cílící na spotřebitelský sektor.

Prezident videoherní společnosti Square Enix, Yosuke Matsuda ve svém novoročním dopisu označil rok 2021 termínem „*NFTs: Rok první*“, kdy poukázal na to, že se právě v tomto roce NFT setkaly s velkým nadšením rychle se rozšiřující uživatelské základny.[6] Zatímco v roce 2020 trh s NFT vygeneroval objem obchodů ve výši odpovídající tehdejším 94,9 milionům amerických dolarů, v roce 2021 se toto číslo mnohonásobně zvýšilo, a to na 24,9 miliard amerických dolarů.[7] Matsuda však poukázal také na možný efekt investiční bubliny:[8] „*pozoruje-*

[5] GARCIA-TERUEL, Rosa M, Héctor SIMÓN-MORENO. The digital tokenization of property rights. A comparative perspective. In: *Computer Law & Security Review*. 2021, r. 41, s. 2-4.; Blockchain technologies and IP ecosystems: A WIPO white paper. [online]. In: *WIPO*. 2022, s. 15. [cit. 22. 10. 2022]. Dostupné z: https://www.wipo.int/export/sites/www/cws/en/pdf/blockchain-for-ip-ecosystem-whitepaper.pdf

[6] MATSUDA, Yosuke. A New Year's Letter from the President [online]. In: *SQUARE ENIX*. 1. 1. 2022. [cit. 22. 10. 2022]. Dostupné z: https://www.hd.square-enix.com/eng/news/2022/html/a_new_years_letter_from_the_president_2.html

[7] HOWCROFT, Elizabeth. NFT sales hit $25 billion in 2021, but growth shows signs of slowing [online]. In: *reuters.com*. 11. 1. 2022. [cit. 23. 10. 2022]. Dostupné z: https://www.reuters.com/markets/europe/nft-sales-hit-25-billion-2021-growth-shows-signs-slowing-2022-01-10/

[8] Investiční bublinou v kontextu finančního trhu rozumíme cyklus charakterizovaný dramatickým růstem tržních hodnot. Je typickým dvěma základními fázemi. První, kdy ceny strmě rostou. Druhou charakterizuje strmý pokles cen; srov. JAROLÍM, Jaroslav. Investiční bublina – jak ji snadno rozpoznat a v čem spočívají rizika? [online]. In: *kryptomagazin.cz*. 31. 6. 2021. [cit. 22. 10. 2022]. Dostupné z: https://kryptomagazin.cz/investicni-bublina-jak-ji-snadno-rozpoznat-a-v-cem-spocivaji-rizika/

me příklady obchodování s NFT s poněkud spekulativním podtextem, bez ohledu na zjištěnou hodnotu poskytovaného obsahu,“ který se posléze projevil. Přes silný start roku 2022 následovalo částečné splasknutí NFT bubliny doprovázené několikaměsíčním poklesem prodejů a snížením tzv. floor prices, tedy minimálních cen jednotlivých NFT kolekcí. I přes to však silnější konec roku 2022 pomohl vykompenzovat slabší měsíce a celkový roční objem prodejů NFT v roce 2022 se téměř vyrovnal roku předchozímu a zachoval nepominutelný význam této technologie.[9]

S rostoucím zájmem o NFT však vyvstaly nejen nové příležitosti, ale i řada právních otázek. Cílem tohoto článku je objasnit určité právní aspekty fenoménu NFT a vyhodnotit výzvy spojené s aplikací ochrany spotřebitele na transakce s NFT. Článek je rozdělen do tří nosných kapitol.

První kapitola je zaměřena na technické vymezení NFT jakožto nezastupitelných tokenů, je popsán proces vytvoření NFT a kategorizace NFT podle způsobu uložení podkladového aktiva.[10]

Druhá kapitola je zaměřena na právní povahu NFT a jeho podřazení pod definici věci v právním smyslu. Fenomén NFT je zkoumán z pohledu tokenizace, jakožto konkretizace práv v tokenech, a přináší rozdělení NFT do kategorií tokenů podle vázanosti NFT na podkladové aktivum sloužící k jeho vytvoření. Následná podkapitola je věnována odlišitelnosti NFT od podkladového aktiva a jejich vzájemnému vztahu. Kapitola je zakončena aspekty vlastnických práv k NFT vytvořenému na základě fyzického podkladového aktiva a k NFT vytvořenému na základě virtuálního podkladového aktiva.

Třetí kapitola zasazuje diskutovaný fenomén NFT do aspektů ochrany spotřebitele. Jsou definovány spotřebitelské vztahy při transakcích s NFT a identifikovány jednotlivé aspekty pro vznik spotřebitelského vztahu jehož předmětem je NFT. Obsáhlejší část kapitoly je věnována informační povinnosti podnikatele prodávajícího NFT vůči spotřebiteli

[9] HAYWARD, Andrew. NFT Sales in 2022 Nearly Matched the 2021 Boom, Despite Market Crash [online]. In: *Decrypt*. 5. 1. 2023. [cit. 10. 3. 2023] Dostupné z: https://decrypt.co/118438/2022-versus-2021-nft-sales

[10] Podkladovým aktivem NFT rozumíme nehmotné nebo hmotné aktivum ve virtualizované podobě, které slouží k vytvoření NFT.

s vymezením jednotlivých prvků informační povinnosti dle § 1820 odst. 1 OZ a blíže je zkoumána problematika odstoupení od smlouvy o koupi NFT. Závěrem je taktéž zmíněn vhled do aspektů ochrany uživatelů digitálního obsahu dle ustanovení § 2389a OZ ve vztahu k NFT.

2. TECHNICKÉ VYMEZENÍ NON-FUNGIBLE TOKENS

Jedním z nejvýznamnějších využití technologie blockchain je schopnost tokenizace aktiv. Token je digitálním záznamem zachyceným v elektronické síti založené na technologii blockchain, který mimo tento systém nemůže existovat.[11]

Konceptem tokenizace rozumíme šifrovanou reprezentaci aktiv v tokenech – programovatelných digitálních jednotkách zaznamenaných v blockchainu.[12]

Z čistě technického hlediska jsou tokeny pouze metadata zaznamenaná v blockchainu. Metadata jsou daty poskytujícími informace o jiných datech. Mohou mít mnoho podob, včetně popisné, strukturní nebo administrativní, a využívají se v rámci různých informačních činností, od vyhledávání a identifikace zdrojů až po organizaci dat.[13]

Z právního pohledu lze na token nahlížet jako na virtuální aktivum *sui generis*. Jedná se o nehmotnou movitou věc, která odpovídá právu jejího vlastníka na přístup k určité službě nebo produktu, které minter[14] tokenu nabízí, nebo právu podílet se určitým způsobem na projektu, který minter tokenu financuje prostředky získanými od investorů.[15]

---

[11] DĚDIČ, Jan, Jan ŠOVAR a Ondřej MIKULA. Proč podle českého soukromého práva nelze uvažovat o (ICO) tokenech jako o cenných papírech. In: *Právní rozhledy*. 2018, roč. 15-16, s. 554.

[12] GUADAMUZ, Andres. The treachery of images: non-fungible tokens and copyright. In: *Journal of Intellectual Property Law & Practice*. 2021, roč. 16, č. 12, s. 1369.

[13] BARRINGTON, Sarah. The Role of Metadata in Non-Fungible Tokens: Marketplace Analysis and Collection Organization. In: *arXiv preprint arXiv*. 2021, s. 2.

[14] Minterem rozumíme subjekt, který vytváří NFT.

[15] DĚDIČ, ŠOVAR, MIKULA, ref. 11, s. 554.

Jedná se tedy o jakýsi soubor dat, který po uvedení do blockchainové sítě může sloužit jako jednoznačná deklarace práv, která minter s tokenem propojil.

NFT jsou specifickou třídou tokenů. Jejich hlavním znakem je jejich nezastupitelnost. Všechny NFT mají již při vytvoření jedinečné a nezastupitelné vlastnosti dané jedinečným TokenID[16] a adresou chytrého kontraktu.[17] NFT můžeme chápat jako digitální certifikáty uložené v blockchainu, které odkazují na virtuální nebo fyzické podkladové aktivum a mohou s tímto podkladovým aktivem pojit určitá práva. NFT mají atributy jedinečnosti, exkluzivity a nezastupitelnosti.[18]

Je na místě se tázat, jaká aktiva mohou být v rámci blockchainové sítě pomocí NFT reprezentována. Z hlediska technické proveditelnosti není aspekt tělesnosti aktiva rozhodující, NFT tak mohou reprezentovat jak věci hmotné, tak věci nehmotné.

Proces vytváření NFT se nazývá minting.[19] Nejčastější sítí blockchainu, na které jsou NFT mintovány, je Ethereum,[20] a nejrozšířenějším protokolem pro realizaci chytrých kontraktů určených k mintingu a následným transakcím NFT na blockchainu Ethereum je token standard[21] ERC-721.[22] Ten každému tokenu dává jedinečný identifikátor, datový soubor, který je výsledkem kombinace kryptografického klíče adresy chytrého kontraktu

[16] TokenID je jedinečný identifikační kód, odlišující jednotlivé NFT v rámci blockchainové sítě.

[17] Chytrý kontrakt je protokol uložený v blockchainu, který se automaticky spustí při splnění určitých podmínek bez nutnosti zprostředkovatele a provede definované operace.

[18] POPESCU, Andrei-Dragos. Non-Fungible Tokens (NFT)-Innovation Beyond the Craze. In: *5th International Conference on Innovation in Business, Economics and Marketing Research*. 2021, s. 26.

[19] Mintingem rozumíme proces vytvoření neboli ražby NFT, v rámci kterého jsou metadata vztahující se k podkladovému aktivu zapsána do blockchainové sítě.

[20] Ethereum je blockchainová síť s funkcí chytrých kontraktů. V současnosti je Ethereum hlavní blockchainovou sítí pro vytváření NFT.

[21] Token standard je soubor dohodnutých pravidel, kterými se řídí mintování tokenů v rámci konkrétní blockchainové sítě.

[22] Non-fungible tokens (NFT) [online]. In: *ethereum.org*. [cit. 17. 11. 2022]. Dostupné z: https://ethereum.org/en/nft/#how-nfts-work

a TokenID.[23] Kupující NFT obdrží digitální certifikát obsahující identifikátor který mu umožňuje připojit se výhradně k chytrému kontraktu a přistupovat k digitálnímu souboru – podkladovému aktivu, jehož použití je omezeno podmínkami stanovenými v chytrém kontraktu spojeném s tímto tokenem.[24]

Tento proces vyžaduje technické znalosti, je tedy běžné, že NFT jsou mintovány prostřednictvím tzv. NFT on-line tržišť. Příkladem populárního NFT on-line tržiště je platforma OpenSea,[25] která umožňuje vytváření, distribuci, nákup a prodej NFT. Výsledkem, bez ohledu na způsob mintingu NFT, bude jeho uložení v digitální kryptopeněžence uživatele.

To, co je uloženo v digitální kryptopeněžence, však není samotné podkladové aktivum. V tomto ohledu je důležité zdůraznit reprezentační charakter NFT, které bez dalšího nepředstavují samotné podkladové aktivum. Jedná se pouze o registraci existence podkladového aktiva a jeho dalších vlastností a relevantních dat v blockchainové síti.

Pokud jde o uložení podkladového aktiva, lze NFT rozdělit na dvě kategorie: (1) NFT off-chain, (2) NFT on-chain.[26]

Uložení off-chain znamená, že podkladové aktivum je uloženo mimo blockchainovou síť, tedy v jakémkoli jiném datovém úložišti mimo blockchain. To, co v této situaci spojuje podkladové aktivum s NFT, jsou metadata uložená v blockchainu, primárně URL adresa odkazující na podkladové aktivum uložené mimo blockchainovou síť.[27]

Příkladem můžeme uvést situaci, kdy držitel NFT bude mít přístup k videu, které je uloženo ve složce Google Drive. V blockchainu však nebu-

---

[23] *„Je důležité zdůraznit, že výsledný NFT může obsahovat další informace, jako je např. jméno díla, jméno autora, licenční podmínky k dílu a mnoho dalších údajů, které se mohou pojit s podkladovým aktivem. TokenID a adresa chytrého kontraktu jsou nejdůležitějšími prvky, neboť jsou spojeny konkrétně s podkladovým aktivem.…“* GUADAMUZ, ref. 12, s. 1371.

[24] Blockchain technologies and IP ecosystems, ref. 5, s. 31.

[25] What is minting? [online]. In: *OpenSea Learn*. [cit. 17. 11. 2022]. Dostupné z: https://opensea.io/learn/what-is-minting-nft

[26] GUADAMUZ, Andres., What Do You Buy When You Buy an NFT? [online]. In: *TechnoLlama*. 28. 3. 2021. [cit. 19. 11. 2022]. Dostupné z: https://www.technollama.co.uk/what-do-you-buy-when-you-buy-an-nft

[27] GUADAMUZ, ref. 12, s. 1371.

de uloženo samotné video, nýbrž URL adresa odkazující na místo uložení souboru v Google Drive.

NFT off-chain[28] jsou využívány primárně z důvodu nižších nákladů na jejich vytvoření. S úsporou energie a finančních nákladů však souvisí nízká spolehlivost uložení podkladového aktiva. I když s URL adresou zapsanou v blockchainu již manipulovat nelze, soubor uložený na centralizovaném serveru se může stát pro vlastníka NFT nedostupným z důvodu chyb v centralizovaném systému, narušení třetí osobou či jednoduše ukončením hostingu webové stránky, na které bylo podkladové aktivum uloženo. K řešení tohoto problému byly navrženy určité postupy pro uložení podkladového aktiva, například použití decentralizovaného úložiště IPFS (Interplanetary File Systems).[29]

Alternativou k uložení podkladového aktiva mimo blockchainovou síť je tzv. NFT on-chain.[30] Při něm dochází k nahrání podkladového aktiva přímo do blockchainové sítě jeho přidáním do metadat chytrého kontraktu NFT.[31] V důsledku toho je v blockchainu trvale uložena reprezentace digitálně obchodovatelného podkladového aktiva.

NFT jsou sice z technického pohledu pouhými metadaty zapsanými v blockchainu, mohou být však prostředkem k digitální revoluci vyřešením otázky jedinečnosti virtuálních aktiv. K tomu je však nutné objasnit jejich právní podstatu a na základě ní kvalifikovat relevantní právní vztahy, jejichž předmětem NFT mohou být.

---

[28] Příkladem NFT off-chain je edice The Bored Ape Yacht Club od studia Yuga Labs. BAYC [online]. In: *boredapeyachtclub.com*. [cit. 25. 11. 2022]. Dostupné z: https://boredapeyachtclub.com/#/

[29] WANG, Qin, Ruija LI, Qi WANG, Shiping CHEN. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. In: arXiv preprint arXiv, s. 13-14.

[30] Příkladem NFT on-chain je edice CryptoPunks, původně vytvořená jako off-chain, posléze byla jednotlivá podkladová aktiva uložena přímo v blockchainu Etherea. CryptoPunks [online]. In: *larvalabs.com*. [cit. 26. 11. 2022]. Dostupné z: https://www.larvalabs.com/cryptopunks

[31] GUADAMUZ, ref. 26.

3. PRÁVNÍ POVAHA NFT

3.1 NFT JAKO VĚC

Jelikož v českém právním řádu dosud nenalezneme výslovná ustanovení o právní povaze NFT, je na místě zkoumat právní povahu NFT z hlediska právem poznaných zavedených institutů, konkrétně zda lze NFT podřadit pod definici věci v právním smyslu.

Občanský zákoník v ustanovení § 489 definuje věc v právním smyslu jako vše, co je „*rozdílné od osoby a slouží potřebě lidí*." Z hlediska materiální povahy dělíme věci na hmotné a nehmotné. Nehmotnými věcmi jsou dle ustanovení § 496 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „OZ") práva, jejichž povaha to připouští a „*jiné věci bez hmotné podstaty.*" Jelikož jsou NFT formou datového kódu, lze o nich mluvit jako o datech. Data jsou často právními texty zaměňována za informace, je na místě si odlišení vymezit.

Polčák důsledně rozlišuje mezi informací a daty. Uvádí, že informace nemůže být věcí dle ustanovení § 489 OZ, kdy informace není statickým jevem nebo existující entitou, nýbrž přírodním fenoménem, který lze z pohledu člověka popsat pouze v čase a nesnese právní objektivizaci. Informaci chápe jako účel právního vztahu, nikoliv však nástroj k jeho dosažení. Rozdílně však chápe data, u kterých uvádí, že mohou být sekundárním objektem právních vztahů, kdy jejich aktuální nebo virtuální užitek lze charakterizovat jako věc v právním smyslu.[32]

S vědomím rozlišení těchto dvou pojmů, které jsou českou právní veřejností nezřídka zaměňovány, lze odkázat na komentář Svobody k ustanovení § 496 OZ, který se této nešťastné záměny dopouští, objektivizaci dat však popisuje vhodně, tedy že nehmotnou věcí v právním smyslu mohou být data v případě, že jsou pro některý ze subjektů práv využitelná jako ekonomická hodnota a zároveň za situace, kdy subjekt, který je jejich pů-

[32] POLČÁK, Radim. Informace a data v právu. In: *Revue pro právo a technologie.* 2016, roč. 7, č. 13, s. 88.

vodcem, je zpřístupní jako možný předmět soukromoprávních vztahů a tato data mají objektivně alespoň potenciální majetkovou hodnotu.[33]

Z výše uvedeného je na místě klasifikovat NFT jakožto nehmotnou věc v právním smyslu, což umožňuje další specifikaci z pohledu tohoto právního institutu.

Občanský zákoník přináší dále dělení věcí na věci movité a nemovité. Již ze samotné podstaty NFT vyplývá, že se jedná o věci povahou movité. Potvrzení této teze mimo jiné přináší i příloha č. 6, bod 9.8 vyhlášky č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Ta uvádí v dotazníku fyzické osoby podle ustanovení § 95 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů „*nezastupitelný token – tzv. NFT dílo*“ jako příklad movitého majetku. Národní bezpečnostní úřad toto následně potvrdil a doplnil ve Věstníku č. NB07/2022,[34] kde uvedl, že NFT jsou virtuální aktiva, která jsou movitým majetkem.

Zásadním atributem, který následuje samotná podstata NFT, je jejich nezastupitelnost, vyplývající již ze samotného názvu – *Non-Fungible tokens* – tzv. nezaměnitelné/nezastupitelné tokeny. Individualita každého NFT vyplývá z podstaty této technologie, protože NFT obsahuje jedinečný nereprodukovatelný kód, který konkrétní token odlišuje od ostatních. Tím se zároveň zaručuje existence pouze jedné instance každého konkrétního NFT.[35]

3.2 KLASIFIKACE NFT

Jednu z klasifikací, která rozlišuje NFT do kategorií dle konkrétních vlastností, přinesla iniciativa Evropské komise s názvem European Block-

[33] SVOBODA, Karel. § 496 Věci hmotné a nehmotné. In: DAVID, Ondřej. a kol. *Občanský zákoník. Komentář. 1. vyd*. Praha: Wolters Kluwer, a. s., 2014. ISSN: 2336-517X.

[34] Informace č. NB07/2022, bezpečnostní způsobilost. cit. z ASPI.

[35] Nikoliv však existence jediného NFT vytvořeného na základě podkladového díla, takových může být neomezeně. Z jednoho podkladového díla totiž můžeme vytvořit nespočet různých NFT. Kvůli jedinečnému TokenID a adrese chytrého kontraktu však nelze zaměnit jedno konkrétní NFT za druhé.

chain Observatory and Forum.[36] V reportu zveřejněném v červnu 2021 nalezneme následující klasifikaci NFT.

1. Asset tokens – Tokeny vázané na aktiva, jež představují konkrétní právo k hmotné nebo nehmotné věci.
2. Utility tokens – Tokeny vázané na právo na poskytnutí služeb, jež jsou spojeny s právem na přístup k určitým službám poskytovaným stranou vydávající token (nebo jinou specifikovanou třetí stranou).
3. Security tokens – Tokeny poskytující držitelům NFT podobná nebo stejná práva jako cenné papíry.

První kategorií NFT jsou tokeny vázané na aktiva, jež představují konkrétní právo k hmotné nebo nehmotné věci, která je podkladovým aktivem NFT. Osoba vytvářející token rozhoduje o právech, která budou s tokenem smluvně provázána, a která budou náležet následnému držiteli NFT. Takovými právy mohou být kupříkladu práva k užití podkladového aktiva jakožto autorského díla, udělené autorem nabyvateli NFT v rámci licenční smlouvy nebo certifikace podkladového aktiva pomocí NFT.[37]

Další kategorií, kterou European Blockchain Observatory and Forum vymezuje jsou NFT vázané na právo na poskytnutí nebo přístup k určitým službám poskytovaným stranou vydávající token (nebo jinou specifikovanou třetí stranou). Právo na poskytnutí služeb však dle autorova názoru samo o sobě nekonstituuje novou kategorii NFT. Z technického aspektu totiž NFT, se kterým bude provázáno právo na poskytnutí služby, nebude ničím specifické. Jeho přidaná hodnota, tedy ono právo na poskytnutí služeb, nebude technicky určena povahou NFT. Poskytnutí služby nebude určeno blockchainovou sítí, nýbrž smluvním vztahem nebo jiným mechanismem, kterým se, ať už strana vydávající token nebo jiná třetí strana, zaváže, že po ověření, zda subjekt je opravdu vlastníkem NFT, poskytne službu. Konkrétním příkladem může být situace, kdy se vlastník hotelu rozhodne vytvořit NFT, jejichž držitelé budou mít právo na poskytnutí exklu-

[36] HERIAN, Robert a kol. NFT–Legal Token Classification. In: *EU Blockchain Observatory & Forum.* 2021, s. 2.

[37] Pro klasifikaci budeme Asset tokeny považovat za tokeny, které jsou smluvně provázané s konkrétními právy k hmotné nebo nehmotné věci, která byla podkladovým aktivem při mintování NFT.

zivních služeb v rámci pobytu v hotelu. V případě, kdy držitel NFT prokáže ověřovateli, že se dané NFT opravdu nachází v jeho digitální kryptopeněžence, budou mu tyto služby poskytnuty.[38]

Relevantní pro klasifikaci NFT je otázka možného zařazení NFT jakožto cenného papíru dle ustanovení § 514 OZ nebo zaknihovaného cenného papíru dle ustanovení § 525 OZ. Výše zmíněný report European Blockchain Observatory and Forum nabízí možnost klasifikace NFT jako tzv. security tokenů, tedy tokenů ve formě digitálních cenných papírů, jež představují vlastnictví aktiva a poskytují držitelům tokenů podobná nebo stejná práva jako cenné papíry.[39] Z pohledu českého práva však o NFT jakožto o cenných papírech hovořit nelze. NFT je virtuální nehmotnou věcí, z toho důvodu není možné na něj pohlížet jako na cenný papír dle ustanovení § 514 OZ, jelikož u NFT chybí spojení s listinou v právním slova smyslu. Zároveň současně neexistuje zákonná povinnost emitentů NFT zapisovat NFT do příslušné zákonem uznané evidence dle ustanovení § 91 zákona č. 256/2004 Sb., o podnikání na kapitálovém trhu, ve znění pozdějších předpisů (dále jen „ZPKT"). NFT je ze své podstaty individuálně určenou věcí, kterou nelze nahradit jiným NFT téhož druhu ani v případě totožného mintera NFT a skutečnosti, že by NFT zaručovalo stejná práva. Z těchto důvodů o NFT nelze mluvit ani jako o zaknihovaném cenném papíru, jehož znakem je právě zastupitelnost.[40] Tento názor zastává i ČNB ve svém Upozornění na rizika investic do alternativních produktů, ve kterém dochází k závěru, že NFT nejsou investičním nástrojem ve smyslu ustanovení § 3 odst. 1 ZPKT.[41]

---

[38] Takovým hotelem je CHORS like a hotel, který držitelům jejich NFT poskytuje exkluzivní služby v rámci jejich pobytu. MetaCHORS Blocks [online]. In: *metachors.com*. [cit. 12. 1. 2023]. Dostupné z: https://www.metachors.com/

[39] HERIAN, Robert a kol., ref. 36, s. 2.

[40] CHLUBNA, Filip. *Práva výkonných umělců a jejich ochrana ve sféře internetu a sociálních sítí*. Praha, 2022, diplomová práce, Univerzita Karlova, Právnická fakulta, s. 81; DĚDIČ, ŠOVAR, MIKULA, ref. 11, s. 554-556.

[41] Upozornění na rizika investic do alternativních investičních produktů (tokeny, participace) [online]. In: *Česká národní banka*. 3. 12. 2021. [cit. 14. 1. 2023]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/upozorneni-pro-verejnost/Upozorneni-na-rizika-investic-do-alternativnich-investicnich-produktu-tokeny-participace/

K upravenému rozřazení, které poskytuje European Blockchain Observatory and Forum, je na místě doplnit další kategorii NFT. Touto kategorií jsou tokeny sloužící jako nezávislá reprezentace podkladových aktiv. Tyto NFT jsou vytvořeny na základě podkladového aktiva, jsou jasným odkazem na ně, minter s nimi však smluvně neprovázal žádná práva k podkladovému aktivu. Jejich hodnota je čistě spekulativní, často vytvářená pouze na základě faktu, že odkazují na známé fyzické předměty, nebo byl jejich tvůrcem známý umělec. Ke konkrétnímu podkladovému aktivu, na základě kterého byly vytvořeny, však nemají žádný právní vztah.

Pro potřeby tohoto článku tedy budeme rozřazovat NFT do dvou kategorií v závislosti na provázanosti NFT s podkladovým aktivem, a to:

1. NFT vázané na podkladová aktiva
2. NFT sloužící jako nezávislá reprezentace podkladových aktiv.

3.3 ODLIŠITELNOST NFT OD PODKLADOVÉHO AKTIVA

Odlišitelnost a případná nutnost odlišení NFT od podkladového aktiva, na jehož základě bylo NFT vytvořeno, je potřebnou úvahou, na základě které můžeme polemizovat o NFT jakožto o věci samostatné nebo jako o součásti věci hlavní, tedy podkladového aktiva. Široká veřejnost často NFT vnímá jako jakýsi certifikát, který bez dalšího zastupuje podkladové aktivum. Bez zásahu zákonodárce však nelze takovéto zastoupení považovat automaticky za právně závazné. Můžeme se v případě NFT obejít bez legislativního zásahu, pokud se domníváme, že NFT jako takové představuje podkladové aktivum?

Nejdříve si přiblížíme situaci, kdy jsou NFT přímo vázány na podkladové aktivum a v případě oddělení od něj by došlo ke snížení jejich hodnoty. Příkladem je NFT politika automobilky Alfa Romeo. Od roku 2022 je každý vůz modelu Tonale doprovázen NFT certifikátem, který je jedinečný pro každý automobil, je přímo propojen s konkrétním vozem, certifikuje zakoupení vozu a následně dokumentuje veškerý servis a údržbu vozidla a další doprovodné informace o konkrétním vozidle.[42] V tomto případě je

[42] NFT [online]. In: *alfaromeo.cz* [cit. 17. 1. 2023]. Dostupné z: https://www.alfaromeo.cz/modely/tonale#modal-gallery-software-popup

NFT pouhým certifikátem, nemá vlastní hodnotu a je přímo závislé na podkladovém aktivu, tedy konkrétním automobilu Alfa Romeo Tonale. Nelze předpokládat, že by NFT, který slouží pouze jako certifikační potvrzení podkladového aktiva, měl sám o sobě hodnotu, a tedy byl věcí odlišnou od podkladového aktiva. Na takovýto NFT bychom mohli vztáhnout doktrinální definici součásti věci dle ustanovení § 505 OZ. Součást věci je vše, co k ní podle její povahy náleží a nemůže být od věci odděleno, aniž by tím došlo k znehodnocení věci. Koukal k ustanovení § 505 OZ zmiňuje, že o součásti věci můžeme hovořit i v případě složených věcí. To jsou věci tvořené součástmi, které mohou mít relativně samostatnou povahu a lze je od věci hlavní oddělit.[43] Při oddělení součásti musí dojít ke znehodnocení hlavní věci. Oddělit NFT od podkladového aktiva v případě výše zmíněné funkcionality certifikačního potvrzení servisní historie vozidla je bezpochyby možné. Oddělení NFT by bylo oddělením samostatné součásti věci, kdy by sice hlavní věc, automobil, na své primární funkčnosti neztratil, ale jeho hodnota by se tím bezpochyby snížila. Tato ponížená hodnota by byla způsobena kupříkladu díky nejasné servisní historii, způsobené oddělením NFT od vozidla. Z těchto důvodů lze hovořit za splnění určitých podmínek a provázanosti NFT s podkladovým aktivem o NFT jakožto o součásti věci.

Druhou kategorií jsou NFT sloužící jako nezávislá reprezentace podkladového aktiva, kdy NFT a podkladové aktivum nejsou nijak propojeny, tedy hodnota podkladového aktiva není přímo navázána na hodnotu NFT. V tomto případě je nutné připustit, že NFT je obchodován nezávisle a představuje svou vlastní hodnotu, přímo nezávislou na hodnotě podkladového aktiva a je tedy věcí samostatnou, nikterak vázanou na podkladové aktivum. Příkladem bychom mohli zmínit aukci NFT memorabilií, vytvořených Julianem Lennonem, synem legendárního hudebníka kapely The Beatles.[44] Virtualizování předmětů (například Lennonův kabát z písně Help! nebo kytara značky Gibson) a následné vytvoření NFT, ke kterým fyzické předměty sloužily jako podkladové aktivum, nevytvořilo automaticky za-

[43] KOUKAL, Pavel. § 505 Základní vymezení součásti věci. In: LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1 – 654)*. Praha: C. H. Beck, 2014, s. 1559.

[44] LENNON CONNECTION: THE NFT COLLECTION [online]. [cit. 17. 1. 2023]. Dostupné z: https://www.juliensauctions.com/about-auction?id=400

stoupení fyzických předmětů pomocí NFT. NFT sloužily pouze jako reprezentace fyzických podkladových aktiv, jejich hodnota se však přímo neodvíjela od hodnoty fyzických podkladových aktiv, které zůstaly ve vlastnictví Juliana Lennona. Může tedy existovat podkladové aktivum a NFT, který jej pouze reprezentuje, a jeho hodnota bude čistě spekulativní, odvíjející se od faktu, že předlohou NFT byl skutečný originál podkladového aktiva nebo tvůrce byl například známým umělcem. Takovýto NFT bude existovat nezávisle na podkladovém aktivu. Pokud hovoříme o věcech s různou hodnotou, lze zároveň hovořit o dvou rozdílných věcech.

Z výše uvedeného lze identifikovat dva způsoby napojení NFT na podkladové aktivum. Prvním z nich je situace, kdy je NFT certifikačním nástrojem smluvně propojeným a přímo odkazujícím na podkladové aktivum, v tomto případě lze mluvit o propojení NFT s podkladovým aktivem jakožto složené věci, NFT by byl tedy ve vztahu k podkladovému aktivu součástí věci. Druhým způsobem je existence dvou odlišných věcí – NFT jakožto samostatné věci a podkladového aktiva.

3.4 VLASTNICKÁ PRÁVA K NFT

Na základě výše zmíněného je třeba rozlišovat dvě hypotézy z hlediska odlišitelnosti NFT od podkladového aktiva. První z nich nastává, kdy NFT inkorporuje podkladové aktivum, tj. NFT není nic jiného než součástí podkladového aktiva, a pak lze připustit, že NFT nemá jinou než evidenční právní existenci, nepředstavuje aktivum odlišné od podkladového aktiva, pouze osvědčuje převod práv a případně existenci práv k podkladovému aktivu. V tomto hypotetickém případě však bude pro *zastoupení* podkladového aktiva v užším slova smyslu (nad rámec pouhého evidenčního aspektu) nutné, aby zákonodárce zasáhl a takové zastoupení právně zakotvil nebo aby toto propojení NFT s podkladovým aktivem bylo smluvně ujednáno. Druhá hypotéza předpokládá, že NFT má odlišnou vnitřní hodnotu, která může být čistě spekulativní. NFT a podkladové aktivum je pak třeba odlišit a přistupovat k nim jako k rozdílným věcem. V tomto případě, pokud existují dvě různé nezávislé věci, nutně vyvstává otázka vztahu mezi nimi.

3.4.1 VLASTNICKÁ PRÁVA K NFT VYTVOŘENÉMU NA ZÁKLADĚ FYZICKÉHO PODKLADOVÉHO AKTIVA

Fyzické podkladové aktivum může být formou digitalizace přeneseno do virtuálního prostředí, kde může sloužit jako podkladové aktivum pro vytvoření NFT.

Obecně lze říci, že NFT nezakládá žádná přímá vlastnická práva k podkladovému aktivu, protože neexistuje žádná přímá právní vazba mezi NFT a podkladovým aktivem. Subjekt, jenž zakoupí NFT, touto transakcí získává vlastnická práva pouze ke konkrétnímu tokenu, obsahujícímu metadata odkazující na podkladové aktivum. Pokud mluvíme o vlastnictví NFT, nelze na něj bez dalšího současně pohlížet jako na vlastnictví fyzického podkladového aktiva, nýbrž na vlastnictví věci, vytvořené na základě podkladového aktiva takovým způsobem, že vzniknou dvě nezávislé věci – první z nich je fyzické podkladové aktivum, druhou z nich je NFT, jistým způsobem odkazující na podkladové aktivum bez přímého vztahu k vlastnickým právům pojícím se k podkladovému aktivu.

V konkrétních případech však může mít NFT přímý, smluvně zakotvený vztah k vlastnickým právům vztahujícím se k podkladovému aktivu, jelikož je součástí podkladového aktiva jako součást věci. Výše již byl zmíněn příklad automobilky Alfa Romeo, která vydává certifikační NFT potvrzující koupi vozu a jeho servisní a další doprovodnou dokumentaci. Dalším příkladem takového certifikačního NFT s přímým vztahem k vlastnickým právům k podkladovému aktivu je NFT vytvořené česko-americkým výrobcem zbraní Colt CZ Group.[45] K limitované edici pistolí CZ 75 Řád Bílého lva byl vlastníkům zbraní přidělen tzv. Certificate of Authenticity and Ownership ve formě NFT. Při převodu vlastnických práv k pistoli je tento certifikát aktualizován tak, aby zohledňoval nového vlastníka pistole. Colt tímto tahem přímo propojil vlastnická práva k pistoli CZ 75 Řád Bílého lva

[45] Colt CZ Group jako první výrobce ručních palných zbraní vstupuje do světa blockchainové technologie [online]. In: *Colt CZ Group*. 16. 12. 2022. [cit. 17. 1. 2023]. Dostupné z: https://www.coltczgroup.com/media-tiskove-zpravy/colt-cz-group-jako-prvni-vyrobce-rucnich-palnych-zbrani-vstupuje-do-sveta-blockchainove-technologie

a NFT, jakožto certifikátu odkazujícímu na pravost pistole.[46] Je na smluvních stranách, prodejci a kupujícím, aby skutečnost převodu vlastnictví oznámili platformě Colt, která převede NFT novému vlastníkovi zbraně, propojení NFT a podkladového aktiva je tedy na bázi oznámení a není automatické. Jedná se o deklaratorní zápis, který demonstruje aktuální právní stav vlastnictví podkladového aktiva, pistole Colt. Je v zájmu kupujícího, aby trval na aktualizaci platformy a převedení NFT na jeho osobu, jakožto nového vlastníka, jelikož NFT ve formě certifikátu potvrzuje autenticitu zbraně a jeho vlastnictví tak přímo odkazuje na vlastnictví podkladového fyzického aktiva.

Můžeme si představit i situaci, kdy by NFT nebylo převedeno na základě prodeje fyzického podkladového aktiva, nýbrž by fyzické podkladové aktivum bylo převedeno na základě prodeje NFT. Vzhledem ke skutečnosti, že právní praxe v této věci odpověď neposkytuje, lze dovodit, že převodem NFT by došlo k převodu vlastnictví podkladového fyzického aktiva na nového vlastníka pouze v případě, pokud by toto bylo mezi stranami smluvně ujednáno. Ve světě již existují případy, kdy došlo k digitalizaci prodeje nemovitostí prostřednictvím převodu vlastnických práv k nemovitosti konkretizovaných v NFT.[47]

3.4.2 VLASTNICKÁ PRÁVA K NFT VYTVOŘENÉMU NA ZÁKLADĚ VIRTUÁLNÍHO PODKLADOVÉHO AKTIVA

Vlastnická práva k virtuálním statkům obecně jsou nelehce uchopitelným právním konstruktem, a to především z důvodu neexistence jasného a společného definičního rámce pojmů používaných v různých jurisdikcích k popisu souvisejících jevů, počínaje základním a všudypřítomným pojmem virtuální aktivum. Virtuální aktiva svým formátem vytvářejí roztříštěnější typ vlastnictví, který se liší od vlastnictví fyzických aktiv.

---

[46] Prodejní podmínky aukcí NFT [online]. In: *Colt CZ Group*. [cit. 18. 1. 2023]. Dostupné z: https://auctionportal.coltczgroup.onblocktrust.com/Home/TnC/auction

[47] K tomu blíže: MORINGIELLO, Juliet M., Christopher K. ODINET. Blockchain Real Estate and NFTs. In: *William & Mary Law Review, Forthcoming, U Iowa Legal Studies Research Paper*. 2022.; The World's First Real Estate NFT [online]. In: *Propy*. [cit. 20. 1. 2023]. Dostupné z: https://propy.com/browse/propy-nft/

Odom, Zimmerman a Forlizzi uvádějí, že virtuálními aktivy mohou být hmotná aktiva, která se stala nehmotnými (například knihy, hudba, fotografie a vstupenky); věci, které nikdy neměly trvalou hmotnou podobu (například archivy elektronických zpráv, profily na sociálních sítích, herní avatary a odznaky na sociálních sítích); a také metadata ze záznamů digitálních zařízení a služeb, které zachycují činnost lidí (například informace o poloze fotografií, historie přehrávání hudby a historie nákupů kreditními kartami).[48] Dále uvádějí tři vlastnosti digitálních virtuálních statků, a to, že nejsou závislé na fyzickém umístění, fyzickém prostoru a fyzické podobě. Na rozdíl od fyzických aktiv nejsou virtuální aktiva omezena na jedno fyzické místo, a proto mohou být dostupná na více místech současně. To vytváří flexibilitu, rozšířenou interakci a dostupnost virtuálních aktiv.[49] Pro vlastníka tak může být obtížné zjistit, kde se virtuální aktivum nachází, což může vést k dočasné nebo dokonce trvalé ztrátě přístupu k virtuálnímu aktivu.[50] Virtuální aktiva na rozdíl od těch fyzických nezabírají fyzický prostor. V této souvislosti mohou být virtuální aktiva vnímána jako neviditelná, a proto je obtížné pochopit jejich velikost, rozsah a v některých případech také to, co obsahují. Z důvodu, že virtuální aktivum není omezeno na fyzickou podobu, může být snadněji kopírováno a napodobováno, s čímž se pojí obtížnější rozlišení originálu od kopie.[51]

Jedním z hlavních záměrů technologie NFT ve vztahu k virtuálním podkladovým aktivům je právě vytvoření jedinečnosti nebo vzácnosti ve vztahu k virtuálnímu aktivu. Vytvořením NFT a registrací virtuálního aktiva, nejčastěji virtuálního uměleckého díla, pod jedinečným hashem[52] se NFT považuje za limitovanou edici s certifikátem pravosti, jejíž podpis je ekvivalentní autogramu umělce. Tato funkce odlišení, certifikace pravosti,

[48] ODOM, William, John ZIMMERMAN a John FORLIZZI. Placelessness, spacelessness, and formlessness: experiential qualities of virtual possessions. In: *Proceedings of the 2014 conference on Designing interactive systems*. 2014, s. 985.

[49] ODOM, ZIMMERMAN, FORLIZZI, ref. 48, s. 987.

[50] ODOM, ZIMMERMAN, FORLIZZI, ref. 48, s. 989.

[51] ODOM, ZIMMERMAN, FORLIZZI, ref. 48, s. 990.

[52] Hashem se rozumí alfanumerická hodnota určená ze souboru dat spojující NFT s jeho metadaty.

má za následek hodnotu NFT, protože nehmotný majetek je jedinečný do té míry, že jeho vlastnosti jsou nenahraditelné a nelze mít za to, že existuje ekvivalent s podobnými vlastnostmi. Je však pravda, že určitá virtuální aktiva mohou být i nadále kopírována, šířena a sdělována veřejnosti do té míry, že pomyslně ztrácejí na své jedinečnosti nebo vzácnosti. Není nic, co by zabránilo minterovi NFT vytvořit další NFT s totožným podkladovým aktivem, a to jak v rámci stejného nativního blockchainu nebo blockchainu odlišného. Neexistuje žádný centrální repozitář, který by tomuto zabránil a konstitutivně určil, že konkrétní podkladové aktivum již bylo použito k vytvoření NFT či nikoliv.

NFT můžeme označit za specifický token, jedinečný díky unikátnímu TokenID a adrese chytrého kontraktu, ukazující na ono konkrétní virtuální podkladové aktivum. V tomto ohledu lze NFT přirovnat k nosičům, jako je CD s hudební skladbou nebo DVD s filmovým dílem. Právo držby a vlastnictví NFT s sebou však obdobně jako je to u nosičů digitálních děl nepřináší vlastnické právo k virtuálnímu podkladovému aktivu, ale pouze vlastnictví jedinečného kódu, který digitální podkladové aktivum označuje.

Příkladem NFT, které vzniklo na základě virtuálního podkladového díla, je digitální obraz Replicator od kanadského umělce Mad Dog Jonese,[53] který se na platformě Nifty Gateway v roce 2021 prodal za tehdejších 4,1 milionu amerických dolarů.[54] Kupující získal vlastnické právo k NFT, které se však samo o sobě nepojí s žádnými právy k virtuálnímu podkladovému aktivu.

Pokud je minter NFT zároveň vlastníkem autorských práv k podkladovému dílu, může udělit nabyvateli NFT licenci k užití podkladového autorského díla, kdy NFT bude sloužit jako reprezentace této udělené licence. Jedná se však pouze o deklaratorní zastoupení, kdy se licence automaticky nepojí s NFT, ale může být v průběhu času nezávisle na něm ukončena.

---

[53] REPLICATOR [online]. In: *maddogjones.com*. [cit. 20. 1. 2023] https://www.maddogjones.com/prints/1

[54] MDJ x Phillips: A Multi-Generational NFT [online]. In: *Phillips*. [cit. 20. 1. 2023] https://www.phillips.com/detail/mad-dog-jones/NY090121/1

NFT, které se pojí s licencí k podkladovému aktivu je například edice CryptoKitties (sbírka pixel art koťat od vývojářského studia AxiomZen), kdy licence umožňuje vlastníkovi NFT komercializovat koťata (podkladová autorská díla) za předpokladu, že taková komercializace nepřinese příjem vyšší než 100 tisíc USD ročně.[55] Zakoupením NFT si tak subjekt kupuje certifikát tokenu, který může, ale nemusí být spojen s licencí poskytující majetková autorská práva vztahující se k virtuálnímu podkladovému aktivu.

U NFT vytvořených na základě virtuálního podkladového aktiva tedy bez dalšího lze mluvit pouze o vlastnictví NFT jako takového, nikoliv zároveň současně o vlastnictví podkladového virtuálního aktiva; to totiž bude často autorským dílem požívajícím autorskoprávní ochrany podle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, ať už půjde o fotografie, hudbu, video, které jsou autorskými díly, tak herní předměty, které jsou v rámci nativního softwaru hry považovány také za derivát autorskoprávní ochrany.

Můžeme však mluvit o větší provázanosti s podkladovým virtuálním aktivem v případech, pokud jsou nabyvateli NFT současně s NFT poskytnuta k užití práva vycházející z duševního vlastnictví autora podkladového aktiva.

4. OCHRANA SPOTŘEBITELE PŘI TRANSAKCÍCH S NFT

Od představení technologie NFT široké veřejnosti se tyto tokeny staly předmětem prodeje, nákupu a distribuce. Z výše uvedeného vyplývá, že NFT je věcí nehmotnou, movitou, nezastupitelnou, je určitým virtuálním statkem či virtuální službou. Je tedy na místě blíže rozebrat existenci spotřebitelského vztahu a ochrany spotřebitele při transakcích s NFT.

Z ustanovení § 1812 odst. 1 OZ vyplývá pro spotřebitelské smlouvy výklad jejich ustanovení ve prospěch spotřebitele. To potvrdil mimo jiné Nejvyšší soud ČR v rozsudku sp. zn. 33 Cdo 5240/2016 ze dne 26. 9. 2017, ve kterém judikoval obecné použití pravidla nejpříznivějšího výkladu pro spo-

[55] CryptoKitties Terms of Use [online]. In: *CryptoKitties*. 15. 11. 2018. [cit. 22. 1. 2023] https://www.cryptokitties.co/terms-of-use

třebitele obecně na veškeré právní úkony, dvoustranné i jednostranné. Zároveň v § 1812 odst. 2 OZ zákonodárce stanovuje, že k ujednáním odchylujícím se od ustanovení zákona stanovených k ochraně spotřebitele se nepřihlíží, a to i v případech, kdy se spotřebitel vzdá zvláštního práva, které mu zákon poskytuje. I přes kogentní povahu ustanovení o ochraně spotřebitele však může být problematické vymáhání spotřebitelských práv v případě sporu, jelikož většina transakcí s NFT zahrnuje určitý mezinárodní prvek.

Velká část z NFT platforem, společností vydávajících NFT a NFT on-line tržišť má sídlo ve Spojených státech amerických a obecně navrhují, aby se na uzavřené smlouvy použilo americké rozhodné právo. Ochranu spotřebitele je však třeba hledat nejen podle práva uvedeného ve smlouvě, ale také podle práva, které je použitelné v daném okamžiku s ohledem na stát, v němž má spotřebitel bydliště. V tomto posledním ohledu je užitečné připomenout, že není vždy snadné rozhodné právo určit, například při neexistenci mezinárodních dohod mezi státy, které by upravovaly smluvní závazkové vztahy.

Pro evropské spotřebitele může být východiskem Nařízení Evropského parlamentu a Rady (ES) č. 593/2008 ze dne 17. června 2008 o právu rozhodném pro smluvní závazkové vztahy, zvané též „*Řím I*“. Jedná se o nařízení Evropského společenství o mezinárodním právu soukromém, které upravuje určení rozhodného práva pro závazkové vztahy, jejichž subjekty mají obvyklé bydliště v některém ze členských států. Jednou ze zásad nařízení Řím I je zásada absolutní svobody volby rozhodného práva pro smluvní závazkové vztahy mezi smluvními stranami vyplývající z čl. 3. V případě, že je smluvní stranou spotřebitel, existují určitá omezení, kdy volba rozhodného práva stranami nesmí mít za následek zbavení spotřebitele ochrany, kterou mu zaručují kogentní ustanovení práva země, v níž má obvyklé bydliště dle čl. 6 odst. 2.

Působnost tohoto nařízení nelze snadno rozšířit na subjekty se sídlem ve státech mimo Evropskou unii, a to právě z důvodu neexistence mezinárodních úmluv upravujících rozhodné právo pro závazkové vztahy s mezinárodním prvkem. Lze však říci, že toto nařízení v každém případě zahrnuje potřebu ochrany spotřebitele, jakožto slabší strany smlouvy, o kte-

rou by měly usilovat všechny subjekty (z Evropské unie i mimo ni), které jednají se spotřebiteli na evropském trhu.

Na unijní úrovni je ochrana spotřebitele upravena směrnicí Evropského parlamentu a Rady 2011/83/EU o právech spotřebitelů, kterou se mění směrnice Rady 93/13/EHS a směrnice Evropského parlamentu a Rady 1999/44/ES a zrušuje směrnice Rady 85/577/EHS a směrnice Evropského parlamentu a Rady 97/7/ES. Ta byla do českého právního řádu uvedena zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, a zákonem č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů (dále jen „ZOS“).

Tato směrnice, aktualizovaná směrnicí Evropského parlamentu a Rady 2019/2161, představuje režim použitelný na širokou škálu smluv uzavíraných mezi podnikateli a spotřebiteli, zejména na kupní smlouvy, smlouvy o poskytování služeb nebo smlouvy o poskytování digitálního obsahu. Vztahuje se jak na smlouvy uzavírané v rámci obchodních prostor, tak na smlouvy uzavírané mimo obchodní prostory nebo distančně.

Novelizace provedená směrnicí (EU) 2019/2161 rozšířila oblast působnosti na smlouvy, na jejichž základě podnikatel poskytuje nebo se zavazuje poskytovat spotřebiteli digitální služby nebo digitální obsah a spotřebitel poskytuje nebo se zavazuje poskytnout podnikateli své osobní údaje. Nařízení mimo jiné stanovuje informační povinnost podnikatele vůči spotřebiteli před uzavřením smlouvy. Níže bude rozebrán spotřebitelský vztah v rámci smlouvy o koupi NFT, aspekty ochrany spotřebitele v jejím rámci a jednotlivé informační povinnosti podnikatele s tím spojené. Nakonec budou rozebrány standardy digitálního obsahu stanovené Směrnicí Evropského parlamentu a Rady č. 2019/770, o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb ve vztahu k NFT.

4.1 DEFINICE SPOTŘEBITELSKÉHO VZTAHU PŘI KOUPI NFT

Dle ustanovení § 419 OZ je spotřebitelem každý člověk, který mimo rámec své podnikatelské činnosti nebo mimo rámec samostatného výkonu svého povolání uzavírá smlouvu s podnikatelem nebo s ním jinak jedná. Podnikatelem poté občanský zákoník rozumí v ustanovení § 420 OZ osobu,

která samostatně vykonává na vlastní účet a odpovědnost výdělečnou činnost živnostenským nebo obdobným způsobem se záměrem činit tak soustavně za účelem dosažení zisku. Pro účely ochrany spotřebitele se za podnikatele považuje také každá osoba, která uzavírá smlouvy související s vlastní obchodní, výrobní nebo obdobnou činností či při samostatném výkonu svého povolání, popřípadě osoba, která jedná jménem nebo na účet podnikatele.

Spotřebitelskými vztahy rozumíme společenské vztahy, vyplývající z uzavírání spotřebitelských smluv dle ustanovení § 1810 OZ, tedy smluv, které uzavírá podnikatel v postavení silnější smluvní strany se spotřebitelem v postavení smluvní strany slabší. Spotřebitelské vztahy tak můžeme definovat pomocí subjektivního prvku, kterým je existence subjektu spotřebitele a subjektu podnikatele.

Výše zmíněné právní konstrukty aplikujeme na koupi NFT a přiblížíme si požadavky, abychom mohli konkrétní právní vztah považovat za uzavření spotřebitelské smlouvy.

Za spotřebitele při nákupu NFT lze považovat subjekt, který splňuje následující požadavky:

- Je fyzickou osobou;
- Zakoupí NFT od subjektu v pozici podnikatele;
- Koupí NFT realizuje svůj osobní, vlastní zájem nebo potřebu, mimo rámec své podnikatelské činnosti nebo mimo rámec samostatného výkonu svého povolání.

S ohledem na identifikaci spotřebitele je důležité rozvinout hlavně třetí požadavek, který není z hlediska koupě NFT vždy jednoznačný.

Pro odpověď na otázku, zda fyzická osoba uzavírající smlouvu je v postavení spotřebitele, je rozhodující především účel jednání takové osoby.[56]

Mezi účely, které lze považovat za účely souladné postavení spotřebitele, lze uvést:[57]

[56] VONDRÁČEK, Ondřej. § 419 Definice spotřebitele. In: PETROV, Jan. a kol. Občanský zákoník. 2. vydání (1. aktualizace). Praha: C. H. Beck, 2022.

[57] Jedná se o demonstrativní výčet vytvořený autorem článku.

- Zakoupení NFT za účelem použití jako profilového obrázku/banneru na sociálních sítích;
- Zakoupení NFT jakožto daru, který spotřebitel má v úmyslu darovat;
- Zakoupení NFT pro použití v kreativních projektech;
- Zakoupení NFT jakožto investice, kdy spotřebitel nejedná v rámci své podnikatelské činnosti nebo v rámci samostatného výkonu svého povolání;
- Zakoupení NFT za účelem dosažení určitého společenského postavení;
- Zakoupení NFT za účelem přístupu k uzavřené komunitě držitelů konkrétního druhu NFT;
- Zakoupení NFT, se kterým se pojí vstupenka na soukromou událost.

Výše uvedené příklady autor uvádí jako demonstrativní výčet situací, kdy by byl kupující subjekt v postavení spotřebitele.

Pro bližší vysvětlení spotřebitelského vztahu souvisejícího s transakčním úkonem zakoupení NFT lze uvést následující modelový případ:

1. Fyzická osoba, občan České republiky, zakoupí NFT za účely:
   - použití jakožto profilového obrázku na svých profilech sociálních sítí;
   - trvalého přístupu na soukromé události pojící se se zakoupením NFT;
   - následně jej má v úmyslu darovat svému příbuznému.
2. NFT zakoupí na NFT on-line tržišti s názvem CzechNFT, provozovaném poskytovatelem on-line tržiště se sídlem v České republice.
3. Prodejcem NFT je NFTalent s.r.o., společnost se sídlem v České republice, která pořádá soukromé události, na které je vstupenkou potvrzení držby jejich NFT s názvem NFTicket.
4. Nativním blockhchainem tohoto NFT je Ethereum a jeho kupní cena činí 0,5 ETH, v době nákupu činící přibližně 60.000,- Kč.

Subjekty zapojenými do výše zmíněného modelového příkladu jsou:

1. Prodejce NFT je právnickou osobou, která naplňuje znaky podnikatele dle ustanovení § 420 OZ.
2. Poskytovatel NFT on-line tržiště je poskytovatelem on-line tržiště dle ustanovení § 2 odst. 2 písm. b) ZOS, kdy poskytuje přístup k nabídkám na prodej a nákup NFT, prodejci mohou prodávat svá NFT na tomto tržišti, kdy poskytovatel tržiště má z prodeje jistou výši provize. Dle ustanovení §2 odst. 2 písm. c) tohoto zákona je podnikatelem.
3. Kupující NFT je fyzickou osobou, která prostřednictvím on-line tržiště projevila zájem o koupi NFT, který kupuje pro své osobní účely, mimo rámec své podnikatelské činnosti a mimo rámec samostatného výkonu svého povolání. V případě uzavření smlouvy o koupi NFT tedy bude v postavení spotřebitele dle ustanovení § 419 OZ.

4.2 ASPEKTY OCHRANY SPOTŘEBITELE PŘI TRANSAKCÍCH S NFT

V rámci zkoumání transakcí s NFT ve spotřebitelských vztazích je na místě zohlednit několik aspektů a zodpovědět určité otázky, které vznikají s ohledem na charakteristické rysy technologie NFT a představují nové problémy ve srovnání s tradičním pojetím spotřebitelských smluv.

4.2.1 IDENTIFIKACE KUPUJÍCÍHO SPOTŘEBITELE

Základním aspektem, určujícím uplatnění ochrany spotřebitele na konkrétní právní vztah, je určení, zda kupujícím subjektem je osoba v postavení spotřebitele, či nikoliv. Vzhledem k anonymitě, která je charakteristická pro blockchainové transakce, nemá prodávající často žádné informace o kupující smluvní straně, nemůže si být jistý, zda kupující činí transakci pro své osobní účely, či naopak koná v rámci své podnikatelské činnosti nebo v rámci samostatného výkonu svého povolání. Určení kupujícího subjektu, jakožto spotřebitele, lze usuzovat například z povahy okolností, za kterých transakci uskutečňuje. Soudní dvůr Evropské Unie (dále jen „SDEU“) ve věci C-105/17 – Kamenova judikoval, že fyzickou osobu, která na on-line tržišti zveřejní současně určitý počet inzerátů, v nichž nabízí k prodeji

zboží, lze považovat za obchodníka a jednání této osoby lze považovat za obchodní činnost, podnikání, řemeslo nebo svobodné povolání. Každý případ je však nutné individuálně posoudit a jasné mantinely pro určení, zda osoba jedná v postavení podnikatele neexistují.

Jedním z možných řešení tohoto problému je tzv. pravidlo KYC (know your customer – česky „*poznej svého zákazníka*“).[58] Poskytovatel NFT on-line tržiště díky němu může vyžadovat od subjektů obchodujících na tržišti základní identifikační údaje za účelem zajištění bezpečného, důvěryhodného a transparentního prostředí a zároveň může zjistit, který subjekt je spotřebitelem a který naopak obchoduje s NFT v rámci své podnikatelské činnosti. Povinnost KYC zavádí článek 30 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, dle kterého je poskytovatel on-line platformy umožňující distanční uzavírání smluv povinen identifikovat subjekt nabízející výrobky nebo služby tak, aby spotřebitel byl před uzavřením smlouvy nebo před tím, než učiní závaznou nabídku, informován, zda je nabízející NFT podnikatelem, či nikoliv. Identifikace kupujícího subjektu však vyžadována není, proto nemusí být jasné, zda kupující subjekt NFT zakoupil pro svůj osobní, vlastní zájem nebo potřebu, mimo rámec své podnikatelské činnosti nebo mimo rámec samostatného výkonu svého povolání či byla koupí NFT realizována podnikatelská činnost za účelem opětného prodeje a realizace zisku.

4.2.2 INFORMAČNÍ POVINNOST PODNIKATELE PRODÁVAJÍCÍHO NFT VŮČI SPOTŘEBITELI

Podstatné informace, které musí podnikatel spotřebiteli poskytnout před uzavřením smlouvy (předsmluvní informace), jsou uvedené v ustanovení § 1811 OZ. Vondráček v komentáři k tomuto ustanovení uvádí, že jeho smyslem je umožnit spotřebiteli určit, kdo je jeho protistranou, do jakých práv a povinností v případě uzavření smlouvy vstupuje a jaké mohou být důsledky uzavřených závazků. S odkazem na rozsudek SDEU ve věci

[58] K autentifikaci pomocí KYC například BAMAKAN, Seyed Mojtaba Hosseini, Nasim NEZHADSISTANI, Omid BODAGHI a Qiang Qu. Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. In: *Scientific Reports*. 2022, roč. 12.

C-472/10, Invitel, uvádí, že spotřebiteli musí být umožněno, aby předem mohl prověřit všechna smluvní ujednání a jejich důsledky, čímž dochází k vyvarování se nejasností a pochybností při výkladu spotřebitelských smluv.[59]

Vzhledem k distančnímu způsobu uzavírání smluv o koupi NFT se však v konkrétnostech použije ustanovení § 1820 OZ, které vymezuje blíže informační povinnost dle ustanovení § 1811 OZ. V případě distančních smluv je smyslem přiznání zvláštní ochrany spotřebiteli omezená možnost získat od podnikatele potřebné informace nutné k tomu, aby se spotřebitel mohl rozhodnout, zda smlouvu uzavře, či nikoliv.[60]

Níže si představíme informační povinnost podnikatele vůči spotřebiteli před uzavřením smlouvy o koupi NFT. Obecně rozebereme relevantní ustanovení, která na podnikatele v případě prodeje NFT dopadají. Toto vymezení může sloužit jako obecná příručka pro splnění informační povinnosti podnikatele vůči spotřebiteli před uzavřením smlouvy o koupi NFT.

Dle ustanovení § 1820 odst. 1 písm. a) OZ musí být spotřebitel před uzavřením smlouvy informován o hlavních vlastnostech zboží nebo služby v rozsahu odpovídajícím použitelnému prostředku komunikace na dálku a povaze zboží nebo služby. Zboží nebo služba musí být vymezena takovým způsobem, aby byl následný předmět plnění dostatečně určitelný a nemohlo dojít k jeho záměně či omylu ze strany spotřebitele. Označení a popis závisí na složitosti poskytovaného zboží či služby tak, aby vymezení bylo průměrnému spotřebiteli srozumitelné.[61] Je tedy nutné poskytnout informace v dostatečném obsahu tak, aby byl průměrný spotřebitel schopný pochopit hlavní znaky a technické vlastnosti prodávaného NFT, kterými jsou kupříkladu:

- Jaký je nativní blockchain NFT?
- Jaká je adresa chytrého kontraktu NFT?

[59] VONDRÁČEK, Ondřej. § 1811 Předsmluvní informace. In: PETROV, Jan. a kol. Občanský zákoník. 2. vydání (1. aktualizace). Praha: C. H. Beck, 2022.

[60] VONDRÁČEK, Ondřej. § 1820 Sdělení před uzavřením smlouvy. In: PETROV, Jan. a kol. Občanský zákoník. 2. vydání (1. aktualizace). Praha: C. H. Beck, 2022.

[61] VONDRÁČEK, ref. 60.

- Kde a jakým způsobem jsou uložena podkladová aktiva?
- Existují licenční poplatky,[62] pokud ano, v jaké výši?
- Kolik obdobných NFT nebo NFT v dané sérii je v oběhu?

V případě, že je k držbě konkrétního NFT vázáno právo na poskytnutí služeb, je nutné konkretizovat i právě toto poskytování služeb, jeho rozsah, časové vymezení a další informace související s poskytovanými službami.

K vlastnostem NFT často patří i specifikace licenčních podmínek, vztahujících se k podkladovému aktivu jakožto uměleckému dílu, a rozsahu udělených majetkových autorských práv. Většina NFT je vytvořena na základě podkladového aktiva, které je autorským dílem. Prodejce tak musí spotřebitele informovat i o rozsahu udělené licence k právům duševního vlastnictví, kupříkladu:

- V jakém rozsahu je udělena licence k užívání autorského díla?
- Jakým způsobem může držitel NFT umělecké dílo, sloužící jako podkladové aktivum, užívat, na jakou dobu?

Dle ustanovení § 1820 odst. 1 písm. b), c), d) OZ musí před uzavřením smlouvy o koupi NFT podnikatel uvést svoji totožnost nebo totožnost osoby, která jedná jeho jménem nebo na jeho účet a adresu sídla, případně adresu provozovny, pokud se liší od adresy sídla, a v případě, že podnikatel jedná za jiného podnikatele, také adresu, na kterou může spotřebitel zaslat stížnost. Zároveň je nutné uvedení telefonního čísla a také adresy pro doručování elektronické pošty, případně i údaje o jiném prostředku on-line komunikace. Informační povinnost vůči spotřebiteli nebude naplněna, pokud prodávající sdělí pouze svou blockchainovou adresu, což je praxe, kterou někteří prodávající NFT praktikují a spotřebiteli další identifikační údaje neposkytují.

Dle ustanovení § 1820 odst. 1 písm. e) OZ musí před uzavřením smlouvy o koupi NFT podnikatel spotřebitele informovat o celkové ceně NFT. Bude se jednat o cenu tzv. mintování NFT určenou v chytrém kontraktu. Tato cena bude nejčastěji vyjádřena v kryptoměně a bude nutné upřesnění, zda, a v jaké výši zahrnuje transakční poplatky, tzv. gas fees, nutné

[62] Licenčními poplatky rozumíme podíl z výnosů opětného prodeje NFT. Jejich výše je stanovena minterem NFT v rámci chytrého kontraktu.

k provedení transakce, tyto poplatky bychom mohli analogicky charakterizovat jako náklady na dodání NFT do digitální kryptopeněženky kupujícího. Z důvodu větší transparentnosti je vhodné zavést přepočet kupní ceny uvedené v kryptoměně na kurz odpovídající kurzu aktuální uznávané měny, tedy kupříkladu přepočet na aktuální kurz české koruny.[63] Dále musí podnikatel dle ustanovení § 1820 odst. 1 písm. f) OZ uvést údaj o přizpůsobení ceny osobě spotřebitele na základě automatizovaného rozhodování, byla-li cena takto přizpůsobena.

Dle ustanovení § 1820 odst. 1 písm. g) OZ musí podnikatel uvést náklady na prostředky komunikace na dálku, které nese spotřebitel, pokud se liší od základní sazby. V naprosté většině případů však budou náklady spotřebitele na použití komunikačních prostředků ve výši základní sazby, kupříkladu ve výši nákladů za přístup k internetu.

Dle ustanovení § 1820 odst. 1 písm. h) OZ je prodávající povinen přesně popsat platební podmínky, čas dodání a plnění v případě zakoupení NFT. Je nutné popsat jednotlivé kroky, které musí spotřebitel následovat, aby došlo k transakci NFT a k jeho připsání do digitální kryptopeněženky kupujícího. Prodávající musí taktéž sdělit spotřebiteli jeho právo podat stížnost a kontaktní místo, skrze které se spotřebitel může na podnikatele obrátit.

Dle ustanovení § 1820 odst. 1 písm. i) OZ musí podnikatel spotřebitele informovat o podmínkách, lhůtě a postupu pro uplatnění práva na odstoupení od smlouvy, jakož i vzorový formulář pro toto odstoupení. O neexistenci práva spotřebitele na odstoupení nebo o podmínkách, za jakých právo na odstoupení od smlouvy zanikne, musí podnikatel spotřebitele informovat dle ustanovení § 1820 odst. 1 písm. l) OZ. Vzhledem ke specifičnosti technologie blockchain ve vztahu k odstoupení od smlouvy, jejímž předmětem je NFT, bude toto rozebráno blíže v kapitole 4.2.3 .

Dle ustanovení § 1820 odst. 1 písm. m) OZ musí podnikatel informovat o existenci práv z vadného plnění, jakož i o právech ze záruky a dalších podmínkách pro uplatňování těchto práv. Informační sdělení musí zahrnovat jednak údaje o odpovědnosti za vady dle ustanovení § 2161 OZ,

[63] Takto to udělal kupříkladu český NFT projekt dm Múzy Inspirace; dm Múzy inspirace [online]. In: *dm-muzy.cz*. [cit. 17. 1. 2023]. Dostupné z: https://www.dm-muzy.cz/#buy-nft

uplatnění práv z vad dle ustanovení § 2165 OZ, případně informaci o podmínkách poprodejního servisu či dalších smluvně zakotvených záručních právech, jež podnikatel poskytuje spotřebiteli nad rámec uvedených zákonných požadavků dle ustanovení § 2113 OZ. Práva poskytnutá spotřebiteli zákonem nesmí být označena jako speciální součást nabídky prodávajícího. Prodávající musí uvést informaci o tom, kde může spotřebitel reklamaci uplatnit dle § 13 ZOS.[64] V případě prodeje NFT tedy musí prodávající uvést výše uvedené údaje, v přehledné formě, nejčastěji je toto realizováno vypracováním reklamačních řádů, které jsou součástí všeobecných obchodních podmínek. Zaručení kvality si u NFT můžeme představit například v případě, že je NFT provázáno s podkladovým aktivem a toto spojení je smluvně potvrzeno. V takovém případě je nutné zaručit kvalitu tohoto podkladového aktiva. Prodávající musí spotřebitele informovat též o právech spotřebitele v případě vadného plnění, dle ustanovení § 2106 OZ v případě vadného plnění jako podstatného porušení smlouvy a dle ustanovení § 2107 OZ v případě vadného plnění jako nepodstatného porušení smlouvy. Dále musí prodávající sdělit spotřebiteli kontaktní místo pro uplatnění reklamace.[65]

Dle ustanovení § 1820 odst. 1 písm. n) OZ musí podnikatel uvést údaj o kodexu chování, pokud se jej podnikatel zavázal dodržovat v souvislosti s některou obchodní praktikou nebo odvětvím jeho podnikání a o tom, jak lze obdržet jeho kopii.

Dle ustanovení § 1820 odst. 1 písm. o) OZ v případě, že má být smlouva uzavřena na dobu neurčitou, nebo má-li být závazek automaticky prodlužován, musí prodejce sdělit údaj o době trvání závazku a podmínky ukončení závazku. Doba trvání závazku bude určena v časových jednotkách (hodiny, dny, měsíce, roky). Podmínky ukončení závazku budou obsahovat informace o možných způsobech vypovězení smlouvy, počátku běhu a délce výpovědní lhůty. Tyto podmínky by měly zejména obsahovat informaci o době, po kterou spotřebitel nemůže vypovědět smlouvu, jejíž doba

[64] VONDRÁČEK, ref. 60.

[65] Příkladem může být Reklamační řád při prodeji nezaměnitelných tokenů drogerie DM [online]. In: *dm-muzy.cz*. [cit. 12. 1. 2023]. Dostupné z: https://www.dm-muzy.cz/static/pdf/dm_NFT_reklamacni_rad.pdf

platnosti se automaticky obnovuje, a od kdy takovou smlouvu již vypovědět může.[66] Nejeden NFT projekt slibuje uživatelům určité výhody udělené *„na celý život.“*[67] Tyto doživotní závazky však nejsou ničím jiným než smlouvou uzavřenou na dobu neurčitou. Je tedy nutné, aby trvání s NFT spojeného poskytování služby bylo časově určeno a byly též stanoveny podmínky ukončení tohoto závazku.

Dle ustanovení § 1820 odst. 1 písm. p) OZ je podnikatel povinen spotřebiteli sdělit nejkratší dobu, po kterou budou trvat spotřebitelovy povinnosti ze smlouvy, mají-li být smlouvou určeny. U některých NFT projektů mezi tyto povinnosti patří omezení převedení práv a povinností vyplývajících ze smlouvy o koupi NFT, kdy podnikatel stanoví povinnost sekundárního prodeje NFT pouze přes konkrétní on-line tržiště, případně stanoví přesný postup sekundárního prodeje. Zároveň vzhledem k faktu, že většina NFT je vytvořena na základě podkladového aktiva, které je autorským dílem, vznikají spotřebiteli povinnosti vytyčené v licenčních podmínkách.

Dle ustanovení § 1820 odst. 1 písm. q) OZ je podnikatel povinen spotřebitele informovat o povinnosti zaplatit zálohu nebo obdobnou platbu, je-li vyžadována, a o jejích podmínkách. Teoretickým konceptem by mohly být NFT vytvořené na míru spotřebiteli s vyššími produkčními náklady, v rámci kterých by podnikatel po spotřebiteli požadoval uhrazení zálohy.

Dle ustanovení § 1820 odst. 1 písm. r) OZ je podnikatel povinen spotřebitele informovat o funkčnosti, kompatibilitě a interoperabilitě digitálního obsahu. Informační povinnost vztahující se k funkčnosti digitálního obsahu a technických ochranných opatření slouží k informování spotřebitele o tom, jak lze digitální obsah využívat.[68] Z velké části lze ustanovení tohoto písmena s ohledem na NFT vztáhnout již pod vymezení dle ustanovení § 1820 odst. 1 písm. a) OZ. Prodejce by měl popsat funkčnost NFT tak, aby byla průměrnému spotřebiteli jasná.

---

[66] VONDRÁČEK, ref. 60.

[67] NFT kolekce KlubList zajišťující doživotní vstupy do vybraných klubů. Klublist [online]. In: *klublist.clubbingtv.com*. [cit. 15. 1. 2023]. Dostupné z: https://klublist.clubbingtv.com/

[68] VONDRÁČEK, ref. 60.

Kompatibilita je schopnost digitálního obsahu fungovat s hardwarem nebo softwarem, se kterým se obvykle používá digitální obsah stejného typu, aniž by bylo nutné jej konvertovat.

Interoperabilita je schopnost digitálního obsahu fungovat s jiným hardwarem nebo softwarem, než s jakým se obvykle používá digitální obsah stejného typu.[69]

Kompatibilita a interoperabilita je často propagovanou vlastností fenoménu NFT. Ekosystémy NFT jsou však izolované v rámci nativního blockchainu, na základě kterého byly vytvořeny. Ethereum na svém webu uvádí: *„NFT jsou kompatibilní s čímkoli, co je postaveno na platformě Ethereum. NFT vstupenku na událost lze vyměnit na každém on-line tržišti Etherea za jakékoliv jiné NFT. Vstupenku můžete vyměnit za umělecké dílo!“*[70] Myslí se tím, že každé NFT s nativním blockchainem Ethereum může být obchodováno na on-line tržištích, které Ethereum podporují.

Není to však takto jednoznačné. Mnohé NFT, ačkoliv jsou vytvořeny na totožném token standardu, nemohou být používány ve stejném prostředí. Každý z těchto NFT je vázán na konkrétní chytrý kontrakt, který obsahuje vlastnosti vázané na daný NFT a také konkrétní akce, které s ním mohou být realizovány. Například již zmíněné NFT CryptoKitties[71] nemohou být obchodovány na nativním tržišti herní NFT platformy Gods Unchained,[72] ačkoliv mají stejný nativní blockchain, tedy Ethereum, token standard ERC-721, jelikož nativní tržiště Gods Unchained podporuje pouze NFT vztahující se právě ke hře Gods Unchained. Obdobně je nutné zmínit, že ačkoliv NFT karty Gods Unchained mohou být obchodovány na otevřených NFT on-line tržištích, budou na nich postrádat svoji funkčnost, jelikož pouze v uzavřeném systému hry Gods Unchained mohou plnit svoji herní funkci.

---

[69] Důvodová zpráva k zákonu č. 374/2022 Sb., kterým se mění zákon č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů, a zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, č. 374/2022 Dz.

[70] Non-Fungible Tokens (NFT), ref. 22.

[71] CryptoKitties, ref. 55.

[72] Gods Unchained Terms of Service [online]. In: *Gods Unchained*. 6. 9. 2021. [cit. 2. 2. 2023]. Dostupné z: https://godsunchained.com/terms/conditions

Právní konstrukty kompatibility a interoperability byly navrženy tak, aby byly technologicky neutrální. Je však nejisté, zda jsou určeny k tomu, aby se přímo vztahovaly na technologicky unikátní fenomén NFT. Je otázkou, zda potřeba regulace a ochrany spotřebitele s ohledem na tradiční poskytovatele digitálního obsahu (například obchody s aplikacemi, platformy sociálních sítí a služby pro sdílení videa), má stejné upotřebení a lze ji analogicky vztáhnout i na služby, které jsou složitější z hlediska kompatibility a interoperability. Blíže bude o standardech digitálního obsahu ve vztahu k NFT pojednáno níže. Informační povinnost je však nutné dodržet, proto v souvislostech s každým konkrétním případem prodeje NFT musí prodávající spotřebiteli sdělit podrobnosti o kompatibilitě a interoperabilitě v co možná největší míře a podrobnostech.

Dle ustanovení § 1820 odst. 1 písm. s) musí před uzavřením smlouvy o koupi NFT podnikatel spotřebitele informovat o existenci, způsobu a podmínkách mimosoudního vyřizování sporů, včetně informace, zda se lze obrátit se stížností na orgán dohledu nebo státního dozoru. Podnikatel tak musí informovat o možnosti využití mimosoudního řešení sporů, nad nímž vykonává dozor Česká obchodní inspekce, která je příslušným orgánem mimosoudního řešení spotřebitelských sporů, případně o dalších institucích pro řešení mimosoudních spotřebitelských sporů.

4.2.3 ODSTOUPENÍ OD SMLOUVY O KOUPI NFT

Právo odstoupit od smlouvy, nazývané také „*právo na rozmyšlenou*“ je jedním z nejdůležitějších práv, kterými spotřebitel v případě smluv uzavíraných distančním způsobem disponuje. Ustanovení § 1829 a násl. OZ umožňují spotřebiteli změnit názor s ohledem na uzavření smlouvy a poskytují mu právo na odstoupení od smlouvy bez udání důvodu do 14 dnů od uzavření smlouvy. V takovém případě může spotřebitel vrátit zboží a získat zpět zaplacené peněžní prostředky včetně nákladů na dodání. Opomenutí informovat spotřebitele o právu na odstoupení od smlouvy stanoví lhůtu pro odstoupení od smlouvy v délce jednoho roku dle ustanovení § 1829 odst. 4 OZ.

Naprostá většina NFT projektů však ve svých obchodních podmínkách informace o uznání práva spotřebitele na odstoupení od smlouvy nezmiňuje. To vyvolává důvodné pochybnosti, které se odráží v otázce použitelnosti práva na odstoupení od smlouvy v případě prodeje NFT.

Z dosavadních závěrů, učiněných v tomto článku, je NFT určitým druhem virtuálního statku. V případě uzavírání smlouvy o koupi NFT se spotřebitelem je tedy nutné spotřebitele informovat právě i o právu na odstoupení od smlouvy. Podnikatel tedy musí dle ustanovení § 1820 odst. 1 písm. i) OZ spotřebitele informovat o právu na odstoupení od smlouvy, pokud tak neučiní, může spotřebitel dle ustanovení § 1829 odst. 4 OZ odstoupit od smlouvy do jednoho roku.

Právo na odstoupení od smlouvy však spotřebiteli nemusí být vždy přiznáno, existují výjimky. Tyto výjimky jsou upraveny v ustanovení § 1837 OZ, níže si rozebereme jednotlivá ustanovení, která se vztahují k nemožnosti odstoupit od smlouvy o koupi NFT.

První z výjimek je upravena v ustanovení § 1837 písm. b) OZ, kdy je cena aktiva závislá na výchylkách finančního trhu nezávisle na vůli podnikatele a k nimž může dojít během lhůty pro odstoupení od smlouvy. Jak již bylo zmíněno, NFT jsou aktiva, jejichž cena je značně spekulativní, nezřídka se proto stává, že po mintování NFT jeho cena výrazně poklesne. Podnikatel musí v takovém případě o neexistenci práva spotřebitele na odstoupení od smlouvy informovat dle ustanovení § 1820 odst. 1 písm. l) OZ. Je však poměrně nejisté, zda by trh s NFT pod tuto výjimku bylo možné podřadit. Vondráček k ustanovení § 1837 písm. b) OZ uvádí, že pod tuto výjimku lze podřadit zboží závisející na výchylkách finančního trhu v širokém smyslu, což zahrnuje nejen regulované trhy či mnohostranné obchodní systémy, ale rovněž trhy komoditní, trhy s emisními povolenkami atp. Pod výjimku naopak nelze podřadit například smlouvy o nákupu klenotů, jejichž cena není výhradně závislá na ceně suroviny ale rovněž na šperkařské práci nebo smlouvy o dodávkách zboží, jejichž cenu mohou strany ve smlouvě ovlivnit.[73]

[73] VONDRÁČEK, Ondřej. § 1837 Výjimky z práva odstoupit od smlouvy. In: PETROV, Jan. a kol. Občanský zákoník. 2. vydání (1. aktualizace). Praha: C. H. Beck, 2022.

Vzhledem k nejednotné regulaci trhů s kryptoaktivy a faktu, že konkrétní série NFT nemá se spekulativní hodnotou NFT trhu jako celku přímou korelaci, by však použití této výjimky ze strany podnikatele bylo přinejmenším riskantní s ohledem na případné spotřebitelské spory.[74]

Druhá výjimka je upravena v ustanovení § 1837 písm. d) OZ. Jednalo by se o případy, kdy by konkrétní NFT bylo vyrobeno podle požadavků spotřebitele nebo bylo přizpůsobeno jeho osobním potřebám. Tato výjimka by se použila u NFT projektů, které nabízejí spotřebiteli možnost kustomizace a upravení NFT dle vlastních potřeb.

Třetí výjimka, která je pro NFT projekty z hlediska použitelnosti nejrelevantnější, jelikož nabízí nejsilnější argumentaci v případném sporu z důvodu existence výslovného souhlasu spotřebitele, je uvedena v ustanovení § 1837 písm. l) OZ. To uvádí, že spotřebitel nemůže odstoupit od smlouvy o dodání digitálního obsahu, který není dodán na hmotném nosiči, poté, co bylo plnění za úplatu započato s předchozím výslovným souhlasem spotřebitele před uplynutím lhůty pro odstoupení od smlouvy a spotřebitel byl poučen, že tím právo odstoupit od smlouvy zaniká a bylo mu poskytnuto potvrzení dle ustanovení § 1824a odst. 1 a 2 nebo § 1828 odst. 3 a 4 OZ.

Tato výjimka se vztahuje na smlouvy o dodání digitálního obsahu prostřednictvím nehmotného nosiče, pokud bylo zahájeno plnění a pokud smlouva ukládá spotřebiteli povinnost platit. Zároveň je vyžadováno kumulativní splnění tří podmínek:

1. spotřebitel dal předchozí výslovný souhlas se zahájením plnění během lhůty pro odstoupení od smlouvy;
2. spotřebitel vzal na vědomí, že tím ztrácí právo na odstoupení od smlouvy;
3. podnikatel poskytl spotřebiteli potvrzení o uzavření smlouvy v souladu s podmínkami Směrnice 2011/83/EU pro distančně uzavřené smlouvy, tedy vyhotovení smlouvy nebo potvrzení

[74] Někteří autoři vidí v případě prodeje NFT spotřebiteli výchylky finančního trhu jako možnou výjimku, způsobující možnost nepřiznání práva na odstoupení od smlouvy viz STAZI, Andrea. Smart contracts, NFT trading and weaker party protection. In: *NFTs and Metaverses versus Law, Springer*. 2023, s. 13.

> o uzavřené smlouvě a potvrzení, že spotřebitel výslovně souhlasí se započetím plnění před uplynutím lhůty pro odstoupení od smlouvy a že bere na vědomí, že udělením souhlasu zaniká jeho právo odstoupit od smlouvy.

Primárním kritériem, které autor považuje z pohledu informační povinnosti vůči spotřebiteli za důležité, je specifikace výslovného souhlasu a jeho požadavky pro splnění informační povinnosti.

Výše zmíněné výjimky, závislé na výslovném souhlasu spotřebitele, nedávno využila společnost Porsche se svou debutovou NFT kolekcí.[75]

Spotřebitelé, kteří měli v úmyslu zakoupit NFT z kolekce Porsche, museli aktivně odsouhlasit zaškrtnutím tzv. checkboxu, že se vzdávají svého práva na odstoupení od smlouvy. Tento souhlas byl podmínkou k uskutečnění transakce.

Společnost Porsche k tomuto kroku přistoupila z jasného důvodu. Vzhledem k velmi volatilní hodnotě NFT by v případě, pokud by cena konkrétního NFT klesla na sekundárním trhu pod tzv. minting price, tedy cenu, za kterou spotřebitel NFT zakoupil, tj. 0,911 Ether, by mohli evropští spotřebitelé využít svého práva na odstoupení od smlouvy a požádat společnost Porsche o vrácení kupní ceny.

Odpověď na požadavky splnění výslovného souhlasu uděleného ze strany spotřebitele nalezneme v Pokynech Evropské komise k výkladu a uplatňování směrnice Evropského parlamentu a Rady 2011/83/EU o právech spotřebitelů (dále jen „Pokyny“).[76] Výslovný souhlas lze získat před uzavřením smlouvy, během uzavírání smlouvy nebo po uzavření smlouvy, pokud se tak stane před začátkem plnění smlouvy. Je nutné, aby výsledný souhlas byl výsledkem pozitivní akce spotřebitele, například zaškrtnutím políčka (checkbox). Použití předem zaškrtnutého políčka nebo použití doložky ve všeobecných obchodních podmínkách nenaplňuje požadavky

[75] Terms and Conditions [online]. In: *Road2dreams NFT-platform*. [cit. 20. 1. 2023]. Dostupné z: https://assets.ctfassets.net/sca5putua729/38fWxlZ78gunAdsQaG8RwJ/596314bc9a258f5bfda4bb8e410b25f4/road2dreams_Terms_and_Conditions_Austria_EN.pdf

[76] Sdělení Komise Pokyny k výkladu a uplatňování směrnice Evropského parlamentu a Rady 2011/83/EU o právech spotřebitelů 2021/C 525/01. https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52021XC1229(04)

výslovného souhlasu, kdy Pokyny odkazují na analogické použití výslovného souhlasu z rozsudku SDEU ve věci C-673/17, Planet 49, týkající se výslovného souhlasu pro zpracování osobních údajů subjektu údajů. Z výše uvedeného proto lze dovodit, že společnost Porsche naplnila požadavky výslovného souhlasu spotřebitele se zahájením plnění během lhůty pro odstoupení od smlouvy, kdy zároveň spotřebitel výslovným souhlasem bere na vědomí vzdání se práva na odstoupení od smlouvy.

Je na místě zmínit, že Porsche je v tomto přístupu jednou z mála společností, která tento způsob zvolila. Většina ostatních NFT projektů spotřebitele o právu na odstoupení od smlouvy neinformuje, případně souhlas se vzdáním se práva na odstoupení od smlouvy zavedla do všeobecných obchodních podmínek, tedy způsobem, který odporuje požadavkům výslovného souhlasu. Je nutností, aby podnikatelé uvedli tyto požadavky do souladu, jinak jim hrozí, že v dobách propadů hodnot NFT by se nejeden spotřebitel mohl domáhat svých práv na odstoupení od smlouvy do jednoho roku dle ustanovení § 1829 odst. 4 OZ, jelikož nebyl o možnosti odstoupení od smlouvy dostatečně informován nebo neudělil výslovný souhlas se započetím plnění před uplynutím lhůty pro odstoupení od smlouvy, které by působilo při splnění informování spotřebitele zánik práva na odstoupení od smlouvy.

4.2.4 NFT A STANDARDY DIGITÁLNÍHO OBSAHU

Ochrana uživatelů věcí v digitální podobě (digitálního obsahu) a digitálních služeb získala v posledních letech silnější postavení díky právním iniciativám EU, kterými jsou (1) Směrnice Evropského parlamentu a Rady č. 2019/771, o některých aspektech smluv o prodeji zboží, a (2) Směrnice Evropského parlamentu a Rady č. 2019/770, o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb (dále jen „Směrnice o digitálním obsahu“). Transpozici těchto směrnic přinesla do českého právního řádu novela, označená ve Sbírce zákonů pod číslem 374/2022 Sb. Tato novela upravuje poskytování digitálního obsahu nebo služeb digitálního obsahu s posílenou ochranou spotřebitele, například pokud jde o informační povinnosti poskytovatelů digitálního obsahu ve vztahu k jeho

funkčnosti, kompatibilitě a interoperabilitě dle ustanovení § 1820 odst. 1 písm. r) OZ, viz kapitola 4.2.2 výše, či posuzování vad digitálního obsahu nebo služeb digitálního obsahu. Ve vztahu k NFT může být ochrana uživatelů digitálního obsahu relevantní, tato podkapitola proto přináší základní exkurz do možných dopadů této úpravy na NFT.

Český právní řád definuje digitální obsah v ustanovení § 2389a OZ jako věc v digitální podobě. Pro lepší pochopení toho, co se pod pojmem digitální obsah skrývá, je však vhodné nahlédnout do Směrnice o digitálním obsahu, která v čl. 2 odst. 1 definuje digitální obsah jako „*data, která jsou vytvořena a poskytována v digitální podobě*," a mezi příklady digitálního obsahu uvádí Směrnice o digitálním obsahu v recitálu 19 mimo jiné „*počítačové programy, aplikace, videosoubory, audiosoubory, hudební soubory, digitální hry, e-knihy a ostatní elektronické publikace*."

Službou digitálního obsahu je dle ustanovení § 2389t OZ služba, která „*uživateli umožňuje vytvářet, zpracovávat či uchovávat data v digitální podobě nebo k nim přistupovat, sdílet data v digitální podobě nahraná či vytvořená tímto nebo jiným uživatelem této služby anebo jakoukoli jinou interakci s těmito daty*."[77] Příklad těchto služeb poskytuje opět recitál 19 Směrnice o digitálním obsahu, kdy takovými službami jsou například služby „*sdílení videa a audiozáznamů a jiných souborů, zpracování textu nebo her nabízených v prostředí cloud computingu a sociálních médií.*"

Vzhledem k tomu, že NFT jsou vytvářeny a dodávány v digitálním formátu, lze polemizovat o tom, zda jsou podřaditelné pod služby digitálního obsahu, jelikož umožňují uživateli – kupujícímu NFT, přístup k datům v digitální podobě. Těmito daty by poté byl digitální obsah – podkladové aktivum, na základě kterého je NFT vytvořeno, a na které NFT v metadatech přímo odkazuje. Preambule směrnice v recitálu 12 uvádí, že „*právní povaha smluv o poskytování digitálního obsahu nebo digitální služby a otázka, zda se jedná o smlouvy o prodeji, poskytování služby, pronájmu nebo o jiný typ smlouvy, případně o smlouvy sui generis, by měla být ponechána na vnitrostát-*

[77] V případě odkazování na zákonná ustanovení týkající se digitálního obsahu autor upozorňuje, že tato ustanovení o poskytování digitálního obsahu se použijí obdobně i na případy, kdy se poskytovatel zavazuje uživateli poskytovat službu digitálního obsahu, viz ustanovení § 2389t OZ.

ním právu.“ Bez zásahu zákonodárce nebo rozhodovací praxe tedy nelze jednoznačně určit, zda lze na NFT pohlížet jako na služby digitálního obsahu, a to hlavně z důvodu rozdílnosti jednotlivých NFT projektů. Lze si například představit, že v případě, kdy by NFT byl součástí herní NFT platformy, ve které by měl svou funkčnost a kompatibilitu, bez pochyb by se tato NFT platforma musela řídit povinnostmi vyplývajícími z poskytování služeb digitálního obsahu. V případě NFT, které existují samy o sobě, tedy nejsou nijak vázané na konkrétní digitální platformy, určení už není tak snadné a bude na rozhodovací praxi, aby některé otázky zodpověděla. Lze si však představit, že bychom mohli definici služby digitálního obsahu rozšířit i na běžné NFT, jejichž primární funkcionalita je odkazování v metadatech na podkladové aktivum, tedy jistý druh poskytování přístupu uživateli k datům v digitální podobě, tedy k podkladovému aktivu.

V případě, že by NFT byly podřazeny pod služby digitálního obsahu, nejrelevantnějšími pro posuzování jejich souladu by byla otázka zpřístupnění digitální služby a otázka souladu digitální služby.

Z hlediska zpřístupnění digitální služby stanovuje ustanovení § 2389b OZ, že není-li ujednáno jinak, poskytovatel digitální služby ji uživateli zpřístupní bez zbytečného odkladu po uzavření smlouvy. To nebude toliko problematické u klasických NFT, jejichž primární funkcionalita je odkazování na podkladové aktivum v metadatech. Ta jsou téměř vždy zpřístupněna kupujícímu doručením NFT do jeho digitální kryptopeněženky automaticky. Problematické by to však mohlo být u NFT, které mají svou funkcionalitu v rámci určité platformy. Kupující NFT, který je součástí herní platformy, tak sice bude mít NFT ve své digitální kryptopeněžence, pokud však nebude splněna jeho primární funkcionalita, tedy zpřístupnění v rámci herního světa, ve kterém NFT plní svou funkci, nebude zpřístupnění v rámci poskytování komplexní digitální služby herní platformy naplněno. V herním NFT prostředí existuje několik platforem, které využily růst hodnot NFT a prodávaly kupujícím služby, které v době prodeje NFT ne-

byly zavedeny.[78] V takovém případě je nutné, aby o očekávaném termínu funkčnosti poskytovatel uživatele informoval. Uživatelé tak investovali do služeb digitálního obsahu, k nimž reálný přístup neměli ještě dlouho po zakoupení NFT.

Pokud jde o požadavky na shodu při poskytování služeb digitálního obsahu uživateli, který je spotřebitelem, ustanovení § 2389i odst. 1 OZ stanovuje, že poskytovatel zejména odpovídá, aby digitální služba:

- odpovídala ujednanému popisu a rozsahu, jakož i jakosti, funkčnosti, kompatibilitě, interoperabilitě a jiným ujednaným vlastnostem;
- byla vhodná pro účely požadované uživatelem, se kterými poskytovatel souhlasil;
- byla poskytovaná s ujednaným příslušenstvím a pokyny k použití, včetně návodu k instalaci, a s uživatelskou podporou.

Ustanovení § 2389i odst. 2 OZ vychází z předchozího ustanovení a definuje objektivní požadavky na soulad, kdy kupříkladu musí být služba digitálního obsahu vhodná k účelu k němuž se obvykle používá, musí odpovídat funkčnostem, kompatibilitě, přístupnosti, kontinuitě a bezpečnosti a musí odpovídat vlastnostem služeb digitálního obsahu téhož druhu, které může uživatel rozumně očekávat i s ohledem na veřejná prohlášení učiněná poskytovatelem. Ustanovení § 2389j OZ poté dopadá na vady spojené s propojením v rámci služeb digitálního obsahu s digitálním prostředím uživatele, které bylo podle smlouvy provedeno poskytovatelem nebo na jeho odpovědnost.

V rámci blockchainové sítě probíhají některé operace, vztahující se k NFT, decentralizovaně, bez možnosti poskytovatele služeb digitálního obsahu, tedy mintera NFT, zasáhnout do průběhu těchto operací, jako příklad můžeme zmínit prodej NFT. Existují však operace, na které má i po vytvo-

[78] Příkladem takového projektu, který již začal s prodejem NFT, jejichž funkcionalita zatím stále není zavedena, je herní NFT projekt Illuvium, který v době psaní článku čeká na spuštění herní platformy. Illuvium Terms & Conditions [online]. In: *illuvium.io*. 28. 2. 2023. [cit. 20. 3. 2023]. Dostupné z: https://illuvium.io/terms-and-conditions

ření NFT minter vliv a jejich soulad se smlouvou o poskytování služeb digitálního obsahu by měl zaručit.

Jako příklad může sloužit situace, kdy minter NFT používá off-chain úložiště podkladového aktiva na centralizovaném serveru. V takovém případě by měl zajistit, aby toto uložení bylo vzhledem k povaze NFT trvalé. V případě, že by toto nezaručil a URL adresa směřující na centralizované úložiště s pokladovým aktivem nebyla funkční, nesplnil by poskytovatel požadavek, aby služba digitálního obsahu odpovídala funkčnosti, která byla ve smlouvě ujednána. Stejně tak, jako v případě výše zmíněných NFT herních platforem, bude poskytovatel této platformy odpovídat za to, aby NFT splňoval standardy stanovené ve smlouvě, byl kompatibilní s herní platformou a plnil své funkcionality. Lze si taktéž představit situaci, kdy NFT nemá očekávané charakteristiky vzácnosti, ke kterým se poskytovatel zavázal. Vzácnost NFT má zásadní význam pro jeho hodnotu a NFT s výrazně nižším stupněm vzácnosti, než spotřebitel na základě uzavřené smlouvy mohl očekávat, nemusí splňovat požadavky na soulad dle ustanovení § 2389i odst. 1 OZ. K takové situaci by mohlo dojít v případě, že minter NFT po prodeji sníží vzácnost prodávaných NFT tím, že na trh uvede více NFT, které jsou součástí dané série, než původně avizoval. Je tedy na místě zvážit vhodnost smluvního ujednání, které stanovuje stupeň vzácnosti daného NFT a zaručuje jeho vzácnost v rámci dané série nebo na základě daného podkladového aktiva.[79]

Výše byly zmíněny jen některé aspekty, které by mohly dopadat na NFT v případě, kdy by byly podřazeny pod služby digitálního obsahu. Jak již však bylo zmíněno výše, otázku, zda regulace ochrany spotřebitele zavedená Směrnicí o digitálním obsahu, dopadne na mintery NFT, zodpoví jednoznačně až rozhodovací praxe.

[79] KOOLEN, Christof, "Apes gone", but what about consumer protection? Applying EU consumer law to the transfer of NFTs [online]. In: *CCM Blog*. 17. 1. 2022. [cit. 20. 3. 2023] https://law.kuleuven.be/ccm/blog/?p=289

5. ZÁVĚR

S rostoucím zájmem o NFT vzrostl i počet právních otázek, vztahujících se k tomuto fenoménu. Cílem této publikace bylo zmapovat možné průsečíky NFT s konkrétními právními instituty a zmapovat výzvy, které se s nimi pojí pro ochranu spotřebitele.

NFT je formou datového kódu, jehož individuální nebo virtuální užitek může být právně objektivizován. Z toho důvodu lze NFT charakterizovat jako věc v právním smyslu s nehmotnou, movitou a nezastupitelnou povahou, kdy právě nezastupitelnost je jeho primárním znakem.

NFT můžeme definovat jako nezastupitelné tokeny, odkazující na virtuální nebo fyzické podkladové aktivum a můžeme je dělit do dvou kategorií v závislosti na provázanosti s podkladovým aktivem. První z nich jsou NFT vázané na podkladová aktiva. S takovými NFT minter smluvně provázal práva k podkladovému aktivu. Příkladem těchto práv mohou být práva k užití podkladového aktiva jakožto autorského díla, udělené autorem nabyvateli NFT v rámci licenční smlouvy, zastoupení podkladového aktiva pomocí NFT nebo certifikace podkladového aktiva. Jejich hodnota se odvíjí od hodnoty podkladového aktiva. Druhou kategorií jsou NFT sloužící jako nezávislá reprezentace podkladových aktiv, které jsou vytvořeny na základě podkladového aktiva, jsou jasným odkazem na ně, nevytvářejí však k podkladovému aktivu žádná práva. Jejich hodnota je primárně spekulativní.

Otázka odlišitelnosti podkladového aktiva od NFT a s tím souvisejících vlastnických práv záleží na provázanosti NFT s podkladovým aktivem. Bez zásahu zákonodárce nebo smluvního ujednání, které by provázalo podkladové aktivum s NFT, budou NFT a podkladové aktivum dvě rozdílné věci, ke kterým vznikají práva nezávisle.

Z důvodu, že je NFT určitým digitálním statkem, může být předmětem spotřebitelských vztahů v případě, že kupujícím subjektem je fyzická osoba, kupující NFT od subjektu v pozici podnikatele a koupí NFT realizuje osobní zájem mimo rámec své podnikatelské činnosti nebo samostatného výkonu

povolání. Podnikatel má v souvislosti s prodejem NFT informační povinnost vůči kupujícímu spotřebiteli dle ustanovení § 1820 odst. 1 OZ.

Vzhledem k povaze NFT je důležité zaměřit se na právo spotřebitele na odstoupení od smlouvy o koupi NFT a možnost nepřiznání tohoto práva ze strany podnikatele. V případě prodeje NFT se může podnikatel odvolávat tří výjimek, za jejichž splnění by právo na odstoupení od smlouvy nemuselo být spotřebiteli přiznáno. První z výjimek je argument, že cena NFT je závislá na výchylkách finančního trhu nezávisle na vůli podnikatele dle ustanovení § 1837 písm. b) OZ. Vzhledem k nejednotné regulaci trhů s kryptoaktivy je však nejisté, zda by se toto ustanovení na prodej NFT vztahovalo. Druhou výjimkou je skutečnost, kdy NFT bylo vyrobeno spotřebiteli na míru dle ustanovení § 1837 písm. d) OZ. Třetí, nejrelevantnější výjimkou, je situace, kdy spotřebitel nemůže odstoupit od smlouvy o dodání digitálního obsahu poté, co bylo plnění za úplatu započato s předchozím výslovným souhlasem spotřebitele před uplynutím lhůty pro odstoupení od smlouvy a spotřebitel byl poučen, že tím právo odstoupit od smlouvy zaniká. Kumulativně tak musí být splněn výslovný souhlas spotřebitele se zahájením plnění během lhůty pro odstoupení od smlouvy, spotřebitel musí vzít na vědomí, že tím ztrácí právo na odstoupení od smlouvy a musí mu být poskytnuto potvrzení dle ustanovení § 1824a odst. 1 a 2 nebo § 1828 odst. 3 a 4 OZ.

S ochranou spotřebitelů v rámci transakcí s NFT úzce souvisí ochrana uživatelů věcí v digitální podobě (digitálního obsahu). Vzhledem k tomu, že NFT jsou vytvářeny a dodávány v digitálním formátu, lze polemizovat o tom, zda jsou podřaditelné pod služby digitálního obsahu, když umožňují uživateli – kupujícímu NFT, přístup k datům v digitální podobě. Pokud by na NFT bylo nahlíženo jako na služby digitálního obsahu, nejrelevantnějšími pro posuzování jejich souladu by byla otázka zpřístupnění digitální služby a otázka souladu digitální služby.

Zpřístupněním digitální služby může v případě NFT být zpřístupnění podkladového aktiva v rámci metadat NFT, toto zpřístupnění bude díky chytrému kontraktu okamžité po převedení NFT do digitální kryptopeněženky kupujícího. Problematické by zpřístupnění digitální služby mohlo být

například pokud by NFT byly součástí herní platformy, kdy by nebyla splněna primární funkcionalita tohoto NFT, tedy zpřístupnění v rámci herního světa, ve kterém plní svou funkci. V takovém případě by zpřístupnění v rámci poskytování komplexní digitální služby herní NFT platformy nebylo naplněno. Pokud jde o požadavky na shodu při poskytování služeb digitálního obsahu uživateli, musí tato služba odpovídat ujednanému popisu a rozsahu, jakosti, funkčnosti, kompatibilitě a interoperabilitě. V rozporu s tímto by byly například NFT, u kterých by odkaz na podkladové aktivum v metadatech nebyl funkční nebo série NFT, kterou minter v rozporu s dříve učiněným prohlášením rozšířil a snížil tak vzácnost jednotlivých NFT.

Ačkoliv NFT přináší z právního pohledu množství otázek, většinu z těchto otázek můžeme zodpovědět na základě existujících právních institutů a jejich obecnosti, která dovoluje definování NFT z právního hlediska. Je tedy na místě zkoumat dopady NFT do konkrétních institutů v souvislosti se zachováním souladu s cílem zákonodárce. Pro zodpovězení konkrétních otázek však bude nutné nadále zkoumat použití této technologie a sledovat rozhodovací praxi a legislativní přístup jak na unijní, tak na národní úrovni.

6. SEZNAM POUŽITÝCH ZDROJŮ

6.1 ODBORNÉ ČLÁNKY

[1] BAMAKAN, Seyed Mojtaba Hosseini, Nasim NEZHADSISTANI, Omid BODAGHI a Qiang Qu. Patents and intellectual property assets as non-fungible tokens; key technologies and challenges. In: *Scientific Reports*. 2022, roč. 12.

[2] BARRINGTON, Sarah. The Role of Metadata in Non-Fungible Tokens: Marketplace Analysis and Collection Organization. In: *arXiv preprint arXiv*. 2021.

[3] DĚDIČ, Jan, Jan ŠOVAR a Ondřej MIKULA. Proč podle českého soukromého práva nelze uvažovat o (ICO) tokenech jako o cenných papírech. In: *Právní rozhledy*. 2018, roč. 15-16.

[4] GARCIA-TERUEL, Rosa M, Héctor SIMÓN-MORENO. The digital tokenization of property rights. A comparative perspective. In: *Computer Law & Security Review*. 2021, r. 41.

[5] GUADAMUZ, Andres. The treachery of images: non-fungible tokens and copyright. In: *Journal of Intellectual Property Law & Practice*. 2021, roč. 16, č. 12.

[6] HERIAN, Robert a kol. NFT–Legal Token Classification. In: *EU Blockchain Observatory & Forum*. 2021.

[7] MORINGIELLO, Juliet M., Christopher K. ODINET. Blockchain Real Estate and NFTs. In: *William & Mary Law Review, Forthcoming, U Iowa Legal Studies Research Paper*. 2022.

[8] NOFER, Michael, Peter GOMBER, Oliver HINZ a Dirk SCHIERECK. Blockchain. In: *Business & Information Systems Engineering*. 2017, r. 59, č. 3.

[9] ODOM, William, John ZIMMERMAN a John FORLIZZI. Placelessness, spacelessness, and formlessness: experiential qualities of virtual possessions. In: *Proceedings of the 2014 conference on Designing interactive systems*. 2014.

[10] POLČÁK, Radim. Informace a data v právu. In: *Revue pro právo a technologie*. 2016, roč. 7, č. 13.

[11] POPESCU, Andrei-Dragos. Non-Fungible Tokens (NFT)-Innovation Beyond the Craze. In: *5th International Conference on Innovation in Business, Economics and Marketing Research*. 2021.

[12] STAZI, Andrea. Smart contracts, NFT trading and weaker party protection. In: *NFTs and Metaverses versus Law*, Springer. 2023.

[13] WANG, Qin, Ruija LI, Qi WANG, Shiping CHEN. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. In: *arXiv preprint arXiv*.

6.2 ELEKTRONICKÉ ZDROJE

[14] BAYC [online]. In: *boredapeyachtclub.com*. [cit. 25. 11. 2022]. Dostupné z: https://boredapeyachtclub.com/

[15] Blockchain technologies and IP ecosystems: A WIPO white paper[online]. In: *WIPO*. 2022, s. 15. [cit. 22. 10. 2022]. Dostupné z: https://www.wipo.int/export/sites/www/cws/en/pdf/blockchain-for-ip-ecosystem-whitepaper.pdf

[16] Colt CZ Group jako první výrobce ručních palných zbraní vstupuje do světa blockchainové technologie [online]. In: *Colt CZ Group*. 16. 12. 2022. [cit. 17. 1. 2023]. Dostupné z: https://www.coltczgroup.com/media-tiskove-zpravy/colt-cz-group-jako-prvni-vyrobce-rucnich-palnych-zbrani-vstupuje-do-sveta-blockchainove-technologie

[17] CryptoKitties Terms of Use [online]. In: *CryptoKitties*. 15. 11. 2018. [cit. 22. 1. 2023] https://www.cryptokitties.co/terms-of-use

[18] CryptoPunks [online]. In: *larvalabs.com*. [cit. 26. 11. 2022]. Dostupné z: https://www.larvalabs.com/cryptopunks

[19] dm Múzy inspirace [online]. In: *dm-muzy.cz*. [cit. 17. 1. 2023]. Dostupné z: https://www.dm-muzy.cz/#buy-nft

[20] Gods Unchained Terms of Service [online]. In: *Gods Unchained*. 6. 9. 2021. [cit. 2. 2. 2023]. Dostupné z: https://godsunchained.com/terms/conditions

[21] GUADAMUZ, Andres., What Do You Buy When You Buy an NFT? [online]. In: *TechnoLlama*. 28. 3. 2021. [cit. 19. 11. 2022]. Dostupné z: https://www.technollama.co.uk/what-do-you-buy-when-you-buy-an-nft

[22] HAYWARD, Andrew. NFT Sales in 2022 Nearly Matched the 2021 Boom, Despite Market Crash [online]. In: *Decrypt*. 5. 1. 2023. [cit. 10. 3. 2023] Dostupné z: https://decrypt.co/118438/2022-versus-2021-nft-sales

[23] HOWCROFT, Elizabeth. NFT sales hit $25 billion in 2021, but growth shows signs of slowing [online]. In: *reuters.com*. 11. 1. 2022. [cit. 23. 10. 2022]. Dostupné z: https://www.reuters.com/markets/europe/nft-sales-hit-25-billion-2021-growth-shows-signs-slowing-2022-01-10/

[24] Illuvium Terms & Conditions [online]. In: *illuvium.io*. 28. 2. 2023. [cit. 20. 3. 2023]. Dostupné z: https://illuvium.io/terms-and-conditions

[25] JAROLÍM, Jaroslav. Investiční bublina – jak ji snadno rozpoznat a v čem spočívají rizika? [online]. In: *kryptomagazin.cz*. 31. 6. 2021. [cit. 22. 10. 2022]. Dostupné z: https://kryptomagazin.cz/investicni-bublina-jak-ji-snadno-rozpoznat-a-v-cem-spocivaji-rizika/

[26] Klublist [online]. In: *klublist.clubbingtv.com*. [cit. 15. 1. 2023]. Dostupné z: https://klublist.clubbingtv.com/

[27] KOOLEN, Christof, "Apes gone", but what about consumer protection? Applying EU consumer law to the transfer of NFTs [online]. In: *CCM Blog*. 17. 1. 2022. [cit. 20. 3. 2023] https://law.kuleuven.be/ccm/blog/?p=289

[28] LENNON CONNECTION: THE NFT COLLECTION [online]. [cit. 17. 1. 2023]. Dostupné z: https://www.juliensauctions.com/about-auction?id=400

[29] MATSUDA, Yosuke. A New Year's Letter from the President [online]. In: *SQUARE ENIX*. 1. 1. 2022. [cit. 22. 10. 2022]. Dostupné z: https://www.hd.square-enix.com/eng/news/2022/html/a_new_years_letter_from_the_president_2.html

[30] MDJ x Phillips: A Multi-Generational NFT [online]. In: *Phillips*. [cit. 20. 1. 2023] https://www.phillips.com/detail/mad-dog-jones/NY090121/1

[31] MetaCHORS Blocks [online]. In: *metachors.com*. [cit. 12. 1. 2023]. Dostupné z: https://www.metachors.com/

[32] NFT [online]. In: *alfaromeo.cz* [cit. 17. 1. 2023]. Dostupné z: https://www.alfaromeo.cz/modely/tonale#modal-gallery-software-popup

[33] Non-fungible tokens (NFT) [online]. In: *ethereum.org*. [cit. 17. 11. 2022]. Dostupné z: https://ethereum.org/en/nft/#how-nfts-work

[34] Prodejní podmínky aukcí NFT [online]. In: *Colt CZ Group*. [cit. 18. 1. 2023]. Dostupné z: https://auctionportal.coltczgroup.onblocktrust.com/Home/TnC/auction

[35] Reklamační řád při prodeji nezaměnitelných tokenů drogerie DM [online]. In: *dm-muzy.cz*. [cit. 12. 1. 2023]. Dostupné z: https://www.dm-muzy.cz/static/pdf/dm_NFT_reklamacni_rad.pdf

[36] REPLICATOR [online]. In: *maddogjones.com*. [cit. 20. 1. 2023] https://www.maddogjones.com/prints/1

[37] Terms and Conditions [online]. In: *Road2dreams NFT-platform*. [cit. 20. 1. 2023]. Dostupné z: https://assets.ctfassets.net/sca5putua729/38fWxlZ78gunAdsQaG8RwJ/596314bc9a258f5bfda4bb8e410b25f4/road2dreams_Terms_and_Conditions_Austria_EN.pdf

[38] The World's First Real Estate NFT [online]. In: *Propy*. [cit. 20. 1. 2023]. Dostupné z: https://propy.com/browse/propy-nft/

[39] Upozornění na rizika investic do alternativních investičních produktů (tokeny, participace) [online]. In: *Česká národní banka*. 3. 12. 2021. [cit. 14. 1. 2023]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/vykon-dohledu/upozorneni-pro-verejnost/Upozorneni-na-rizika-investic-do-alternativnich-investicnich-produktu-tokeny-participace/

[40] What is minting? [online]. In: *OpenSea Learn*. [cit. 17. 11. 2022]. Dostupné z: https://opensea.io/learn/what-is-minting-nft

6.3 PRÁVNÍ PŘEDPISY A DALŠÍ AKTY

[41] Důvodová zpráva k zákonu č. 374/2022 Sb., kterým se mění zákon č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů, a zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, č. 374/2022 Dz.

[42] Informace č. NB07/2022, bezpečnostní způsobilost. cit. z ASPI.

[43] Nařízení Evropského parlamentu a Rady (ES) č. 593/2008 ze dne 17. června 2008 o právu rozhodném pro smluvní závazkové vztahy

[44] 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

[45] Sdělení Komise Pokyny k výkladu a uplatňování směrnice Evropského parlamentu a Rady 2011/83/EU o právech spotřebitelů 2021/C 525/01. https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52021XC1229(04)

[46] Směrnice Evropského parlamentu a Rady (EU) 2019/2161 ze dne 27. listopadu 2019, kterou se mění směrnice Rady 93/13/EHS a směrnice Evropského parlamentu a Rady 98/6/ES, 2005/29/ES a 2011/83/EU, pokud jde o lepší vymáhání a modernizaci právních předpisů Unie na ochranu spotřebitele

[47] Směrnice Evropského parlamentu a Rady 2011/83/EU o právech spotřebitelů, kterou se mění směrnice Rady 93/13/EHS a směrnice Evropského parlamentu a Rady 1999/44/ES a zrušuje směrnice Rady 85/577/EHS a směrnice Evropského parlamentu a Rady 97/7/ES

[48] Směrnice Evropského parlamentu a Rady č. 2019/770, o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb

[49] Směrnice Evropského parlamentu a Rady č. 2019/771, o některých aspektech smluv o prodeji zboží

[50] Vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

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

[52] Zákon č. 256/2004 Sb., o podnikání na kapitálovém trhu, ve znění pozdějších předpisů

[53] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů

[54] Zákon č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů

[55] Zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

6.4 KOMENTÁŘOVÁ LITERATURA

[56] KOUKAL, Pavel. § 505 Základní vymezení součásti věci. In: LAVICKÝ, Petr a kol. *Občanský zákoník I. Obecná část (§ 1 – 654)*. Praha: C. H. Beck, 2014, s. 1559.

[57] SVOBODA, Karel. § 496 Věci hmotné a nehmotné. In: DAVID, Ondřej. a kol. *Občanský zákoník. Komentář. 1. vyd.* Praha: Wolters Kluwer, a. s., 2014. ISSN: 2336-517X.

[58] VONDRÁČEK, Ondřej. § 1837 Výjimky z práva odstoupit od smlouvy. In: PETROV, Jan. a kol. *Občanský zákoník. 2. vydání (1. aktualizace)*. Praha: C. H. Beck, 2022.

[59] VONDRÁČEK, Ondřej. § 1811 Předsmluvní informace. In: PETROV, Jan. a kol. *Občanský zákoník. 2. vydání (1. aktualizace)*. Praha: C. H. Beck, 2022.

[60] VONDRÁČEK, Ondřej. § 1820 Sdělení před uzavřením smlouvy. In: PETROV, Jan. a kol. *Občanský zákoník. 2. vydání (1. aktualizace)*. Praha: C. H. Beck, 2022.

[61] VONDRÁČEK, Ondřej. § 419 Definice spotřebitele. In: PETROV, Jan. a kol. *Občanský zákoník. 2. vydání (1. aktualizace)*. Praha: C. H. Beck, 2022.

6.5 ZÁVĚREČNÉ PRÁCE

[62] CHLUBNA, Filip. *Práva výkonných umělců a jejich ochrana ve sféře internetu a sociálních sítí*. Praha, 2022, diplomová práce, Univerzita Karlova, Právnická fakulta.

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 the 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 690:2011 citation standard.

Referencing examples are available in interpretations of the aforementioned citation standard (e. g. at www.ezdroje.muni.cz/prehled/zdroj.php?lang=en&id=441).

Individual sources are referenced in the text by upper index. The actual citation of the source is then contained in a footnote.

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.

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 14 | YEAR 2023 | NUMBER 28

Review of Law and Technology
Peer-reviewed scientific journal for technological areas of law and jurisprudence, listed in the List of non-impact peer-reviewed journals published in the Czech Republic and ERIH PLUS database.
Only the contributions submitted for the Discussion and Topic sections are peer-reviewed.
Published bi-annually. This issue was published on 31st December 2023.
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. Anna Blechová
Editorial Staff: JUDr. Mgr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek, Ph.D.
Editor: Mgr. Martin Erlebach
Editorial Board: prof. JUDr. Radim Polčák, Ph.D. (honorary chairman), JUDr. Zuzana Adamová, Ph.D., prof. JUDr. Michael Bogdan, B.A., LL.M., jur. dr. (Lund), JUDr. Marie Brejchová, LL.M., JUDr. Jiří Čermák, prof. JUDr. Bc. Tomáš Gřivna, Ph.D., doc. 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 Ptašnik, Ph.D., JUDr. Danuše Spáčilová, JUDr. Eduard Szattler, Ph.D., JUDr. Tomáš Ščerba, Ph.D.
Layout: Mgr. Martin Loučka, doc. JUDr. Matěj Myška, Ph.D.
Print: POINT CZ, s.r.o., Milady Horákové 20, 602 00 Brno
The publication of this issue of the Review of Law and Technology was funded by the project „Právo a technologie XI“, MUNI/A/1293/2022.

MUNI LAW

Ústav práva a technologií

děkuje svým partnerům za podporu v roce 2023

ROWAN LEGAL

ZÁKONY PRO LIDI

Wolters Kluwer

CODEXIS®

PRÁVNÍ PROSTOR

pwc

Diskuze

Norbert Halas: **Možnosti trestnej činnosti v metaverse**

Pavla Stanková: **Vyšetřování kybernetické kriminality a její předpokládaný budoucí vývoj**

Anotace

A. Blechová, K. Bónová, M. Erlebach, Š. Chvojka, A. Karpjáková, A. Krištofík, P. Loutocký, T. Mizerová, K. Mlčáková, J. Stojan, J. Vostoupal: **Přehled aktuální judikatury II/2023**

Essays

K. Dvořáček, H. C. Özdemir, J. Raše: **Essays II/2023**

Recenze závěrečných prací

L. Bohuslav, Z. Červínek, J. Chmelík, P. Kalenský, F. Kasl, P. Koukal, T. Křivka, P. Loutocký, J. Míšek, S. Pospíšilová, M. Šolc, J. Vostoupal: **Recenze závěrečných prací II/2023**

Recenze

Adam Jareš: **Lechner, T.: Nařízení eIDAS a české adaptační zákony. Recenze a úvaha o poměru elektronické identifikace a elektronických podpisů**

Téma

Jaroslav Konečný: **Non-fungible Tokens a ochrana spotřebitele**

MUNI PRESS