21

REVUE PRO PRÁVO A TECHNOLOGIE

Ústav práva a technologií Právnické fakulty Masarykovy univerzity

Ročník 11 / Rok 2020 / Číslo 21

Revue.law.muni.cz

XII. národní konference | 17. - 18. září 2020

České právo a informační technologie 2020

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

Konference bude rozdělena na plenární panelovou diskusi a jednání v šesti odborných sekcích. Pořadatel konference vyzývá zájemce o aktivní účast, aby hlásili své příspěvky do následujících odborných sekcí. Písemná vyhotovení příspěvků budou nabídnuta k publikaci v recenzovaném časopise Revue pro právo a technologie (revue.law.muni.cz)

Další informace na webu
cpit.law.muni.cz

KONFERENCE PROBĚHNE ONLINE

Program konference

Digitální služba
Moderuje Radim Polčák (ÚPT PrF MU)

1. Právní informatika
Moderuje Jakub Harašta (ÚPT PrF MU)

2. Transpozice směrnice o autorském právu na jednotném digitálním trhu
Moderuje Matěj Myška (ÚPT PrF MU)

3. (R)evoluce ochrany spotřebitele online
Moderuje Pavel Loutocký (CERIT-EU FI MU)

4. Oprávněný zájem ve zpracování osobních údajů
Moderuje Jakub Míšek (ÚPT PrF MU)

5. Kybernetická obrana a bezpečnost
Moderuje Ivana Kudláčková (ÚPT PrF MU)

6. Elektronické důkazy v trestním řízení
Moderuje Václav Stupka (CERIT-EU FI MU)

REVUE PRO PRÁVO A TECHNOLOGIE

Ročník 11 | Rok 2020 | Číslo 21

DISKUZE

Martin Eliášek, Jakub Kól, Miloš Švaňa: Automatická klasifikace významových celků v judikatuře 3

Adam Jareš: Kryptoměny a občanské právo 21

Ivana Kudláčková: Kybernetická zbraň: Přístupy k její definici 47

Pavel Mates: Právo na digitální služby 73

Rostislav Sliwka: Poskytovatel služeb sdílení obsahu online dle směrnice (EU) 790/2019 .. 91

Veronika Žolnerčíková: Prokazování příčinné souvislosti u škod způsobených propojenými autonomními vozidly 129

ANOTACE

Jaromír Fronc: Google, právo být zapomenut a Listina základních práv EU 153

Jakub Harašta: Nikdo nesmí vlastnit právo 161

D. Collett, F. Kasl, J. Klodwig, I. Kudláčková, P. Loutocký, J. Míšek, A. Stárková, J. Svoboda, P. Vydrová, V. Žolnerčíková: Přehled aktuální judikatury I/2020 169

RECENZE

Jan Svoboda: Michna, Lukáš. Programování pro právníky: Právníkův průvodce možnostmi, jak si se znalostí základů programování usnadnit práci a zpříjemnit život 195

Revue pro právo a technologie
Odborný recenzovaný časopis pro technologické obory práva a právní vědy zařazený na Seznamu recenzovaných neimpaktovaných periodik vydávaných v České republice a v databázi ERIH PLUS.
Recenzovány jsou příspěvky v sekci Diskuze a Téma.
Vychází dvakrát ročně. Toto číslo vyšlo 30. 6. 2020.
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. Matěj Myška, Ph.D., Ústav práva a technologií Právnické fakulty Masarykovy univerzity, Veveří 70, 611 80 Brno, ČR, tel: +420 549 494 751, fax: +420 541 210 604, e-mail: revue@law.muni.cz | www.revue.law.muni.cz
Zástupce šéfredaktora: Ing. Mgr. František Kasl
Redakce: JUDr. Mgr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek, Ph.D.
Tajemnice redakce: Anna Blechová
Editorka: Anna Blechová
Redakční rada: doc. 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, doc. 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., 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, 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 VIII“, MUNI/A/0989/2019.
Časopis © Masarykova univerzita, 2020

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 www.revue.law.muni.cz.

DOPORUČENÝ ROZSAH PŘÍSPĚVKŮ:

Sekce Téma:	30 – 80 normostran
Sekce Diskuze:	5 – 30 normostran
Sekce Anotace:	2 – 10 normostran
Sekce Recenze:	1 – 5 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 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: 31. března

Do zimního čísla: 30. září

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 www.revue.law.muni.cz resp. Vám je na vyžádání ráda sdělí redakce (kontaktní e-mail: revue@law.muni.cz).

https://doi.org/10.5817/RPT2020-1-1

AUTOMATICKÁ KLASIFIKACE VÝZNAMOVÝCH CELKŮ V JUDIKATUŘE

MARTIN ELIÁŠEK,[1] JAKUB KÓL,[2] MILOŠ ŠVAŇA[3]

ABSTRAKT

Příspěvek popisuje experiment se strojovým učením, kdy na minimálním datasetu bylo pomocí kombinace známých algoritmů strojového učení dosaženo relativně vysoké úspěšnosti klasifikace významových celků. Významovými celky se zde rozumí např. hlavička, procesní historie a argumentace stran.

KLÍČOVÁ SLOVA

judikatura, strojové učení, počítačové zpracování přirozeného jazyka

ABSTRACT

This paper describes a machine learning experiment that showed relatively high-fidelity classification of denotation segments on a minimal dataset using a combination of known machine learning algorithms. By denotation segments we mean segments such as header, proceeding history and party argumentation.

[1] Martin Eliášek vystudoval Právnickou fakultu Masarykovy univerzity a ve společnosti ATLAS Consulting spol. s r.o. působí na pozici právník-analytik, tj. podílí se na přípravě, kontrole a čištění dat v systému, e-mail: eliasek@atlasgroup.cz.

[2] Jakub Kól vystudoval aplikovanou informatiku na Univerzitě ve Hradci Králové a u společnosti ATLAS Consulting spol. s r.o. působí jako expert na strojové učení. Vedle počítačového zpracování přirozeného jazyka (natural language processing) se zabývá také počítačovým zpracováním obrazu (computer vision), e-mail: kol@atlasgroup.cz.

[3] Miloš Švana je softwarový inženýr s tituly z Technické univerzity v Ostravě a Vysokého učení technického v Brně, pro společnost ATLAS Consulting spol. s r.o. pracoval jako externista, e-mail: milos.svana@gmail.com.

KEYWORDS

case law, machine learning, natural language processing

1. ÚVOD

Právní profese se již mnoho let nedá vykonávat bez právních informačních systémů. Ačkoliv původně sloužily pouze k zobrazení aktuálního znění zákona, postupem času se jejich funkce rozšiřovaly a dnes je již nezbytnou součástí každého většího právního informačního systému také databáze judikatury.

Judikatura představuje ohromné množství dat, z velké části v podobě nestrukturovaného textu. Právní informační systém musí umět tento text uživateli nejen zobrazit, ale i v něm vyhledávat. Kromě fulltextového vyhledávání jde také o vyhledávání souvislostí, a to jak mezi právními předpisy a judikaturou, tak mezi judikáty navzájem.

Základním typem souvislosti mezi judikáty jsou citace. Na kvantitativní úrovni (např. počet citujících/citovaných judikátů) je lze pomocí moderních výpočetních prostředků relativně snadno analyzovat. Větší výzvu však představuje úroveň kvalitativní.

Jedním z potenciálních směrů kvalitativní analýzy je rozlišování citací podle jejich výskytu v různých částech soudních rozhodnutí. Díky tomu je pak možné rozlišovat jejich relativní hodnotu. Pokud je například judikát citován v popisu předchozího řízení, nemá takový význam, jako když na něj odkazuje ve své argumentaci strana sporu. Největší význam pak má pochopitelně judikatura citovaná v argumentaci samotného soudu.

Pro realizaci zmíněného typu analýzy je nutná segmentace soudních rozhodnutí na menší významové celky. Vzhledem k rozsáhlosti judikatury by manuální zpracování lidským expertem bylo časově náročné a neefektivní. V tomto příspěvku proto navrhujeme model pro automatické rozlišování významových částí soudních rozhodnutí založený na metodách strojového učení a zpracování přirozeného jazyka.

V následující části článku poskytneme přehled základních teoretických poznatků potřebných pro pochopení prezentovaných metod. V třetí části

popíšeme vstupní data použitá pro trénování a verifikaci navrženého modelu. Samotnému modelu se pak věnuje část čtvrtá. V části páté analyzujeme výsledky testování a kvalitu modelu. V závěru pak načrtneme potenciální využití námi navrženého modelu v praxi a další směry vývoje.

2. PŘEHLED TEORETICKÝCH POZNATKŮ A PŘEDCHOZÍHO VÝZKUMU

2.1 STROJOVÉ UČENÍ A KLASIFIKACE

Strojové učení je v současnosti jednou z nejperspektivnějších oblastí studia umělé inteligence. Jeho základní myšlenka spočívá ve snaze nahradit při tvorbě algoritmů pro zpracování dat programátora automatickým učením. Strojové učení se ve značné míře aplikuje například při vyhledávání obrázků nebo strojovém překladu.

V úvodu zmíněný problém automatické segmentace soudních rozhodnutí představuje typický úkol řešený pomocí strojového učení. Klasifikaci lze definovat jako zařazení určité entity do některé z konečného počtu předem definovaných tříd nebo kategorií. Aby bylo možné entity klasifikovat pomocí počítačových programů, musí být popsané pomocí číselných hodnot jejích atributů.

Příklad 1: Příkladem klasifikace, kterým začíná mnoho učebnic věnovaných strojovému učení, je zařazení konkrétního květu kosatce do jednoho ze tří poddruhů této rostliny – iris setosa, iris versicolor a iris virginica. Tyto poddruhy reprezentují třídy nebo kategorie. Jako číselné atributy pro popis každého květu použijeme délku kališního lístku, šířku kališního lístku, délku okvětního lístku a šířku okvětního lístku. Všechny hodnoty budou uvedeny v centimetrech. Konkrétní květ pak můžeme reprezentovat posloupností naměřených číselných hodnot zmíněných atributů, např: (5.1 3.5 1.4 0.2). V terminologii matematiky se tato posloupnost nazývá vektor. Jelikož se tento vektor skládá ze 4 čísel, můžeme ho označit jako čtyřdimenzionální.

Aby se počítač mohl naučit, jak automaticky klasifikovat určitou skupinu objektů, musíme mu poskytnout tzv. trénovací množinu. Tato

množina se skládá z entit, resp. jejich opisu pomocí daných číselných atributů - tj. vektorů, pro které již známe zařazení do konkrétní třídy.

Příklad 2: Trénovací množina pro klasifikaci květů z příkladu 1 může mít podobu tabulky s pěti sloupci: délka kališního lístku, šířka kališního lístku, délka okvětního lístku, šířka okvětního lístku a ručně (odborníkem) identifikovaný poddruh. Řádky této tabulky pak budou reprezentovat konkrétní květy – naměřenou hodnotu všech atributů a třídu, do které skutečně patří.

Počítačové algoritmy strojového učení se z trénovací množiny dokáží „naučit“ jak klasifikovat entity stejného typu, které předtím „neviděly“ (nejsou součástí trénovací množiny). Jedním z úkolů vědců v oblastí strojového učení je navrhování těchto algoritmů. Za roky výzkumu jich přitom bylo vytvořeno hned několik. Podrobný popis všech existujících možností je nad rámec tohoto článku. Zaměříme se proto jen na algoritmus *Support Vector Machine*, který je součástí navrhovaného přístupu pro automatickou klasifikaci soudních rozhodnutí. V případě zájmu o seznámení se s dalšími často používanými alternativami se čtenář může obrátit např. na Hana, Kambera a Peie[4] nebo Raschku[5].

2.2 ALGORITMUS SUPPORT VECTOR MACHINE

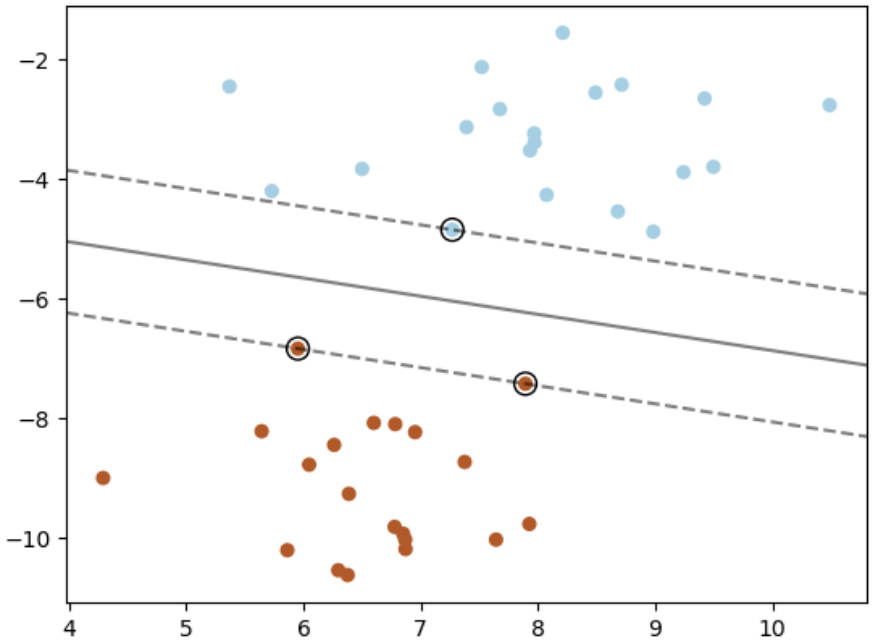
Support Vector Machine, zkráceně SVM je jedním z algoritmů používaných pro automatické trénování klasifikátorů pomocí dat z trénovací množiny. V jeho základní podobě se jedná o tzv. lineární klasifikátor, tj. hledá hranici mezi třídami v podobě přímky a je omezený na rozlišování mezi dvěma třídami.

Kdybychom pro popis entit v trénovací množině použili pouze 2 číselné atributy, pak je možné každou entitu zobrazit jako bod na grafu. Úkolem algoritmu SVM je najít přímku, která co nejlépe od sebe odděluje 2 třídy trénovací množiny. Za nejlepší je přitom považovaná přímka

[4] HAN, Jiawei, Micheline KAMBER a Jian PEI. *Data Mining: Concepts and Techniques*. Third Edition. Waltham: Elsevier, 2011. ISBN 978-0-12-381479-1.

[5] RASCHKA, Sebastian. *Python Machine Learning*. Birmingham: Packt, 2015. ISBN 978-1-78355-513-0.

maximalizující velikost prázdného prostoru neobsahujícího žádné body na jejích obou stranách.



Obrázek 1: Ilustrace principu Support Vector Machine.

Výše popsaný princip je ilustrovaný na obrázku 1. Osy grafu reprezentují určité číselné atributy. Lze si zde například představit, že vodorovná osa značí rychlost větru v km/h a osa svislá teplotu v °C. Jednotlivé body reprezentují vektory reálně naměřených hodnot z trénovací množiny, přičemž body zabarvené červeně jsou naměřené v zimě a body zabarvené modře na podzim. Klasifikátor má tedy rozpoznávat mezi těmito dvěma ročními obdobími. Nepřerušovaně je vyznačená přímka, kterou algoritmus SVM identifikoval jako nejlepší. Přerušovaně je pak ohraničen prázdný prostor na obou stranách přímky. Body ležící přesně na těchto hranicích se nazývají podpůrné vektory (angl. *support vectors)*.

Po tom, co SVM nalezne přímku oddělující obě třídy, je už klasifikace období podle naměřené teploty a rychlosti větru poměrně jednoduchá. Graficky by stačilo nové měření zobrazit jako bod na grafu a určit, jestli se nachází nad nebo pod dělící přímkou.

Při praktické aplikaci SVM lze narazit hned na několik značných komplikací. Jednou z nich je fakt, že existuje mnoho klasifikačních úloh, kdy potřebujeme rozlišit mezi více než dvěma třídami. Tato situace se běžně řeší tím, že se natrénuje několik samostatných SVM klasifikátorů, které pak mezi sebou „hlasují“, do které třídy bude nová neznámá entita zařazená.

Druhým problémem je, že situace, kdy lze body tříd od sebe oddělit dokonale jako na obrázku 1, jsou v praxi pouze ojedinělé. Proto se při reálném tréningu připouští možnost, že několik bodů dané třídy se může nacházet na opačné straně přímky.

SVM dokáže obecně pracovat s více než dvěma číselnými atributy opisujících klasifikované entity (tedy s více než dvoudimenzionálními vektory). Tuto situaci už nelze jednoduše vizualizovat, ale matematické vzorce pracující s dvěma dimenzemi fungují i pro stovky dimenzí.

2.3 KLASIFIKACE TEXTOVÝCH DAT

Jak bylo zmíněno výše, klasifikační algoritmy očekávají, že všechny objekty budou reprezentovány jako vektory, tedy posloupnosti číselných hodnot. Jedním z nejtěžších úkolů v rámci klasifikace textových dat je tedy nalezení vhodné číselné reprezentace textu. Mnoho autorů a vědců se specializuje pouze na řešení tohoto problému. Nejpoužívanější přístupy shrnuje např. Aggarwal a Zhai [6].

Relativně intuitivní způsob číselné reprezentace textu je pomocí rodiny metod známých jako *Bag of Words*. Textový dokument, odstavec nebo věta je reprezentovaná posloupností čísel, kde každá pozice zastupuje určené slovo. V nejjednodušším případě pak konkrétní pozice může mít hodnotu 1, pokud se dané slovo v dokumentu nachází, nebo 0, pokud tomu tak není.

[6] AGGARWAL, Charu C. a ChengXiang ZHAI. *Mining text data*. New York: Springer, 2012. ISBN 978-1-4614-3222-7.

Alternativně můžeme místo hodnot 0 a 1 použít přesný počet výskytů daného slova v dokumentu.

Příklad 3: Pomocí Bag of Words chceme vytvořit číselnou reprezentaci následujících vět: „Dnes svítí slunce.“ a „Dnes neprší ani nefouká“. Prvním krokem je vytvoření seznamu všech unikátních slov. V tomto případě se jedná o slova „dnes“, „svítí“, „slunce“, „neprší“, „ani“, „nefouká“. Následně stačí zjistit, zda se dané slovo v konkrétní větě nachází, a správně na danou pozici v číselném vektoru zadat hodnotu 0 nebo 1, jak ilustruje tabulka 1.

	dnes	svítí	slunce	neprší	ani	nefouká
Věta 1	1	1	1	0	0	0
Věta 2	1	0	0	1	1	1

Tabulka 1: Ukázka reprezentace textu pomocí Bag of Words

První větu je tedy možné reprezentovat vektorem čísel (1 1 1 0 0 0), větu druhou pak vektorem (1 0 0 1 1 1).

S metodami *Bag of Words* jsou spojené dvě zásadní nevýhody: (a) Běžně se od klasifikačních algoritmů očekává zpracování i tisíců dokumentů. Tyto dokumenty obsahují velké množství unikátních slov, což vede k tomu, že vektory reprezentující text mají řádově i desetitisíce dimenzí. Většina hodnot v těchto vektorech je přitom 0 (jedná se o tzv. *řídké* vektory). Zpracování takového množství dat je výpočtově náročné. (b) Reprezentace pomocí *Bag of Words* ignoruje jak pořadí slov v dokumentu, tak i jejich sémantiku (význam). Tyto prvky mohou být pro přesnou automatickou klasifikaci nápomocné, často dokonce nezbytné.

2.4 EMBEDDINGS

Kvůli výše zmíněným nevýhodám je dnes *Bag of Words* přístup postupně nahrazovaný tzv. *embeddings*. Podobně jako v případě *Bag of Words* i *embeddings* reprezentují text ve formě vektorů. Na rozdíl od *Bag of Words* jsou ale tyto vektory o mnoho menší – k popsání textu je zpravidla

potřebných jen několik set čísel. Tyto vektory jsou *husté* – většina, ne-li všechny hodnoty v nich jsou nenulové.

Embeddings se dají použít pro reprezentaci libovolných textových dokumentů, ale jejich primárním cílem je reprezentace jednotlivých slov. Zde se projevuje jejich největší výhoda, a sice schopnost do určité míry zachytit sémantiku (význam). Slova s podobným významem jsou reprezentována vektory, ve kterých se jednotlivé číselné hodnoty od sebe liší jen málo. Se slovy reprezentovanými pomocí *embeddings* je navíc možné manipulovat pomocí základních operací jako sčítání a odečítání.

Příklad 4: Pokud od reprezentace slova „král“ pomocí embeddings odečteme reprezentaci slova „muž“ a přičteme slovo „žena“, měl by výsledný vektor být velice podobný reprezentaci slova „královna“. Sčítaní a odčítaní vektorů přitom spočívá ve sčítaní a odčítaní hodnot na jednotlivých pozicích. Po sečtení třídimenzionálních vektorů (5 1 8) a (2 4 1) tedy získáme vektor (7 5 9).

Jednou z nevýhod *embeddings* je, že je problematické interpretovat, co jednotlivé číselné hodnoty ve vektorech znamenají. Vytvoření *embedding* reprezentace slova se nedá realizovat pomocí předem daného postupu, jak je tomu u *Bag of Words*. Tento problém se proto sám o sobě řeší pomocí metod strojového učení.

Jedním z nejpoužívanějších přístupů ke tvorbě *embeddings* je *Word2Vec*.[7] Je založený na myšlence, že slova s podobným významem se vyskytují v podobném kontextu, tj. v jejich okolí v textu se opakují podobná slova. Pro nalezení embeddings je nutné disponovat rozsáhlou množinou textových dokumentů. V praxi se například využívá archiv Wikipedie. Pomocí metod strojového učení se pak trénuje matematický model, schopný predikovat slovo podle slov nacházejících se v jeho okolí. Alternativně je možné použít i opačný přístup, tedy predikci několika okolních slov pro dané vstupní slovo. *Embeddings* jsou pak vedlejším produktem řešení tohoto problému. Typicky se používají Word2Vec

[7] MIKOLOV, Tomáš, Kai CHEN, Greg CORRADO a Jefrey DEAN. *Efficient Estimation of Word Representations in Vector Space.* CoRR, 2013. Dostupné z: https://arxiv.org/abs/1301.3781

embeddings s 300 dimenzemi – slovo je tedy reprezentováno jako posloupnost 300 čísel.

Word2Vec byl později původními autory použit jako základ metody *Doc2Vec*[8], která, jak název napovídá, vytváří *embeddings* pro libovolné textové dokumenty (věty, odstavce, celé texty). Je založená na jednoduché agregaci *Word2Vec embeddings* jednotlivých slov v dokumentu, tj. počítaní sumy nebo průměrné hodnoty. Zachovává se přitom dimensionalita: pokud *Word2Vec embeddings* pro reprezentaci jednotlivých slov v dokumentu měli 300 dimenzí, pak i *Doc2Vec embedding* reprezentující dokument jako celek bude mít 300 dimenzí.

2.5 SEGMENTACE SOUDNÍCH ROZHODNUTÍ V ČEŠTINĚ

Samotnému problému segmentace soudních rozhodnutí v českém jazyce na menší významové celky se věnuje Harašta[9], jehož přístup je založený na predikci pomocí *conditional random fields.* Pro trénování a verifikaci přitom využívá rozhodnutí pouze nejvyšších soudních instancí.

3. DATASET

Dokumenty pro trénování a verifikaci modelu byly vybrány z databáze právního informačního systému Codexis. Z nejnovějších 15 tisíc soudních rozhodnutí bylo náhodně zvoleno 260 tak, aby vzorek věrohodně reprezentoval obsah databáze. Tabulka 2 zobrazuje počty ve výběru podle typu soudní instance.

Typ instance	**Počet rozhodnutí**	**Podíl na datasetu**
Nejvyšší soud	89	34.23 %

[8] MIKOLOV, Tomáš a Quoc V. LE. *Distributed Representations of Sentences and Documents.* CoRR, 2014. Dostupné z: https://arxiv.org/abs/1405.4053

[9] HARAŠTA, Jakub, Jaromír ŠAVELKA, František KASL a Jakub MÍŠEK. Automatic Segmentation of Czech Court Decisions into Multi-Paragraph Parts. *Jusletter IT*. Weblaw AG, 2019, roč. 4, 23. Mai 2019, s. 1-10. ISSN 1664-848X. Dostupné z: https://www.muni.cz/en/research/publications/1534440

Ústavní soud	51	19.62 %
Krajské soudy	50	19.23 %
Nejvyšší správní soud	43	16.54 %
Vrchní soudy	14	5.38 %
Městský soud v Praze	10	3.85 %
Okresní a obvodní soudy	2	0.77 %
Zvláštní senát NS a NSS	1	0.38 %

Tabulka č. 2: Dokumenty v trénovací/verifikační množině podle typu soudní instance

Soudní rozhodnutí byla následně ručně anotovaná pomocí nástroje *Dataturks.*[10] Anotace proběhla dvoufázově, kdy určité části dokumentů byly označovány jako *Ostatní* a po anotaci celého korpusu anotátor tyto segmenty analyzoval podrobněji a zařadil je do nejbližší podobné třídy nebo ponechal odstavec bez anotace. Neoznačené tak zůstaly např. informace o tom, že veškerou citovanou judikaturu lze nalézt na určitém URL.

3.1 TŘÍDY

Každý anotovaný odstavec je přiřazený do jedné z následujících významových tříd:

1. **Hlavička** - Identifikace soudu, stran a zpravidla i napadeného rozhodnutí
2. **Výrok** - Rozhodnutí soudu

[10] Dostupný na: https://dataturks.com/

3. **Věcná historie** - Skutková zjištění
4. **Procesní historie** - Popis předcházejícího řízení, včetně argumentace stran a soudů uplatněných v těchto řízeních; zahrnuje i předchozí správní řízení
5. **Argumentace stran** - Argumenty, námitky a návrhy stran (vč. konstatování, že se někdo nevyjádřil nebo že nemá námitky)
6. **Argumentace soudu** - Prakticky zbytková kategorie, zahrnuje mj. i citace aplikovatelných zákonných ustanovení, popis procesního postupu rozhodujícího soudu nebo obiter dictum
7. **Závěr** - Závěrečné shrnutí argumentace soudu (např. "Z těchto důvodů soud … zamítl/odmítl/zrušil.") obsahuje také instrukce pro soud nižší instance, pokud se věc vrací
8. **Náklady** - Odůvodnění rozhodnutí o nákladech řízení, jakož i informace, že o nákladech řízení nebude rozhodnuto nebo že nebudou odůvodněny
9. **Poučení** - Formální poučení soudu, nadepsáno slovem Poučení

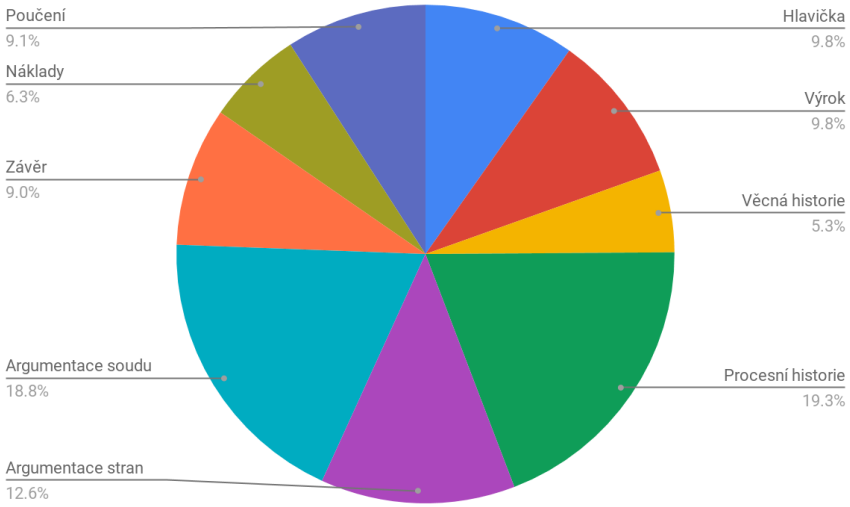
Uvedená taxonomie byla založená na metodice Harašty[11] avšak s několika podstatnými rozdíly. Z původní třídy *Hlavička* se vyčlenila třída *Výrok*, neboť toto rozdělení považujeme za praktické pro další zpracování soudních rozhodnutí (např. detekce opravných prostředků nebo formátování textu). Byla zavedena třída *Věcná historie*, neboť součástí datasetu jsou i prvoinstanční rozhodnutí. Třída *Patička* byla rozdělena na třídy *Náklady* a *Poučení*. Dále byla zavedena třída *Závěr*, kterou lze považovat za poměrně experimentální, protože segmenty do ní patřící byly v první fázi anotace označeny jako *Ostatní*. Dataset neobsahuje žádné poznámky pod čarou ani disenty.

Z časových důvodů byly položky třídy *Argumentace soudu* anotované zpravidla jako úsek od počátku soudní argumentace až po její závěr. V argumentaci soudu se někdy opakují skutková zjištění, rekapituluje se

[11] HARAŠTA, Jakub, Jaromír ŠAVELKA, František KASL a Jakub MÍŠEK. Automatic Segmentation of Czech Court Decisions into Multi-Paragraph Parts. *Jusletter IT*. Weblaw AG, 2019, roč. 4, 23. Mai 2019, s. 1-10. ISSN 1664-848X. Dostupné z: https://www.muni.cz/en/research/publications/1534440

procesní historie a argumentace stran, ale pro potřeby klasifikace judikatorních odkazů je toto rozlišení bezpředmětné, jelikož ke všem judikátům citovaným v této pasáži se soud nějakým způsobem vyjadřuje. Takto prováděná anotace judikátu byla mnohem rychlejší, než kdyby anotátor pročítal a anotoval každý odstavec soudní argumentace zvlášť. Zvolený postup však mohl mít negativní dopad na kvalitu natrénovaného modelu.

Celkem bylo anotováno 2684 odstavců. Podíl jednotlivých tříd je možné vidět na obrázku č. 2. Nejvíce jsou zastoupeny třídy *Procesní historie* a *Argumentace soudu*, nejméně naopak třídy *Věcná historie* a *Náklady*.



Obr. č. 2: Podíl jednotlivých významových tříd na celkovém počtu anotovaných odstavců.

4. MODEL PRO AUTOMATICKOU SEGMENTACI SOUDNÍCH ROZHODNUTÍ

Řešený problém automatické segmentace soudních rozhodnutí chápeme jako klasifikační úlohu, tedy zařazení jednotlivých odstavců jedné z předem stanovených tříd. Většina algoritmů pro automatickou klasifikaci dokáže

pracovat pouze s číselnými daty (viz teoretická část). Navržené řešení je proto nutné rozdělit do dvou po sobě následujících kroků: (1) převod odstavců do číselné reprezentace a (2) natrénovaní modelu pro automatickou klasifikaci.

K vytvoření numerické reprezentace textu je použitá metoda Doc2Vec, která je detailněji popsána v sekci 2.4. K natrénování byl přitom použitý korpus 364 199 soudních dokumentů z databáze Codexis obsahujících celkem 8 932 074 odstavců, přičemž dimensionalita výsledných vektorů byla nastavena na standardní hodnotu 300.

Doc2Vec vektory jsou dále rozšířeny o informaci o pozici klasifikovaného odstavce v soudním rozhodnutí složené z:

1. relativní pozice prvního znaku odstavce v dokumentu (kolik procent dokumentu se nachází před odstavcem),
2. relativní pozice posledního znaku odstavce v dokumentu (kolik procent dokumentu se nachází za odstavcem),
3. relativní délky odstavce (kolik procent dokumentu je tvořeno daným odstavcem).

Každý odstavec je tedy reprezentován jako 303dimenzionální vektor. Mimochodem, na základě vypočtených ANOVA F-hodnot lze konstatovat, že atributy pozice jsou pro rozlišení jednotlivých tříd odstavců nejdůležitější. Není to překvapivé, jelikož některé části rozhodnutí jsou typicky na začátku či konci odůvodnění, a existuje určitá neformálně ustálená struktura soudních rozhodnutí, kdy nejdříve se popíše procesní historie a až poté se uvádí argumenty stran, a nakonec argumenty samotného soudu.

Číselné reprezentace odstavců jsou následně použity jako vstup pro druhou fázi, tedy trénování modelu pro automatickou klasifikaci. Pro tuto část byl zvolen algoritmus SVM, detailně popsaný v sekci 2.2.

5. METODOLOGIE TESTOVÁNÍ NAVRŽENÉHO MODELU

Celý průběh experimentu lze rozdělit do následujících kroků:

1. Vytvoření trénovacího datasetu (viz část třetí)

2. Natrénování modelu pro převod textu do číselné reprezentace metodou Doc2Vec
3. Převod anotovaných odstavců z kroku 1 do číselné reprezentace pomocí modelu z kroku 2
4. Natrénování SVM klasifikátoru
5. Testování klasifikátoru na neznámých datech

Je nutno zdůraznit, že Doc2Vec model byl natrénován pomocí rozsáhlé databáze programu Codexis, přičemž nebyla vyžadována žádná ruční anotace. Až trénování SVM klasifikátoru využilo anotaci dokumentů k sestavení trénovací množiny.

5.1 POUŽITÝ HARDWARE

Celý experiment byl realizovaný na serveru vybaveném procesorem AMD Ryzen 7 2700X, 64 GB DDR4 RAM, 250 GB NVMe SSD úložištěm a dvěma grafickými kartami Nvidia RTX 2080Ti. Na serveru byl nainstalovaný operační systém Ubuntu 18.04.

5.2 POUŽITÝ SOFTWARE

Implementace navrženého modelu je realizována pomocí standardních knihoven pro strojové učení v programovacím jazyce Python. Pro implementaci Doc2Vec modelu byla použita knihovna *gensim* a pro samotnou klasifikaci a verifikaci knihovna *scikit-learn*[12]. Experimenty byly spuštěné v prostředí Jupyter umožňující interaktivní práci se zdrojovým kódem v jazyce Python, R nebo Julia, snadnou replikaci a sdílení experimentů.

6. VÝSLEDKY EXPERIMENTŮ

Výše popsaný model byl vyhodnocen pomocí metody *7-fold cross-validation.* Při použití této metody je trénovací dataset rozdělený na 7 částí, přičemž 6 z nich je použito pro trénování klasifikátoru a 1 slouží pro vyhodnocení jeho kvality. Trénování a vyhodnocení se přitom opakuje sedumkrát[13], přičemž pro vyhodnocení kvality je vždy použitá jiná část datasetu.

[12] Dostupná na https://scikit-learn.org/stable/

V rámci vyhodnocení byly sledované následující parametry:

1. precision – kolik (podíl) ze vzorků algoritmem zařazených do dané třídy do ní skutečně patří
2. recall – kolik (podíl) ze vzorků skutečně patřících do dané třídy bylo algoritmem do této třídy zařazeno
3. f1-score – interpretovatelné jako vážený průměr precision a recall.

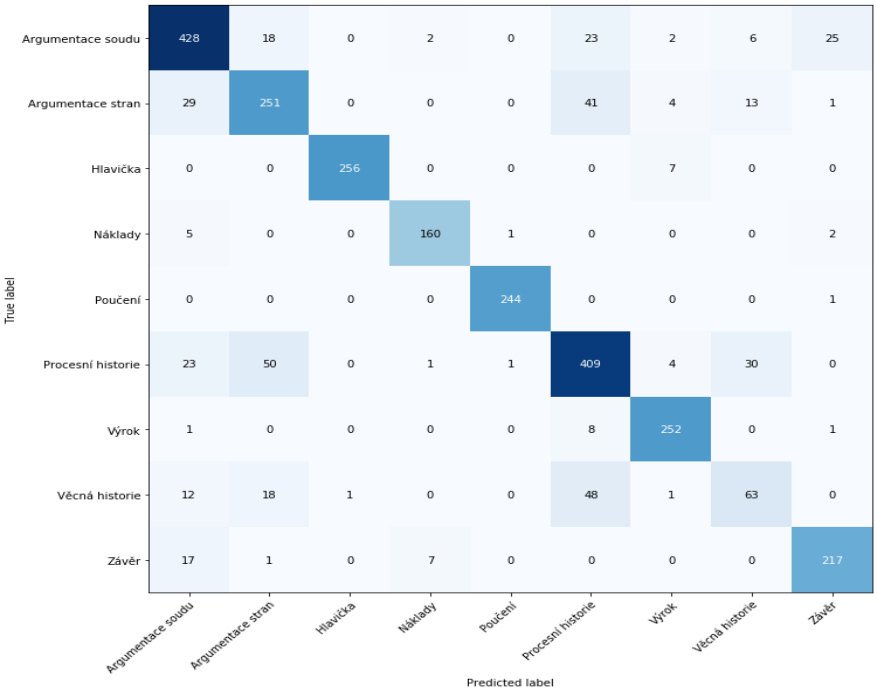
Výsledky modelu jsou porovnány s výsledky *Zero Rule* klasifikátoru, který každý vzorek jednoduše zařadí do nejpočetnější třídy v trénovacím datasetu, a s výsledky stratifikovaného náhodného třídění, které každému vzorku přidělí náhodnou třídu, přičemž je respektována distribuce tříd v trénovacím datasetu.

	Zero Rule			**Stratif. náhodné třídění**			**Doc2Vec + SVM**		
	prec.	recall	f1	prec.	recall	f1	prec.	recall	f1
Argumentace soudu	0.00	0.00	0.00	0.23	0.23	0.23	0.83	0.85	0.84
Argumentace stran	0.00	0.00	0.00	0.11	0.11	0.11	0.74	0.74	0.74
Hlavička	0.00	0.00	0.00	0.11	0.11	0.11	1.00	0.97	0.99
Náklady	0.00	0.00	0.00	0.07	0.08	0.08	0.94	0.95	0.95
Poučení	0.00	0.00	0.00	0.15	0.16	0.15	0.99	1.00	0.99
Procesní historie	0.19	1.00	0.32	0.21	0.20	0.20	0.77	0.79	0.78
Výrok	0.00	0.00	0.00	0.12	0.12	0.12	0.93	0.96	0.95
Věcná historie	0.00	0.00	0.00	0.04	0.04	0.04	0.56	0.44	0.49

[13] Mezi jednotlivými průchody klasifikátor již naučené "zapomene". Netestují se naučená data, ale schopnost algoritmu se učit.

Závěr	0.00	0.00	0.00	0.12	0.11	0.12	0.87	0.90	0.89
Celková Přesnost	0.193			0.145			0.850		

Tabulka č. 3: Průměrné hodnoty vypočtené z jednotlivých testovacích měření v rámci cross-validace



Obr. č. 3: Matice záměn (confusion matrix) ukazující anotované třídy (vlevo) a klasifikované třídy (dole)

Výslednou přesnost 85 % považujeme za více než dostačující, protože klasifikace odstavců do daných tříd není vždy jednoduchý úkol. U některých tříd navíc k omylům prakticky nedochází, a to i při natrénování na velmi malém datasetu.

Nejproblematičtější třídou je Věcná historie. Odstavce patřící do této kategorie klasifikátor na rozdíl od jejich anotace označuje jako Procesní historii, Argumentaci stran nebo Argumentaci soudu. Je tomu jednak proto, že tato třída má v trénovací množině nejmenší počet vzorků, ale především proto, že skutková tvrzení jsou běžnou součástí jak Procesní historie, tak Argumentace. Pokud bychom klasifikovali jednotlivé věty, bylo by možné oddělit skutková tvrzení od procesních a právních, ale jelikož byly klasifikovány celé odstavce, jde o záležitost krajně neřešitelnou.

Ze stejného důvodu Procesní historie prorůstá do Argumentace stran a soudu. Je pochopitelné, že ve svojí argumentaci se strany i soud velmi často odkazují na proběhnuvší řízení. Zde navíc dost záleží na tom, v jakém řízení bylo rozhodnutí vydáno, protože odstavec "Proti rozhodnutí se žalovaný odvolal z důvodu ..." může být procesní historií u Ústavního a Nejvyššího soudu, ale Argumentací stran u krajského či vrchního soudu. Když k tomu přičteme neduh, že soudy o sobě často mluví ve třetí osobě (slovy "Krajský soud shledal žalobu nedůvodnou" může začínat Argumentace soudu vydaná krajským soudem, nebo může jít o popis předchozího řízení), jsou jednotlivé odstavce bez znalosti procesního práva reálně neklasifikovatelné.

6.1 MODIFIKACE MODELU

Kromě modelu popsaného v předchozích sekcích byly testovány i jeho další modifikace. Zkoušeno bylo například použití vyššího počtu dimenzí u Doc2Vec vektoru nebo zahrnutí Doc2Vec vektoru předchozího odstavce do popisu odstavce aktuálního. Tyto změny však nepřinesly žádné výrazné zlepšení.

V rámci fáze klasifikace byly testovány další metody běžně doporučované pro klasifikaci textu: rozhodovací stromy, *random forests,* jednoduché neuronové sítě nebo SVM s polynomiálním a *radial basis function* kernelem. S výjimkou neuronových sítí ale tyto varianty dosahovaly výrazně horších výsledků. Přesnost dosažená neuronovou sítí byla se zvoleným lineárním SVM klasifikátorem porovnatelná, nedostatkem ale byla delší doba potřebná pro trénování modelu.

7. ZÁVĚR

Prezentovaný model pro automatickou klasifikaci významových celků v soudních rozhodnutích dosahuje uspokojivých výsledků. Především při početnějších třídách lze pozorovat výrazné zlepšení oproti algoritmu navrženém Haraštou et al. (2019). Jak bylo zmíněno v úvodu, model bude dále použit pro klasifikaci judikatorních citací. Pro sofistikovanější využití se může jako vhodnější alternativa ukázat tzv. měkká klasifikace, při které model místo predikce konkrétní třídy určí pravděpodobnost zařazení do jednotlivých tříd. Vzhledem k použitým nástrojům a knihovnám toto rozšíření vyžaduje jen triviální úpravy zdrojového kódu.

Perspektivním směrem dalšího výzkumu je využití metod hlubokého učení *(deep learning)*, např. konvolučních nebo rekurentních neuronových sítí. Pro jejich trénování je ale nutné podstatně rozšířit dataset anotovaných částí soudních rozhodnutí.

8. SEZNAM POUŽITÝCH ZDROJŮ

[1] AGGARWAL, Charu C. a ChengXiang ZHAI. *Mining text data.* New York: Springer, 2012. ISBN 978-1-4614-3222-7.

[2] HAN, Jiawei, Micheline KAMBER a Jian PEI. *Data Mining: Concepts and Techniques.* Third Edition. Waltham: Elsevier, 2011. ISBN 978-0-12-381479-1.

[3] HARAŠTA, Jakub, Jaromír ŠAVELKA, František KASL a Jakub MÍŠEK. Automatic Segmentation of Czech Court Decisions into Multi-Paragraph Parts. *Jusletter IT*. Weblaw AG, 2019, roč. 4, 23. Mai 2019, s. 1-10. ISSN 1664-848X. Dostupné z: https://www.muni.cz/en/research/publications/1534440

[4] MIKOLOV, Tomáš, Kai CHEN, Greg CORRADO a Jefrey DEAN. *Efficient Estimation of Word Representations in Vector Space.* CoRR, 2013. Dostupné z: https://arxiv.org/abs/1301.3781

[5] MIKOLOV, Tomáš a Quoc V. LE. *Distributed Representations of Sentences and Documents*. CoRR, 2014. Dostupné z: https://arxiv.org/abs/1405.4053

[6] RASCHKA, Sebastian. *Python Machine Learning.* Birmingham: Packt, 2015. ISBN 978-1-78355-513-0.

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

https://doi.org/10.5817/RPT2020-1-2

KRYPTOMĚNY A OBČANSKÉ PRÁVO

ADAM JAREŠ[1]

ABSTRAKT

Kryptoměny nejsou v současné chvíli v oblasti soukromého práva jakkoliv výslovně upraveny a jejich regulaci je možné nalézt pouze ve veřejnoprávních předpisech. Cílem textu je posouzení, jakým způsobem na kryptoměny nahlíží občanský zákoník, jaké právní vztahy vznikají při zápisu transakce do nového bloku v rámci protokolu blockchain a zda lze považovat kryptoměny za věc ve smyslu její legální definice v občanském zákoníku. Text se následně věnuje diskuzi o důsledcích dosažených závěrů.

KLÍČOVÁ SLOVA

blockchain, kryptoměny, bitcoin, občanský zákoník, věc v právním smyslu, nabídka a akceptace, transakce

ABSTRACT

Cryptocurrencies are not currently regulated by civil law and it is possible to find their regulation only in public law. The main aim of this text is to examine how the Civil Code can deal with cryptocurrencies, what legal relationships arise when a transaction is included into a new block within a blockchain protocol, and whether cryptocurrencies could be regarded as a "thing" in a legal sense within the meaning of its legal definition in the Civil Code. Text then focuses on a discussion about consequences of the author's conclusions.

[1] Mgr. Adam Jareš, doktorand katedry občanského práva Fakulty právnické ZČU, kontaktní e-mail: ajares@kpo.zcu.cz

KEYWORDS

blockchain, cryptocurrencies, bitcoin, civil code, thing in a legal sense, offer and acceptance, transactions

1. ÚVOD

Vývoj v oblasti elektronické kontraktace a transakcí je dotčen fenoménem virtualizace, který se ostatně projevuje v celém oboru práva informačních technologií.[2] Jeho projevem je také protokol blockchain, jehož prostřednictvím jsou provozovány kryptoměny jako určitá alternativa k tzv. fiat měnám, tedy měnám s nuceným oběhem. Jejich fungování má nejen technologické a ekonomické konotace, ale i ty právní, kterým je věnován tento text, jenž na kryptoměny nahlíží optikou zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „obč. zák.“).

Důkazem toho, že se kryptoměny skutečně dostávají do zájmu širší veřejnosti, může být i skutečnost, že se jim postupně dostává pozornosti i v textech, které nejsou určeny pouze technologickým nadšencům či investorům a spekulantům. Příkladem může být článek Deníku N, který se věnuje desetiletému výročí kryptoměny bitcoin. Ten začíná následujícím textem: *„Potíž s bitcoinem spočívá v tom, že to není věc, ale příběh. Není to vlastně technický ani ekonomický fenomén, jeho popis a vysvětlení spadá mnohem víc do sociologie a psychologie.“*[3] Pro jeho účely je tento závěr platný. Předkládaný text si ale za cíl klade posouzení kryptoměn a kryptoměnových peněženek z pohledu občanského práva – klasifikovat je jako věc ve smyslu obč. zák. a zhodnotit, jaké právní vztahy vznikají mezi jednotlivými uživateli konkrétního blockchainu, resp. konkrétní kryptoměny. Zváženy budou také důsledky těchto závěrů ve vztahu

---

[2] POLČÁK, Radim, KASL, František, LOUTOCKÝ, Pavel. MÍŠEK, Jakub, STUPKA, Václav. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu, *Právník*, roč. 2019, č. 1, s. 86; nebo POLČÁK, Radim. *Právo informačních technologií.* Praha: Wolters Kluwer ČR, 2018, s. 8.

[3] KOUBSKÝ, Petr. Před deseti lety vymyslel Satoshi Nakamoto peníze, kterými si budou navzájem platit roboti. *Deník N*, [online]. Dostupné z: https://denikn.cz/11417/pred-deseti-lety-vymyslel-satoshi-nakamoto-penize-kterymi-si-budou-navzajem-platit-roboti [cit. 2019-02-17].

k absolutním majetkovým právům, zejména právu dědickému a zástavnímu.

2. STRUČNÝ POPIS PROTOKOLU BLOCKCHAIN A DEFINICE KRYPTOMĚNY

Pro zasazení do širšího kontextu a jako východisko pro další text je vhodné začít stručným popisem protokolu blockchain a definovat pojem „kryptoměny".

Je možné souhlasit s konstatováním, že *„[i] nejjednodušší počítač je natolik složitou strukturou, že jeho skutečné fungování není do důsledku schopen pochopit ani profesionál."*[4] Internet využívalo podle odhadu v roce 2017 jen v Evropě přes 501 milionů uživatelů.[5] Těžko ale odhadnout, jaké procento těchto uživatelů by dokázalo uspokojivým způsobem popsat a vysvětlit, jak vlastně internet jako takový funguje. Totéž platí zde. Pro uživatele konkrétní kryptoměny, ani pro její právní klasifikaci není nutné chápat všechny aspekty jejího technologického pozadí. Cílem zde tedy není detailní vysvětlení technické stránky fungování kryptoměn, je nicméně nezbytné do něj přinést alespoň základní vhled.

První kryptoměna – bitcoin[6] – vznikla před 10 lety a teoreticky jí dala základ práce *Bitcoin: A Peer-to-Peer Electronic Cash System*[7] publikovaná v roce 2009. V ní je představena peer-to-peer síť Bitcoin, ve které dochází k online transakcím jednotek kryptoměny bitcoin bez využití jakékoliv finanční instituce jako důvěryhodné třetí strany zprostředkovávající tuto transakci.

---

[4] POLČÁK, Radim, KASL, František, LOUTOCKÝ, Pavel. MÍŠEK, Jakub, STUPKA, Václav. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*, AV ČR, Ústav státu a práva, 2019, roč. 2019, č. 1, s. 86.

[5] International Telecommunication Union. *Percentage of Individuals using the Internet*. [online]. Dostupné z: https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2018/Individuals_Internet_2000-2017_Dec2018.xls, [cit. 2019-03-20].

[6] Text dále užívá „bitcoin" pro kryptoměnu a „Bitcoin" jako název konkrétního protokolu blockchain, prostřednictvím kterého dochází k převodům kryptoměny bitcoin.

[7] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*, [online] Dostupné z: https://bitcoin.org/bitcoin.pdf [cit 2019-03-20].

Kromě zprostředkování transakce síť také řeší problém možného dvojího použití prostředků *(double spending)*.[8] K vysvětlení je možné uvést příklad finanční hotovosti. Pokud použiji při platbě obchodníkovi hotovost, nemůžu tutéž stokorunu použít vícekrát. V případě bezhotovostního převodu mezi dvěma bankovními účty brání dvojímu použití prostředků samotné banky jako třetí osoby zprostředkovávající bezhotovostní převod. U bitcoinu však třetí osoba jako zprostředkovatel transakce chybí, a proto musí fungovat systém bránící užití týchž prostředků vícekrát. Výše zmíněná práce přišla s originálním řešením, kdy je elektronická mince definována jako řetěz elektronických podpisů. Transakce mezi dvěma stranami pak probíhá prostřednictvím protokolu nazývaného blockchain.[9]

Blockchain je typ technologie, resp. protokolu distribuovaných záznamů (anglicky DLT – *Distributed Ledger Technology*). Jde o distribuovanou – decentralizovanou – databázi (někdy popisovanou jako decentralizovaná účetní kniha) používanou mezi všemi uživateli konkrétní sítě a kryptoměny – v tomto případě Bitcoinu. Jakákoliv transakce provedená v této síti je ověřována ostatními uživateli (nazývanými jako těžaři) z toho hlediska, zda převáděné jednotky kryptoměny daný uživatel skutečně vlastní, a zda nejde o prostředky, které uživatel použil vícekrát. Těžaři ověřují transakce, přičemž každou jimi ověřenou transakci přidají do tzv. bloku s dalšími transakcemi a následně mezi sebou soutěží o to, který z těžařů vytěží nový blok, tedy bude moci vytvořit nový blok s ověřenými transakcemi, jenž je odeslán ostatním uživatelům. To probíhá zjednodušeně řečeno tak, že výpočetní zařízení jednotlivých těžařů tipují[10] nižší nebo stejnou hodnotu velice složitého čísla, které je přidělené novému bloku a matematickou funkcí převedena do tzv. hashe[11]. Uhodnout daný hash je natolik složité, že

---

[8] STROUKAL, Dominik. SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti.* Praha: Grada. 2018. s. 27.

[9] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*, [online] Dostupné z: https://bitcoin.org/bitcoin.pdf [cit 2019-03-20]. s. 2.

[10] Srov. KASL, František. Blockchain, společenská smlouva digitálního věku? *Revue pro právo a technologie*. 2018, č. 17, s. 13.

[11] Složité vstupní číslo je zde matematickou funkcí převedeno do menšího 64místného „čísla“ – jeho otisku (hashe) –, který je prostřednictvím výpočetní techniky „hádán“ těžaři. Příklad hashe je následující: 00000000000000000176d22e825c9a1941660e4b8f9d1d6918b791

za použití specializované výpočetní techniky tento proces trvá něco kolem 10 minut. Těžař, který příslušný hash uhodne, vytvoří blok s jím ověřenými transakcemi, který je distribuován mezi ostatní uživatele sítě.[12]

Těžba nového bloku je natolik nákladná, složitá a nejistá, že těžaři musí dostat nějakou odměnu. Za nově vytvořený (vytěžený) blok dostane těžař určitý počet nově do sítě emitovaných bitcoinů. V době přípravy článku jde o 12,5 bitcoinu.[13] Nad rámec této odměny těžaři ještě náleží poplatky spojené s transakcemi zapsanými do „vytěženého" bloku.

Každý nový blok obsahuje kromě záznamu o stavu sítě také své vlastní identifikační údaje *(hash)* a identifikační údaje předchozího bloku. Nelze tak vytvořit fiktivní blok, který by nepasoval do celého „řetězu" ostatních (kvůli vzájemně propojenému řetězu bloků je protokol nazývaný jako *blockchain*). Kromě bezpečnosti proti „falšování" je databáze zapsaná v blockchainu také odolná proti svému zničení. Neexistuje totiž žádná centrální autorita, která by ji spravovala, ale je distribuována mezi všechny uživatele.[14] Blok je nejdůležitější součást protokolu blockchain, protože zahrnutím transakce do bloku je transakce potvrzena. Blok v prostředí bitcoinu také obsahuje transakci, jejímž prostřednictvím vznikají nové bitcoiny a dostávají se tak do oběhu.

Vzhledem k uvedenému charakteru protokolu blockchain a jejich samotnému názvu, jsou kryptoměny přítomné pouze ve své nehmotné podobě. Vlastněné jednotky kryptoměny pak má uživatel uloženy v některém druhu virtuální peněženky, vlastnictví k nim prokazuje prostřednictvím kryptografie a převod jednotek mezi dvěma adresami

---

f32416618.

12 Proof of Work. *Investopedia*. [online]. Dostupné z: https://www.investopedia.com/terms p/proof-work.asp, [cit. 2020-01-20].

13 K 27.3.2020 má 12,5 bitcoinu hodnotu přes 2,8 milionu českých korun (dle kryptoměnové směnárny CoinBase https://www.coinbase.com/).

14 Srov. např. KASL, František. Blockchain, společenská smlouva digitálního věku? *Revue pro právo a technologie*. 2018, č. 17, s. 11. Zde autor dochází k závěru, že *„[z] hlediska legitimity je atraktivní, že mechanismus nemá zjevnou centrální definiční autoritu, ale stanoví oprávněnost vnitřních pravidel skrze aktivitu širokého spektra uživatelů, kteří se spolupodílejí na jeho vytváření a jeho užíváním schvalují jeho obsah."*

peněženky je možný pouze prostřednictvím blockchainu.[15] To však neplatí pro hardwarové peněženky, které si lze představit zjednodušeně například jako flashdisk s uloženými jednotkami kryptoměn, který je možné jednoduše fyzicky někomu předat, a pro situace, kdy má uživatel svůj privátní a veřejný klíč k virtuální peněžence pouze fyzicky vytištěný v listinné podobě a obojí může opět pouze fyzicky předat dalšímu uživateli.

Adresu lze definovat jako jednoznačnou identifikaci odesílatele nebo příjemce platby. Vlastnictví takové adresy je poté prokazováno prostřednictvím transakce podepsané tzv. soukromým klíčem.

Je třeba uvést, že tento popis neplatí obecně pro všechny kryptoměny. Způsob „těžby“ nových bitcoinů a ověřování transakcí těžaři je v této a obdobných sítích nazývaný jako *proof of work*. Některé jiné kryptoměny užívají *proof of stake*, kdy je právo vytvořit nový blok připisováno mimo jiné dle množství vlastněných jednotek kryptoměny.[16] Existují však i další typy důkazů, resp. způsobů dosažení konsenzu o stavu dané kryptoměny – např. *delegated proof of stake, proof of importance, proof of authority*[17] či *proof of activity*[18].

Pro ilustraci lze uvést další rozdíly mezi různými kryptoměnami. V případě bitcoinu je s vytěžením bloku spojena odměna v podobě do sítě nově přidaných bitcoinů. U některých kryptoměn jsou nové jednotky distribuovány mezi uživatele jiným způsobem nebo naprosto náhodně. Množství bitcoinů, které budou celkem vydány je finální.[19] V jiných kryptoměnách je toto množství naopak neomezené či je naopak v síti od počátku v oběhu již finální množství jednotek a nové jednotky se netěží.[20]

---

[15] LÁNSKÝ, Jan. *Kryptoměny*. 1. vydání. Praha: C. H. Beck, 2018. s. 3.

[16] Proof of Stake. *Investopedia*. [online]. Dostupné z: https://www.investopedia.com/terms/p/proof-stake-pos.asp, [cit. 2020-01-20].

[17] LÁNSKÝ, Jan. *Kryptoměny*. 1. vydání. Praha: C. H. Beck, 2018. s. 20 a násl.

[18] BENTOV, Iddo et al. Proof of activity: extending bitcoin's proof of work via proof of stake. In *Proceedings of the ACM SIGMETRICS 2014 Workshop on Economics of Networked Systems, NetEcon 2014:* [online]. Dostupné z: https://eprint.iacr.org/2014/452.pdf [cit. 2020-01-20].

[19] STROUKAL, Dominik. SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti.* Praha: Grada. 2018. s. 32.

[20] LÁNSKÝ, Jan. *Kryptoměny*. 1. vydání. Praha: C. H. Beck, 2018. s. 32 a násl.

Na základě výše uvedeného bude pro účely tohoto textu kryptoměna definována jako druh virtuální měny[21]:

1. jejíž vlastnictví se prokazuje pouze prostřednictvím kryptografie,
2. vlastnictví je evidováno prostřednictvím decentralizované a distribuované databáze blockchain, a
3. její transakce mezi uživateli je možné provádět pouze elektronicky prostřednictvím konkrétního protokolu blockchain.[22]

3. ZÁKONNÁ ÚPRAVA KRYPTOMĚN

Jediným zákonným ustanovením, které se výslovně věnuje virtuálním měnám, jejichž zástupcem jsou i kryptoměny, je § 2 odst. 1 písm. l) zákona č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. Ten virtuální měnou pro účely tohoto zákona rozumí elektronicky uchovávanou jednotku bez ohledu na to, zda má nebo nemá emitenta, a která není peněžním prostředkem podle zákona o platebním styku[23], ale je přijímána jako platba za zboží nebo služby i jinou osobou odlišnou od jejího emitenta.

Na evropské úrovni jsou virtuální měny definovány směrnicí Evropského parlamentu a Rady (EU) 2015/849, o předcházení využívání finančního systému k praní peněz nebo financování terorismu[24], jako digitální reprezentace hodnoty, která není vydána či garantována centrální bankou ani orgánem veřejné moci, není nutně spojena se zákonně stanovenou měnou a nemá právní status měny či peněz, je však fyzickými nebo právnickými osobami přijímána jako prostředek směny a může být elektronicky převáděna, uchovávána a obchodována.

---

[21] Ne všechny virtuální měny jsou spojeny s kryptografií.

[22] Pro vyčerpávající definici kryptoměny srov. LÁNSKÝ, Jan. *Kryptoměny*. 1. vydání. Praha: C. H. Beck, 2018, s. 3.

[23] Nyní zákon č. 370/2017 Sb., o platebním styku.

[24] Směrnice Evropského parlamentu a rady (EU) 2015/849 ze dne 20. května 2015, o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES

Pokud kryptoměny nejsou nijak výslovně regulovány, je na místě otázka, zda je jejich užívání vlastně legální. S odkazem na zásadu legální licence, tedy že každý může činit, co není zákonem zakázáno[25], lze odpovědět, že ano. Je však nutné vzít v úvahu zákaz převodu finančních prostředků nad stanovený limit mimo bezhotovostní platby prostřednictvím bankovního převodu. V této souvislosti Ministerstvo financí vyzývá veškeré povinné osoby, *„aby v souvislosti s nákupem/prodejem jakékoli digitální měny, jako je například Bitcoin, byla jako velmi riziková k posouzení a k rozhodnutí o dalších opatřeních podle okolností každá platba nad hodnotu 1.000 EUR a vždy jako podezřelý obchod postupem podle § 18 AML zákona oznámena transakce nad hodnotu 15.000 EUR.“*[26]

Soukromoprávní předpisy však virtuální měny ani kryptoměny nijak nedefinují. Občanskoprávní teorie se však již kryptoměnám a protokolu blockchain začíná pomalu věnovat, jak vyplývá mimo jiné z přehledu použité literatury uvedeného v závěru tohoto textu.

4. NABÍDKA A POPTÁVKA PŘI UŽÍVÁNÍ KRYPTOMĚNY

4.1 OBECNĚ K NABÍDCE A POPTÁVCE

Bylo uvedeno, že v případě převodu jednotek kryptoměny bitcoin mezi jednotlivými uživateli, resp. adresami jejich virtuálních peněženek, je nutné, aby transakci ověřili ostatní uživatelé „těžící“ nové jednotky kryptoměny a konkrétní těžař transakci zařadil do nově vytvářeného bloku transakcí. Původně byly transakce těžaři ověřovány bez poplatku. Postupně však začal narůstat celkový počet transakcí a zároveň lze do nového bloku zařadit jen množství transakcí odpovídající jeho velikosti. Proto je možné ke každé transakci připojit poplatek v libovolné výši, který při jejím zařazením do nového bloku náleží těžaři, jež tento nový blok vytěží. V zásadě pak platí, že připojí-li uživatel k transakci vyšší poplatek, je

[25] Článek 2 odst. 4 ústavního zákona č. 1/1993 Sb., Ústava České republiky.

[26] Metodický pokyn č. 2 Finančního analytického útvaru Ministerstva financí ze dne 16. září 2013, Č.j.: MF-86584/2013/24.

transakce do nového bloku v rámci protokolu blockchain zapsána dříve, než srovnatelná transakce bez poplatku nebo s nižším poplatkem.[27]

S ohledem na uvedený postup je vhodné posoudit, jaký vztah vzniká mezi uživateli, kteří převádí jednotky kryptoměny, a těžaři, kteří transakci ověřují a zapisují do nového bloku transakcí.

V § 1731 obč. zák. čteme, že z návrhu na uzavření smlouvy, resp. z nabídky musí být zřejmé, že nabízející má úmysl uzavřít určitou smlouvu s osobou, vůči které je nabídka určena. Nabídka je perfektní, pokud z právního jednání směřujícího k uzavření smlouvy plyne vůle navrhovatele být smlouvou vázán, obsahuje-li alespoň podstatné náležitosti smlouvy a je možné uzavřít ji jednoduchou, bezvýhradní akceptací nabídky. Podstatnými náležitostmi smlouvy jsou ty, které je nutno dohodnout, aby na základě právního jednání byla uzavřena smlouva, resp. ty náležitosti, o nichž některá ze stran prohlásí, že o nich musí být dosaženo dohody.[28]

Základní definice nabídky tedy stanovuje, že nabídka musí jasně vyjadřovat oferentovu vůli uzavřít konkrétní smlouvu s osobou, vůči které je nabídka učiněna. To znamená, že nabídka musí být obecně adresována konkrétní osobě. Na druhou stranu ne vždy je nabídka vůči konkrétní osobě směřována. Pravděpodobně nejčastější neadresná nabídka je nabídka dodat zboží nebo poskytnout určitou službu učiněná ve spojení s podnikatelskou činností oferenta prostřednictví reklamy, katalogu nebo vystavením v obchodě. Nikoliv pouze podnikatelé ale mohou činit neadresné nabídky. Ustanovení § 1780 odst. 1 obč. zák. definuje veřejnou nabídku jako projev vůle navrhovatele, kterým se obrací na neurčité osoby s návrhem na uzavření smlouvy. Zároveň platí, že podnět k uzavření smlouvy, z něhož neplyne úmysl uzavřít určitou smlouvu nebo který nemá náležitosti podle § 1732 odst. 1 obč. zák., se považuje za výzvu k podávání nabídek.

---

[27] Srov. např. STROUKAL, Dominik. SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti.* Praha: Grada. 2018. s. 70.

[28] PELIKÁNOVÁ. Irena. PELIKÁN, Robert. in ŠVESTKA, Jiří. DVOŘÁK, Jan. FIALA, Josef a kol. *Občanský zákoník. Komentář.* [Systém ASPI]. Praha: Wolters Kluwer ČR. Komentář k § 1732. [cit. 2019-11-20].

4.2 PRÁVNÍ VZTAH PŘI PŘEVÁDĚNÍ KRYPTOMĚNY

Budeme-li aplikovat výše uvedené v předchozí části na fungování kryptoměn a převodu jednotek kryptoměny mezi adresami virtuálních peněženek uživatelů, dojdeme k závěru, že mezi uživatelem převádějícím jednotky a těžařem, který tuto transakci zahrne do nového bloku zařazovanému do blockchainu vzniká relativní závazkový vztah.

Tento závěr lze ilustrovat na příkladu kryptoměny bitcoin, nicméně bude přiměřeně platný i pro jiné kryptoměny. Uživatel se rozhodne, že převede stanovený počet jednotek a připojí k této transakci poplatek v jím stanovené výši. Tím je konstituována veřejná nabídka ve smyslu § 1780 odst. 1 obč. zák. Uživatel zde nabízí, že po uznání transakce za platnou a jejím zapsání do blockchainu bude těžaři zaplacen připojený poplatek. Tato oferta nemůže být adresná a je směřována předem neurčeným osobám proto, že těžař nemůže garantovat to, že z jeho strany bude nový blok vytěžen, tedy že získá právo zapsat nový blok do blockchainu. Toto právo totiž vzniká v zásadě na základě náhody – uhodnutím předem stanoveného *hash* nového bloku.

Zapsáním transakce do nového bloku je oferta těžařem akceptována a je mu vyplacen připojený poplatek. Zde je nutné uvést, že vzhledem k samotnému nastavení sítě (protokolu blockchain) není možné, aby v této situaci vznikla povinnost, kterou by pak bylo možné, resp. nutné vymáhat. Není totiž možné, aby těžař inkasoval poplatek bez zapsaní transakce do blockchainu, a zároveň není možné transakci zapsat a neobdržet stanovený poplatek. V případě tohoto postupu jde o jednoduchou formu smart kontraktu, který se sám vykoná, tedy automatický vyplatí připojený poplatek.

Také je třeba konstatovat, že žádnému z těžařů v žádném okamžiku nevyplývá povinnost transakci ověřit a zapsat. Záleží na tom, zda síť dojde ke konsenzu, že transakce je platná, tedy že převodce převáděnými jednotkami skutečně disponuje či je nepřevádí podruhé (tzv. *doublespending*), a že těžař přijme nabídku za stanovený poplatek transakci zapsat. Ze strany těžaře v podstatě dojde k posouzení, zda se mu vyplatí do nového bloku transakci zapsat za tento poplatek, nebo zapíše transakci

jinou, zabírající více místa, k níž je však připojen vyšší poplatek. Pokud se konkrétní těžař při vytváření nového bloku rozhodne transakci do nového bloku nezapsat, neznamená to, že by převodce musel transakci zadávat znovu. Jiný těžař může při vytěžení dalšího bloku transakci zapsat do něj.

5. KRYPTOMĚNA JAKO VĚC DLE OBČANSKÉHO ZÁKONÍKU

5.1 OBECNÝ VÝKLAD O VĚCECH DLE OBČ. ZÁK.

Věcí v právním smyslu rozumí obč. zák. svým § 489 vše, co je rozdílné od osoby a slouží k potřebě lidí.

Aby obč. zák. podle § 489 považoval nějaký předmět za věc, musí splňovat kumulativně dva znaky:

1. být rozdílný od osoby, a
2. sloužit k potřebě lidí.

Vše, co tedy v objektivní realitě není osobou, a zároveň člověku slouží k potřebě, je věcí v právním smyslu. Potřebnost je dána užitečností věci pro člověka, kterou se rozumí užitek předmětu pro vlastníka a objektivní způsobilost přinášet vlastníkovi především hospodářský, ale i estetický či jiný užitek.

Právní teorie připojuje ještě jeden znak, a to že věc může být předmětem subjektivních majetkových práv, zejména práva vlastnického.[29] Tento znak je nepřímo součástí § 496 odst. 1 obč. zák., který hmotnou věcí rozumí ovladatelnou část vnějšího světa, která má povahu samostatného předmětu. Je-li pro věc typické, že je předmětem vlastnického práva, a nebude-li jakákoliv hmotná součást objektivní reality ovladatelná, těžko bude moci být hmotnou věcí v právním smyslu. U nehmotných věcí sice není možné o faktické fyzické ovladatelnosti mluvit, to ale nebrání tomu, aby byly předmětem vlastnických práv.

[29] DAVID, Ondřej, KINDL, Tomáš. in ŠVESTKA, Jiří. DVOŘÁK, Jan. FIALA, Josef. a kol. *Občanský zákoník. Komentář.* [Systém ASPI]. Wolters Kluwer [cit. 2019-11-20]. Komentář k § 489; nebo DVOŘÁK, Jan. ŠVESTKA, Jiří. ZUKLÍNOVÁ, Michaela. a kol. *Občanské právo hmotné. Svazek I. Díl první. Obecná část*. 2. Aktualizované a doplněné vydání. Praha: Wolters Kluwer ČR, 2016, s. 377.

Vezmeme-li v úvahu všechny tři podmínky pro klasifikaci předmětu jako věci v občanskoprávním pojetí, dojdeme k závěru, že jim kryptoměny vyhovují:

1. Odlišné od právnických a fyzických osob jsou.
2. Slouží k potřebě lidí – mohou být za určitých podmínek prostředkem směny nebo představovat investici. Jejich uživatelé je mohou v rámci blockchainu směnit za jiné věci či práva, mohou na ně nahlížet jako na uchovatele hodnoty či je jako investici nakoupit za měnu s nuceným oběhem s očekáváním nárůstu jejich hodnoty.

   S ohledem na decentralizaci kryptoměn a jejich nezávislosti na státu v nich jiní uživatelé mohou hledat finanční svobodu. Často bývají kryptoměny v této souvislosti skloňovány s jejich tvrzenou anonymitou. Kryptoměny se v míře anonymity liší, nicméně v případě bitcoinu lze mluvit spíše o pseudonymitě.[30]
3. Kryptoměny jsou způsobilé být předmětem subjektivních majetkových práv. Lze je držet a je možné s nimi nakládat. S ohledem na to, že jsou kryptoměny obchodovány na různých burzách, a lze je obchodovat prostřednictvím kryptoměnových „směnáren“, je možné stanovit jejich hodnotu v penězích (§ 492 obč. zák.).

S ohledem na výše uvedené tedy autor konstatuje, že jednotky kryptoměny odpovídají legální definici věci v občanském právu. Tento závěr podporuje i teleologický výklad § 489, kdy široké definici věci v tomto ustanovení vyhovuje rozsáhlá paleta hmotných i nehmotných předmětů. Obč. zák. věc vymezuje záměrně takto široce, aby toto pojetí oproti předchozí úpravě více vyhovovalo čl. 11 odst. 1 Listiny základních práv a svobod[31] i pojetí mezinárodních smluv a nadnárodních úprav. Důvodová zpráva k obč. zák. výslovně zmiňuje, že široké vymezení věci pojmově zahrnuje i *„předměty spadající do kategorií průmyslového a jiného*

[30] K anonymitě kryptoměn blíže viz LÁNSKÝ, Jan. *Kryptoměny.* 1. vydání. Praha: C. H. Beck, 2018, s. 57.

[31] *„Každý má právo vlastnit majetek. Vlastnické právo všech vlastníků má stejný zákonný obsah a ochranu. Dědění se zaručuje.“*

duševního vlastnictví, zaknihovaných cenných papírů, investičních nástrojů typu opcí, swapů, futures nebo forwardů atd.).“[32] Je-li věc vymezena takto široce, je možné pod definici věci podřadit i jednotky kryptoměny.

Kryptoměny, na rozdíl od měn s nuceným oběhem, nemají svou hotovostní alternativu.[33] Výše bylo uvedeno, že vlastnictví jednotek kryptoměny se prokazuje výhradně prostřednictvím kryptografie, jejich vlastnictví je evidováno v elektronicky vedené databázi a disponovat s nimi lze pouze elektronicky prostřednictvím protokolu blockchain. Lze je tedy klasifikovat jako nehmotnou věc.

Vzhledem k tomu, že k vlastnictví jednotky kryptoměny se neváže žádná povinnost vlastníka ani jiné osoby něco dát, konat, strpět nebo se něčeho zdržet, nebude možné klasifikovat virtuální měnu jako právo. Ustanovení § 1011 obč. zák. konstatuje, že vše, co někomu patří, všechny jeho věci hmotné i nehmotné, je jeho vlastnictvím. Z pohledu občanského práva a uživatele kryptoměny bude tedy vlastně irelevantní, zda bude kryptoměna považována za právo, anebo za jinou věc bez hmotné podstaty, když oba tyto závěry znamenají, že je věcí.

Sporu nebude o tom, že kryptoměny jsou věcí movitou.[34] Jednoduché to ale není s rozlišením, zda budou věcí zastupitelnou či nezastupitelnou. Zastupitelná je taková věc, která může být nahrazena jinou věcí téhož druhu a množství. Ostatní věci jsou nezastupitelné. Typickým příkladem zastupitelné věci jsou peníze. Ač mezi měnami s nuceným oběhem a kryptoměnami nalezneme mnoho odlišností, není podle autora důvod, proč by zákonné peníze měly být považovány za zastupitelnou věc, a jednotky kryptoměny za věc nezastupitelnou.

Peníze mohou sice v některých případech plnit sběratelskou funkci nebo být jinak individuálně určeny například u bankovek určených čísly. I na jednotky kryptoměny lze nahlížet jako na jedinečný datový záznam, jelikož jejich vlastnictví je prokazováno prostřednictvím asymetrické kryptografie.

---

[32] Srov. důvodová zpráva k obč. zák, § 498.

[33] I přes to, že například název kryptoměny „Bitcoin Cash“ by sváděl k opačnému závěru.

[34] Pravda je ale taková, že najdou-li se lidé, kteří budou tvrdit, že Země je placatá, mohou se objevit i lidé tvrdící, že kryptoměna je věc nemovitá.

Touto optikou by pak bylo možné jednotky individualizovat a považovat je za věc nezastupitelnou. Na druhou stranu je avšak otázka, zda toto individuální určení má pro vlastníka nějaký význam, ale vyloučit se to zřejmě nedá. Ale stejně jako běžnému uživateli fiat měny pravděpodobně nebude záležet na tom, jestli bude mít v peněžence konkrétní bankovku určenou sérií a pořadovým číslem nebo jinou bankovku totožné hodnoty z jiné série, nebude zřejmě ani záležet uživateli kryptoměny, jestli k jeho adrese náleží jednotky, které se dostaly do oběhu v úterý ve 12:15 nebo ve středu ve 14:00.

5.2 CENNÉ PAPÍRY

Obč. zák. považuje za věc také cenný papír[35] jako listinu, se kterou je právo spojeno takovým způsobem, že je po vydání cenného papíru nelze bez této listiny uplatnit ani převést, a zaknihovaný cenný papír, v jehož případě je cenný papír nahrazen zápisem do příslušné evidence a nelze jej převést jinak než změnou zápisu v této evidenci.[36] Pro kryptoměny jako takové je jejich klasifikace jako cenného papíru, resp. zaknihovaného cenného papíru vyloučena. K tomuto závěru dochází i Česká národní banka, která konstatovala, že bitcoin nevykazuje znaky investičního nástroje ve smyslu § 3 zákona č. 256/2004 Sb., o podnikání na kapitálovém trhu, protože nemá povahu cenného papíru, zaknihovaného cenného papíru ani derivátu.[37]

Teoreticky by bylo možné uvažovat jako o cenných papírech u tzv. tokenů používaných prostřednictvím protokolu blockchain. Tokeny mohou mít platební formu sloužící ke směně za nějaké zboží či službu, pak se svým charakterem blíží kryptoměnám. Většinou ale budou používány jako přístup k nějaké službě založené na blockchainu nebo k účasti na projektu

[35] PAULY, Jan. *Teoretické a legislativní základy cenných papírů.* [Systém ASPI]. Wolters Kluwer. 2016. Kapitola 1. [cit. 2020-03-14]. nebo MAREK, Radan. in MAREK, Radan, JEŽEK, Václav. *Cenné papíry v novém občanském zákoníku.* 1. vydání. Praha: Nakladatelství C. H. Beck, 2013, s. 1.

[36] § 514 a § 525 odst. 1 obč. zák.

[37] Obchodování s bitcoiny / Je k obchodování s bitcoiny nebo k jejich směně potřebné povolení ČNB? [online]. Dostupné z: https://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/stanoviska_a_odpovedi/pdf/obchodovani_s_bitcoiny.pdf [cit. 2019-03-17].

financovaném právě emisí tokenů. V této souvislosti jsou tokeny někdy přirovnávány k dluhopisům nebo akciím. Akciím jsou zřejmě nejpodobnější tzv. *equity* tokeny, které reprezentují podíl na právnické osobě, a vlastník se jimi podílí na jejím řízení.

Mimo jiné vzhledem k legální definici cenného papíru jako listiny a nutnosti zapsat zaknihovaný cenný papír do evidence, které blockchain nebude vyhovovat (srov. § 91 zákona č. 256/2004 Sb., o podnikání na kapitálovém trhu), nebude ani tokeny možné podřadit pod cenné papíry ani zaknihované cenné papíry.[38]

Na druhou stranu o některých formách tokenů by mohlo být uvažováno jako o převoditelných cenných papírech, jakožto pojmu práva Evropské unie.[39]

5.3 ADRESA A PENĚŽENKA JAKO VĚC

Při širokém vymezení věci občanským zákoníkem bude podle autora možné za nehmotnou věc považovat i adresu v rámci kryptoměnové sítě, ke které jednotky kryptoměny náleží. Nebudou zřejmě pochybnosti o charakteristice hardwarové peněženky, na které jsou nahrány jednotky (resp. kryptoměnová adresa), jako hmotné věci. Tu však lze vnímat pouze jako hmotný substrát, na kterém je uložen soukromý a veřejný klíč k příslušné adrese. Sporné může být, zda za věc považovat i adresu samotnou. S ohledem na širokou definici věci v občanském zákoníku by se autor přikláněl k tomu, že ano, a to s přihlédnutím ke všem dříve uvedeným závěrům s tím, že v případě adresy půjde o nezastupitelnou věc s ohledem na její jedinečnost v rámci sítě. Každá adresa je totiž identifikována svým unikátním veřejným klíčem, ke kterému patří

[38] V podrobnostech lze odkázat na text, ve kterém jsou tokeny také klasifikovány jako věci, kdy podle autorů *„je token nehmotnou movitou věcí odpovídající právu jejího vlastníka na přístup k určité službě nebo produktu, které emitent tokenu nabízí, nebo právu podílet se určitým způsobem na projektu, který emitent tokenu financuje prostředky získanými od investorů.“* DĚDIČ, Jan. ŠOVAR, Jan. MIKULA, Ondřej. Proč podle českého soukromého práva nelze uvažovat o (ICO) tokenech jako o cenných papírech. *Právní rozhledy*. 2018, č. 15–16, s. 554–556.

[39] V podrobnostech srov. HOBZA, Martin. ICO a tokeny optikou práva kapitálového trhu: mohou být tokeny investičními cennými papíry? *Bulletin advokacie*. 2019, č. 3, s. 41–46.

neodmyslitelně klíč soukromý. Tedy jednu adresu nebude možné nahradit jednoduše jinou, a to ani v případě, že by na ní bylo nahráno totožné množství jednotek.

Tento úsudek lze podpořit tím, že i bankovní účet je možné považovat po 1. 1. 2014 za věc. Bankovní účet sice jako takový není zákonem vymezen a občanský zákoník pouze definuje smlouvu o účtu tak, že se jí ten, kdo vede účet, zavazuje zřídit od určité doby v určité měně účet pro jeho majitele, umožnit vložení hotovosti na účet nebo výběr hotovosti z účtu nebo provádět převody peněžních prostředků z účtu či na účet. Je tedy možné ho označit za evidenci pohledávky majitele za osobou, která účet vede, a *vice versa* dluhu osoby vedoucí účet vůči jejímu majiteli. Po účinnosti občanského zákoníku je možné bankovní účet vzhledem k vymezení věci v § 489 obč. zák. považovat za nehmotnou movitou věc.[40]

6. KRITICKÝ POHLED NA PŘEDCHOZÍ ZÁVĚRY

Je možné připustit, že debata o podrobné charakteristice jednotek kryptoměn jako věci je do jisté míry akademická a pro jejich běžného uživatele bezpředmětná. Zde má autor na mysli například jejich klasifikaci jako nehmotnou věc či právo. Je-li právo, jehož povaha to připouští, občanským zákoníkem zařazeno mezi nehmotné věci, vlastníku jednotek kryptoměny zřejmě nebude záležet na tom, zda bude vlastníkem jiné věci bez hmotné podstaty, anebo práva, jehož povaha to připouští – a tedy nehmotné věci.

Tuto debatu lze také do jisté míry přirovnat k obdobné, která byla vedena ohledně zařazení cenných papírů mezi věci či jiné majetkové hodnoty před účinností obč. zák. Doktrína dříve vesměs nepovažovala cenný papír za věc, ale za statek naplňující znaky jiné majetkové hodnoty. A to přes to, anebo právě proto, že tehdy platný zákon č. 591/1992 Sb., o cenných papírech, hned ve svém prvním paragrafu určoval, že na cenné papíry se vztahují ustanovení o věcech movitých. Cenný papír tedy nebyl věcí v právním smyslu, ale soudy například dovozovaly, že může být

[40] ELEK, Štefan; LIŠKA, Petr; MAREK, Karel. *Bankovní obchody.* [Systém ASPI]. Kapitola III, § 1. Wolters Kluwer [cit. 2020-03-14].

postižen výkonem rozhodnutí nebo že je možné ho vydržet.[41] Pro držitele cenného papíru, jenž se věcí nezabýval na akademické úrovni, tak byl výsledek relativně bezvýznamný – na cenný papír se vztahovala ustanovení o movitých věcech, bylo možné ho vydržet a mohl být předmětem výkonu rozhodnutí. Záleží pak jeho vlastníkovi na tom, jestli je věcí v právním smyslu nebo ne? Zřejmě nikoliv.

Tématu textu je však ještě blíže debata o tom, zda je zaknihovaný cenný papír spíše „zaknihované právo", tj. právo, jehož povaha to připouští, a tedy nehmotnou věcí, anebo rovnou jinou věcí bez hmotné podstaty.[42] Zde také vlastníkovi zaknihovaného cenného papíru půjde primárně o to, zda se bude moci při uplatnění práv prokázat výpisem z příslušné evidence zaknihovaného papíru, a zda bude moci se zaknihovaným papírem v rámci této evidenci relativně volně disponovat, a to bez ohledu na výsledek této diskuze.

Podobně lze připomenout spory ohledně charakteristiky doménových jmen a jejich ochrany. Ty by však po účinnosti obč. zák. měly být ukončeny, a to vzhledem k širokému pojetí definičního ustanovení o věcech.[43]

Považujeme-li kryptoměnu za věc, znamená to, že její jednotky budou způsobilé být předmětem absolutních i relativních subjektivních práv. Budou předmětem vlastnického práva jako absolutního práva a budou způsobilé býti předmětem závazku jako práva relativního. Je ale nutné připustit, že tento závěr má své limity vzhledem k povaze kryptoměn a možnostem s jejich jednotkami reálně disponovat.

Občanský zákoník pojímá vlastnictví jako vlastníkovo právo vlastnictvím v mezích právního řádu libovolně nakládat a jiné osoby z toho

---

[41] Např. rozhodnutí Nejvyššího soudu 21 Cdo 2587/99 či 29 Odo 1216/2005.

[42] Srov. např. SZOSTOK, David. Cenný papír a zaknihovaný cenný papír jako věc v právním smyslu, *Soukromé právo*, 2016, č. 11. či VÍTEK, Jindřich. Právní úprava cenných papírů v občanském zákoníku. *Obchodní právo*, 2012, č. 12.

[43] MACGREGOR PELIKÁNOVÁ, Radka. (Ne)jasné pojetí doménových jmen a jejich režimu v novém občanském zákoníku. *Rekodifikace & Praxe*, 2015, č. 3(1).

vyloučit.[44] Jako jednotlivá oprávnění vlastníka bývají uváděna dílčí práva: věc užívat, požívat, nakládat s ní, zničit ji či ji opustit.[45]

Tato oprávnění jsou však v prostředí protokolu blockchain limitována jeho pravidly a asymetrickou kryptografií. Jakákoliv dispozice s jednotkami kryptoměny je závislá na pravidlech konkrétní sítě. Zároveň je třeba vzít v úvahu, že formálně mohu být vlastníkem jednotek kryptoměny, resp. adresy, na které jsou v určitém okamžiku zapsané, nicméně bez znalosti soukromého kryptografického klíče k této adrese s nimi nebudu schopný provést jakoukoliv dispozici. Na této skutečnosti nezmění nic ani teoretické rozhodnutí soudu, které bude vlastníkovi přikazovat vydat jednotky kryptoměny zapsané na konkrétní adrese specifikované veřejným klíčem, když bez soukromého klíče a součinnosti těžařů, jak bylo uvedeno výše, nebude možné převod uskutečnit.

Těžko se také může vlastník rozhodnout jednotky kryptoměny zničit. Dalo by se hovořit například o spálení jediného výtisku listiny se zapsaným soukromým klíčem či o úderech kladivem do hardwarové peněženky, na které budou zapsány. K faktickému zničení těchto jednotek však nedojde – v síti budou existovat dále, jen s nimi nebude žádný z uživatelů (včetně jejich vlastníka) schopen jakkoliv disponovat. Jediné ze zmíněných oprávnění vlastníka, které bude proveditelné vždy, bude tedy právo věc opustit.[46]

Charakteristika jednotek kryptoměny jako věci také znamená, že je možné je užít v rámci různých institutů občanského práva. I toto užití má své hranice, které je možné ilustrovat na příkladu klasického institutu občanského práva – na zástavním právu – a také na právu dědickém.

---

[44] § 1012 obč. zák.

[45] Srov. např. SPÁČIL, Jiří in SPÁČIL, Jiří a kol. *Věcná práva. Věcná práva, katastr nemovitostí a správa cizího majetku.* Praha C. H. Beck, 2018, s. 53.

[46] V této věci lze odkázat na článek POLČÁK, Radim. Informace a data v právu. *Revue pro právo a technologie*, MUNI, roč. 2016, č. 13, s. 68–91. Zde je prezentován závěr, že data mohou být předmětem absolutních práv pouze za předpokladu, že *"jsou data tak pevně spojena se svým nosičem nebo službou zajišťujícím jejich dostupnost, že nelze docílit jejich samostatného užití. Druhý výjimečný případ nabízí silné šifrovací nástroje, jejichž aplikace umožňuje prakticky svázat užití dat s užitím dešifrovacího postupu."*

Zástavou může být každá věc, s níž lze obchodovat, a zástavní právo lze zřídit i k věci, k níž zástavnímu dlužníku vznikne vlastnické právo teprve v budoucnu.[47] Vzhledem k dříve uvedeným závěrům lze konstatovat, že jednotky kryptoměny budou způsobilou zástavou – jsou věcí a lze s nimi obchodovat.

Alternativně bude možné zastavit i samotnou adresu v rámci konkrétní sítě či hardwarovou peněženku. Pro podporu závěru o charakteristice kryptoměnové adresy jako věci bylo použito srovnání s bankovním účtem, který lze za věc považovat také.[48] Zde je však této analogii třeba vymezit hranice z toho důvodu, že způsobilou zástavou bude sice pohledávka majitele účtu vůči bance, nikoliv bankovní účet jako takový.[49]

Problém při zastavení adresy jako takové nebude v naplnění zákonného předpokladu vzniku zástavního práva k movité věci (zástavní právo k movité věci ze zákona vzniká odevzdáním věci zástavnímu věřiteli[50]) ani v jejím zpeněžení po splatnosti dluhu. Nepůjde však zamezit tomu, aby s jednotkami kdokoliv další disponoval. Předá-li totiž zástavní dlužník zástavnímu věřiteli (anebo třetí osobě ve smyslu § 1318 obč. zák.) soukromý i veřejný klíč k adrese, neznamená to samozřejmě, že je po jejich předání nebude moci k převodu jednotek použít. Tomu zástavní věřitel prakticky nemůže zabránit, s výjimkou relativního závazku zřízeného mezi zástavním dlužníkem a věřitelem. Stejně to bude platit i pro zastavení hardwarové peněženky, která sice může být jednoduše odevzdána, resp. po splatnosti dluhu zpeněžena. To však opět neznamená, že zástavní dlužník nebo třetí osoba mezitím nemůže s jednotkami disponovat. Adresa například může být naklonovaná na dvou a více různých hardwarových peněženkách, které převod jednotek umožní.

---

[47] § 1310 obč. zák.

[48] LIŠKA, Petr. *Účet, jednorázový vklad, akreditiv a inkaso v občanském zákoníku.* [Systém ASPI]. Wolters Kluwer [cit. 2020-03-14]. Část první, hlava II.

[49] K tomu např. ŠVESTKA, Jiří, DVOŘÁK, Jan, FIALA, Josef a kol. *Občanský zákoník. Komentář. Svazek III.* [Systém ASPI] Praha: Wolters Kluwer ČR, 2014 [cit. 2020-03-14]. Komentář k § 1310.

[50] § 1317 obč. zák.

Pokud oproti tomu budou jako zástava užity přímo jednotky kryptoměny, tyto obtíže odpadnou. Zástavní dlužník převede smluvený počet jednotek ze své adresy na adresu zástavního dlužníka nebo třetí osoby ve smyslu § 1318 obč. zák. Po splatnosti zajištěného dluhu se pak zástavní věřitel uspokojí způsobem dohodnutým se zástavcem či zástavním věřitelem, například prodejem jednotek na některé kryptoměnové burze.

Jednotky kryptoměny, resp. adresa, na níž budou v době smrti zůstaviteli zapsány, budou způsobilé tvořit pozůstalost.[51] Dědic ale nebude moci nabýt jednotky kryptoměny bez adresy, protože bez ní v podstatě neexistují. Měl by tedy nabýt kryptoměnovou adresu. K dispozicím s jednotkami k ní náležejícím ale bude třeba zároveň znát soukromý a veřejný klíč k této adrese. Pokud tuto znalost mít nebude, bude pro něj adresa naprosto bezcenná. To platí i pro zdědění hardwarové peněženky, v jejímž případě bude dispozici s jednotkami třeba potvrdit heslem, pinem nebo jiným způsobem, bez nichž k žádnému převodu jednotek nedojde.

Dědická daň byla s účinností od 1. 1. 2014 zrušena. Nebude tedy v uvedeném případě docházet k tomu, že by dědic nabyl adresu s určitým počtem jednotek, musel by ale z jejího nabytí zaplatit dědickou daň, a to i navzdory tomu, že by pro něj neměla žádnou hodnotu, když by s jednotkami nemohl jakkoliv disponovat.

Dříve dosažené závěry také naráží na to, že internet v podstatě nemá hranice a složitě se v přeshraničních sporech určuje rozhodné právo. V jeho prostoru je oslaben význam polohy a vzdálenosti, do styku přicházejí různé osoby bez ohledu na jejich aktuální místní příslušnost.[52] To bude platit i v prostředí protokolu blockchain, který má – alespoň v případě velkých kryptoměnových sítí – skutečně globální charakter. Také to, že české právo považuje kryptoměnu za věc, ještě neznamená, že tento závěr bude mít nějaký význam u přeshraničního sporu, ve kterém bude užito jako rozhodného práva jiného právního řádu, který věc v právním smyslu bude chápat odlišněji.

---

[51] Srov. § 1475 odst. 2 a § 495 obč. zák.

[52] KASL, František. Blockchain, společenská smlouva digitálního věku? *Revue pro právo a technologie*. 2018, č. 17, s. 6.

7. VÝSLOVNÁ ÚPRAVA?

Je možné klást otázku, zda je na místě prostřednictvím soukromého práva výslovně regulovat kryptoměny. Autoři knihy o Bitcoinu uvádějí, že *„je obtížné psát knihu o něčem, co se mění každý den. Bitcoin je nový a je to živoucí ekosystém, kde dochází neustále k inovacím.“*[53] Touto citací lze v zásadě na předloženou otázku jednoduše odpovědět.

Obecně platí, že technologie vždy byly a budou o krok napřed před právní úpravou. Tomu odpovídá neschopnost českého zákonodárce účinným způsobem speciálně upravit například platformy typu UBER, Airbnb a jiné či alespoň zavést jejich zákonnou definici.

Platí-li tedy, že právo bude vždy informační technologie a jejich vývoj schopno stíhat víceméně neúspěšně, je vhodnější užívat při jejich konfrontaci s právem spíše obecné instituty než zavádět nové. I kupříkladu otázky spojené s vysoce specifickou oblastí doménových jmen lze řešit bez speciální úpravy.[54] Například Telec pak vyzývá, abychom se pokusili *„na nové jevy v právu včetně otázek informačních a komunikačních technologií nahlížet ´starýma´ civilistickýma očima.“*[55]

Těmto závěrům odpovídá i výše řečené o projevech virtualizace ve vývoji informačních technologií a v oboru práva informačních technologií. Zároveň to, že se v oboru práva informačních technologií nezavádí nějaké zásadní nové instituty, o něm ale nevypovídá nic negativního. I přes to, že informační technologie sice nepřinesly nic zásadně nového, Polčák uvádí, že rozkrytí jejich filozofické podstaty obohatilo právní teorii, filozofii a zprostředkovaně i právní praxi.[56]

Na druhou stranu je ale nutné právo některým aspektům technologického rozvoje a jeho směřování otevřít. Jen jako jeden z příkladů z mnoha lze zmínit Německo, které v září 2019 přijalo strategii využití

---

[53] STROUKAL, Dominik. SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Praha: Grada. 2018. s. 22.

[54] MACGREGOR PELIKÁNOVÁ, Radka. (Ne)jasné pojetí doménových jmen a jejich režimu v novém občanském zákoníku. *Rekodifikace & Praxe*, 2015, č. 3(1).

[55] TELEC, Ivo. Poznámky k internetu a proměnám práva. *Právní rozhledy*. 2013, č. 12.

[56] POLČÁK, R. *Právo informačních technologií.* Praha: Wolters Kluwer ČR, 2018, s. 9

blockchainu a jeho potenciálu k postupu digitální transformace[57] anebo záměr, aby ve Spojených státech amerických byly kryptoměny, jejichž hodnota je vázána na fiat měnu, považovány za cenné papíry[58]. Existující regulaci již má také například Lichtenštejnsko, jehož parlament 3. 10. 2019 s účinností od 1. 1. 2020 přijal zákon upravující užití tokenů založených na protokolu blockchain.[59]

V souladu s uvedeným závěrem o preferenci užití obecných institutů bylo v předchozím textu ukázáno, že na kryptoměny lze aplikovat některá ustanovení občanského zákoníku. Autor textu si je nicméně vědom limitů tohoto závěru, jelikož právo v prostředí protokolu blockchain do jisté míry tahá za kratší konec. Ačkoliv na ně lze aplikovat některá zákonná ustanovení, veškeré dispozice s jednotkami kryptoměny jsou limitovány pravidly protokolu blockchain a asymetrickou kryptografií, nikoliv právem. Formálně sice může být uživatel kryptoměny vlastníkem jejích jednotek, ale například bez znalosti soukromého kryptografického klíče ke konkrétní adrese s nimi nebude schopen jakkoliv nakládat. Na této skutečnosti nezmění nic ani rozhodnutí soudu ani zákon. Toto bylo v textu článku ukázáno na institutech zástavního a dědického práva.

Svět mimo internet, resp. mimo kyberprostor je primárně řízen přírodními zákony. Člověkem vydaný zákon tak bude například těžko úspěšně předepisovat, kdy má a nemá sněžit. Co je a není možné v rámci protokolu blockchain je naproti tomu určeno jeho pravidly. Ta sice nejsou neměnná a v případě blockchainů typu Bitcoin je lze změnit za předpokladu akceptace nových pravidel většinou uživatelů.[60] Na rozdíl od přírodních zákonů budou tedy uživatelé schopni zákonitosti konkrétního

---

[57] Bundesmisterium der Finanzen. *German Government Adopts Blockchain Strategy*. [online]. Dostupné z: https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Financial_markets/Articles/2019-09-18-Blockchain.html. [cit. 2019-11-9].

[58] *Discussion Draft: Stablecoins are Securities Act of 2019*. [online] https://financialservices.house.gov/uploadedfiles/bills-116pih-ssa.pdf. [cit. 2019-11-16].

[59] Regierung des Fürstentums Liechtenstein. *Landtag stimmt dem Blockchain-Gesetz einstimmig zu*. [online] https://www.regierung.li/de/mitteilungen/222957/?typ=news [cit. 2019-11-10].

[60] KASL, František. Blockchain, společenská smlouva digitálního věku? *Revue pro právo a technologie*. 2018, č. 17. s. 11.

blockchainu do jisté míry změnit. To ale nic nevypovídá o vymahatelnosti práva a soudních rozhodnutí v jeho rámci, resp. o možnosti jeho zásadní zákonné regulace. Nezbývá tedy zřejmě než pokrčit rameny a konstatovat *„code is law“*.[61]

8. ZÁVĚR

Kryptoměnou text rozumí druh virtuální měny, jejíž vlastnictví se prokazuje pouze prostřednictvím kryptografie a je evidováno prostřednictvím protokolu blockchain, bez nějž není možné s jednotkami kryptoměny jakkoliv disponovat.

Na vztahu mezi uživatelem převádějícím jednotky kryptoměny a těžařem bylo ilustrováno užití ustanovení občanského zákoníku o nabídce a akceptaci. Bylo konstatováno, že z pohledu občanského práva lze kryptoměny podřadit pod definici věci ve smyslu § 489 obč. zák., a to věc nehmotnou, movitou a podle názoru autora zastupitelnou. Kryptoměny však nelze v současné chvíli považovat za cenný papír ani zaknihovaný cenný papír tak, jak je chápe český právní řád.

Nakládání s jednotkami kryptoměny je však spíše než právem omezeno pravidly protokolu blockchain. Veškeré dispozice s nimi jsou závislé na znalosti soukromého kryptografického klíče ke konkrétní adrese, interakci s ostatními uživateli a zákonitostmi sítě. Bude sice možné kryptoměnovou peněženku, resp. adresu zastavit, vzhledem k zákonitostem protokolu blockchain to ale bude problematické. Stejně tak bude možné kryptoměnovou adresu zdědit. Bez znalosti soukromého klíče však dědic z takového dědictví příliš nadšený zřejmě nebude, protože s jednotkami nebude schopný disponovat, tedy je ani prodat za fiat měnu.

Klasifikace jednotek kryptoměny jako věci má rovněž své limity s ohledem na problematické určení rozhodného práva v případných sporech s mezinárodním prvkem.

Autor textu také souhlasí se závěrem, že je v případě informačních technologií spíše vhodnější užívat obecné právní instituty než zavádět nové.

---

[61] LESSIG, Lawrence. *Code: Version 2.0.* New York: Basic Books, 2006.

Pro protokol blockchain a kryptoměny to platí také. Na druhou stranu je ale vhodné umožnit jejich širší užití tak, jak to činí některé právní řády.

9. SEZNAM POUŽITÝCH ZDROJŮ

[1] BENTOV, Iddo et al. Proof of activity: extending bitcoin's proof of work via proof of stake. In *Proceedings of the ACM SIGMETRICS 2014 Workshop on Economics of Networked Systems, NetEcon 2014:* [online]. Dostupné z: https://eprint.iacr.org/2014/452.pdf [cit. 2020-01-20].

[2] *Bundesmisterium der Finanzen. German Government Adopts Blockchain Strategy.* [online]. Dostupné z: https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/

Financial_markets/Articles/2019-09-18-Blockchain.html. [cit. 2019-11-9].

[3] DĚDIČ, Jan. ŠOVAR, Jan. MIKULA, Ondřej. Proč podle českého soukromého práva nelze uvažovat o (ICO) tokenech jako o cenných papírech. *Právní rozhledy*. 2018, č. 15-16, s. 554–556.

[4] *Discussion Draft: Stablecoins are Securities Act of 2019.* [online] https://financialservices.house.gov/uploadedfiles/bills-116pih-ssa.pdf. [cit. 2019-11-16].

[5] DRAŠTÍK, Alexandr. FREMR, Robert. DURDÍK, Tomáš a kol. *Trestní zákoník. Komentář.* [Systém ASPI]. Wolters Kluwer [cit. 2019-03-20].

[6] DVOŘÁK, Jan. ŠVESTKA, Jiří. ZUKLÍNOVÁ, Michaela a kol. *Občanské právo hmotné. Svazek I. Díl první. Obecná část.* 2. Aktualizované a doplněné vydání. Praha: Wolters Kluwer ČR, 2016.

[7] ELEK, Štefan; LIŠKA, Petr; MAREK, Karel. *Bankovní obchody.* [Systém ASPI] Wolters Kluwer [cit. 2020-03-14].

[8] HOBZA, Martin. ICO a tokeny optikou práva kapitálového trhu: mohou být tokeny investičními cennými papíry? *Bulletin advokacie*. 2019, č. 3, s. 41–46.

[9] International Telecommunication Union. *Percentage of Individuals using the Internet*. [online] Dostupné z: https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2018/

Individuals_Internet_2000-2017_Dec2018.xls, [cit. 2019-03-20].

[10] KASL, František. Blockchain, společenská smlouva digitálního věku? *Revue pro právo a technologie*. 2018, č. 17.

[11] KOUBSKÝ, Petr. Před deseti lety vymyslel Satoshi Nakamoto peníze, kterými si budou navzájem platit roboti. *Deník N*, [online]. Dostupné z: https://denikn.cz/11417/pred-deseti-lety-vymyslel-satoshi-nakamoto-penize-kterymi-si-budou-navzajem-platit-roboti [cit. 2019-02-17].

[12] LÁNSKÝ, Jan. *Kryptoměny.* 1. vydání. Praha: C. H. Beck, 2018.

[13] LESSIG, Lawrence. *Code: Version 2.0.* New York: Basic Books, 2006.

[14] LIŠKA, Petr. *Účet, jednorázový vklad, akreditiv a inkaso v občanském zákoníku.* [Systém ASPI]. Wolters Kluwer [cit. 2020-03-14].

[15] MAREK, Radan, JEŽEK, Václav. Cenné papíry v novém občanském zákoníku. 1. vydání. Praha: Nakladatelství C. H. Beck, 2013.

[16] MACGREGOR PELIKÁNOVÁ, Radka. (Ne)jasné pojetí doménových jmen a jejich režimu v novém občanském zákoníku. *Rekodifikace & Praxe*, 2015, č. 3(1).

[17] Metodický pokyn č. 2 Finančního analytického útvaru Ministerstva financí ze dne 16. září 2013, Č.j.: MF-86584/2013/24.

[18] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*, [online] Dostupné z: https://bitcoin.org/bitcoin.pdf [cit. 2019-03-20].

[19] NĚMEC, Libor. TORNOVÁ, Jarmila., K právní regulaci kryptoměn. Díl II. *Právní rádce.* roč. 2018, č. 7.

[20] Obchodování s bitcoiny / Je kobchodování sbitcoinynebo k jejichsměně potřebné povolení ČNB? [online]. Dostupné z: https://www.cnb.cz/miranda2/export/sites/www.cnb.

cz/cs/faq/stanoviska_a_odpovedi/pdf/obchodovani_s_bitcoiny.pdf [cit. 2019-03-17].

[21] PAULY, Jan. *Teoretické a legislativní základy cenných papírů.* [Systém ASPI]. Wolters Kluwer. 2016. [cit. 2020-03-14].

[22] POLČÁK, Radim, KASL, František, LOUTOCKÝ, Pavel. MÍŠEK, Jakub, STUPKA, Václav. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*, AV ČR, Ústav státu a práva, 2019, roč. 2019, č. 1, s. 86–98.

[23] Proof of Work. *Investopedia*. [online]. Dostupné z: https://www.investopedia.com/

terms/p/proof-work.asp, [cit. 2020-01-20].

[24] Proof of Stake. *Investopedia*. [online]. Dostupné z: https://www.investopedia.com/

terms/p/proof-stake-pos.asp, [cit. 2020-01-20].

[25] Regierung des Fürstentums Liechtenstein. *Landtag stimmt dem Blockchain-Gesetz einstimmig zu.* [online] https://www.regierung.li/de/mitteilungen/222957/?typ=news [cit. 2019-11-10].

[26] SPÁČIL, Jiří a kol. *Věcná práva. Věcná práva, katastr nemovitostí a správa cizího majetku.* Praha C. H. Beck, 2018.

[27] STROUKAL, Dominik. SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti*. Praha: Grada. 2018.

[28] SZOSTOK, David. Cenný papír a zaknihovaný cenný papír jako věc v právním smyslu, *Soukromé právo*, 2016, č. 11, s 4 a násl.

[29] ŠVESTKA, Jiří, DVOŘÁK, Jan, FIALA, Josef a kol. *Občanský zákoník. Komentář. Svazek I.* Praha: Wolters Kluwer ČR, 2014.

[30] ŠVESTKA, Jiří, DVOŘÁK, Jan, FIALA, Josef a kol. *Občanský zákoník. Komentář. Svazek III.* Praha: Wolters Kluwer ČR, 2014.

[31] TELEC, Ivo. Poznámky k internetu a proměnám práva. *Právní rozhledy*. 2013, č. 12.

[32] TRÁVNÍK, Pavol. *Bitcoin v českém právu*, [online]. Dostupné z https://medium.com/@

pavol.travnik/bitcoin-v-českém-právu-308a82c78ebf [cit. 2019-07].

[33] VÍTEK, Jindřich. Právní úprava cenných papírů v občanském zákoníku. *Obchodní právo*, 2012, č. 12.

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

---

https://doi.org/10.5817/RPT2020-1-3

KYBERNETICKÁ ZBRAŇ: PŘÍSTUPY K JEJÍ DEFINICI[1]

IVANA KUDLÁČKOVÁ[2]

ABSTRAKT

Odhalení počítačového červa Stuxnet v roce 2010 lze označit za zlomový okamžik, který zintenzivnil debaty o kybernetických zbraních. K těm je v odborné literatuře přistupováno různými způsoby, proto si tento příspěvek klade za cíl tyto rozdílné přístupy k definici pojmu kybernetická zbraň zmapovat a následně je aplikovat na reálné kybernetické incidenty.

Právě odhalení Stuxnetu je pro svůj dopad výchozím bodem, od kterého byla prováděna rešerše literatury, která se zabývá pojmem kybernetická zbraň. Za tímto účelem byly analyzovány odborné příspěvky publikované v období let 2010-2019 zařazené v databázích DBLP Computer Science Bibliography Website, Scopus a Web of Science.

Provedená analýza posloužila k představení hlavních přístupů ke kybernetickým zbraním. Definice byly poté podrobeny analýze a byly identifikovány dva hlavní faktory způsobující názorový nesoulad.

KLÍČOVÁ SLOVA

kybernetická zbraň, kybernetický incident, malware, Stuxnet

---

[1] Tento článek vznikl za podpory projektu "Centrum excelence pro kyberkriminalitu, kyberbezpečnost a ochranu kritických informačních infrastruktur" (CZ.02.1.01/0.0/0.0/16_019/0000822).

[2] Mgr. Bc. Ivana Kudláčková, výzkumná pracovnice, Ústav práva a technologií, Právnická fakulta, Masarykova univerzita, ivana.kudlackova@mail.muni.cz.

ABSTRACT

Discovery of Stuxnet (a computer worm) in 2010 can be described as a turning point leading to intensification of cyber weapons discussions. This paper aims to map different approaches to the term cyber weapons and apply them to real cyber incidents respectively.

Discovery of Stuxnet is determined as a starting point from which the literature review dealing with the concept of cyber weapons was carried out. Papers published within the period 2010-2019 in DBLP Computer Science Bibliography Website, Scopus and Web of Science databases were analysed.

The analysis helped to introduce three main approaches to cyber weapons. These approaches were then analysed and two main factors causing discrepancy were identified.

KEYWORDS

cyber weapon, cyber incident, Stuxnet, malware

1. ÚVOD

Tým německých expertů v čele s bezpečnostním konzultantem Ralphem Langerem v září 2010 zveřejnil zprávu, která popisovala fungování a dopad počítačového červa jménem Stuxnet.[3] Tento den a události po něm následující lze bezesporu chápat jako významný milník možného nasazení a významu kybernetických zbraní. Sám Ralph Langer v r. 2011 uvedl, že *„minulý rok znamenal zlom v historii kybernetické bezpečnosti – příchod první kybernetické zbraně známé jako Stuxnet.“*[4] Za klíčový lze tento okamžik označit především ze dvou hlavních důvodů. Zaprvé, Stuxnet byl svojí povahou čistě kybernetickým incidentem, který nebyl doprovázen kinetickými prostředky. Zadruhé, Stuxnet přímo způsobil zničení jaderných

[3] V současné chvíli je k dispozici aktualizovaná verze této zprávy. LANGER, Ralph. *To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve.* [online]. 2013 [cit. 25.10.2019]. Dostupné z: https://www.langner.com/wp-content/uploads/2017/04/To-kill-a-centrifuge.pdf .

[4] LANGER, Ralph. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security Privacy*. 2011, 9(3), str. 49.

centrifug, které musely být nahrazeny za nové a tento incident tedy vyvolal hmotnou škodu, která se projevila ve fyzickém světě. Do té doby probíhající debaty o potenciálu kybernetických zbraní tak získaly reálné obrysy. Poprvé byl explicitně vyřčen názor, že Stuxnet je kybernetickou zbraní, což posléze vedlo k rozproudění dalších debat. Pozornost byla mj. zaměřena na konkrétní parametry, které musí být splněny, aby mohl být určitý nástroj označen za kybernetickou zbraň.

Předkládaný příspěvek mapuje debatu odborné veřejnosti právě od r. 2010, kdy došlo k odhalení Stuxnetu, až do r. 2019. V tomto časovém období se čím dál častěji objevoval termín kybernetická zbraň, jenž doposud nemá normativní zakotvení. Výchozí situací je stav, kdy se termín kybernetická zbraň používá v různých významech, a to s ohledem na zázemí, ze kterého konkrétní autor pochází. Zcela nepřekvapivě pak bude mít odlišnou představu o takové zbrani právník, který rozhoduje o souladu jejího nasazení s právem; voják, jehož cílem je získat vojenskou výhodu; policy-maker, jenž bude uvažovat o možné eskalaci vzájemných vztahů v případě, že k nasazení kybernetické zbraně dojde. Každý z nich tedy sleduje jiné zájmy a klade důraz na jiné prvky. Autor nepovažuje existenci různých přístupů v jednotlivých odvětvích za *a priori* problematické. Z ryze praktické stránky je ale problematická situace, kdy jednotlivci nejsou dostatečně obeznámeni s přístupy ostatních. Pouze prostřednictvím vzájemného pochopení odlišností lze docílit efektivní spolupráce mezi jednotlivými profesemi. Specialisté z jednotlivých oblastí spolu navzájem komunikují, a to např. v rámci kybernetických cvičení, a pokud je používán termín, kterému ovšem jednotlivci připisují odlišný význam a jedinci si těchto odlišných přístupů nejsou vědomi, může to způsobit komplikace. Pokud je kupříkladu politikou konkrétního státu přístup, že nedojde k nasazení kybernetických zbraní, musí si být právník vědom toho, co je považováno za kybernetickou zbraň na politické úrovni, a upozornit na situace, kdy by mohlo příp. k takovému nasazení dojít. Pokud naopak bude mít voják zcela jasno o tom, co je kybernetickou zbraní, tak může nastat situace, kdy její nasazení nebude konzultovat s právníkem (který by její

nasazení mohl nedoporučit, protože z právního úhlu bude za kybernetickou zbraň považovat něco jiného).

Autor si neklade za cíl představit jednotnou a ustálenou definici kybernetické zbraně, neboť taková snaha by se zcela minula účinkem z důvodu jejího nesouladu s běžnou realitou. Autor reaguje na stav, kdy mezi odbornou veřejností doposud chybí zmapování odlišných přístupů a jejich aplikace na konkrétní případy. Z těchto důvodů jsou hlavní cíle tohoto článku následující. Zaprvé, cílem je poskytnout ucelený přehled přístupů k definici pojmu kybernetická zbraň. Tohoto cíle je dosaženo prostřednictvím analýzy odborných článků a výstupů z konferencí publikovaných v letech 2010-2019. Tato analýza následně poslouží i k naplnění druhého cíle, kterým je syntéza těchto přístupů a identifikování slabých míst. Druhý cíl bude naplněn prostřednictvím aplikace jednotlivých definic na reálné kybernetické incidenty, které ve svých příspěvcích zmiňovali sami autoři. Tato analýza tak poslouží k objasnění jednotlivých přístupů a vzájemnému porozumění v případě reálné kybernetické operace.

Za tímto účelem je příspěvek koncipován následujícím způsobem. V první kapitole je vysvětlena metoda sběru a zpracování dat. Dále je pozornost věnována samotným výsledkům. Druhá kapitola představí již proběhlé kybernetické incidenty, jejichž spouštěč může či taktéž nemusí být označen za kybernetickou zbraň. Třetí kapitola se zaměří na autory, již poskytují přímou definici kybernetické zbraně. Čtvrtá kapitola je pak věnována příkladům různých typů kybernetických nástrojů, které autoři přímo či nepřímo za kybernetickou zbraň označují. Pátá kapitola je zaměřena na autory, jejichž přístupy nespadají do žádných předchozích kapitol. Poslední kapitola je pak nejdůležitější, neboť představuje onen diskuzní přínos, kdy dojde k aplikaci definicí na konkrétní incidenty a k identifikaci slabých míst.

2. METODA SBĚRU A ZPRACOVÁNÍ DAT

K získání prvotního setu všech relevantních zdrojů byly využity databáze DBLP computer science bibliography (dále jen „DBLP“), Scopus a Web of

Science. Za klíčová slova byla zvolena slovní spojení cyber weapon nebo též cyberweapon. V časovém rozmezí let 2010-2019 bylo celkově napříč databázemi identifikováno 124 výsledků v následujícím rozložení: DBLP (34 výstupů), Scopus (47 výstupů) a Web of Science (43 výstupů). Následně byl počet výstupů redukován, a to na základě následujících parametrů. Nejdříve byly odstraněny výstupy, které se opakovaly napříč databázemi, ojediněle byl některý výstup několikrát i ve stejné databázi. V této chvíli počet výstupů klesl na 76, s rozložením DBLP (33 výstupů), Scopus (27 výstupů), Web of Science (16 výstupů). Toto rozložení výsledků je dáno postupem, kterým došlo k vyřazení opakujících se výstupů. Za výchozí databázi byla určena databáze DBLP, vůči které pak byly porovnávány výstupy databáze Scopus (proto počet originálních děl klesl v databázi Scopus tak razantním způsobem). Následně byla databáze Web of Science porovnána s databázemi DBLP a Scopus, proto je počet výstupů v databázi Web of Science nejnižší.

Následně probíhala další selekce, která se skládala ze tří kroků. Cílem prvního kroku bylo určit výstupy, které je možné označit za článek odborného časopisu či článek vznikající v návaznosti na konferenci. Tento postup byl zvolen z důvodu prvku recenzního řízení, které je právě u těchto dvou typů žádaným standardem. Cíleně tak nebylo pracováno s kapitolami knížek nebo jejich pouhými recenzemi. Vyřazeno bylo 21 výstupů. Druhý krok je možné označit za subjektivní kritérium, neboť jeho cílem bylo určit, zda je daný článek či výstup z konference v souladu se stanoveným cílem zmapování přístupů k definici kybernetické zbraně. Vyřazeny tak byly takové výstupy, kde jediná zmínka o kybernetických zbraních byla např. v seznamu literatury, či jediná spojitost s tématem spočívala v názvu časopisu, který obsahoval slovo kybernetický. Tímto krokem neprošlo 11 výstupů. Poslední krok je nutné jednoznačně označit za limit výzkumu. Některé výstupy, který by pravděpodobně prošly výše zmíněnými kritérii, totiž nebyly k dispozici v kompletním znění, neboť nebyla k dispozici licence Masarykovy univerzity, která by umožnila přístup. Celkově tedy nebyl umožněn přístup k 10 výstupům.

Na první pohled byl vcelku rozsáhlý set 124 výsledků redukován na pouhých 34 výstupů, a to s rozložením DBLP (18), Scopus (14) a Web of Science (2). Přestože se může na první pohled jevit, že je problematika již dopodrobna zpracována a existuje dostatek zdrojů, spousta otázek doposud zůstává nezodpovězených. S výstupy je až na výjimku v kapitole *Ostatní přístupy* pracováno v chronologickém pořadí, kdy rozhodující je rok, ve kterém došlo k publikaci. Tento přístup byl zvolen z důvodu snahy reflektovat změnu též s ohledem na postupující čas.

3. KYBERNETICKÉ INCIDENTY

Analýza již proběhlých kybernetických incidentů poskytuje vhodný rámec, skrze něhož lze uceleně přistoupit ke kybernetickým zbraním. Přestože tento přístup není nejjednodušší a je vyžadována nejenom znalost průběhu, ale mnohdy i technických detailů samotných incidentů, umožní komplexní pochopení celé problematiky. V této kapitole je dán prostor k seznámení se s fakty jednotlivých případů, pozornost ale nebude záměrně věnována případu testování nového systému s cílem vyřadit navigaci GPS mimo provoz, neboť v tomto případě se jedná o pouhé podezření.[5]

Nejčastěji zmiňovaným incidentem je bezesporu počítačový červ Stuxnet, jehož cílem bylo obohacovací uranové středisko v Íránu (v Natanz). Samotný Stuxnet způsobil, že se jednotlivé centrifugy začaly točit příliš rychle nebo naopak pomalu, což v některých případech vedlo k jejich explozi a vzniku materiální škody. Poškozené centrifugy musely být vyměněny za nové. Jednalo se o *„světově první kybernetickou zbraň zaměřenou na kritické průmyslové kontrolní systémy.“*[6] Zároveň je Stuxnet označován za *„nejúspěšnější kybernetickou zbraň“*[7], která změnila *„pravidla hry, a to vzhledem k její složitosti, účelu a výkonu.“*[8] Jiní autoři se podrobněji

[5] HAMBLING, David. Hints of a new cyberweapon: GPS spoofing may have thrown vessels off course in the Black Sea. *New Scientist.* 2017, 235(3139), str. 6.

[6] BARZASZKA, Ivanka. Are cyber-weapons effective? *The RUSI Journal.* 2013, 158(2), str. 48.

[7] KOBLENTZ, Gregory D.; MAZANEC, Brian M. Viral Warfare: The Security Implications of Cyber and Biological Weapons. *Comparative Strategy.* 2013, 32(5), str. 423.

[8] MAITRA, Amit K. Offensive cyber-weapons: technical, legal, and strategic aspects. *Environment Systems and Decisions.* 2015, 35(1), str. 173.

věnovali technické stránce Stuxnetu a popisovali proces, který vedl k požadovanému výsledku[9], našli se ovšem i tací, kteří na Stuxnet odkázali bez dalšího.[10]

Tento počítačový červ ale není jediným incidentem, se kterým autoři pracují. Dále se lze obeznámit s průběhem výbuchu transsibiřského plynovodu v roce 1982,[11,12] který je třeba zasadit do kontextu Studené války. Pro bezchybný chod plynovodu potřeboval Sovětský svaz získat speciální software obdobný dnešním SCADA systémům. Existuje podezření, že dodaný software CIA úmyslně pozměnila takovým způsobem, aby došlo k vytvoření přetlaku v potrubí, a to prostřednictvím manipulace s regulačními ventily. Samotný výbuch tedy nebyl způsoben výpadkem systému, ale právě příliš silným tlakem. Odpůrci této teorie naopak tvrdí, že chyba byla na straně pracovníka, který rostoucí tlak i nadále udržoval, aby nedošlo k přerušení toku zemního plynu.[13]

Jak již z názvu vypovídá, v případě experimentu Aurora se nejednalo o reálný útok, neboť se uskutečnil jako pouhý pokus v energetickém oddělení národní laboratoře ve státě Idaho. Cílem experimentu bylo zjistit, zda by hacker mohl zasáhnout do řídícího systému provozujícího generátor

---

9 Srovnej RID, Thomas; McBURNEY, Peter. Cyber-Weapons. *The RUSI Journal.* 2012, 157(1), str. 9. PETERSON, Dale. Offensive Cyber Weapons: Construction, Development, and Employment. *Journal of Strategic Studies*. 2013, 36(1), str. 121. CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists.* 2013, 69(5), str. 34. BELLOVIN, Steven M.; LANDAU, Susan; LIN, Herbert S. Limiting the undesired impact of cyber weapons: technical requirements and policy implications. *Journal of Cybersecurity*. 2017, 3(1), str. 60.

10 Srovnej TYUGU, Enn. Situation awareness and control errors of cyber weapons. **In:** *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*. 2013, str. 143.

11 RID, Thomas; McBURNEY, Peter. Cyber-Weapons. *The RUSI Journal.* 2012, 157(1), str. 9.

12 CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists.* 2013, 69(5), str. 33.

13 Srovnej CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists.* 2013, 69(5), str. 34.

a způsobit tak jeho poškození.[14] Video poukazující na zranitelnost těchto systémů je k dispozici v několika verzích na YouTube.[15]

Skutečným incidentem pak byly DDoS útoky v Estonsku v r. 2007, jež byly s největší pravděpodobností reakcí na přesunutí sochy vojáka představující sovětský válečný památník 2. světové války. Pouliční nepokoje byly doprovázeny sérií DDoS útoků trvajícími tři týdny. Zároveň bylo mimo provoz 58 estonských webových stránek, v součtu více než dvě hodiny byly též nefunkční online služby největší estonské banky.[16]

Útok uskutečněný Izraelem na syrský vzdušný obranný systém v r. 2007 byl naopak pouhým prostředkem, který posloužil k efektivnějšímu útoku na syrský jaderný objekt. Cílem kybernetického útoku bylo přimět obranný systém k tomu, aby po určitý časový úsek nezobrazoval žádná přibližující se letadla a umožnil tak provést útok kinetickými prostředky na fyzický objekt, což se i zdárně podařilo.[17]

Posledním z incidentů je nasazení počítačového viru Shamoon proti saudskoarabské ropné společnosti Saudi Aramco. Shamoon způsobil zničení pevných disků a též došlo k vymazání dokumentů, které byly nahrazeny obrázkem hořící americké vlajky.[18]

Někteří autoři tedy cíleně s kybernetickými incidenty pracují, nejasná situace ale nastává v případě, kdy autoři na tyto incidenty pouze bez dalšího odkazují a neprovádí podrobnější zhodnocení. Slabinou tohoto přístupu je fakt, že může docházet k nežádoucímu zjednodušení celé situace tím, že budou tyto incidenty plošně a bez další analýzy označeny přívlastkem kybernetický a jejich spouštěč pak bude považován za kybernetickou zbraň. V případech, kdy autor cíleně neodpovídá na otázku, zda zmínka o kybernetickém incidentu je zároveň odpovědí na to, zda je

---

[14] CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists.* 2013, 69(5), str. 34.

[15] Například Staged cyber attack reveals vulnerability in power grid. Dostupné z: https://www.youtube.com/watch?v=fJyWngDco3g [vid. 5. února 2020].

[16] RID, Thomas; McBURNEY, Peter. Cyber-Weapons. *The RUSI Journal.* 2012, 157(1), str. 8.

[17] Tamtéž, str. 9.

[18] CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists.* 2013, 69(5), str. 34.

její spouštěč bez další považován za kybernetickou zbraň, je nutné pracovat s oběma variantami (tedy, že se může, ale nemusí jednat o kybernetickou zbraň) a přistupovat k hodnocení situace kriticky. K tomuto kritického zhodnocení se přiklání i autor článku, jenž cíleně využije výše uvedené incidenty k samotné analýze v kapitole *Diskuze.*

4. DEFINICE KYBERNETICKÉ ZBRANĚ

V této kapitole jsou zmíněni autoři, již cíleně představují definici kybernetické zbraně. Prvním z nich je dvojice autorů Lorents a Ottis, již svůj výzkum založili na formální logice s matematicky prokazatelnými výsledky a představili tři vzájemně provázané koncepty, a to zbraň, zbraň informačních technologií (zbraň IT) a kybernetickou zbraň. Za zbraň označují *„systém, který je navržen tak, aby poškodil strukturu nebo operace jiného systému.“*[19] Pro účely tohoto příspěvku je rozhodující pochopení rozdílů mezi zbraní IT a kybernetickou zbraní. Zatímco obě tyto zbraně jsou založeny na informačních technologiích, liší se ve svých cílech. Zbraň IT má širší záběr a je navržena tak, aby *„poškodila strukturu nebo operace jiného systému.“*[20] Lze si představit systém sloužící k přesné lokalizaci vojenského cíle, kterým může být např. budova, která bude posléze zničena pozemní silou. Podmnožinou zbraní IT je kybernetická zbraň, jež má sloužit k *„poškození struktury nebo provozu některých jiných systémů založených na informačních technologiích.“*[21] Tito autoři tedy vnímají kybernetickou zbraň z pohledu cíle, kterým má být prvek obsahující informační technologii.

Obdobně poukazují na souvislost mezi zbraní jako nadřazeným termínem a kybernetickou zbraní jako její množinou autoři Rid a McBurney, svou pozornost ale zaměřili na cíl, kterého má kybernetická zbraň dosáhnout. Takováto zbraň je pak “ *počítačový kód, který je používán nebo navržen tak, aby byl používán s cílem ohrožovat nebo způsobovat fyzické,*

---

[19] LORENTS, Peeter; OTTIS, Rain. Knowledge based framework for cyber weapons and conflict. **In:** *Conference on Cyber Conflict Proceedings 2010.* Tallinn: CCD COE Publications, 2010, str. 139.

[20] Tamtéž.

[21] Tamtéž.

funkční nebo duševní poškození struktur, systémů nebo živých bytostí."[22] Cílem kybernetické zbraně tedy nemusí být pouze systém založený na informační technologii, ale utrpět újmu mohou i jiné objekty. Zároveň představují dělení zbraní na tzv. obecné s nízkým potenciálem (používají připodobnění k paintballovým zbraním, v kybernetickém světě pak odkazují na malware) nebo takové, které jsou specifické a disponují vysokým potenciálem (ty připodobňují k antiradarovým střelám, či k malware, který je schopen proniknout do chráněných a fyzicky izolovaných systémů a je schopen autonomně ovlivnit výstupy systému tak, aby spáchal přímou újmu)[23]. Autoři také upozorňují na nepatrný rozdíl mezi tím, co lze ještě označit za kybernetickou zbraň a co již ne. Určení této hranice má své bezpečnostní, politické a právní důsledky. V této souvislosti zmiňují nezbytný prvek úmyslu, neboť *"ani vysoce sofistikovaný malware, který je vyvíjen a používán pouze za účelem skryté exfiltrace dat ze sítě nebo stroje, není zbraní."*[24]

S prvkem úmyslu pracuje i L. Arimatsu, jež tvrdí, že pouze pokud je prokázáno, že malware má *„útočné schopnosti a existuje úmysl jej používat způsobem, který odpovídá jeho útočné schopnosti, může být považován za kybernetickou zbraň."*[25]

Myšlenku dělení zbraní dle jejich potenciálu nevědomky rozvíjí E. Tyugu. Pozornost věnuje sice pouze pokročilým malwarům (bez bližší specifikace), zároveň ale kybernetické zbraně definuje velmi široce či až vágně, kdy uvádí, že se jedná o *„agenty působící v kyberprostoru, (…) skládající se ze všech výpočetních zařízení, dat a softwaru přístupných prostřednictvím sítě (internet, mobilní sítě atd.)."*[26] Odkazuje sice na Stuxnet

---

[22] RID, Thomas; McBURNEY, Peter. Cyber-Weapons. *The RUSI Journal.* 2012, 157(1), str. 7.

[23] Tamtéž, str. 7 a 8.

[24] Tamtéž, str. 11.

[25] ARIMATSU, Louise. A treaty for governing cyber-weapons: Potential benefits and practical limitations. **In:** *Conference on Cyber Conflict Proceedings 2012*. Tallinn: CCD COE Publications, 2012, str. 98.

[26] TYUGU, Enn. Situation awareness and control errors of cyber weapons. **In:** *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*. 2013, str. 144.

a též na malware Flame[27], ale oproti předchozím autorům tato definice vyvolává více otázek, než nabízí odpovědí.

Více odpovědí naopak nabízí A. K. Maitra, jenž je zároveň prvním autorem pracujícím s vícero definicemi. S ohledem na v té době již existující Tallinnský manuál[28] představuje kybernetické zbraně jako *„kybernetické prostředky k válčení, které jsou svým designem, použitím či zamýšleným použitím schopné způsobit zranění či smrt osob."*[29] Tento přístup je třeba chápat v kontextu Tallinnského manuálu, jehož první vydání je zaměřeno na aplikaci mezinárodního práva v kontextu kybernetické války. Tato definice už tak nereflektuje stav, kdy může být kybernetická zbraň nasazena i v situacích, které nelze označit za kybernetickou válku. Dále se inspiruje přístupem autorů Rid a McBurney a zaměřuje se na cíl, kterým má být *„poškození počítačového nebo telekomunikačního systému mající povahu kritické infrastruktury."*[30] Svoji roli tak nehraje pouze schopnost samotné zbraně, ale též i to, vůči čemu nebo komu je nasazena. Zároveň A. K. Maitra hodnotí možný budoucí vývoj situace a absenci definice kybernetické zbraně označuje za mezeru v právu.[31]

Na problém absence globální definice naráží i autoři Maathuis, Pieters a Berg a předkládají myšlenku, že kybernetickou zbraní je *„počítačový kód vytvořený a/nebo používaný k pozměnění či poškození systému (resp. komponentu informační a komunikační technologie) s cílem dosáhnout (vojenských) cílů proti protivníkům uvnitř a/nebo mimo kyberprostor."*[32] Nad to se autoři dále věnují jednotlivým složkám této definice a blíže vysvětlují

---

[27] Tamtéž, str. 143.

[28] Tady je ovšem odkazováno na jeho první verzi publikovanou v r. 2013, druhá verze vyšla v r. 2017.

[29] MAITRA, Amit K. Offensive cyber-weapons: technical, legal, and strategic aspects. *Environment Systems and Decisions.* 2015, 35(1), str. 179.

[30] Tamtéž, str. 179.

[31] Tamtéž, str. 176.

[32] Cyber weapons: a profiling framework - Clara Maathuis, Wolter Pieters, Jan van den Berg, 2016, s. 4. MATHIUS, Clara; PIETERS, Wolter; BERG, Jan van den. Cyber weapons: a profiling framework. In: *2016 IEEE International Conference on Cyber Conflict (CyCon U.S.) Proceedings*. USA: IEEE eXpress Conference Publishing. 2016, str. 97.

jejich význam. Jejich přístup lze označit za unikátní, jdoucí do hloubky a nevyhýbající se obtížným prvkům celé definice.

Žádoucího efektu na systém může být docíleno různými způsoby, proto se za kybernetickou zbraň dá označit též software, jenž *„může způsobit destruktivní, škodlivé nebo znehodnocující účinky na systém nebo síť, proti které je namířen."*[33] Žádný z těchto autorů už ale neposkytuje bližší vysvětlení či nenabízí příklady, které by napomohly lepší představě o tom, jakými způsoby mohou tyto účinky nastat. Vodítko nabízejí až Kushwaha a Watson, již si kladou tuto otázku a poskytují na ni odpověď. Pokud tedy kybernetické zbraně mají *„způsobit zranění nebo smrt osob nebo poškození či zničení předmětů, musí kompromitovat systémy, které mají dopad na lidský život; tedy systémy spravující kritickou infrastrukturu včetně jaderných nebo vojenských zařízení, vládní infrastrukturu apod."*[34]

Schopnost způsobit újmu je tak klíčovým prvkem kybernetických zbraní. V souvislosti se vzájemným vztahem mezi pojmy kybernetická zbraň a malware na to upozorňují autoři Eggenschwiler a Silomon. Nestačí tyto pojmy nějak mechanicky rozlišovat, je nezbytné zaměřit se na znaky, které konkrétní malware vykazuje. Do množiny kybernetických zbraní bude malware spadat pouze za předpokladu, že vykazuje schopnost způsobit újmu, pouhé *„nasazení malwaru za účelem skryté exfiltrace dat ze sítě"*[35] tak není dostačující. Na schopnost kybernetické zbraně způsobit újmu nelze nahlížet optikou konvenčních zbraní, a to z toho důvodu, že kybernetické zbraně mají kratší životnost, resp. mají pouze dočasnou schopnost způsobit újmu, a to do té doby, než je chyba v konkrétním systému opravena.

S postupujícím časem lze sledovat nejnovější trend přejímání definic, které představily buď státy nebo organizace, konkrétně NATO. Ustupuje tak snaha autorů přicházet s inovativními způsoby, kterak uchopit pojem

---

[33] BELLOVIN, Steven M.; LANDAU, Susan; LIN, Herbert S. Limiting the undesired impact of cyber weapons: technical requirements and policy implications. *Journal of Cybersecurity*. 2017, 3(1), str. 60.

[34] KUSHWAHA, Neal; WATSON, Bruce William. Cyber weapons and the U.S. **In:** *Proceedings of the 17th European Conference on Cyber Warfare and Security*. 2018, str. 1.

[35] EGGENSCHWILLER, Jacqueline; SILOMON, Jantje. Challenges and opportunities in cyber weapon norm construction. *Computer Fraud & Security*. 2018, 12, str. 12.

kybernetická zbraň. Autoři se tak například inspirují definicí, kterou představilo Centrum excelence při Severoatlantické alianci (NATO CCD COE), jež za kybernetickou zbraň označuje *„software, firmware nebo hardware navržený nebo použitý tak, abych způsobil škodu v počítačové doméně.“*[36] Ze stanovisek států je často zmiňována definice Ministerstva obrany Spojených států amerických, které za kybernetickou zbraň považují *„zařízení, počítačový program nebo techniku, včetně jakékoli kombinace softwaru, firmwaru nebo hardwaru, určené k vytvoření efektu v nebo prostřednictvím kyberprostoru.“*[37]

Jakkoli doposud zmíněné přístupy k definici kybernetické zbraně mohou působit konstruktivně, opačný názor zastává F. B. Hare, jenž se vymezil vůči dosavadním autorům, kteří do centra pozornosti umístili počítačový kód a jím zamýšlený účinek, který je schopen vyvolat. Hare zpochybnil tento přístup a označil ho za *„dostačující v diskuzi o počítačové kriminalitě, ale již znemožňující produktivní diskuzi o vojenské aplikaci kybernetické síly.“*[38] K tomuto závěru dospěl z důvodu požadavku přísného hodnotícího procesu, který se uplatňuje při vývoji konvenčních zbraní. V případě počítačového kódu si nelze představit situaci, kdy by armádní složky jednoduše nasadily takovýto kód, aniž by ho před tím nepodrobily přísnému hodnotícímu procesu.[39] Přestože s touto myšlenkou kritizovaní autoři cíleně nepracují, je na zvážení, zda jimi zastávané přístupy jsou v rozporu s požadavkem, který prezentuje Hare.

---

[36] YAMIN, Muhammad Mudassar; KATT, Basel; KIANPOUR, Mazaher. Cyber Weapons Storage Mechanisms. In: *Security, Privacy, and Anonymity in Computation, Communication, and Storage.* 2019, str. 354. KALLBERG, Jan. The Second Amendment and Cyber Weapons: Constitutional Relevance of Digital Gun Rights. *IEEE Technology and Society Magazine.* 2019, 38(2), str. 73.

[37] KALLBERG, Jan. The Second Amendment and Cyber Weapons: Constitutional Relevance of Digital Gun Rights. *IEEE Technology and Society Magazine.* 2019, 38(2), str. 73.

[38] HARE, Forrest B. Precision cyber weapon systems: An important component of a responsible national security strategy? *Contemporary Security Policy.* 2019, 40(2), str. 195.

[39] Tamtéž, str. 195.

5. VÝČET PŘÍKLADŮ KYBERNETICKÝCH ZBRANÍ

Zcela odlišný přístup k definici kybernetické zbraně zaujímají autoři, kteří se ve svých příspěvcích neuchylují k přímé definici. Naopak využívají obecné technické termíny a mnohdy je pouze z kontextu samotného příspěvku možné usoudit, zda autor má sklon určitý technický pojem využít jako prostředek k vyjádření toho, co je to kybernetická zbraň.

Při tomto přístupu narážíme na dva problémy. Prvním z nich je nejasný vztah mezi pojmem malware a kybernetická zbraň. Autor se tak mnohdy zaměřuje na jejich vývoj a možný budoucí potenciál bez toho, aby poskytl řádné teoretické ukotvení. Lze se tak dozvědět, že malware a kybernetické zbraně se *„stávají sofistikovanějšími, nezávislejšími a inteligentnějšími“*[40], ale již není řečeno, co to malware a kybernetická zbraň znamená. Tento přístup bohužel není ojedinělý.[41] Pokud není primárním cílem autorů mluvit o kybernetických zbraních, ale zaměřují svoji pozornost na nějaké související či specifičtější téma, tak lze sledovat tendenci opomíjení představení alespoň nějaké pracovní definice. Příkladem může být výzkum zkoumající prvek kontroly kybernetických zbraní z důvodu zamezení kolaterálních škod, autoři ovšem vzápětí poukazují na nejstarší malwary, které v sobě nějaké kontrolní prvky měly zakomponovány.[42] Jak autoři vnímají vztah mezi kybernetickou zbraní a malwarem zůstává nejasné.

Druhým problémem je specifikace jednotlivých druhů malwaru bez uvedení spojitosti mezi kybernetickou zbraní, malwarem a jejich jednotlivými druhy. Je otázkou, zda *„software, který poškozuje uživatele, počítač nebo síť, lze považovat za malware včetně virů, trojských koní, červů, rootkitů a spywaru“*[43], už také nenaplňuje definici kybernetické zbraně. Autoři se k této otázce nevyjadřují. V některých případech lze nalézt

[40] TYUGU, Enn. Command and control of cyber weapons. **In:** *Conference on Cyber Conflict Proceedings 2012*. Tallinn: CCD COE Publications, 2012, str. 334.

[41] Srovnej KIRAVUO, Timo; SÄRELÄ, Mikko; MANNER, Jukka. Weapons against Cyber-Physical Targets. **In:** *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops Proceedings.* USA: IEEE Computer Society Conference Publishing Services. 2013, str. 321.

[42] Srovnej RAYMOND, David; CONTI, Gregory J.; CROSS, Tom; FANELLI, Robert. A control measure framework to limit collateral damage and propagation of cyber weapons. **In:** *Conference on Cyber Conflict Proceedings 2013*. Tallinn: CCD COE Publications, 2013, str. 182.

odpověď na tuto otázku v kontextu konkrétního příspěvku, kdy autor například uvede, že *„kombinací ransomware s červí technologií a zranitelnostmi nultého dne dohromady vzniká nová ransomware kybernetická zbraň.“*[44] Přestože tento výše uvedený přístup není tak frekventovaný jako možnost představení přímé definice, nachází i přesto několik zastánců.

6. OSTATNÍ PŘÍSTUPY

Tato kapitola představuje značně složité a nejméně uchopitelné pojetí kybernetických zbraní, protože se pouze s velkými obtížemi daří nalézt indikátory, které by odpovídaly na otázku, co je to kybernetická zbraň.

Jedním z přístupů je snaha autorů nalézt inspiraci v právních úpravách jiných zbraní. Je tedy možné se například inspirovat Úmluvou o chemických zbraních a uvažovat o vhodnosti aplikace této úpravy na právní regulaci kybernetických zbraní.[45] Jiní autoři vedle sebe naopak pokládají biologické a kybernetické zbraně, ale již bez toho, aby osvětlili jejich podobu a vzájemný vztah.[46] Lze se také setkat s polemikou, zda lze kybernetické zbraně označit za zbraně hromadného ničení či nikoli. Přestože J. Carr představuje definici zbraní hromadného ničení, již tak nečiní v případě kybernetických zbraní a klade tak více otázek, než nabízí odpovědí.[47] Jiný přístup zastává B. B. Hatch, jenž uvádí, že pokud by bylo kybernetickou operací způsobeno *„přehřátí jaderné elektrárny, došlo by k otevření přehradní hráze nad obydlenou oblastí či by bylo způsobeno zničení či deaktivace služeb řízení letového provozu s následkem leteckých havárií“*[48],

---

[43] ZHIOUA, Sami. The Middle East under Malware Attack Dissecting Cyber Weapons. In: *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops Proceedings.* USA: IEEE Computer Society Conference Publishing Services. 2013, str. 11.

[44] WELSH, Thomas. A Cybersecurity Threat Model for the Detection of a Ransomware Cyberweapon in a Networked Computing Environment. **In:** *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3).* 2019, str. 212.

[45] Srovnej GEERS, Kenneth.Cyber Weapons Convention. *Computer Law & Security Review.* 2010, 26(5), str. 549-550.

[46] Srovnej KOBLENTZ, Gregory D.; MAZANEC, Brian M. Viral Warfare: The Security Implications of Cyber and Biological Weapons. *Comparative Strategy.* 2013, 32(5), str. 419-421.

[47] Srovnej CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists.* 2013, 69(5), str. 33.

tak by byla způsobena škoda takového rozsahu, aby jejího původce bylo možné označit za zbraň hromadného ničení.

Další přístup spočívá v určení limitů, které jsou na kybernetické zbraně kladeny. Může se jednat o limity ekonomické, etické či technologické.

Autoři Mezzour, Carley a Carley se jako jedni z mála zabývají otázkou, kdo stojí za financováním kybernetických zbraní. Ekonomický aspekt se dostává do popředí v případě, kdy je kybernetická zbraň sponzorována státem, pak je její nasazení považováno za *„sofistikovaný, politicky motivovaný kybernetický útok.“*[49] Ekonomickou stránkou věci lze chápat i připodobnění *„velikosti kybernetické kriminality k obchodování se zbraněmi či drogami.“*[50] Už ale není zřejmé, zda je třeba kybernetickou kriminalitu a obchod s kybernetickými zbraněmi chápat odděleně či nikoli. Jiní řeší etické meze, které je třeba brát v potaz, pokud by kybernetické zbraně mohly být použity *„k útoku anonymně na dálku a způsobovaly by velký chaos.“*[51] Technickým aspektům se věnují autoři Pavur a Martinovič, již uvažují o možnosti nasazení kybernetických protisatelitních zbraní[52] či autoři Kim a Eon, již se snaží nastavit parametry, které musí kybernetická zbraň splňovat, aby co nejúčinněji detekovala svůj cíl a zasáhla nejzranitelnější místo cílového systému.[53] Naprosto odlišným případem je situace, kdy autor v úvodu deklaruje, že kybernetické kapacity (bez bližšího vysvětlení vztahu kybernetických kapacit a kybernetických zbraní) nejsou

---

[48] HATCH, Benjamin B. Defining a Class of Cyber Weapons as WMD: An Examination of the Merits. *Journal of Strategic Security.* 2018, 11(1), str. 47.

[49] Srovnej MEZZOUR, Ghita; CARLEY, Kathleen M.; CARLEY, L. Richard. Remote assessment of countries' cyber weapon capabilities. *Social Network Analysis and Mining*. 2018, 8(1), str. 3.

[50] FILSHTINSKIY, Stas. Privacy and security: Cybercrime, Cyberweapons, Cyber Wars: Is There Too Much of It in the Air? *Communications of the ACM.* 2013, 56(6), str. 28.

[51] LIN, Patrick; ALLHOFF, Fritz; ROWE, Neil C. Computing Ethics: War 2.0 Cyberweapons and Ethics. *Communications of the ACM.* 2012, 55(3), str. 24.

[52] Srovnej PAVUR, James; MARTINOVIC, Ivan. The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space. In: *Conference on Cyber Conflict Proceedings 2019*. Tallinn: CCD COE Publications, 2019, str. 213-230.

[53] Srovnej KIM, Ki Hoon; EOM, Jung Ho. Modeling of Cyber Target Selection for Effective Acquisition of Cyber Weapon Systems. *International Journal of Security and Its Applications*. 2016, 10(11), str. 301.

cílem příspěvku[54] a zaměří se na jejich vlastnosti, kterou mohou vzbuzovat humanitární obavy natolik, aby vedly k zákazu těchto technologií. Je diskutabilní, nakolik je vhodným přístupem zamýšlet se nad limity, jež by mohly být kladeny na technologie, když tyto technologie nejsou řádně popsány.

Závěrem lze uvést několik až překvapivých přístupů. Singer již v úvodu upozorňuje, že *„přesná kvalifikace kybernetického nástroje (…) není pro právní problém, který je v příspěvku diskutován, rozhodující.“*[55] Dokud tedy představa autorů o kybernetické zbrani spadá do mezí jejich výzkumu, tak nepovažují za důležité se tomuto aspektu věnovat. Zcela okrajovým a značně bizarním přístupem je pak bez dalšího použití termínu kybernetická zbraň pouze v názvu článku.[56]

7. DISKUZE

Výše uvedené přístupy ke kybernetickým zbraním jsou nyní v této kapitole aplikovány na reálné kybernetické incidenty, jejichž fakta byla již popsána ve druhé kapitole. Tento krok poslouží k naplnění druhého cíle tohoto článku, kterým je syntéza těchto přístupů a nalezení slabých míst. Z tohoto důvodu je pozornost věnována identifikaci jednotlivých faktorů, které ve svém souhrnu vedou k fragmentaci názorů nejenom napříč obory, ale i mezi specialisty v jednom konkrétním odvětví. Pro analýzu nebyly použity přístupy všech výše zmíněných autorů, ale pouze těch, jež poskytli definici, kterou bylo možné na kybernetický incident aplikovat. Pokud tedy autor ve své práci žádnou definici neuvedl, nebyl do této analýzy zařazen.

---

[54] Srovnej BAER, Merritt. Toward Criteria for International Cyber Weapons Bans. In: *2013 World Cyberspace Cooperation Summit IV (WCC4) Proceedings.* IEEE Explore. 2013, str. 1.

[55] SINGER, Tassilo V. P. Update to revolving door 2.0: The extension of the period for direct participation in hostilities due to autonomous cyber weapons. **In:** *Conference on Cyber Conflict Proceedings 2017*. Tallinn: CCD COE Publications, 2017, str. 125.

[56] Srovnej KARLSSON, Marcus; LARSSON, Erik G. Massive MIMO as a cyber-weapon. **In:** *2014 48th Asilomar Conference on Signals, Systems and Computers Proceedings*. 2014, str. 661-665. NGUYEN, Nam-Phong; NGO, Hien Quoc; DUONG, Trung Quang; TUAN, Hoang Duong; COSTA, Daniel Benevides da. Full-Duplex Cyber-Weapon With Massive Arrays. *IEEE Transactions on Communications.* 2017, 65(12), str. 5544-5558.

Pro analýzu byl zvolen následující postup. Rozhodujícím indikátorem bylo profesní zaměření každého autora. Autoři tak byli rozřazeni do následujících skupin – IT, matematika, policy-making, politologie, právo, filozofie a armáda. Následně byla každá definice aplikována na kybernetický incident a byla položena otázka, zda konkrétní incident byl příkladem nasazení kybernetické zbraně či nikoli. Výstupem této analýzy je tabulka uvedená níže.

	STUXNET	TRANSSIBIŘSKÝ PLYNOVOD	DDOS ÚTOKY V ESTONSKU	SYRSKÝ VZDUŠNÝ OBRANNÝ SYSTÉM	SHAMOON A SAUDI ARAMCO
RAIN OTTIS (IT)	ANO	ANO	ANO	ANO	ANO
PETER MCBURNEY (IT)	ANO	ANO	ANO	ANO	ANO
ENN TYUGU (IT)	ANO	ANO	ANO	ANO	ANO
MAATHUIS A PIETERS (IT)	ANO	ANO	ANO	ANO	ANO
BELLOVIN, LANDAU A LIN (IT)	ANO	ANO	ANO	ANO	ANO
KUSHWAHA, WATSON (IT)	ANO	ANO	ANO	ANO	ANO
YAMIN, KATT A KIANPOUR (IT)	ANO	ANO	NE	ANO	ANO
ZHIOUA (IT)	ANO	ANO	NE	ANO	ANO
SILOMON (IT)	ANO	NE	NE	NE	ANO
MEZZOUR, CARLEY A CARLEY (IT)	NE	NE	NE	ANO	NE
ROWE (IT)	NE	NE	NE	NE	NE
WELSH (IT)	NE	NE	NE	NE	NE
LORENTS (MATEMATIKA)	ANO	ANO	ANO	ANO	ANO
BERG (MATEMATIKA)	ANO	ANO	ANO	ANO	ANO

KALLBERG (POLICY-MAKING)	ANO	ANO	ANO	ANO	ANO
EGGENSCHWILER (POLICY-MAKING)	ANO	NE	NE	NE	ANO
MAITRA (POLICY-MAKING)	NE	NE	NE	NE	NE
RID (POLITOLOGIE)	ANO	ANO	ANO	ANO	ANO
ARIMATSU (PRÁVO)	ANO	NE	NE	NE	ANO
LIN A ALLHOFF (FILOZOFIE)	NE	NE	NE	NE	NE
HATCH (ARMÁDA)	NE	NE	NE	NE	NE

Již na první pohled je zřejmé, že dosažení shody ohledně přístupu ke kybernetickým zbraním je obtížné nejenom napříč všemi profesemi, ale i v rámci konkrétního odvětví.

Mezi autory pocházejícími z IT prostředí bylo možné nalézt shodu pouze v případě, kdy používali pro kybernetickou zbraň obecný termín počítačový kód a zaměřili svoji pozornost na účinek spočívající ve schopnosti kybernetické zbraně vyvolat poškození určité struktury. V tomto případě jsou pak všechny incidenty příkladem kybernetické zbraně. Situace již ale není jednoznačná v případě, kdy autoři používají specifičtější termíny. Příkladem jsou autoři Yamin, Katt a Kianpour a taktéž Zhioua, již za kybernetickou zbraň označují určitý software. V tomto případě nelze za kybernetickou zbraň označit DDoS útoky v Estonsku. Silomon se přiklonila ke specifičtějšímu termínu malware, který okruh možných kybernetických zbraní dále zúžil, neboť malware byl použit pouze v případě Stuxnetu a Shamoon proti Saudi Aramco. K větší specifikaci přistoupil Welsh, jenž se zaměřil pouze na ransomware, který nebyl nasazen v žádném z incidentů. Někteří autoři do svých úvah zahrnuly i prvky netechnického charakteru.

Autoři Mezzour, Carley a Carley nevědomky poukazují na problém přičitatelnosti, neboť svoji pozornost zaměřili na státem sponzorovanou kybernetickou zbraň. V tomto případě by bylo možné za kybernetickou zbraň označit pouze útok na syrský vzdušný obranný systém. Rowe se zaměřil na schopnost způsobení velkého chaosu, který ovšem nebyl dosažen ani v jednom z incidentů.

Absolutní shody bylo dosaženo mezi matematiky, již se zaměřili na faktor vyvolání určitého poškození systému a za použití kybernetické zbraně tak lze označit všechny incidenty. V neprospěch ale hovoří minimální vzorek.

Výraznější rozkol lze sledovat mezi autory zabývající se policy-making. Zatímco Kallberg se při popisu kybernetické zbraně přiklonil k obecnějšímu termínu technika, Eggenschwiller zvolila konkrétnější termín malware. Maitra se naopak zaměřil na konkrétnost účinku, který spatřoval v zapříčinění zranění či úmrtí osob.

Zbývající obory politologie, právo, filozofie a armáda měly každý pouze jednoho představitele, možnost nějakých zobecnitelných závěrů je tedy značně omezená. Politolog Rid se přiklonil k široce pojatému účinku spočívajícím v poškození struktury, proto jsou příkladem kybernetických zbraní všechny incidenty. Na účinek v úzkém pojetí se zaměřili filozofové Lin a Allhoff a představitel armádního prostředí Hatch. Naopak Arimatsu při právní analýze pracovala s termínem malware.

Závěrem této analýzy lze vyvodit dva základní faktory vedoucí k názorové fragmentaci napříč či v rámci jednotlivých oblastí. Prvním z nich je obecnost či naopak konkrétnost technického parametru, kdy lze vyvodit závěr, že s větší mírou konkrétnosti se zmenšuje pravděpodobnost označit kybernetický incident za příklad nasazení kybernetické zbraně. Za nejobecnější termín vyvolávající nejmenší rozpory lze označit spojení počítačový kód, konkrétnější je poté termín software a následně malware. Pokud je tedy v diskuzi použit obecný termín počítačový kód, dovoluje tento termín označit incident za kybernetickou zbraň s větší pravděpodobností, než pokud je použit termín software či malware.

Druhý faktor je zaměřen na konkrétnost samotného účinku. Opětovně lze dovodit stejný závěr, že čím konkrétněji je uchopen účinek, tím méně pravděpodobné je, že bude původce kybernetického incidentu označen za kybernetickou zbraň. Příklad lze najít v obecném termínu poškození, nebo naopak v konkrétním účinku chaosu nebo zranění či úmrtí osob.

8. ZÁVĚR

Tento článek si vytyčil dva hlavní cíle. Prvním cílem bylo poskytnout ucelený přehled přístupů k definici pojmu kybernetická zbraň. Za tímto účelem byla zmapována odborná literatura (resp. odborné články a příspěvky z konferencí), které byly v letech 2010-2019 zařazeny v databázích DBLP Computer Science Bibliography Website, Scopus a Web of Science. V rámci druhého cíle došlo k aplikaci jednotlivých definic na reálné kybernetické incidenty a též došlo k identifikaci dvou hlavních faktorů způsobujících názorovou odlišnost.

První kapitola byla věnována metodě sběru a zpracování dat, kdy bylo vysvětleno, jakými kroky bylo docíleno stavu, kdy z původního počtu 124 výstupů bylo v tomto výzkumu pracováno s pouhými 34 výstupy. Přestože se při zběžném seznámení s touto problematikou může zdát, že relevantní literatury je dostatek, tento výzkum prokázal opak. Dosavadní výzkumy neposkytují odpovědi na všechny otázky a některým otázkám se autoři cíleně vyhýbají.

Druhá kapitola se věnovala kybernetickým incidentům a otázce, zda je jejich spouštěč kybernetickou zbraní či nikoli. Nejčastěji zmiňovaným incidentem byl počítačový červ Stuxnet, jehož cílem bylo uranové obohacovací středisko v Íránu. Jakkoli se na první pohled může zdát tento přístup nápomocný, skrývá v sobě jedno zásadní riziko. Pokud nebude zřetelně vyjasněn vztah mezi kybernetickou zbraní a konkrétním kybernetickým incidentem, může docházet bez dalšího k označení kybernetického incidentu za případ nasazení kybernetické zbraně bez ohledu na to, zda bylo naplněno například zmíněné kritérium úmyslu.

Třetí kapitola se zaměřila na autory, kteří ve svých dílech pracují s přímou definicí kybernetické zbraně. Často zmiňovaným prvkem byl

úmysl, se kterým je zbraň konstruována a následně i nasazena. Proto lze za kybernetickou zbraň označit takový kybernetický nástroj, který má útočné schopnosti a je schopen způsobit újmu nejenom jinému kybernetickému nástroji, ale též živým bytostem. Dalším častěji zmiňovaným kritériem pak byl určitý stupeň technologické dokonalosti kybernetické zbraně, který je definován jejím potenciálem dosáhnout stanoveného cíle. S postupujícím časem reagovali autoři na situaci, kdy státy nebo mezinárodní organizace představily své vlastní definice. Přejata tak byla například definice Spojených států amerických či NATO CCD COE.

Čtvrtá kapitola se zaměřila na příklady různých typů kybernetických nástrojů, které autoři výjimečně přímo, ale ve většině případů nepřímo označili za kybernetickou zbraň. Tento přístup v sobě skrýval dvě hlavní úskalí. Prvním z nich byl nevyjasněný vztah mezi pojmy malware a kybernetická zbraň. Druhým problémem byly odkazy na různé druhy malware, a to opětovně bez bližšího vysvětlení vzájemného vztahu. Především tito autoři nereflektovali například prvek úmyslu, který by ovlivnil to, zda je některý malware možné označit za kybernetickou zbraň.

Pátá kapitola pak reflektovala zbývající přístupy, které nebylo možné zařadit do předchozích kapitol. Autoři se tak kupříkladu uchylují k úvahám, zda lze najít možnou inspiraci pro právní regulaci kybernetických zbraní v právní úpravě chemických či biologických zbraní, nebo zbraní hromadného ničení. K těmto úvahám dochází opětovně bez vysvětlení, co je považováno za kybernetickou zbraň. Jiní autoři se zaměřili na představení ekonomických, etických či technologických limitů, které jsou na kybernetické zbraně kladeny.

V rámci poslední kapitoly došlo k aplikaci jednotlivých přístupů na reálné kybernetické incidenty. Tato analýza posloužila k identifikaci dvou hlavních faktorů vedoucích k názorové odlišnosti. První z nich spočívá v technickém parametru, kdy lze shrnout, že s větší mírou konkrétnosti technického parametru se zmenšuje pravděpodobnost označit kybernetický incident za příklad nasazení kybernetické zbraně. Druhý faktor se týká účinku, kdy lze dovodit, že čím konkrétnější účinek, tím méně

pravděpodobné je, že bude původce kybernetického incidentu označen za kybernetickou zbraň.

Závěrem lze uvést, že zkoumaná problematika kybernetických zbraní není vyčerpaným tématem a představuje pouze první krok v obsáhlé analýze možných dopadů jejich nasazení. Při konkrétním zkoumání přístupů k definici by bylo vhodné věnovat pozornost nejenom odborné literatuře, ale též stanoviskům států.

9. SEZNAM LITERATURY

[1] ARIMATSU, Louise. A treaty for governing cyber-weapons: Potential benefits and practical limitations. In: *Conference on Cyber Conflict Proceedings 2012*. Tallinn: CCD COE Publications, 2012, str. 91-109. ISBN 978-9949-9040-9-9.

[2] BAER, Merritt. Toward Criteria for International Cyber Weapons Bans. In: *2013 World Cyberspace Cooperation Summit IV (WCC4) Proceedings.* IEEE Explore. 2013, str. 1-3.

[3] BARZASZKA, Ivanka. Are cyber-weapons effective? *The RUSI Journal.* 2013, 158(2), str. 48-56.

[4] BELLOVIN, Steven M.; LANDAU, Susan; LIN, Herbert S. Limiting the undesired impact of cyber weapons: technical requirements and policy implications. *Journal of Cybersecurity.* 2017, 3(1), str. 59-68.

[5] CARR, Jeffrey. The misunderstood acronym: Why cyber weapons aren't WMD. *Bulletin of the Atomic Scientists.* 2013, 69(5), str. 32-37.

[6] EGGENSCHWILLER, Jacqueline; SILOMON, Jantje. Challenges and opportunities in cyber weapon norm construction. *Computer Fraud & Security.* 2018, 12, str. 11-18.

[7] FILSHTINSKIY, Stas. Privacy and security: Cybercrime, Cyberweapons, Cyber Wars: Is There Too Much of It in the Air? *Communications of the ACM.* 2013, 56(6), 28-30.

[8] GEERS, Kenneth.Cyber Weapons Convention. *Computer Law & Security Review.* 2010, 26(5), str. 547-551.

[9] HAMBLING, David. Hints of a new cyberweapon: GPS spoofing may have thrown vessels off course in the Black Sea. *New Scientist.* 2017, 235(3139), str. 6.

[10] HARE, Forrest B. Precision cyber weapon systems: An important component of a responsible national security strategy? *Contemporary Security Policy.* 2019, 40(2), str. 193-213.

[11] HATCH, Benjamin B. Defining a Class of Cyber Weapons as WMD: An Examination of the Merits. *Journal of Strategic Security.* 2018, 11(1), str. 43-61.

[12] KALLBERG, Jan. The Second Amendment and Cyber Weapons: Constitutional Relevance of Digital Gun Rights. *IEEE Technology and Society Magazine.* 2019, 38(2), str. 71-77.

[13] KARLSSON, Marcus; LARSSON, Erik G. Massive MIMO as a cyber-weapon. **In:** *2014 48th Asilomar Conference on Signals, Systems and Computers Proceedings.* 2014, str. 661-665. ISBN 978-1-4799-8297-4.

[14] KIM, Ki Hoon; EOM, Jung Ho. Modeling of Cyber Target Selection for Effective Acquisition of Cyber Weapon Systems. *International Journal of Security and Its Applications.* 2016, 10(11), str. 293-302.

[15] KIRAVUO, Timo; SÄRELÄ, Mikko; MANNER, Jukka. Weapons against Cyber-Physical Targets. **In:** *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops Proceedings.* USA: IEEE Computer Society Conference Publishing Services. 2013, str. 321-326. ISBN 978-0-7685-5023-7.

[16] KOBLENTZ, Gregory D.; MAZANEC, Brian M. Viral Warfare: The Security Implications of Cyber and Biological Weapons. *Comparative Strategy.* 2013, 32(5), str. 418-434.

[17] KUSHWAHA, Neal; WATSON, Bruce William. Cyber weapons and the U.S. In: *Proceedings of the 17th European Conference on Cyber Warfare and Security.* 2018, str. 1-11. ISBN: 978-1-911218-85-2.

[18] LANGER, Ralph. Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security Privacy.* 2011, 9(3), str. 49-51.

[19] LANGER, Ralph. To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. [online]. 2013 [cit. 25. 10. 2019]. Dostupné z: https://www.langner.com/

wp-content/uploads/2017/04/To-kill-a-centrifuge.pdf.

[20] LIN, Patrick; ALLHOFF, Fritz; ROWE, Neil C. Computing Ethics: War 2.0 Cyberweapons and Ethics. *Communications of the ACM.* 2012, 55(3), str. 24-26.

[21] LORENTS, Peeter; OTTIS, Rain. Knowledge based framework for cyber weapons and conflict. In: *Conference on Cyber Conflict Proceedings 2010.* Tallinn: CCD COE Publications, 2010, str. 129-142. ISBN: 978-9949-9040-1-3.

[22] MAITRA, Amit K. Offensive cyber-weapons: technical, legal, and strategic aspects. *Environment Systems and Decisions.* 2015, 35(1), str. 169-182.

[23] MATHIUS, Clara; PIETERS, Wolter; BERG, Jan van den. Cyber weapons: a profiling framework. In: *2016 IEEE International Conference on Cyber Conflict (CyCon U.S.) Proceedings.* USA: IEEE eXpress Conference Publishing. 2016, str. 94-101. ISBN 978-1-5090-5258-5.

[24] MEZZOUR, Ghita; CARLEY, Kathleen M.; CARLEY, L. Richard. Remote assessment of countries' cyber weapon capabilities. *Social Network Analysis and Mining.* 2018, 8(1), str. 1-15.

[25] NGUYEN, Nam-Phong; NGO, Hien Quoc; DUONG, Trung Quang; TUAN, Hoang Duong; COSTA, Daniel Benevides da. Full-Duplex Cyber-Weapon With Massive Arrays. *IEEE Transactions on Communications.* 2017, 65(12), str. 5544-5558.

[26] PAVUR, James; MARTINOVIC, Ivan. The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space. In: *Conference on Cyber Conflict Proceedings 2019.* Tallinn: CCD COE Publications, 2019, str. 213-230. ISBN 978-9949-9904-5-0.

[27] PETERSON, Dale. Offensive Cyber Weapons: Construction, Development, and Employment. *Journal of Strategic Studies.* 2013, 36(1), str. 120-124.

[28] RAYMOND, David; CONTI, Gregory J.; CROSS, Tom; FANELLI, Robert. A control measure framework to limit collateral damage and propagation of cyber weapons. **In:** *Conference on Cyber Conflict Proceedings 2013.* Tallinn: CCD COE Publications, 2013, str. 181-196. ISBN 978-9949-9211-5-7.

[29] RID, Thomas; McBURNEY, Peter. Cyber-Weapons. *The RUSI Journal.* 2012, 157(1), str. 613.

[30] SINGER, Tassilo V. P. Update to revolving door 2.0: The extension of the period for direct participation in hostilities due to autonomous cyber weapons. In: *Conference on Cyber Conflict Proceedings 2017.* Tallinn: CCD COE Publications, 2017, str. 121-133. ISBN 978-9949-9904-1-2.

[31] TYUGU, Enn. Command and control of cyber weapons. In: *Conference on Cyber Conflict Proceedings 2012.* Tallinn: CCD COE Publications, 2012, str. 333-343. ISBN 978-9949-9040-9-9.

[32] TYUGU, Enn. Situation awareness and control errors of cyber weapons. In: *IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA).* 2013, str. 143-148. ISBN 9781467324366.

[33] WELSH, Thomas. A Cybersecurity Threat Model for the Detection of a Ransomware Cyberweapon in a Networked Computing Environment. **In:** *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3).* 2019, str. 212. ISBN 9781538670026.

[34] YAMIN, Muhammad Mudassar; KATT, Basel; KIANPOUR, Mazaher. Cyber Weapons Storage Mechanisms. In: *Security, Privacy, and Anonymity in Computation, Communication, and Storage.* 2019, str. 354-367. ISBN 9783030249076.

[35] ZHIOUA, Sami. The Middle East under Malware Attack Dissecting Cyber Weapons. In: *2013 IEEE 33rd International Conference on Distributed Computing Systems Workshops Proceedings.* USA: IEEE Computer Society Conference Publishing Services. 2013, str. 11-16. ISBN 978-0-7685-5023-7.

[36] Staged cyber attack reveals vulnerability in power grid. Dostupné z: https://www.youtube.com/watch?v=fJyWngDco3g [vid. 5. února 2020]

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

---

https://doi.org/10.5817/RPT2020-1-4

PRÁVO NA DIGITÁLNÍ SLUŽBY

PAVEL MATES[1]

ABSTRAKT

Článek je kritickým rozborem zákona o právu na digitální služby, který je veřejnosti prezentován jako významný krok k posílení práva fyzických a právnických osob, jakožto klientů veřejné moci a zjednodušení jejich postavení. Prokazuje, že většina práv není nijak nových, naopak vesměs existují v platné právní úpravě již dosud a spíše nejsou aplikována. Poukazováno je na to, že jeho uplatnění si bude vyžadovat masové využívání informačních technologií, bez nichž nebude možno práva na tyto služby využívat. Zdůrazněno konečně je, že zákon neobsahuje efektivní prostředky, kterými by bylo vymáhání práv a jím odpovídajících povinností zajištěno.

KLÍČOVÁ SLOVA

digitální služby, digitální úkony, základní registry, agendové informační systémy, autentizace, identifikace, informace

ABSTRACT

The article is a critical analysis of the Digital Services Right Act, which is presented to the public as an important step towards strengthening the rights of natural and legal persons as clients of public authorities and simplifying their status. It shows that most of the rights are not new, on the contrary, they exist in the current legislation and are not applied. It is pointed out that its application will require massive use of information technology, without which the rights to these services will not be available. Finally, it is stressed that the law does not

[1] Doc. JUDr. Pavel Mates, Csc., kontaktní e-mail: 9122@mail.vsfs.cz.

contain effective means of ensuring the enforcement of rights and its corresponding obligations.

KEYWORDS

digital services, digital operations, basic registers, agenda information systems, authentication, identification, information

1. ÚVOD

Oblíbenou, ba až povinnou, byla v literatuře 19. století spojka "aneb", dnes považována za archaismus, jíž se uváděl jakýsi podnázev literárních děl. Nicméně právě v souvislosti se zákonem č. 12/2020 Sb. o právu na digitální služby a o změně některých zákonů, se její použití přímo nabízí a to ve spojení s názvem divadelní hry Williama Shakespearea "Much Ado About Nothing" nebo jednodušeji proč vůbec tolik povyku.

Zákon byl projednáván a posléze přijat v podobě tzv. komplexního pozměňovacího návrhu, na kterém se shodly všechny strany zastoupené v Poslanecké sněmovně, nepochybně proto, že žádná nechtěla riskovat nařčení, že brání digitalizaci a tedy nechce ulevit občanům při kontaktech se správními úřady, resp. orgány veřejné moci vůbec.[2] Při jeho bližší analýze ovšem vyvstává otázka, je-li opravdu jeho 14 paragrafů takovým přínosem, jak tvrdí předkladatelé a zda mnohé z toho, co obsahuje, již nenalezneme ve stávající úpravě, kterou by možná postačilo jen v nepříliš rozsáhlé míře doplnit nebo dokonce jen uplatňovat.

2. PŮSOBNOST ZÁKONA A ZÁKLADNÍ POJMY

Působnost zákona je stanovena široce, vztahuje se na poskytování digitálních služeb orgány veřejné moci při výkonu jejich působnosti a reguluje právo fyzických a právnických osob činit digitální úkony vůči těmto orgánům a synallagmaticky povinnost orgánů veřejné moci přijímat digitální úkony a poskytovat digitální služby.

[2] Např. https://www.lupa.cz/clanky/zakon-o-pravu-na-digitalni-sluzby-prosel-snemovnou-co-pri-tom-spadlo-pod-stul/

Pojem orgán veřejné moci zákon nevymezuje a zákonodárce zřejmě počítá s tím, že bude použita *per analogiam* legální definice zákona o základních registrech (zák. č. 111/2009 Sb.), podle jejíhož § 2 písm. c) se jím rozumí státní orgán, územní samosprávný celek a fyzická nebo právnická osoba, byla-li jí svěřena působnost v oblasti veřejné správy.[3]

Toto vymezení je významné právě pro určení toho, koho stanovené povinnosti stíhají a kdo může být naopak oprávněným. V praxi jimi budou v prvé řadě orgány veřejné správy, především pak ty, které jsou správci příslušných registrů a informačních systémů, dále také soudy, státní zastupitelství, veřejné sbory, veřejné a státní vysoké školy, profesní komory a následná aplikační praxe ukáže, které další orgány státu a jiných subjektů budou do této množiny zařazeny (*stricto sensu* jsou jimi totiž i vláda nebo Parlament).[4]

Pojem uživatel služby vymezuje zákon tak, že jím může být pouze fyzická osoba nebo právnická osoba (nepochybně i podnikající fyzická osoba), které je tato služby poskytována, nebo která činí digitální úkon, za podmínky, že přitom nemá postavení orgánu veřejné moci. Jestliže se bude vycházet z širšího vymezení orgánu veřejné moci, které je obsaženo v citované zákonné definici, pak by např. správní orgán neměl na tuto službu nárok nikdy, bude-li však použito pojímání užší, tak jak je chápe judikatura, mohly by i tyto orgány být uživateli tam, kde budou vystupovat mimo výkon moci, v rámci tzv. fiskální správy, kde již není rozhodováno

[3] V podstatě shodné vymezení obsahuje v legislativní zkratce § 1 odst. 1 písm. a) o elektronických úkonech autorizované konverzi dokumentů (zák. č. 300/2008 Sb.). Nutno k tomu dodat, že zákonodárce se zde, nikoli vhodně, odchýlil od toho, jak tento pojem dlouhodobě chápe judikatura, která orgán veřejné moci vymezuje jako ten, vůči němuž není subjekt, o němž je rozhodováno, v rovnoprávném postavení a obsah rozhodnutí není závislý na vůli tohoto subjektu (např. usnesení Ústavního soudu sp. zn. I. ÚS 2783/08, sp. zn. II. ÚS 1790/07 a sp. zn. II. ÚS 75/93).

[4] Pokud jde o školy a školská zařízení omezuje se povinnost poskytovat digitální služby toliko na ty úkony, u nichž je toto poskytnutí vyznačeno v katalogu služeb. Obce a kraje při výkonu samostatné působnosti, mají právo, ale nikoli povinnost digitální služby poskytovat. Otázkou je, zda lze reálně uvažovat, že by digitální služby mohly poskytovat tzv. veřejné stráže a lze jen doufat, že nebudou zařazeny do katalogu služeb.

o právech a druhá strana vztahu je v rovnoprávném postavení vůči správnímu orgánu, takže by nebyl důvod, jim toto postavení nepřiznat.[5]

Zákon definuje pojem digitální služby jakožto úkon, který vykonává orgán veřejné moci vůči uživateli služby v rámci agendy. Pro určení, že jde o takový úkon, musí být splněna formální podmínka, jíž je jeho zařazení do katalogu služeb. Nadbytečný se jeví dovětek, že tento úkon musí být veden v elektronické podobě, protože pojmově jiná možnost u digitálních forem ani v úvahu nepřichází. *Ex lege* je jím rovněž úkon, který je vykonávaný kontaktním místem veřejné správy, čímž se působnost zákona v tomto rozsahu rozšiřuje i na subjekty, které nejsou, podle žádné z definic ani judikatury, orgány veřejné moci.[6]

V podstatě shodně je vymezen též digitální úkon, jako ten, který je uživatelem služby realizován vůči orgánu veřejné moci v rámci jeho agendy a to opět za podmínky, že je vedený v katalogu služeb, jako úkon v elektronické podobě, což prakticky znamená, že se musí dít způsobem umožňující dálkový přístup, tedy internetem.

Klíčovým pro realizaci digitálních služeb, je pojem katalog služeb, vzhledem k tomu, že jak zmíněno, jen úkony, v něm vedené mají povahu digitální služby, resp. digitálního úkonu. Jejich seznam má být veden v základním registru agend, orgánů veřejné moci, soukromoprávních uživatelů a některých práv a povinností, čím by se měl adresátům současně dostat úplný přehled o tom, na které z těchto služeb a od kterých orgánů mají nárok. [7]

3. DRUHY DIGITÁLNÍCH SLUŽEB

Zákon autoritativně stanoví v § 3, že uživatel digitální služby má právo tuto využívat a orgán veřejné moci ji musí poskytovat. V této souvislosti vyznívá problematicky ustanovení § 14 odst. 1 zákona, podle něhož nepodnikající

[5] Např. KOPECKÝ, M., Správní právo. Obecná část, Praha: C. H. Beck, 2019, s. 7.

[6] Podle § 8a zákona o informačních systémech veřejné správy (zák. č. 365/2000 Sb.) jsou kontaktními místy veřejné správy také držitelé poštovní licence, banka, pojišťovna, zdravotní pojišťovna a poskytovatel univerzální služby podle zákona o elektronických komunikacích a Hospodářská komora České republiky.

[7] Viz § 3 a § 48 a následující zákona o základních registrech (zák. č. 111/2009 Sb.).

fyzická osoba nemůže být nucena využívat digitální služby nebo činit digitální úkony podle tohoto zákona. Nelze totiž pochybovat o tom, že by mohly být právnické osoby a podnikající fyzické osoby nuceny tyto služby využívat, resp. činit digitální úkon, již jen proto, že v zákoně se všude hovoří o právu něco činit, získávat, využívat atd., takže není zřejmé, proč zákonodárce považoval tuto regulaci za nezbytnou.[8]

V ustanovení § 4, kde je zakládáno právo činit digitální úkon, zákon v podstatě rekapituluje stávající možnosti, jak provádět tyto úkony způsobem nevzbuzujícím pochyby o subjektu projevujícím vůli ani o jejím obsahu. Předpokládá se, že tak jako dosud, bude možno úkon činit datovou schránkou, dále prostřednictvím kontaktního místa veřejné správy,[9] sítě elektronických komunikací dokumentem, který je podepsán buď uznávaným elektronickým podpisem[10] nebo opatřen uznávanou elektronickou pečetí, informačním systémem veřejné správy, způsobem, který umožňuje prokázání totožnosti uživatele služby za použití elektronické identifikace (např. občanským průkazem s kontaktním elektronickým čipem, v němž je nahrán identifikační certifikát a někdy v příštích letech možná i jinými identifikačními doklady)[11] a autorizaci takového úkonu uživatelem služby, následné prokázání projevu vůle učinit

[8] Taková povinnost ovšem může být založena zvláštním zákonem, jako je tomu podle § 72 odst. 4 daňového řádu, který pro případ, že má daňový subjekt nebo jeho zástupce zpřístupněnu datovou schránku nebo zákonem uloženou povinnost mít účetní závěrku ověřenou auditorem, ukládá povinnost činit podání pouze datovou zprávou s využitím dálkového přístupu.

[9] Seznam digitálních úkonů, které bude možno činit prostřednictvím kontaktního místa veřejné správy, má určit vláda nařízením.

[10] Uznávaný elektronický podpis, je jak známo "český vynález" (otázkou nakolik nezbytný, ale diskuse o tom si vyžaduje jiný prostor), jehož definici obsahuje § 6 odst. 2 zákona o službách vytvářejících důvěru pro elektronické transakce (zák. č. 297/2016 Sb.), podle níž se jím rozumí zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis, zatímco na jiných místech použitý pojem kvalifikovaný elektronický podpis je vymezen v čl. 3 odst. 12 eIDAS jako zaručený elektronický podpis, který je vytvořen kvalifikovaným prostředkem pro vytváření elektronických podpisů a který je založen na kvalifikovaném certifikátu pro elektronické podpisy.

[11] Úroveň záruky prostředku pro elektronickou identifikaci je určena v katalogu služeb a není-li zde uvedena, může si podle § 12 zákona uživatel služby zvolit, jakým prostředkem ji provede, nejméně však musí být v úrovni značná, podle kritérií stanovených v čl. 8 odst. 2 eIDAS.

úkon[12] a konečně i jiným, způsobem, který v budoucnu stanoví zákon. Jako zásada přitom platí, že pokud zákon výslovně nestanoví podobu úkonu vůči orgánu veřejné moci, má uživatel služby právo jej činit jako digitální úkon.

Současně s tím je uložen orgánům veřejné moci závazek zveřejňovat tzv. interaktivní elektronické formuláře, čímž se rozumí ty, které po prokázání totožnosti uživatele služby s využitím elektronické identifikace (např. zmíněným občanským průkazem), zajistí automatizované doplnění údajů, které jsou nezbytné pro poskytnutí digitální služby.[13] Formát, strukturu a obsah tohoto formuláře mají orgány veřejné moci zveřejňovat, a jestliže tak neučiní, může uživatel služby realizovat digitální úkon v každém výstupovém formátu podle zákona o archivnictví a spisové služby.[14]

K definičním znakům technologií, jejichž prostřednictvím lze učinit digitální úkon patří, že nutně zanechávají digitální stopu (což je vyjádřeno i ve známé formulce, podle níž internet nezapomíná). Zákonodárce nicméně vyšel z toho, že nikoli u všech druhů digitálních služeb má uživatel takovou stopu, resp. záznam k dispozici, což by mohlo digitální úkon, v případě, kdy budou vzneseny pochyby o tom, že byl učiněn, degradovat. Jakkoli jde o situace spíše ojedinělé, považoval přesto za potřebné v § 5 zákona zakotvit právo na osvědčení digitálního úkonu. Jím se zavádí povinnost orgánu veřejné moci, náleží-li do skupiny tzv. veřejnoprávních původců ve smyslu § 3 odst. 1 zákona o archivnictví a spisové službě, aby vždy poté, co byl vůči němu učiněn digitální úkon, poskytl uživateli služby osvědčení, že se tak stalo. Způsob, jímž má být osvědčení poskytnuto je na uživateli služby, který má na výběr, zda se tak stane do datové schránky, na Czech Point nebo prostřednictvím portálu

[12] Takový postup upravuje např. § 9 a následující zákona o informačních systémech veřejné správy (zák. č. 365/2000 Sb.) při získávání výpisu ze zápisu vedeného v elektronické podobě v příslušném informačním systému.

[13] Ani zde nejde o novinku, protože povinnost vytvářet tyto formuláře již existuje. Např. podle § 54 odst. 1 zákona o základních registrech platí, že při ohlašování agendy v základním registru agend, orgánů veřejné moci, soukromoprávních uživatelů a některých práv a povinností mají být předkládány formuláře v elektronické podobě pro podání a jiné úkony.

[14] Seznam těchto výstupových formátů je obsažen v § 23 vyhlášky č. 259/2012 Sb., o podrobnostech výkonu spisové služby, ve znění pozdějších předpisů; podrobnosti k tomu viz LECHNER, T., Elektronické dokumenty v právní praxi, Praha: Leges, 2013, s. 164-165.

veřejné správy. Toto osvědčení má obsahovat důvěryhodné zachycení obsahu digitálního úkonu nebo jeho jinou identifikaci, dále určení subjektu, který jej učinil, adresáta úkonu a způsob, datum a čas, kdy byl proveden. Opatřeno musí být kvalifikovanou elektronickou pečetí a kvalifikovaným časovým razítkem příslušného orgánu veřejné moci.

Osvědčení se bude nepochybně poskytovat k žádosti nikoli automaticky o každém digitálním úkonu, což lze dovodit i z toho, že je na uživateli, aby zvolil způsob osvědčení.

Zákon ovšem neřeší situaci, kdy orgán veřejné moci bude popírat, že k digitálnímu úkonu vůbec došlo, protože pak by musela být tato skutečnost nejprve prokázána a důkazní břemeno leží na uživateli služby, jako je tomu podle konstantní judikatury např. u podání, která byla učiněna e-mailem vůči orgánům veřejné moci, kdy, nepodaří-li se dohledat podání v elektronické podatelně orgánu veřejné moci, jde tento nedostatek k tíži podatele.[15]

K zjednodušení procedur při jednáních s orgány veřejné moci, ale i v soukromoprávním styku, má sloužit právo na nahrazení úředně ověřeného podpisu nebo uznávaného elektronického podpisu (§ 6 zákona). Nadále tedy v případech, kdy je požadováno úřední ověření vlastnoručního podpisu či uznávaného elektronického podpisu, bude tento požadavek považován za splněný za využití elektronického podpisu na dokumentu nedílně spojeném s kvalifikovaným elektronickým podpisem a kvalifikovaným časovým razítkem subjektu, který je oprávněný ověřovat pravost podpisu, jímž se tak přímo provede tzv. legalizace, čili ověřením toho, že před ním dotyčný dokument podepsal, resp. uznal podpis za vlastní, aniž by bylo třeba provést jeho konverzi. Druhou možností jak ověření provést je využití elektronického podpisu na dokumentu nedílně spojeném se záznamem informačního systému veřejné správy, které musí být opatřeno kvalifikovanou pečetí a kvalifikovaným elektronickým razítkem správce tohoto systému, z něhož plyne, že došlo k elektronické

[15] Např. usnesení Nejvyššího správního soudu čj. 8 Afs 82/2006-68, rozsudek Nejvyššího správního soudu čj. 7 Azs 113/2015-32 a rozsudek Krajského soudu v Hradci Králové - pobočka v Pardubicích čj. 52/2015-42.

identifikaci toho, kdo byl podepisujícím a to prostřednictvím kvalifikovaného systému takové identifikace s úrovní záruk vysoká.[16] Odpovědnost za to, že podpisujícím byl skutečně uživatel služby, zde nese příslušný správce informačního systému, resp. stát.

Platí konečně, že požadavek úředního ověření podpisu se považuje za splněný s využitím elektronického podpisu, lze-li s využitím údajů v základním registru obyvatel či portálu veřejné správy ověřit, že kvalifikovaný certifikát pro elektronický podpis, jímž byl dokument podepsán, patří podepisujícímu.[17]

V zakotvení práva na využívání údajů či též práva na sdílení, zákonodárce nepochybně usiluje o prosazení, mnohokrát proklamované a v praxi zatím ne příliš uplatňované zásady, že obíhat mají údaje, nikoli jejich nositelé, tedy občané a právnické osoby.[18]

Podle § 7 zákona nesmějí orgány veřejné moci vyžadovat od účastníků řízení, resp. ani jiných dotčených osob údaje, které jsou vedené v některém základním registru či agendovém informačním systému, samozřejmě za podmínky, že jsou jim zpřístupněné pro výkon agendy, jakož i ty, k nimž získají přístup na základě souhlasu uživatele služby. Jako nadbytečný se jeví dovětek, že takto získané údaje jsou zavázány využívat, protože, proč by si je jinak opatřovaly. Tím se, ovšem zákonným způsobem, modifikuje

---

[16] Viz čl. 8 odst. 2 písm. c) nařízení eIDAS, resp. prováděcí nařízení Evropské komise k němu č. 2015/1502.

[17] Je-li však vyžadováno pro právní jednání, aby byla plná moc udělena formou veřejné listiny (§ 567 občanského zákoníku) v písemné formě a úředně ověřeným podpisem (§ 441 odst. 2 občanského zákoníku), lze k ověření použít pouze kvalifikovaný elektronický podpis a kvalifikované časové razítko osoby, která je oprávněná k legalizaci.

[18] Takový komfort byl slibován již v souvislosti s přijetím zákona o základních registrech, v jehož důvodové zprávě se mimo jiné uvádí, že se jím zvýší komfort fyzických a právnických osob, které nebudou muset předkládat stejné údaje různým úřadům ani shánět a předkládat doklady, protože si je příslušný orgán veřejné moci bude moci obstarat sám (Sněmovní tisk č. 598/0 5. volební období). Tuto zásadu chce zákonodárce naplňovat i tím, že podle novelizovaného znění § 6 odst. 2 správního řádu si má správní orgán opatřovat podklady přednostně s využitím úředních evidencí, do nichž mají přístup a od dotčených osob je smí vyžadovat toliko, stanoví-li tak právní předpis, což ovšem principiálně platilo i dosud. V této souvislosti si lze položit otázku, proč nebyly stejně měněny či doplněny také jiné procesní předpisy a zda se tedy zde bude postupovat pouze podle obecné úpravy zákona o digitálních službách.

zásada, že orgány veřejné moci mají přístupu do informačních systémů v rozsahu určeném zvláštním zákonem.

Náležitosti souhlasu zákon neupravuje. Protože je dáván ohledně osobních údajů, je třeba respektovat požadavky stanovené pro podmínky souhlasu v čl. 4 odst. 11 Nařízení Evropského parlamentu a Rady EU 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů (dále GDPR), podle něhož musí být souhlas svobodný, konkrétní, informovaný a jednoznačný projev vůle, jímž se dává souhlas se zpracováním osobních údajů. V praxi může vyvolat problémy to, že není stanoveno, který uživatel může relevantně souhlas dát. Vzhledem k tomu, že se tu nejedná o zpracování pro účely nabízení služeb informační společnosti, nepřichází v úvahu hranice 15 roku věku, kterou má na mysli § 7 zák. č. 110/2019 Sb., o zpracování osobních údajů, nemůže to být ani kritérium nabytí svéprávnosti před dovršením 18 roku věku přiznáním svéprávnosti nebo uzavřením manželství podle § 30 a následujících občanského zákoníku, protože to platí jen pro účely právních jednání podle občanského zákoníku. S ohledem na to může tedy souhlas zřejmě dát pouze osoba zletilá, tj. ta, která dovršila 18 rok věku.[19]

V rozsahu uděleného souhlasu se neuplatňuje povinnost mlčenlivosti, která váže toho, kdo má k údajům v informačním systému přístup.

Závisí na rozhodnutí uživatele služby, v jakém rozsahu a na jakou dobu tento souhlas udělí, může tedy být dán některému nebo všem orgánům, na dobu neurčitou i určitou dobu, atd. a stejně tak, je na něm zda a v jakém rozsahu souhlas odvolá a to bez jakýchkoli podmínek nebo důsledků. Jakmile bude odvolání orgánům veřejné moci doručeno, musí přestat údaje zpracovávat.[20]

Oznámení o souhlasu i jeho odvolání je třeba učinit vůči Ministerstvu vnitra výhradně prostřednictvím jím zveřejněného elektronického

[19] Pro tento závěr hovoří i to, že podle § 58 odst. 1 zákona o základních registrech zůstává zachována osobě starší 18 let možnost udělit souhlas s tím, aby byly poskytnuty referenční údaje v jím vymezeném rozsahu jiné fyzické nebo právnické osobě do datové schránky této osoby.

[20] Toto právo dává ovšem uživatelům služeb čl. 7 GDPR, takže si lze opět možno položit otázku, proč jej zákon reprodukuje.

formuláře na portálu veřejné správy, které jej pak zapíše do příslušného základního registru, což se může dít toliko za použití uznávaného elektronického podpisu.

V oprávnění na zápis práva, povinnosti nebo právní skutečnosti chce zákonodárce aktivovat možnost již v současnosti obsaženou v § 50 zákona o základních registrech, podle něhož mají být do základního registru práv a povinností, zapisovány také údaje o právech a povinnostech fyzických a právnických osob, včetně údajů o rozhodnutích orgánů veřejné moci, která dosud nebyla realizována, resp. využívána. Podle ustanovení § 8 zákona lze provést, k žádosti uživatele služby, zápis do tohoto základního registru práva, povinnosti a právní skutečnosti plynoucí z úkonu orgánu veřejné moci, který je uveden v katalogu služeb. Toto oprávnění přichází v úvahu pouze ohledně těch z uvedených práv, povinností či skutečností, které nejsou zapsány v některém základním registru ani agendovém informačním systému, protože by jistě bylo protismyslné, aby byly tyto informace zapisovány dvakrát. Na uživateli je, které z údajů si takto nechá zapsat a dostává se mu tak výhody tím, že je orgány veřejné moci budou muset využívat, resp. dotyčný je již nebude muset prokazovat (např., že je držitel nějakého veřejnoprávního oprávnění nebo dosáhl určitého vzdělání). Celý proces má vypadat tak, že uživatel zašle Ministerstvu vnitra vyplněný elektronický formulář, které jej postoupí příslušnému orgánu veřejné moci a poté, co jím bude osvědčena a potvrzena existence práva, povinnosti či právní skutečnosti ministerstvo, jakožto správce a editor registru práv a povinností, do něj učiní zápis. Zákon příslušným orgánům veřejné moci ukládá, aby zápis práva, povinnosti a právní skutečnosti průběžně aktualizovaly a zjistí-li rozpor mezi zapsaným a skutečným stavem, mají jej prostřednictvím Ministerstva vnitra bez zbytečného odkladu odstranit. Lze předpokládat, že plnění tohoto úkolu bude nepochybně značně náročné, protože orgány veřejné moci budou muset permanentně sledovat, které z práv, povinností a skutečností jsou zapsány. Otázkou přitom je, jaké důsledky bude mít, pokud aktualizaci neprovedou nebo tak neučiní bez zbytečného odkladu, což si bude také vynucovat i výklad tohoto neurčitého pojmu.

Uživatelé služby získávají dále právo zjednodušeného prokázání nebo osvědčení právních skutečností (§ 9 zákona). Učinit tak mohou dvojím způsobem: 1) odkazem na údaje vedené v základním registru či agendovém informačním systému; 2) výpisem z informačního systému veřejné správy, který je vydáván v elektronické podobě a nese záruku věrohodnosti a neporušenosti.[21]

S tím pak souvisí i to, že uživatel služby, který prokáže svoji totožnost, nemusí při uplatňování svého práva, splnění povinnosti či doložení právní skutečnosti poskytovat údaje (v podobě dokladu, rozhodnutí, průkazu apod.), jsou-li tyto vedeny v základním registru, resp. agendovém informačním systému, k němuž má příslušný orgán veřejné moci přístup. Samozřejmou podmínkou se jeví, že uživatel toto svoje právo aktivně uplatní, tedy poukáže na to, že údaj je již někde veden.

Jako v podstatě nadbytečné se jeví výslovné zakotvení zásady, podle níž nesmí orgán veřejné moci vyžadovat dokumenty v listinné podobě, jsou-li mu předloženy v podobě elektronické, protože tak plyne z práva činit digitální úkon, ale prakticky i § 22 odst. 3 zákona o elektronických úkonech a autorizované konverzi dokumentů, podle něhož v případech, že má být předložen správnímu orgánu, soudu anebo jinému státnímu orgánu dokument v listinné podobě, je tato povinnost splněna předložením jeho výstupu, který vznikl na základě konverze.

K právu na zápis adresy, na níž mají být doručovány písemnosti (§ 3 odst. 3 zákona o evidenci obyvatel, zák. č. 133/2000 Sb. a § 18 odst. 1, resp. § 31 zákona o základních registrech), přibývá oprávnění nechat si zapsat do základního registru obyvatel a registru osob také údaje o elektronické adrese nebo telefonním čísle (§ 10 zákona). Tyto tzv. kontaktní údaje mohou být užívány pro účely informací podle zákona o právu na digitální služby, resp. i jiných informací, které souvisejí s poskytováním této služby a je na uživateli, aby si určil, které z nich mu mají být zasílány. Toto právo bude opět realizováno u Ministerstva vnitra,

[21] Rovněž tato možnost dnes již prakticky existuje v podobě práva na vydání ověřeného výstupu z informačního systému veřejné správy podle § 14 odst. 1 zákona o základních registrech.

prostřednictvím elektronického formuláře a služby, které pro tento účel zřídí.[22]

Právo na přístup k informacím, které jsou vedeny o uživateli služby v základních registrech a agendových informačních systémech (§ 11 zákona) dílem fakticky reprodukuje toto oprávnění již stanovené ve zvláštních zákonech a také právo na informace a přístup k osobním údajům zakotvené v čl. 13-15 GDPR.[23]

Sám zákon o digitálních službách limituje toto právo tím, že vylučuje v § 14 odst. 2 svoji působnost na bezpečnostní řízení, prováděného Národním bezpečnostním úřadem a generálně ohledně zpravodajských služeb. Stejně tak tomu ovšem bude i v těch případech, kdy poskytnutí takové informace zvláštní zákon vylučuje nebo váže její poskytnutí na splnění zvláštních podmínek (jako příklad lze uvést informační systémy vedené Policií České republiky, Vězeňské služby nebo rejstřík fyzických osob vyloučených z účasti na hazardních hrách).

V souvislosti s tím je zaváděno tzv. notifikační právo uživatelů digitálních služeb a jemu odpovídající informační povinnost orgánů veřejné moci. Konkrétně získávají uživatelé možnost, aby jim bylo sděleno, že končí platnost jejich občanského průkazu, cestovního pasu nebo řidičského průkazu a to nejpozději 30 dní před uplynutím této lhůty prostřednictvím datové zprávy zaslané do datové schránky. Dále mají právo na zasílání informace o končící platnosti dokladu, průkazu nebo osvědčení na kontaktní údaj a za tím účelem si jej mohou nechat zapsat do registru práv a povinností. Předpokladem realizace těchto práv je nepochybně iniciativa ze strany uživatelů služby, kteří tedy musí o poskytnutí informace požádat.

---

[22] Zákonodárce se zde nepochybně inspiroval úpravou předpisů, které dávají možnosti poskytovat takové kontaktní údaje ve zvláštních případech, jako je tomu podle zákona o občanských průkazech (zák. č. 328/1999 Sb., podle něhož může být v žádosti o vydání občanského průkazu uvedeno telefonní číslo pro veřejnou mobilní telefonní síť nebo adresu elektronické pošty pro účely poskytnutí informace o možnosti převzetí občanského průkazu.

[23] Jako příklad lze uvést zákon o evidenci obyvatel, který zakládá právo obyvateli staršímu 15 let, aby mu Ministerstvo vnitra, krajský úřad, obecní úřad obce s rozšířenou působností a ohlašovna poskytly údaje vedené v informačním systému k jeho osobě, takové informace lze ovšem získat i z informačních systémů, které jsou všeobecně přístupné, jakým je obchodní rejstřík, seznamy členů profesních komor nebo letecký rejstřík.

Notifikační právo zahrnuje rovněž oprávnění uživatele být zpraven o každé změně jeho údajů a svých o právech a povinnostech vedených v základních registrech a agendových informačních systémech. Tato informace se mu má dostat neprodleně poté, kdy ke změně došlo a to opět prostřednictvím datové schránky. Údaje jsou mu zasílány jen v rozsahu základního registru, resp. agendového informačního systému, jehož je orgán veřejné moci správcem. Obdobně jako je tomu u práva na zápis práv a povinností i zde si lze položit otázku, jaké důsledky bude mít, jestliže informace nebude podána neprodleně nebo dokonce vůbec.

Aby právo na digitální služby bylo reálné, zavádí zákon v § 13 právo na tzv. technickou neutralitu dikcí, podle níž se tyto služby zveřejňují bez závislosti na konkrétní platformě, resp. technologii, jinak řečeno, nesmí být při poskytování digitálních služeb použito takové řešení, které by omezovalo použití běžně dostupných technologií hardwaru nebo softwaru.[24] Toto pravidlo se ovšem neuplatňuje tam, kde by jeho aplikace byla nepřiměřeně náročná ekonomicky, nebyly by splněny požadavky na bezpečnost informačního systému nebo by tomu bránil právem chráněný veřejný zájem, což jsou jak patrno kritéria značně neurčitá, takže lze očekávat problémy při jejich výkladu.

Výstup digitální služby v podobě poskytnuté informace, potvrzení, osvědčení atd., má být zásadně poskytnut v otevřeném formátu tj. takovém, který je přístupný bez omezení a je-li to možné, také ve strojově čitelném.

4. ITINERÁŘ REALIZACE ZÁKONA

Poněkud neortodoxním způsobem hodlá zákonodárce zajistit realizaci zákona, když v § 14 ukládá vládě, aby do 12 měsíců po nabytí účinnosti stanovila pro období následujících čtyř let harmonogram a technické způsoby provedení digitalizaci úkonů, které jsou obsaženy v katalogu služeb a dosud nejsou poskytovány jako digitální služby nebo prováděny

[24] Zákon zde v podstatě doslova přebírá definice obsažené čl. 2 směrnice Evropského Parlamentu a Rady č. 2003/98/ES o opakovaném použití informací veřejného sektoru, ve znění směrnice č. 2013/37/EU.

jako digitální úkony.[25] Jakou formou se tak má stát stanoveno není, nepochybně však přichází v úvahu pouze vydání nařízení, protože pouhé usnesení vlády by nezavazovalo samosprávné subjekty. Neurčitě pak vyznívá pokyn ohlašovatelům agend, aby zajistili digitalizaci úkonů. Po uplynutí čtyřletého období mají být všechny tyto úkony poskytovány též jako digitální služby, resp. být umožněno, aby se prováděly jako digitální úkony. *Sine ira et studio* musí nutně napadnout otázka, jaké důsledky bude mít, pokud by vláda tomuto závazku nedostála, ohlašovatelé agend nezajistili digitalizaci úkonů a služby a úkony nebyly jako digitální poskytovány.

Jestliže bude pozapomenuto nějaký úkon zařadit do katalogu služeb má orgán veřejné moci po uplynutí pěti let od účinnosti zákona povinnost poskytovat jej jako digitální službu nebo umožnit, aby byl prováděn jako digitální úkon, ledaže by to zvláštní zákon vylučoval. Tím by tedy měly být na základě obecné úpravy poskytovány digitální služby i tam, kde to v současnosti zvláštní zákon výslovně nestanoví.

Zásadní důležitost pro realizaci zákona bude mít naplnění katalogu služeb, což budou mít prakticky v rukách samy orgány veřejné moci a lze jen odhadovat, nakolik budou vstřícné tomu, aby si rozšiřovaly svoje úkoly.[26]

5. NĚKOLIK DALŠÍCH OTAZNÍKŮ NA ZÁVĚR

Je jistě chvályhodné, že jak se praví hned v úvodu důvodové zprávy a je opakováno na řadě jejich dalších míst, že cílem zákona je posílit práva fyzických a právnických osob, jakožto klientů veřejné moci a zjednodušit tak jejich postavení. Důležitým předpokladem k tomu je, zda budou ochotni aktivovat si příslušné elektronické prostředky, bez nichž nemohou práva na

[25] Poněkud nadbytečné se jeví dovětek, že digitalizovat nelze služby, u nichž to jejich povaha vylučuje, což jsou *per se* ty, které musí být provedeny výhradně fyzickým předáním dokumentu (např. identifikačních dokladů nebo státní poznávací značky motorového vozidla).

[26] S ohledem na technologickou náročnost realizace některých práv, nabývají ustanovení o právu na digitální úkon, ověření elektronického podpisu, využívání údajů, zápis práva, povinnosti a právní skutečnosti a na zápis kontaktního údaje účinnosti až prvním dnem 25 měsíce po vyhlášení zákona, k čemuž došlo 17. ledna 2020.

digitální služby realizovat, zejména uznávaný elektronický podpis a datovou schránku. Podle nejčerstvějších údajů si k 1. 11. 2019 zřídilo dobrovolně datovou schránku 176 750 fyzických osob a 182 691 podnikajících fyzických osob, což představuje zhruba třetinu z celkového počtu datových schránek, k čemu významně napomohla to, že se do datových schránek lze přihlašovat přes mobilní aplikaci Mobilní klíč a dále došlo k napojení informačního systému datových schránek na národní identitní autoritu, čímž se umožnilo přihlašování eObčankou. [27]

V tomto směru jsou tedy spíše důvody k optimismu, méně však již v tom, zda se budou běžní zájemci o digitální služby schopni v zákoně orientovat a využívat tak svá práva. Zákon je "uživatelsky nevlídný", protože nutně vychází z terminologie regulace IT technologií, takže zde bude velmi záležet, slovy V. Knappa, na jeho účinnosti sociální, která může být dosti vzdálená účinnosti formální.[28]

Lze přitom očekávat, že aplikační praxe odhalí nejrůznější problémová místa zákona, např. za jakých podmínek bude záviset uplatnění jednotlivých práv na aktivitě uživatelů služeb a kdy mají být realizována orgány veřejné moci ex lege.

Třebaže ustanovení zákona jsou mnohdy formulována při vymezení povinností jejich poskytovatelů, kogentně, vyznívá zákon jako celek spíše vágně, mnohdy jako deklarace. Pro jeho realizaci se může stát "Achillovou patou" především to, že nestanoví prostředky, jimiž by bylo možno stanovená práva a jím odpovídající povinnosti vymáhat. Jistě si lze představit situaci, kdy se uživatel bude takové služby domáhat a nepochybně na ní má subjektivní veřejné právo a orgán veřejné moci mu její poskytnutí odepře. Takový otazník přitom může být v podstatě vystaven u každého z práv zakotvených tímto zákonem. Konkrétně např. orgán veřejné moci bude na účastníkovi řízení požadovat, aby předložil k žádosti některý z podkladů, ačkoli jde o údaj, k němuž má přístup, odmítne akceptovat výpis z informačního systému prokazující právní

[27] Viz https://www.mvcr.cz/clanek/datove-schranky-po-10-letech-usetrene-miliardy-i-zasadni-narust-uzivatelu.aspx, konkrétní čísla jsou pak obsažena v odkazu na této adrese na článek Datové schránky v číslech.

[28] KNAPP, V. Teorie práva, Praha: C. H. Beck, 1995, s. 165.

skutečnost, neprovede zápis právní skutečnosti, nezašle mu informace na zapsaný kontaktní údaj, nesplní notifikační povinnost vůbec nebo opožděně a zvláštní komplikace lze očekávat v případě, že použije při zpřístupnění digitální služby technologii, která podle uživatele není neutrální a přístup k digitální službě bude podle něj znemožněn nebo jen ztížen, což se nutně stane otázkou složitého znaleckého posuzování. Podle stávající úpravy bude zřejmě jedinou možností obrátit se v takovém případě na správní soud, tzv. zásahovou žalobou podle § 82 a následujících soudního řádu správního, vzhledem k tomu, že zákon nepředpokládá, že o odepření služby bude vydáváno rozhodnutí.[29] S ohledem na délku jednání soudů to bude, ovšem znamenat, že se zamýšlený efekt zákona může přinejmenším nemálo otupit, budou-li tyto spory opravdu vedeny za účelem jeho naplnění.

6. SEZNAM ZDROJŮ

6.1 MONOGRAFIE

[1] KNAPP, V. Teorie práva, Praha: C. H. Beck, 1995.

[2] KOPECKÝ, M., Správní právo. Obecná část, Praha: C. H. Beck, 2019.

[3] LECHNER, T., Elektronické dokumenty v právní praxi, Praha: Leges, 2013.

6.2 ELEKTRONICKÉ ZDROJE

[4] https://www.lupa.cz/clanky/zakon-o-pravu-na-digitalni-sluzby-prosel-snemovnou-co-pri-tom-spadlo-pod-stul/.

[5] https://www.mvcr.cz/clanek/datove-schranky-po-10-letech-usetrene-miliardy-i-zasadni-narust-uzivatelu.aspx.

6.3 JUDIKATURA

[6] Usnesení Ústavního soudu sp. zn. I. ÚS 2783/08.

[7] Usnesení Ústavního soudu sp. zn. II. ÚS 1790/07.

[8] Usnesení Ústavního soudu sp. zn. II. ÚS 75/93.

[9] Usnesení Nejvyššího správního soudu čj. 8 Afs 82/2006-68.

[29] Podle stanoviska Nejvyššího správního soudu představuje nezákonný zásah také nezákonná nečinnost v případě, kdy správní orgán neučiní nějaký úkon, jiný než rozhodnutí (např. usnesení rozšířeného senátu Nejvyššího správního soudu čj. 7 Aps 3/2008-98 a rozsudek Nejvyššího správního soudu čj. 6 Ans 1/2013-66).

[10] Rozsudek Nejvyššího správního soudu čj. 7 Azs 113/2015-32.

[11] Rozsudek Krajského soudu v Hradci Králové-pobočka v Pardubicích čj. 52/2015-42.

[12] Usnesení rozšířeného senátu Nejvyššího správního soudu čj. 7 Aps 3/2008-98.

[13] Rozsudek Nejvyššího správního soudu čj. 6 Ans 1/2013-66.

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

---

https://doi.org/10.5817/RPT2020-1-5

POSKYTOVATEL SLUŽEB SDÍLENÍ OBSAHU ONLINE DLE SMĚRNICE (EU) 790/2019[1]

ROSTISLAV SLIWKA[2]

ABSTRAKT

Článek se zabývá pojmem poskytovatele služeb sdílení obsahu online (PSSOO), který byl do evropského práva zaveden směrnicí (EU) 2019/790 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu (DSM směrnice). Postupně jsou rozebrány jednotlivé definiční prvky, ať už přímo uvedené v definici v čl. 2 DSM směrnice, tak vyplývající z navazujících recitálů odůvodnění DSM směrnice. Na praktických příkladech je dovozována aplikace jednotlivých kritérií v praxi. Ačkoliv definice PSSOO není ve všech ohledech jednoznačná, článek se snaží jednotlivá úskalí za pomoci judikatury Soudního dvora EU a dalších zdrojů rozebrat a nalézt možný praktický výklad daných definičních prvků.

KLÍČOVÁ SLOVA

poskytovatel služeb sdílení obsahu online, PSSOO, odpovědnost ISP, směrnice (EU) 790/2019, jednotný digitální trh

---

[1] Článek původně vznikal jako modulová práce v rámci programu LL.M. v právu informačních a komunikačních technologií Masarykovy univerzity.

[2] Mgr. Rostislav Sliwka, Autor je absolventem Právnické fakulty Univerzity Karlovy a studentem programu LL.M. v právu informačních a komunikačních technologií Masarykovy univerzity. Aktuálně působí jako právník v OSA – Ochranném svazu autorském pro práva k dílům hudebním, z.s. Kontaktní e-mail: rostasliwka@gmail.com.

ABSTRACT

This article deals with the online content sharing service provider (OCSSP) as enacted in the European law by Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market (DSM Directive). It analyses each of the definition elements explicitly enacted in Article 2 of the DSM Directive, as well as these resulting from recitals to the DSM Directive. Possible application of each of these elements is then shown on practical examples. Even though the definition of OCSSP is not clear in all aspects, this article is trying to describe and evaluate all the conundrums at stake and to find a practical interpretation of each definition element with help of CJEU case law and other existing sources.

KEYWORDS

online content sharing service provider, OCSSP, ISP liability, Directive (EU) 790/2019, digital single market

1. ÚVOD

Velmi zjednodušeně a obecně lze říci, že každá osoba odpovídá za své jednání, tj. za to, že se chová po právu a dodržuje své právní povinnosti. V případě, že tuto premisu poruší, vzniká zde povinnost odčinit, co bylo jejím protiprávním jednáním způsobeno. Právní vývoj v oblasti internetu dospěl v judikatuře a později též v legislativě k tomu, že za specifických podmínek může nastat situace, kdy osoba odpovídá též za to, že umožňuje třetím osobám určitým způsobem užívat internet a nahrávat na něj obsah. Mluvíme proto o tzv. odpovědnosti poskytovatelů služeb informační společnosti (poskytovatelů připojení k internetu, platforem pro sdílení obsahu ad.) za cizí obsah na internetu. Ačkoliv tak nejde čistě o odpovědnost těchto subjektů za chování třetích osob, svým způsobem se tomu blíží. I z toho důvodu legislativa nejprve v USA a později též v EU dospěla k tomu, že je třeba stanovit podmínky vyloučení této odpovědnosti

v případech, kdy poskytovatelé služeb informační společnosti dodrží stanovená pravidla.[3]

S přijetím nové evropské směrnice (EU) 790/2019[4] vyvstala praktická otázka, kdy lze uplatnit na vyloučení odpovědnosti poskytovatelů služeb hostingu (tj. ukládání informací poskytovaných příjemcem služby) podmínky dle čl. 14 směrnice 2000/31/ES[5] a kdy dle čl. 17 DSM směrnice. Ačkoliv čl. 17 odst. 3 DSM směrnice uvádí, že *„pokud poskytovatel služeb pro sdílení obsahu online provádí sdělení nebo zpřístupnění veřejnosti za podmínek stanovených v této směrnici, nevztahuje se na situace, na něž se vztahuje tento článek, omezení odpovědnosti podle čl. 14 odst. 1 směrnice 2000/31/ES,“* s ohledem na obsah definice služeb, na něž se vztahuje čl. 17 DSM směrnice, může dojít k situacím, kdy je užití té či oné úpravy značně nejisté. Nebude zřejmě výjimečné ani to, že se určitá služba bude muset podřídit oběma úpravám v závislosti na obsahu jí vykonávaných činností.[6]

Z těchto důvodů se zde nabízí blíže rozebrat to, na které subjekty se bude vztahovat úprava čl. 17 DSM směrnice, nově označované jako poskytovatelé služeb sdílení obsahu online (dále jen „PSSOO“).

V tomto článku se proto budu zabývat jednotlivými definičními prvky PSSOO uvedenými v čl. 2 odst. 6 DSM směrnice a na to navazujících recitálech a budu se snažit rozklíčovat jejich možná úskalí. Rovněž se

---

[3] Blíže viz HUSOVEC, Martin. Zodpovednosť na internete podľa českého a slovenského práva. 1. vyd. Praha: CZ.NIC, 2014, s. 31 an. ISBN 978-80-904248-8-3 či ANDRUŠKO, Alena. Internet, informační společnost a autorské právo. 1. vyd. Praha: Wolters Kluwer ČR, s. 94 an. ISBN 978-80-7552-327-3.

[4] Směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 15. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN-CS/TXT/?uri=CELEX:32019L0790&from=cs (dále jen „DSM směrnice“).

[5] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 15. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32000L0031 (dále jen „E-Com směrnice“).

[6] Tak například odpovědnost za odstranění tzv. „*hate speech*“ bude podléhat bezpečnému přístavu dle čl. 14 směrnice E-Com, zatímco odpovědnost za autorskoprávní obsah čl. 17 DSM směrnice.

pokusím uvést některé praktické aspekty spojené s již probíhajícími jednáními nad implementací čl. 17 v národním zákonodárství. Cílem článku je proto primárně upozornit na problémy definice PSSOO a naznačit možné cesty, jak jednotlivé elementy definice vyložit, popřípadě též dospět k tomu, jakým způsobem by měl být čl. 17 implementován do národních právních řádů. Základní vědeckou metodou článku je tudíž analýza, na kterou navazuje syntéza získaných poznatků.

Předem je třeba uvést, že literatury, která by se zabývala samotnou definicí PSSOO, je v době psaní článku poskrovnu neboť pozornost je aktuálně upřená více na povahu práva na sdělování veřejnosti uvedenému v čl. 17 a podmínkami vyloučení odpovědnosti PSSOO.[7] Pokusím se proto čerpat z dostupných zdrojů, které doplním o vlastní znalosti související s prací v kolektivním správci a s účastí na implementačních pracích v ČR.

2. DEFINICE POSKYTOVATELE SLUŽEB DLE ČL. 17 DSM SMĚRNICE

DSM směrnice obsahuje definici poskytovatele služeb pro účely čl. 17 této směrnice – tedy tzv. *poskytovatele služeb sdílení obsahu online* – v čl. 2 odst. 6 této směrnice. Dle této definice jím je:

„poskytovatel služby informační společnosti, jehož hlavním účelem nebo jedním z hlavních účelů je uchovávat velký počet děl chráněných autorským právem nebo jiných předmětů ochrany nahrávaných jeho uživateli a zpřístupňovat je veřejnosti, přičemž poskytovatel tato díla a jiné předměty ochrany uspořádává a propaguje za účelem zisku.“

Nápomocí pro určení PSSOO jsou recitály 61 až 63 DSM směrnice. Pokud tyto recitály podrobíme analýze v duchu judikatury SDEU, tj. nebudeme je vykládat ve smyslu zcela odporujícím znění ustanovení směrnice, která doplňují, lze z těchto za stávajícího stavu dojít alespoň

[7] Viz například HUSOVEC, Martin, QUINTAIS, J. P. *How to license Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms*. [online] 27 s. [cit. 27. 12. 2019]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfmabstract_id = 3463011.

k částečnému pochopení pojmu PSSOO.[8] Tak dle recitálu 62 by se definice měla vztahovat „*pouze na online služby, které hrají důležitou úlohu na trhu online obsahu tím, že soutěží s ostatními online službami poskytujícími obsah, jako jsou služby audiovizuálního online přenosu, pro stejné cílové skupiny*." Stejný recitál pak doplňuje definici v čl. 2 odst. 6 směrnice v tom smyslu, že propagace a kategorizace předmětů ochrany probíhá nejen za účelem zisku, ale též „s *cílem přilákat širší publikum*."

Článek 2 odst. 6 DSM směrnice dále uvádí výčet služeb, na které se úprava odpovědnosti dle čl. 17 a *priori* nevztahuje.

2.1 SLUŽBA INFORMAČNÍ SPOLEČNOSTI

Definice PSSOO se vztahuje pouze na poskytovatele služeb informační společnosti. Pod pojmem „služba" zde rozumíme vlastní dynamickou činnost daného subjektu, tedy poskytování služby spočívající v určité vlastní aktivitě, nerozumíme tím statický subjekt tuto službu poskytující či entitu poskytovatele samotnou. Toto rozlišení lze předvést na příkladu taxislužby. Zajímá nás zde samotná činnost spočívající v přepravování osob včetně jejich zavazadel, nikoliv povaha subjektu běžně označovaného jako taxislužba. Proto je vždy třeba posuzovat faktickou aktivitu poskytovatele, tedy zda u dané konkrétní činnosti samotné (zde v poskytování služby ukládání obsahu nahrávaného uživateli a jeho následném zpřístupňování dalším uživatelům této služby) může být vyloučena odpovědnost za cizí obsah. Rovněž je pak třeba vždy posoudit danou složku činnosti poskytovatele služeb, neboť ne vždy bude veškerá činnost daného poskytovatele spadat pod pojem služba informační společnosti.[9] Obsah celého termínu „služba informační společnosti" je pak čl. 2 písm. a) E-Com směrnice odkazován na čl. 1 odst. 2 směrnice 98/34/ES[10] ve znění směrnice

---

[8] Viz bod 16 odůvodnění rozhodnutí Soudního dvora (pátého senátu) ze dne 2. 4. 2009 ve věci C-134/08, Hauptzollamt Bremen, ECLI:EU:C:2009:229.

[9] HUSOVEC, Martin, op. cit., s. 97.

[10] Směrnice Evropského Parlamentu a Rady 98/34/ES ze dne 22. června 1998 o postupu při poskytování informací v oblasti norem a technických předpisů. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 17. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A31998L0034.

98/48/ES,[11] která byla později nahrazená směrnicí (EU) 2015/1535[12] obsahující obdobnou definici v čl. 1 písm. b). Touto službou se tak rozumí „*každá služba poskytovaná zpravidla za úplatu, na dálku, elektronicky a na individuální žádost příjemce služeb*.“

Technická informační směrnice celou definici doplnila o další ustanovení a přílohu, které především rozšiřují negativní výčet služeb, které pod pojem služby informační společnosti nespadají.[13] Službou informační společnosti tak není například běžné televizní vysílání (tj. např. terestrické vysílání České televize) či služby poskytované offline.

2.1.1 SLUŽBA POSKYTOVANÁ ZPRAVIDLA ZA ÚPLATU

Pojem „zpravidla za úplatu“ neznamená to, že poskytování služby musí být vždy úplatné v běžném smyslu, tj. peněžním plněním uživatele poskytovateli. Tímto protiplněním může být též čas uživatele, jeho osobní údaje či zhlédnutí reklamy.[14] Bývalá směrnice 98/48/ES uváděla v recitálu 19, že tento pojem je reflexí judikatury SDEU. Technická informační směrnice se touto částí definice nijak blíže nezabývá. Je však na místě dovozovat, že tento pojem lze stále vykládat obdobně. Polčák tento termín vykládá prakticky tak, že jde o službu, u níž „*je obvyklé vybírat úplatu*.“ Též dovozuje, že tato úplata nemusí „*být nutně vybírána od toho, komu je příslušná služba poskytována*,“[15] čímž je pamatováno na běžné fungování např. sociálních sítí či internetových vyhledávačů, které přímo od uživatelů úplatu nepřijímají.

---

[11] Směrnice Evropského parlamentu a Rady 98/48/ES ze dne 20. července 1998, kterou se mění směrnice 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 17. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A31998L0048.

[12] Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 17. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv:OJ.L_.2015.241.01.0001.01.CES (dále jen „technická informační směrnice“).

[13] Viz čl. 1 písm. b) body i) až iii) technické informační směrnice.

[14] HUSOVEC, op. cit., s. 98.

[15] POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, s. 142.

2.1.2 SLUŽBA POSKYTOVANÁ NA DÁLKU

Služba poskytovaná na dálku byla samotnou směrnicí 98/34/ES definována jako „*služba poskytovaná bez současné přítomnosti obou stran*.“[16] Zcela stejným způsobem ji definovala i technická informační směrnice.[17] Příloha č. 1 této směrnice pak negativním způsobem uvádí, že mezi takové služby nepatří například rezervace letenek pomocí počítačové sítě v provozovně cestovní kanceláře za přítomnosti zákazníka či zpřístupnění elektronické hry v herně za přítomnosti zákazníka. Obecným vodítkem pro posouzení služby jako poskytované na dálku je to, zda plnění, resp. služba jako celek je poskytována bez současné přítomnosti obou stran, bez ohledu na to, zda samotná smlouva mezi poskytovatelem a příjemce byla uzavřena za jejich současné přítomnosti.[18]

2.1.3 SLUŽBA POSKYTOVANÁ ELEKTRONICKY

Technická informační směrnice obdobně jako původní směrnice 98/34/ES definuje službu poskytovanou elektronicky jako „*službu odeslanou z výchozího místa a přijatou v místě jejího určení prostřednictvím elektronického zařízení pro zpracování a uchovávání dat (včetně digitální komprese) a jako celek odeslanou, přenesenou nebo přijatou drátově, rádiově, opticky nebo jinými elektromagnetickými prostředky*.“[19] Příloha č. 1 k technické informační směrnici uvádí v negativním výčtu tři skupiny služeb, které pro účely definice služby infomační společnosti nejsou poskytované elektronicky – služby materiální povahy, ačkoli jsou poskytovány elektronickými přístroji;[20] služby poskytované off-line;[21] a služby, které nejsou poskytovány elektronickými systémy pro zpracování či ukládání dat.[22] Z toho vyplývá, že

---

[16] Článek 1 odst. 2 směrnice 98/34/ES.

[17] Článek 1 odst. 1 písm. b) bod i) technické informační směrnice.

[18] POLČÁK, Radim a kol. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, s. 74.

[19] Článek 1 odst. 1 písm. b) bod ii) technické informační směrnice.

[20] Např. bankomaty či automaty na jízdenky.

[21] Směrnice zde jako příklad uvádí pouze prodej kompaktních disků nebo programového vybavení na disketách.

[22] Např. hlasové telefonní služby či prodej po telefonu.

nepostačuje pouhá přítomnost elektronického zařízení při poskytování dané služby. Toto zařízení musí též zprostředkovat odeslání a příjem dat mezi poskytovatelem a příjemcem služby a tato data zpracovat.

2.1.4 SLUŽBA POSKYTOVANÁ NA INDIVIDUÁLNÍ ŽÁDOST PŘÍJEMCE

Směrnice tuto podmínku definuje lakonicky jako „*službu poskytovanou přenosem dat na individuální žádost.*“[23] Jak však uvádí generální advokát Maciej Szpunar, „*posouzení individuální žádosti zřejmě nečiní v praxi potíže*.“[24] Individuální žádost příjemce tak může spočívat v zadání webové adresy do prohlížeče či v kliknutí na hyperlink odkazující na danou službu.[25] Požadavek individuální žádosti však nevyžaduje interaktivnost dané služby, neboť žádost se projevuje již v jednání příjemce vedoucímu k užívání služby samotné.[26]

Příjemcem služby se rozumí „*každá fyzická nebo právnická osoba, která k profesním či jiným účelům využívá služeb informační společnosti, zejména pro vyhledávání či zpřístupňování informací.*“[27] Ačkoliv jde o definici pro účely E-Com směrnice, nečiní nejspíše žádný problém na tuto odkázat i pro účely DSM směrnice. Drobnou nesrovnalostí může být, že definice služby informační společnosti užívá pojmu příjemce, zatímco definice PSSOO dále pracuje s pojmem uživatel. Jelikož však definice příjemce uvádí, že takový příjemce užívá službu i k jiným než profesním účelům, neměla by tato odlišnost činit v praxi žádné obtíže.

---

[23] Článek 1 odst. 1 písm. b) bod iii) technické informační směrnice.

[24] Stanovisko generálního advokáta Macieje Szpunara přednesené dne 30. dubna 2019 ve věci C-390/18, AIRBNB, bod 37.

[25] HUSOVEC, op. cit., s. 100.

[26] Tedy postačí se přihlásit na webovou stránku služby Netflix. Možnost výběru sledovaného pořadu je z pohledu definice služby informační společnosti za splnění ostatních podmínek irelevantní. Tento aspekt je relevantní až z pohledu autorského práva (viz právo na zpřístupnění díla veřejnosti v čl. 3 směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. 5. 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 22. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32001L0029&from=EN (dále jen „informační směrnice“).

[27] Článek 2 písm. d) směrnice E-Com.

2.2 NEGATIVNÍ VYMEZENÍ PSSOO

Ačkoliv se to může jevit na první pohled nesystematické, považuji za vhodné nejprve určit, co PSSOO není. Nejde zde však o variaci Cimrmanovy teorie externismu, nýbrž o názorné zdůraznění faktu, že daná úprava skutečně cílí na relativně úzkou skupinu větších online platforem umožňujících svým uživatelům sdílet obsah. Nicméně se v tomto případě ztotožňuji s názorem společnosti Seznam, že určitý standard odpovědnosti za cizí obsah chráněný autorským právem by měly dodržovat i platformy na regionální úrovni, nikoliv jen celosvětoví hráči.[28] Tudíž dotčenou nemůže být pouze služba YouTube, a to i s ohledem na povahu směrnice a prováděcích zákonů jakožto obecně závazných předpisů.

Recitál 62 DSM směrnice poměrně podrobně upravuje, co PSSOO není. První pomocné vodítko vlastně vychází ze samotné definice v čl. 2 odst. 6, totiž že „*tyto služby by neměly zahrnovat služby, které mají* ***jiný hlavní účel*** *než umožnit uživatelům nahrávat a sdílet velké množství obsahu chráněného autorským právem s cílem dosahovat z této činnosti zisk*.“ Problematické může být, že toto vyjádření nereflektuje definici v čl. 2 odst. 6 a možnou pluralitu hlavních účelů.[29]

2.2.1 ELEKTRONICKÉ KOMUNIKAČNÍ SLUŽBY

Za PSSOO se pro účely čl. 17 DSM směrnice nepovažují elektronické komunikační služby ve smyslu směrnice (EU) 2018/1972.[30] Tato směrnice tento pojem vysvětluje ve svém čl. 2 bodu 4). Jde o „*službu obvykle poskytovanou za úplatu prostřednictvím sítí elektronických komunikací*“

---

[28] Viz prezentace společnosti Seznam ze 4. jednání dialogu Evropské komise k čl. 17 ze dne 16. 12. 2019. Dostupné z: https://ec.europa.eu/digital-single-market/en/news/fourth-meeting-stakeholder-dialogue-article-17-directive-copyright-digital-single-market.

[29] Srov. vyjádření „*hlavní nebo jeden z hlavních účelů*“ v čl. 2 odst. 6 DSM směrnice. Problematické je samo o sobě vyjádření „*jeden z hlavních účelů*“, neboť výraz „*hlavní*“ logicky předpokládá, že je daný jev jediný, nejvýznamnější. Je však zřejmé, že chce definice zachytit více subjektů spadajících pod definici PSSOO.

[30] Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 23. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legalcontent/CS/TXT/uri=uriserv:OJ.L_.2018.321.01.0036.01.CES&toc=OJ:L:2018:321:TOC („směrnice o elektronické komunikaci“).

zahrnující službu přístupu k internetu ve smyslu nařízení (EU) 2015/2120,[31] interpersonální komunikační službu[32] a služby spočívající zcela nebo převážně v přenosu signálů.[33] Směrnice jako výjimku z těchto služeb uvádí služby poskytující obsah či vykonávající redakční dohled nad obsahem přenášeným prostřednictvím sítí a služeb elektronických komunikací.[34]

Odůvodnění směrnice o elektronické komunikaci uvádí, že službou elektronické komunikace je například služba VoIP[35] či webová e-mailová služba.[36] Směrnice o elektronické komunikaci pak uvádí, že za interpersonální komunikační služby lze považovat pouze ty, které zahrnují komunikaci mezi konečným počtem fyzických osob určených odesílatelem komunikace. Služba by rovněž měla spočívat v interaktivní komunikaci. Z toho důvodu službou elektronické komunikační služby nejsou například

[31] Takovou službou se rozumí „*veřejně dostupná služba elektronických komunikací, která poskytuje přístup k internetu, a tím propojení s prakticky všemi koncovými body internetu, bez ohledu na použitou technologii sítě a použité koncové zařízení.*“ Viz čl. 2 bod 2) nařízení Evropského parlamentu a Rady (EU) 2015/2120 ze dne 25. listopadu 2015, kterým se stanoví opatření týkající se přístupu k otevřenému internetu a mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací a nařízení (EU) č. 531/2012 o roamingu ve veřejných mobilních komunikačních sítích v Unii. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 23. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32015R2120.

[32] Dle čl. 2 bodu 5) směrnice o elektronické komunikaci se takovou službou rozumí „*služba obvykle poskytovaná za úplatu, která prostřednictvím sítí elektronických komunikací umožňuje přímou interpersonální a interaktivní výměnu informací mezi konečným počtem osob, kdy osoby, které komunikaci zahajují nebo se jí účastní, určují jejího/její příjemce a která nezahrnuje služby, které interpersonální a interaktivní komunikaci umožňují pouze jako nepodstatnou pomocnou funkci, která je ze své podstaty spjata s jinou službou.*“

[33] Směrnice jako příklad uvádí přenosové služby používané pro poskytování služby komunikace mezi stroji a pro vysílání.

[34] Viz čl. 2 odst. 4 směrnice o elektronické komunikaci. Český překlad směrnice je velmi nepřesný, tudíž jde o překlad autora.

[35] Jde o tzv. „*Voice over Internet Protocol*“, tedy o přenos digitalizovaného hlasu přes internetový protokol. Viz Voice over Internet Protocol. *wikipedia.org* [online]. Wikipedia [cit. 25. 11. 2019]. Dostupné z: https://cs.wikipedia.org/wiki/Voice_over_Internet_Protocol.

[36] Recitál 15 směrnice o elektronické komunikaci.

internetové stránky, video na vyžádání, sociální sítě, blogy či lineární rozhlasové nebo televizní vysílání.[37]

Z toho vyplývá, že PSSOO především nemůže být subjekt, který fakticky slouží pouze jako technický prostředek přenosu dat v rámci elektronických komunikací či jako zprostředkovatel elektronické komunikace mezi konečným počtem fyzických osob. O tom svědčí i uvedená výjimka z definice čl. 2 odst. 4 směrnice o elektronické komunikaci, která předpokládá jistou aktivní roli poskytovatele služby, pokud jde o obsah přenášených informací. Pod definici PSSOO tak nespadá například služba Skype, e-mailový klient Kerio či běžní poskytovatelé připojení k internetu.

2.2.2 CLOUDOVÉ SLUŽBY

Článek 2 odst. 6 DSM směrnice z definice PSSOO vyjímá též „*mezipodnikové cloudové služby a cloudové služby, které uživatelům umožňují nahrávat obsah pro vlastní potřebu.*“ Recitál 62 směrnice pak doplňuje, že jde o služby, které „*uživatelům umožňují nahrávat obsah k soukromým účelům, jako jsou platformy na ukládání či výměnu dat.*“

Cloudové služby jsou z definice PSSOO vyňaty především z toho důvodu, že jejich hlavním účelem zpravidla není zpřístupňování velkého množství předmětů ochrany veřejnosti. I tak však může být jejich služeb zneužíváno pro sdílení chráněných děl například prostřednictvím sdílení odkazů na jiných platformách na uložené soubory na dané cloudové službě. Z toho důvodu recitál 62 odůvodnění DSM směrnice doplňuje, že v případě, kdyby daná služba primárně umožňovala či usnadňovala pirátství v oblasti autorských práv, nevztahuje se na ní mechanismus výjimek z odpovědnosti dle čl. 17.[38] Důležité proto je, že pokud platforma naplní definici PSSOO, je dle čl. 17 DSM směrnice odpovědná za sdělování veřejnosti. V případě, že navíc primárně umožňuje nebo usnadňuje pirátství, je stále odpovědná za

---

[37] Recitál 17 směrnice o elektronické komunikaci.

[38] Viz VISSER, Dirk J.G. *Trying to understand the article formerly known as '13'*. [online] s. 3. [cit. 8. 12. 2019]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354494. Toto ustanovení je v duchu závěrů rozhodnutí Soudního dvora (druhého senátu) ze dne 14. 6. 2017. ve věci C-610/15, Stichting Brein („rozhodnutí ve věci Pirate Bay“).

sdělování veřejnosti, ale nemůže využít mechanismu vyloučení této odpovědnosti. Nicméně lze zřejmě dovodit, že pirátské služby nemusí ani zcela naplnit definici PSSOO, aby bylo možné dovodit jejich přímou autorskoprávní odpovědnost, viz dále.

Argument cloudového uložiště pro zálohu dat uživatelů často využívají filehostingová uložiště typu Ulož.to či Hellshare, která tvrdí, že slouží pouze k zálohování dat.[39] Dle mého názoru se bude definice PSSOO aplikovat právě i na tato úložiště, o čemž svědčí vyvíjející se evropská judikatura v posledních letech[40] a fakt, že směrnice vyjímá jen ty cloudové služby, které umožňují nahrávání souborů k soukromým účelům a pro vlastní potřebu uživatele. Volně tu lze užít analogie s výjimkou pro rozmnožování pro osobní potřebu a vlastní vnitřní potřebu ve smyslu § 30 a 30a autorského zákona,[41] která nespočívá v možnosti takto rozmnožená díla dále veřejně sdílet třetím osobám. Pokud proto dané cloudové uložiště umožňuje takto nahrané soubory zpřístupňovat veřejnosti a podpůrně k tomu navíc poskytuje prostředky k vyhledávání těchto souborů kýmkoliv, lze se stěží ztotožnit s tím, že jde o cloudové uložiště vyňaté z působnosti čl. 17 DSM směrnice. Během prvního jednání nad implementací čl. 17 na Ministerstvu kultury ČR též ze strany mnoha subjektů zaznělo, že služba

[39] Viz např. rozhodnutí Městského soudu v Praze ze dne 22 .2. 2019, sp. zn. 34 C 5/2017 (DILIA, divadelní, literární, audiovizuální agentura, z.s. vs. Uloz.to cloud a.s.) či rozhodnutí Městského soudu v Praze ze dne 25. 3. 2019, sp. zn. 32 C 41/2014 (OSA – Ochranný svaz autorský pro práva k dílům hudebním, z.s. vs. Hellspy SE a I&Q Group, spol. s r.o.). Obě tato rozhodnutí jsou v době psaní tohoto článku nepravomocná.

[40] Srov. německá rozhodnutí proti službě RapidShare (např. rozhodnutí Bundesgerichtshof ze dne 15. 8. 2013, sp. zn. I ZR/79/12. *dejure.org* [online] Dejure, 2013 [cit. 10. 12. 2019]. Dostupné z: https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=15.08.2013&Aktenzeichen=I%20ZR%2079/12 či známější rozhodnutí téhož soudu ve sporu Atari vs. RapidShare ze dne 12. 7. 2012, sp. zn. I ZR/18/11. *dejure.org* [online] Dejure, 2013 [cit. 10. 12. 2019]. Dostupné z: https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=12.07.2012&Aktenzeichen=I%20ZR%2018/11.

[41] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů. In: Beck-online [online právní informační systém]. Nakladatelství C. H. Beck [cit. 1. 12. 2019]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seamdocumentId=onrf6mrqgayf6mjsgewtema&groupIndex=2&rowIndex=0 (dále jen „autorský zákon“).

Ulož.to je příkladem PSSOO.[42] Pomocná vodítka zřejmě doplní též probíhající řízení u SDEU o žádosti o rozhodnutí o předběžné otázce ve věci Uploaded.net.[43]

2.2.3 ONLINE TRŽIŠTĚ

Pro vynětí online tržišť, jejichž hlavní činností je maloobchodní online prodej, z definice PSSOO existuje stejný argument jako u cloudových služeb, tj. online tržiště nemají mezi hlavními účely zpřístupňování velkého množství předmětů ochrany veřejnosti. Typickým příkladem takových služeb jsou například služby Amazon eBay či služba Alibaba.com.

Odpovědnost takovýchto platforem byla zevrubně analyzována s ohledem na odpovědnost poskytovatele služeb informační společnosti dle čl. 14 E-Com směrnice v rozhodnutí SDEU ve věci C-324/09 (L'Oréal),[44] kde byla žalovanou stranou právě služba eBay. Z rozhodnutí lze dovodit, že online tržištěm jsou služby, které zprostředkovávají maloobchodním prodejcům prodej jejich zboží přímo spotřebitelům. Slovy rozhodnutí jde o tržiště, „*na kterém jsou zobrazovány inzeráty na výrobky prodávané osobami, které se za tímto účelem registrovaly u společnosti eBay a vytvořily si u ní účet prodávajícího*," přičemž „*eBay si z uskutečněných transakcích účtuje určitý procentní podíl*."[45] Takovéto služby tak stále mohou využívat mechanismu vyloučení odpovědnosti ve smyslu čl. 14 E-Com směrnice ohledně veškerého obsahu dostupného na jejich službách. Zajímavostí je argument YouTube, který zazněl během implementačních jednání v Nizozemsku, aby prováděcí předpis uvedl jako příklad takového online tržiště též obchody s mobilními aplikacemi typu „*app store*".[46]

---

[42] Jednání pracovní skupiny č. IX k implementaci čl. 17 na Ministerstvu kultury ČR dne 11. 12. 2019.

[43] Viz shrnutí žádosti o rozhodnutí o předběžné otázce ze dne 6. 11. 2018 ve věci C-683/18, Elsevier Inc. proti Cyando AG („věc Uploaded.net").

[44] Rozhodnutí Soudního dvora (velkého senátu) ze dne 12. července 2011 ve věci C-324/09, L'Oréal a další („rozhodnutí ve věci L'Oréal").

[45] Bod 28 odůvodnění rozhodnutí ve věci L'Oréal.

[46] Viz Implementatiewetsvoorstel Richtlijn auteursrecht in de digitale eengemaakte markt. *overheid.nl* [online]. Overheid [cit. 1. 12. 2019]. Dostupné z: https://www.internetconsultatie.nl/auteursrecht/reacties

2.2.4 DALŠÍ SLUŽBY

DSM směrnice nakonec z definice PSSOO vyjímá platformy pro vývoj a sdílení softwaru s otevřeným zdrojovým kódem, neziskové vědecké nebo vzdělávací archivy a neziskové online encyklopedie. Hlavním argumentem pro vynětí těchto služeb je jejich neziskový charakter.[47]

Příkladem těchto platforem je například webová encyklopedie Wikipedia či platforma pro vývoj softwaru GitHub. U Wikipedie stojí za zmínku aktivní role nadace Wikimedia spravující též projekt Wikipedie v boji proti přijetí DSM směrnice, a to i přes faktické vynětí Wikipedie z definice PSSOO. Důvodem je obava nadace, že čl. 15 a 17 DSM směrnice povedou k faktickému omezování dostupností informací na internetu, což bude mít dle jejího názoru dopad též na kvalitu obsahu na službě Wikipedia.[48]

2.3 POZITIVNÍ VYMEZENÍ PSSOO

Již na první pohled je evidentní, že pozitivní vymezení PSSOO především předpokládá aktivní roli daného poskytovatele ve vztahu k obsahu chráněnému autorským právem nebo právy souvisejícími dostupného na jeho službě. PSSOO tak nikdy nebude pouhým technickým prostředkem ve smyslu § 18 odst. 3 autorského zákona. Rovněž tak jím nebude žádná ze služeb spadajících pod bezpečné přístavy pro prostý přenos a ukládání do vyrovnávací paměti dle E-Com směrnice, neboť definice předpokládá aktivní roli platformy stran obsahu ukládaného uživateli služby na této službě.

2.3.1 HLAVNÍ ÚČEL NEBO JEDEN Z HLAVNÍCH ÚČELŮ

I v případě, že na dané službě bude docházet k ukládání a následnému zpřístupňování velkého množství předmětů ochrany, nemusí daná služba

---

[47] VISSER, Dirk J.G., op. cit. s. 3.

[48] Viz We do not support the EU Copyright Directive in its current form. Here's why you shouldn't either. *wikimediafoundation.org* [onlince]. Wikimedia Foundation [cit. 1. 12. 2019]. Dostupné z: https://wikimediafoundation.org/news/2019/02/28/we-do-not-support-the-eu-copyright-directive-in-its-current-form-heres-why-you-shouldnt-either/.

automaticky spadat pod definici PSSOO. Nutným předpokladem je totiž to, že tato činnost je hlavním nebo jedním z hlavních účelů dané služby. Vodítkem pro posouzení tohoto účelu mohou být například podmínky užití služby či marketing dané platformy. Například podřazení služeb Ulož.to a YouTube pod definici PSSOO dle kritéria jednoho z hlavních účelů je dle jejich podmínek užití jednoznačné.[49] Nezbývá však než vždy posoudit reálnou činnost a její okolnosti.

DSM směrnice uvádí v recitálu 62, že takové služby*„mají v rámci svého obvyklého používání umožnit přístup veřejnosti k obsahu chráněnému autorským právem nebo k jiným předmětům ochrany, které nahráli jejich uživatelé." Dále zpřesňuje, že definice by měla zahrnovat „online služby, které hrají důležitou úlohu na trhu online obsahu tím, že soutěží s ostatními online službami poskytujícími obsah, jako jsou služby audiovizuálního online přenosu, pro stejné cílové skupiny."*

Jak je zřejmé z již probíhajících jednání nad implementacemi v členských státech, služba YouTube se snaží na výše uvedených odůvodněních pokud možno co nejvíce zúžit obsah definice PSSOO.[50] Hlavním argumentem pro YouTube je požadavek soutěže s ostatními online službami. Tento požadavek je přímým promítnutím avizovaného boje EU proti tzv. „*value-gap*" problému, tj. rozdílu v odměnách hrazených (popř. též vůbec nehrazených) platformami s uživateli nahrávaným obsahem a tzv. „*digital service providers*" (dále jen „DSP").[51] YouTube proto apeluje na to, aby byla odpovědnost PSSOO dle čl. 17 DSM směrnice stanovena jen ve

[49] Viz např. podmínky užití služby YouTube, které uvádějí: „*Služba umožňuje objevovat, sledovat a sdílet videa a další obsah a nabízí fórum, ve kterém se mohou navzájem spojit, informovat a inspirovat lidé z celého světa. Navíc funguje jako distribuční platforma pro tvůrce originálního obsahu a malé i velké inzerenty*." – Podmínky poskytování služeb. *youtube.com* [online]. YouTube [cit. 12. 12. 2019]. Dostupné z https://www.youtube.com/static?gl=CZ&template=terms. Velmi zajímavé jsou podmínky služby Ulož.to, které v čl. 2 uvádějí: „*Poskytovatel umožňuje prostřednictvím Serveru Uživateli využívat tyto Služby: poskytování úložného prostoru pro Nahrané soubory, jejich správu, opětovné stažení a jejich sdílení prostřednictvím sítě internet; možnost stahovat sdílené Nahrané soubory dalších Uživatelů; … sledování LIVE souborů a možnost sdělovat LIVE soubory dalším Uživatelům*." Viz Všeobecné smluvní podmínky užívání služeb poskytovaných společností Uloz.to cloud a.s. (mimo jiné) na stránkách uloz.to. *uloz.to* [online]. Ulož.to [cit. 12. 12. 2019]. Dostupné z: https://uloz.to/podminky/vseobecne-smluvni-podminky.

[50] Viz sub 45.

specifických oblastech, kde dochází ke zřejmé soutěži platforem s uživateli nahrávaným obsahem a DSP, ať už pokud jde o množství zpřístupněných děl či o postavení na trhu.[52] Největším příkladem takové soutěže je hudební trh, kde proti sobě soutěží služby YouTube a Soundcloud na straně jedné a platformy typu Spotify, Deezer či Tidal na straně druhé. Ačkoliv je YouTube obecně vnímán jako platforma pro sdílení audiovizuálního obsahu a nikoliv čistě hudebního, je třeba upozornit na to, že je jednou z nejčastěji užívaných platforem pro streaming hudby a hudební obsah generuje značnou část příjmů služby.[53] U ostatních druhů předmětů ochrany dle YouTube k takové soutěži nedochází (například u fotografií), tudíž by YouTube neměl být pro oblast práv k fotografiím posuzován jako PSSOO.

Tato argumentace je ze strany YouTube pochopitelná, nicméně osobně se domnívám, že sektorový přístup nebyl pro samotné určení odpovědných PSSOO zamýšlen, na rozdíl od dalších aspektů samotných povinností PSSOO dle čl. 17, kdy je třeba posuzovat též typ předmětů ochrany

---

[51] Viz např. LIEBOWITZ, Stan. *Economic Analysis of Safe Harbour Provisions* [online]. [cit. 13. 12. 2019]. Dostupné z: https://www.cisac.org/CISAC-University/Library/Studies-Guides/Economic-Analysis-of-Safe-Harbour-Provisions či MONTAGNANI, Maria Lillá; TRAPOVA, Alina. New Obligations for Internet Intermediaries in the Digital Single Market - Safe Harbors in Turmoil? *Journal of Internet Law* [online]. 2019, vol. 22, č. 7, s. 3-11 [cit. 15. 11. 2019]. Dostupné z: https://ssrn.com/abstract=3361073.

[52] Ve svém vyjádření k implementačním pracím v Nizozemsku tak Google uvedl: „A *targeted implementation should recognize that the Directive only addresses the upload services for users competing with content distribution services that are the same have content and target the same audience*.“ (neoficiální překlad z holandštiny) Viz sub 45.

[53] Dle studie IFPI na vzorku 34 tisíc osob používá 77 % z nich YouTube k poslechu hudby. Obecně pak lidé stráví 3 a půl hodiny týdně poslechem hudby prostřednictvím audiovizuálních služeb na vyžádání. Viz Music Listening 2019. ifpi.org [online]. IFPI [cit. 28. 5. 2020]. Dostupné z: https://www.ifpi.org/downloads/Music-Listening-2019.pdf. Analýza společnosti Pex dále uvádí, že ačkoliv je jako čistě hudební označeno pouze 5 % videí na YouTube (videa takto ovšem označují sami uživatelé při uploadu), představují tato videa podle počtu přehrání 22 % všech zhlédnutí. Pokud pak jde o nejpopulárnější videa na YouTube, představuje hudební obsah více než 80 % těchto videí. Navíc videa obsahující alespoň 10 vteřin hudby tvoří více než 84 % ze všech videí na YouTube. Viz Youtube is generating $32k every minute – but how much of that money is being driven by music? musicbusinessworldwide.com [online]. Music Business Worldwide [cit. 28. 5. 2020]. Dostupné z: https://www.musicbusinessworldwide.com/youtube-is-generating-32k-every-minute-but-how-much-of-that-money-is-being-driven-by-music/.

nahrávaných uživateli.[54] O tomto svědčí užití obecného pojmu děl a předmětů ochrany v textu DSM směrnice.[55] Neblahým důsledkem této argumentace je totiž pro daného PSSOO hrozící souběžné uplatnění režimu vyloučení odpovědnosti dle DSM směrnice a E-Com směrnice pro různé druhy předmětů ochrany. Nicméně je třeba připustit, že v případě specifických druhů předmětů ochrany (například díla architektonická) jsou povinnosti vyplývající z čl. 17 pro PSSOO prakticky nerealizovatelné. S ohledem na další podmínky odpovědnosti PSSOO dle čl. 17 (vynaložení veškerého úsilí k získání licence a nutná spolupráce nositelů práv) se však lze domnívat, že PSSOO se své odpovědnosti v těchto oblastech zřejmě snadno zprostí, neboť tato práva nejsou zpravidla spravována na kolektivním principu a samotná povaha užití těchto děl je odlišná než například u hudebních či audiovizuálních děl.

Například německá vláda pak ve svém stanovisku ke konečnému textu směrnice uvedla, že „*úprava je zaměřena pouze na platformy, které jsou dominantní na trhu a které umožňují uživatelům nahrávat velké množství chráněného obsahu a které na tomto zakládají svůj obchodní model, jako například YouTube či Facebook*.“[56] Osobně se však domnívám, že směrnice necílí pouze na dominantní hráče na trhu, což potvrzuje i recitál 62 odůvodnění směrnice, dle kterého PSSOO „*hrají důležitou úlohu na trhu online obsahu tím, že soutěží s ostatními online službami poskytujícími obsah, (…), pro stejné cílové skupiny*.“ Směrnice tak nijak nestanovuje požadavek dominance trhu, mluví pouze o důležité roli na trhu. Z toho důvodu není nutné, aby měl daný poskytovatel služby určité procentuální zastoupení na trhu ve smyslu dominantního soutěžitele dle práva na ochranu hospodářské soutěže.

Matoucím však může být aspekt „stejných cílových skupin“, neboť cílovou skupinu lze vymezit různými způsoby, přičemž se tyto skupiny

---

[54] Viz čl. 17 odst. 5 DSM směrnice.

[55] Srov. práva k hudebním dílům online ve směrnici 2014/26/EU.

[56] Volný překlad autora, viz stanoviska členských států ke konečnému textu směrnice o autorském právu na jednotném digitálním trhu publikovaná pod č. 7986/19 ADD 1 REV 2 dne 15. 4. 2019. *data.consilium.europa.eu* [online]. Rada EU [cit. 13. 12. 2019]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-7986-2019-ADD-1-REV-2/en/pdf.

mohou různě překrývat. Zřejmě však půjde o posuzování působnosti dané platformy v určitém segmentu trhu, např. trh streamingu audiovizuálního obsahu, trh stahování literárních děl či streaming hudby, tedy půjde o cílové skupiny v daném segmentu, tj. čtenáři, posluchači či diváci. Služba YouTube tak zjevně usiluje o cílovou skupinu v oblasti audiovize (spolu se službami Netflix či HBO Go) a v oblasti hudby (služby Spotify či Apple Music). Služba ulož.to nad to usiluje například o cílovou skupinu čtenářů tím, že umožňuje též sdílení e-knih (spolu s iBooks či obchodem e-knih Alza) či fotografií (viz například služba Instagram).

2.3.2 KRITÉRIUM UCHOVÁVÁNÍ VELKÉHO POČTU PŘEDMĚTŮ OCHRANY

Kritérium uchovávaní velkého počtu předmětů ochrany je na první pohled velmi vágním a obecným ustanovením, u něhož je zcela evidentní, že bližší vodítka pro jeho posouzení bude muset určit judikatura. Často jsou zde proto slyšet hlasy, které kritizují právní nejistotu na straně online platforem.[57] Tyto skutečnosti mohou vést k tomu, že členské státy přistoupí spíše k co nejjednodušší implementaci, která se nebude příliš odchylovat od textu směrnice. Tuto úvahu podporuje též ten fakt, že licencování online platforem ze strany zástupců nositelů práv (kolektivní správci, vydavatelé), je poměrně fragmentované. Ačkoliv jsou služby jako YouTube či Facebook pro činnost v EU usídlené na území Irska, platí, že pro licencování předmětů ochrany se uplatní zásada teritoriality autorského práva, a tudíž budou tyto platformy nucené vypořádávat práva v jednotlivých zemích EU, ledaže daný nositel práv či zástupce nositelů práv bude svá práva licencovat na multiteritoriální bázi.

Nicméně možných postupů pro posouzení lze přeci jen alespoň pár nalézt, k čemuž navádí též recitál 63 odůvodnění DSM směrnice, který říká, že posouzení „*by mělo být prováděno případ od případu a mělo by zohledňovat kombinaci prvků, jako je cílové publikum služby a počet souborů obsahu chráněného autorským právem nahraných uživateli těchto služeb*.“

[57] Jednání pracovní skupiny č. IX k implementaci čl. 17 na Ministerstvu kultury ČR dne 11. 12. 2019.

Jednou z možností je tak například porovnat počet předmětů ochrany dostupných na dané službě s ostatními obdobnými službami na trhu. Izolované užití tohoto kritéria by však mohlo vést ke značnému zúžení odpovědných PSSOO, neboť bychom v konečném důsledku mohli dospět k tomu, že jedinými PSSOO by byly pouze celosvětové služby jako je YouTube či Dailymotion. V důsledku uplatnění možného požadavku nositelů práv na zamezení dostupnosti jejich děl na určitých platformách může rovněž v důsledku docházet k velkým rozdílům mezi platformami. Rovněž se tu nabízí úvaha nad tím, zda má takové posouzení být sektorově specifické či zda má zohledňovat celkové počty předmětů ochrany dostupných na službě bez ohledu na druh předmětu ochrany. S ohledem na recitál 63 DSM směrnice se nabízí přiklonit se k druhému uvedenému řešení, což však může být prolomeno aspektem existující soutěže na trhu v dané oblasti, viz výše.

Druhou možností je porovnat poměr souborů obsahujících předměty ochrany se soubory bez autorskoprávně chráněného obsahu na dané platformě, což vychází též z recitálu 63 odůvodnění směrnice, dle kterého by se měl zohledňovat „*počet souborů obsahu chráněného autorským právem nahraných uživateli těchto služeb*.“ Tímto řešením se odbourává problém srovnání největších světových platforem s menšími, regionálními platformami. Může nicméně dojít k situaci, kdy veškerý obsah dostupný na službě je chráněn autorským právem, avšak množství obsahu na službě nebude objektivně dosahovat velkého počtu ve srovnání s ostatními platformami. Ačkoliv se může objevit názor, že téměř každý soubor bude v podstatě chráněný, s tímto se neztotožňuji, neboť je třeba brát v potaz širokou skupinu děl volných či děl užitých na základě zákonné výjimky. Nadto je třeba uvést, že množství souborů žádné dílo či předmět ochrany ve smyslu autorskoprávním obsahovat nebude.[58] Problematickou kategorií mohou být různé osobní fotografie či videa z dovolených.

[58] Pokud skutečně využiji služby úložiště k zálohování dat, mohou tato data spočívat např. v textových souborech nesplňujících podmínky ochrany autorského literárního díla. Může jít též o excelové soubory s číselnými údaji nesplňující definiční znaky databáze.

Třetí možností je stanovení určitého *de minimis* počtu předmětů ochrany dostupných na službě pro její určení jako PSSOO. V tomto případě se však domnívám, že by šlo o nevhodné a příliš rigidní řešení, nehledě na to, že by takové určení muselo být zřejmě stanoveno pro každý typ předmětů ochrany zvlášť. Navíc by šlo též o porušení požadavku na individuální posouzení každé služby dle recitálu 63 odůvodnění DSM směrnice. Nadto je třeba podotknout, že určení kritéria pro posouzení *velkého počtu* předmětů ochrany za pomoci doktríny *de minimis* je mírně logicky rozporné.

Osobně se proto kloním spíše pro kombinaci prvních dvou uvedených postupů, a to i přesto, že zde může vyvstat výše uvedená komplikovaná otázka souborů typu domácích videí či fotografií z dovolené, které značně posouvají hranici počtu předmětů ochrany dostupných na dané službě. Tyto soubory je však dle mého názoru třeba do velkého počtu předmětů ochrany uchovávaných a zpřístupňovaných danou službo třeba počítat, neboť fungování těchto platforem je založeno na možnosti i tyto soubory obecně zpřístupňovat veřejnosti, tudíž platforma i z těchto generuje určitý zisk. Lze dospět k tomu, že praktickým řešením těchto nejasností může být zakotvení specifických režimů kolektivní správy, ať už v podobě zákonných domněnek zastoupení či v podobě tradiční rozšířené kolektivní správy.[59] Takto platforma nabude právní jistoty o rozsahu poskytnuté licence a jednotlivým nositelům práv bude ponechána možnost vykonávat svá práva individuálně. Limitem však je skutečnost že kolektivní správa není vykonávána pro všechny předměty ochrany (např. počítačové programy či databáze).

Zajímavostí nicméně může být úvaha francouzských legislativců, kde je určité pevné stanovení hranice velkého počtu předmětů ochrany nezbytné pro určení trestněprávní odpovědnosti PSSOO a výše trestů.[60]

---

[59] Viz čl. 12 DSM směrnice a na to navazující úvahy EU o širším uplatnění těchto režimů projevující se v aktuálně prováděných studiích o fungování kolektivní správy ve smyslu čl. 40 směrnice 2014/26/EU a čl. 12 odst. 6 DSM směrnice.

[60] Informace autora z jednání tzv. Madrid Group, pracovní skupiny právníků evropských kolektivních správců sdružených v organizaci GESAC („*Groupement Européen des Sociétés d'Auteurs et Compositeurs*").

Problematické zde může být posouzení prvku „cílového publika“ služby. Není tu zcela jasné, zda se tím myslí počet osob v cílovém publiku či povaha tohoto publika (například lidé od 15 do 26 let). Rovněž tak je obtížné odlišení od pojmu „*cílové skupiny*“ v recitálu 62 DSM směrnice. Osobně se domnívám, že jde spíše o počet osob v publiku, neboť publikum lze připodobnit pojmu veřejnosti ve smyslu čl. 3 informační směrnice, přičemž judikatura SDEU v této otázce konstantně uvádí, že veřejnost se „*týká blíže neurčeného počtu potenciálních diváků či posluchačů a kromě toho vyžaduje dosti vysoký počet osob*.“[61] Kritériem pro určení PSSOO totiž v tomto kontextu dle mého názoru nemůže být to, že publikum služby je určité povahy (ať už věkové, genderové či jiné), ale spíše to, jaký je dosah dané služby. Pokud by totiž službu užívalo několik konkrétních osob na základě přístupových údajů, bude dle judikatury SDEU k pojmu sdělování veřejnosti otázkou, zda je vůbec splněna podmínka veřejnosti. Pokud je počet uživatelů služby naopak značný, můžeme spíše dospět k tomu, že dosah služby je velký, čímž je též zvyšována možná újma nositelů práv, tudíž je podřazení takové služby pod PSSOO pravděpodobnější.

Určitá vodítka k posouzení tohoto prvku přinese zřejmě rozhodnutí SDEU ve věci Uploaded.net, kde je dotazováno, zda daný poskytovatel služeb hostingu sděluje předměty ochrany veřejnosti, pokud se služba „*využívá pro zákonné účely, avšak provozovatel si je vědom toho, že je také dostupné značné množství obsahů (více než 9500 děl), které porušují autorská práva*.“[62] Žádost o předběžnou otázku doplňuje, zda se takové posouzení změní, pokud „*jsou prostřednictvím služby sdíleného hostování zpřístupněny nabídky, které porušují autorská práva a představují 90 – 96 % z celkového rozsahu užívání*.“[63]

Samotné uchovávání, resp. ukládání či hosting, spočívá primárně v poskytnutí části datové kapacity poskytovatele služby k uložení informací poskytnutých příjemcem na jeho žádost. V praxi tak jde zejména o případy

[61] Rozhodnutí Soudního dvora (druhého senátu) ze dne 8. 9. 2016 ve věci C-160/15, GS Media, bod 36.

[62] Viz předběžné otázky ve věci Uploaded.net.

[63] Tamtéž.

webhostingu (např. poskytoval Forpsi[64]), datového úložiště (např. služby YouTube, Instagram či Uschovna.cz) nebo sociální sítě (Facebook, Twitter).[65]

Pojem informace popisuje Polčák za pomoci výkladu kybernetiky jako dynamický proces boje živých organismů proti entropii, tj. rozkladné tendenci.[66] Informace je v tomto vědeckém pojetí procesem, který zvyšuje míru organizace živých organismů a jejich společenství. Ve smyslu čl. 14 E-Com směrnice i čl. 17 DSM směrnice však jde o užití pojmu informatiky, neboť za informaci v tomto smyslu považujeme „*údaje, hodnoty nebo strojově zpracovávaná data.*“[67] Tedy synonymem pojmu *informace* ve smyslu poskytovatele služeb hostingu je spíše pojem *data*. Oproti E-Com směrnici však musí PSSOO uchovávat předměty ochrany, nikoliv jakákoliv data. Ačkoliv však autorskoprávní ochrany nabývají i díla vyjádřená v objektivně vnímatelné podobě bez jejich trvalé fixace na určitý nosič,[68] je v případě užití v digitálním online prostředí nutná materializace do podoby datové.

Během prvního jednání pracovní skupiny Ministerstva kultury k implementaci čl. 17 však zazněla zajímavá poznámka ze strany zástupců menších internetových platforem, kteří uváděli, že pod definici PSSOO mohou spadnout velmi malé platformy (konkrétně uváděli např. webovou stránku fanoušků tzv. tuningu aut, kteří na tuto stránku vkládají odkazy na videa), protože je na nich dostupné velké množství obsahu. Tato poznámka však byla zamítnuta s poukazem na to, že hyperlinky na videa na službě YouTube nebudou považovány za uchovávání obsahu.[69] Domnívám se však, že je třeba zde případně vzít v potaz judikaturu SDEU ve věci přímé

---

[64] Viz Webhosting. *forpsi.com* [online]. Forpsi [cit. 8. 11. 2019]. Dostupné z: https://www.forpsi.com/webhosting/.

[65] HUSOVEC, Martin, op. cit., s. 104.

[66] POLČÁK, Radim, op. cit., s. 20 an.

[67] Viz Informace. *příručka.ujc.cas.cz* [online]. Ústav pro jazyk český Akademie věd ČR [cit. 8. 11. 2019]. Dostupné z: http://prirucka.ujc.cas.cz/?slovo=informace.

[68] TELEC, Ivo.; TŮMA, Pavel. *Autorský zákon: Komentář*. 2. vyd. Praha: C. H. Beck, 2019, s. 22.

[69] Jednání pracovní skupiny č. IX k implementaci čl. 17 na Ministerstvu kultury ČR dne 11. 12. 2019.

odpovědnosti platformy pro sdílení obsahu za sdělování veřejnosti,[70] která v podstatě vedla k přijetí čl. 17 DSM směrnice, a ve věcech týkajících se sdělování veřejnosti pomocí hypertextových odkazů.[71] Tedy teoreticky by takový server mohl být odpovědný za zpřístupňování předmětů ochrany veřejnosti, ačkoliv nebude sám fakticky uchovávat velké množství předmětů ochrany. Tento závěr podporuje též fakt, že z DSM směrnice lze dovodit to, že pirátská služba nemusí fakticky naplnit definici PSSOO, viz dále. U „nepirátských služeb" bude posouzení obtížnější a bude záviset na okolnostech jejich činnosti.

2.3.3 PŘEDMĚTY OCHRANY NAHRÁVANÉ UŽIVATELI

Tato část definice vyplývá již ze samotné povahy služby informační společnosti spočívající v ukládání informací na žádost jejích uživatelů. Režim PSSOO a čl. 17 DSM směrnice se proto neuplatní v případě, kdy předměty ochrany nahrává samotná služba.

Čl. 17 poté zakotvuje ve svém odst. 2 tzv. rozšíření účinků smluvní licence poskytnuté platformě ze strany nositele práv, tj. tato licence pokrývá i úkony uživatelů služby spadající pod čl. 3 informační směrnice. Problematické může ovšem být to, že při užití předmětů ochrany online jejich nahráním na internet dochází též k užití práva na rozmnožování dle čl. 2 informační směrnice.[72] V tomto ohledu jde o zřejmé opomenutí směrnice. Lze nicméně předpokládat, že nositelé práv a především pak platformy budou trvat na tom, aby uzavřené licence pokrývaly i práva na rozmnožování. Nepříjemným praktickým důsledkem však může být, že práva na rozmnožování nebudou posuzována ve světle režimu čl. 17. To může být praktický problém primárně v případě licencování hudebních děl z populárního angloamerického repertoáru, u nějž práva na rozmnožování

[70] Viz rozhodnutí ve věci Pirate Bay.

[71] Viz například rozhodnutí ve věci GS Media.

[72] Viz např. definice práv k hudebním dílům online dle čl. 3 písm. n) směrnice Evropského parlamentu a Rady 2014/26/EU ze dne 26. 2. 2014 o kolektivní správě autorského práva a práv s ním souvisejících a udělování licencí pro více území k právům k užití hudebních děl online na vnitřním trhu. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 12. 12. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014L0026&from=EN.

drží velcí nakladatelé, zatímco práva provozovací zpravidla spravují kolektivní správci. Z toho důvodu se nabízí pamatovat na toto při implementaci směrnice do národních řádů, aby byl režim práv na rozmnožování a sdělování veřejnosti stejný a aby tak byly pokryty i tyto úkony uživatelů služby. V ČR je možností například inspirace § 100 autorského zákona, tj. stanovit, že licence pro PSSOO zahrnuje oprávnění k výkonu práv užít předmět ochrany rozmnožováním dle § 13 a sdělováním veřejnosti dle § 18 autorského zákona nezbytných k poskytování služby online.

2.3.4 ZPŘÍSTUPŇOVÁNÍ PŘEDMĚTŮ OCHRANY

České znění směrnice uvádí, že jedním z hlavních účelů PSSOO je zpřístupňovat předměty ochrany veřejnosti.[73] Jde však o zřejmý omyl v překladu anglického znění směrnice.

DSM směrnice ve svém recitálu 66 uvádí, že PSSOO „*poskytují přístup k obsahu.*“ Anglické znění zde pro poskytování přístupu uvádí spojení „*give the public access to*.“ Zatímco však anglické znění definice PSSOO v čl. 2 odst. 6 směrnice opět používá výše uvedeného spojení, české znění zde uvádí termín „zpřístupňovat veřejnosti“. Tento termín ovšem v právu EU označuje specifickou subkategorii práva na sdělování veřejnosti, tj. práva na zpřístupnění předmětů ochrany veřejnosti takovým způsobem, že každý jednotlivec ze strany veřejnosti má k těmto předmětům ochrany přístup z místa a v době, které si zvolí, ve smyslu čl. 3 informační směrnice. V anglickém znění je toto právo označováno jako tzv. „*making available right*“. Negativní dopad tohoto ztracení se v překladu samotné definice je pak nejlépe vidět přímo v čl. 17 odst. 1 DSM směrnice, dle kterého PSSOO „*provádějí sdělení veřejnosti nebo zpřístupnění veřejnosti pro účely této směrnice, pokud poskytují veřejnosti přístup*“ k předmětům ochrany.

Ponechání pojmu „zpřístupňování veřejnosti“ v čl. 2 odst. 6 DSM směrnice namísto správného „poskytování přístupu veřejnosti“ by tak mohlo vést k mylnému výkladu, kdy pro podřazení daného subjektu pod definici PSSOO bychom museli zkoumat, zda je jedním z jeho účelů

[73] Ve znění k 31. 3. 2020.

provádět pouze a jenom toto konkrétní zpřístupňování předmětů ochrany ve smyslu čl. 3 informační směrnice. Rovněž by úprava byla vnitřně rozporná, pokud čl. 17 odst. 1 uvádí, že PSSOO též sděluje předměty ochrany veřejnosti.

Záměrem tohoto definičního prvku tak jistě bylo brát v potaz co nejvíce subjektů ukládajících obsah poskytnutý svými uživateli, které nějakým způsobem poskytují veřejnosti přístup k obsahu, a teprve poté dále hodnotit další aspekty dané služby. O tomto svědčí též úvodní obecná ustanovení recitálu DSM směrnice: *„Aby bylo možné dosáhnout řádně fungujícího a spravedlivého tržního prostředí pro autorské právo, měla by existovat rovněž pravidla upravující (…) užití děl nebo jiných předmětů ochrany poskytovateli online služeb, kteří ukládají obsah nahrávaný uživateli a umožňují k němu přístup.“*[74]

Zajímavostí je informace dánských nositelů práv o tom, že v Dánsku dochází prostřednictvím Facebookových skupin ke streamingu filmů formou webcastingu, tj. nedochází k uložení souborů na servery Facebooku a nejde rovněž o sdělování předmětů ochrany na vyžádání.[75] Lze předpokládat, že takové užití je mimo rozsah čl. 17 a spadá pod působnost bezpečných přístavů dle E-Com směrnice, ačkoliv je spíše v zájmu platforem zajistit si licence i na takováto užití.

2.3.5 USPOŘÁDÁVÁNÍ PŘEDMĚTŮ OCHRANY

Aspekt uspořádávání předmětů ochrany vychází zejména z rozhodnutí SDEU ve věci Pirate Bay. SDEU zde dospěl k odpovědnosti platformy též s poukazem na to, že:

„zpřístupněním a správou takové online platformy pro sdílení, o jakou jde ve věci v původním řízení, jednají tito provozovatelé s plnou znalostí důsledků svého jednání s cílem poskytnout přístup ke chráněným dílům ***prostřednictvím indexace a sestavení seznamu*** *souborů torrent na uvedené platformě,* ***které uživatelům této platformy umožňují tato díla nacházet*** *a sdílet je,“*[76] *popř.*

---

[74] Viz bod 3 recitálu DSM směrnice.

[75] TELEC, TŮMA, op. cit., s. 228-229.

[76] Viz bod 36 odůvodnění rozhodnutí ve věci Pirate Bay.

stahovat. Kromě toho „online platforma pro sdílení TPB nabízí vedle vyhledávače i rejstřík, v němž jsou díla zařazena do různých kategorií podle povahy děl, jejich druhu nebo oblíbenosti, v nichž jsou roztříděna zpřístupněná díla, přičemž dohled nad umístěním díla do patřičné kategorie zajišťují provozovatelé této platformy. Uvedení provozovatelé mimoto odstraňují zastaralé nebo chybné soubory torrent a aktivně filtrují některý obsah.“[77]

Toto kritérium tak předpokládá aktivní roli platformy ve správě obsahu nahraného uživateli, tj. zejména v jeho indexaci, filtraci, vkládání metadat, sestavování seznamů či zařazování do určitých kategorií na platformě, které umožňují snadné vyhledávání obsahu uživateli platformy.[78] Ačkoliv pak například kategorizaci může reálně provádět samotný uživatel při nahrávání souboru, je podstatné to, že využitelnost této kategorizace nastává jen v případě, že jí platforma akceptuje a zpracuje, tj. zpravidla uživatelům umožňuje soubor nějakým způsobem označit a zařadit a dává mu k tomu prostředky, přičemž soubor je následně indexován. Příkladem může být zařazování nahrávaných videí na platformě YouTube do kategorií hudba, film a animace, sport, komedie ad. či vyhledávání na službě Ulož.to přes kategorie videa, obrázků, audia či dokumentů. S tím souvisí též funkcionalita tzv. našeptávače, který uživatelům na základě jejich dotazu ve vyhledávacím poli nabízí konkrétní text k hledání. Jeho existence tak již sama o sobě může být důkazem toho, že obsah na službě je přinejmenším indexovaný a určitým způsobem uspořádaný, ledaže je našeptávač založen jen na nejčastěji hledaných slovech. V takových případech však můžeme mluvit alespoň o propagaci obsahu.

Jistým problémem v praxi může být též aspekt aktivního odstraňování zastaralých souborů, který bude někdy obtížné prokázat. Osobně se však domnívám, že pro uspořádávání obsahu ve smyslu čl. 2 odst. 6 DSM směrnice postačí indexace či kategorizace, neboť tato činnost i bez odstraňování starého obsahu svědčí o aktivní roli PSSOO vůči ukládanému obsahu.

---

[77] Viz bod 38 tamtéž.

[78] Viz bod 62 odůvodnění DSM směrnice, kde jako příklad uspořádávání uvedena kategorizace.

Není jasné, zda uspořádávání předmětů ochrany ve smyslu čl. 2 odst. 6 DSM směrnice vyžaduje též možnost vyhledávat obsah přímo pomocí vyhledávače na dané službě. Ačkoliv to může na první pohled vyplývat z rozhodnutí SDEU ve věci Pirate Bay,[79] vágnost definice PSSOO a předběžná otázka ve věci Uploaded.net mohou nakonec vést k tomu, že postačí vyhledávání prostřednictvím odkazů vložených na jiné webové stránky či přes služby třetích stran, přičemž takové vyhledávání umožní již samotná indexace obsahu.[80]

Původní návrh DSM směrnice zde užíval termínu „*optimalizování prezentace nahraných děl nebo předmětů ochrany*,“ čímž odkazoval na rozhodnutí ve věci L'Oréal.[81] Změna na termín „*uspořádávání předmětů ochrany*“ souvisí pravděpodobně s později vydaným rozhodnutím SDEU ve věci Pirate Bay. Tudíž pojem uspořádávání je zřejmě užší než pojem optimalizace ve smyslu rozhodnutí L'Oréal, tj. pro jeho uplatnění je potřeba splnění vícero kritérií.

2.3.6 PROPAGACE PŘEDMĚTŮ OCHRANY

Ačkoliv to tak na první pohled nepůsobí, aspekt propagace předmětů ochrany je jedna z nejsložitějších otázek definice PSSOO. Otázkou je již to, co je to propagace sama o sobě? Postačí tak např. existence našeptávače či existence seznamu nejstahovanějšího nebo nejsledovanějšího obsahu? Nebo musí propagace spočívat v inzerci konkrétních předmětů ochrany? Nebo jde o propagaci služby jako takové?

Již rozhodnutí SDEU ve věci L'Oréal stanovilo aktivní roli poskytovatele služeb informační společnosti též díky tomu, že služba eBay „*poskytuje pomoc, která spočívá zejména v optimalizaci prezentace dotčených nabídek*

[79] Viz bod 38 odůvodnění rozhodnutí SDEU ve věci Pirate Bay.

[80] Předběžná otázka uvádí, že zde „*provozovatel neposkytuje informace o obsahu ani vyhledávací funkci, avšak jím poskytované neomezené odkazy na stahování umísťují na internet třetí strany v podobě hromadných odkazů, které obsahují informace o obsahu souborů a umožňují vyhledávání určitých obsahů*.“

[81] Viz bod 38 návrhu směrnice Evropského parlamentu a Rady o autorském právu na jednotném digitálním trhu ze dne 14. 9. 2016, publikováno pod COM(2016) 593 final. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 13. 12. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52016PC0593&from=EN (dále jen“ návrh DSM směrnice“).

k prodeji nebo jejich propagaci." V tomto ohledu lze dovodit, že by propagace měla spočívat v propagaci předmětů ochrany dostupných na službě, nepostačí tak propagace služby samotné. Nabízí se otázka, zda k propagaci předmětů ochrany může dojít též skrze nástroje třetích stran, neboť eBay prováděl navíc „*reklamu pro určité zboží prodávané na on-line tržišti pomocí zobrazování inzerce provozovateli takových internetových vyhledávačů, jako je Google*."[82]

Recitál 62 odůvodnění DSM směrnice blíže specifikuje, že k propagaci dochází „*s cílem přilákat širší publikum, mimo jiné prostřednictvím (...) využívání cílené propagace v rámci obsahu*." Propagace tedy musí cílit na cílové publikum v rámci obsahu služby, nikoliv v rámci služby. Lze si proto představit například inzerci služby na jiných serverech či jiných médiích propagující dostupnost jejího určitého obsahu či propagaci daného konkrétního obsahu přes tzv. Google Ads při vyhledávání na službě Google. Pokud je tedy propagován obsah služby, zřejmě nic nebrání propagaci též prostřednictvím služeb třetích stran (tj. např. propagace kategorie filmů dostupných na službě přes reklamu na webové stránce třetí strany).

Jistě lze za propagaci považovat i situaci, kdy sama domovská stránka dané platformy nabízí doporučená videa, jako je tomu u služby YouTube, nebo nabízí seznamy nejstahovanějších či nejlépe hodnocených videí, jako je tomu např. na české službě datoid.cz. Složitější je však situace v případě našeptávačů. Tato funkcionalita totiž může fungovat vícero způsoby. Zejména tak může jít o doplňování hledaných klíčových slov na základě již uložených souborů na službě. Na druhou stranu může jít jen o kombinované výstupy ze slov již dříve hledaných uživateli služby. V prvním případě lze záměrnou propagaci dovodit. V druhém případě bychom museli zřejmě trvat na tom, že již samotné umožnění funkcionality je propagací obsahu, přičemž danému uživateli je předkládáno, co je aktuálně ostatními uživateli poptáváno. Je však třeba pamatovat na to, že propagovat je třeba předměty ochrany, přičemž našeptávač bude zpravidla vyhledávat též soubory bez chráněného obsahu.[83]

[82] Bod 31 odůvodnění rozhodnutí ve věc L'Oréal.

Domnívám se tak, že bližší výklad bude v tomto případě muset poskytnout až SDEU, neboť dalším vodítkem může aktuálně být pouze samotný původní návrh DSM směrnice, který v recitálu 38 uváděl, že *„je třeba ověřit, zda poskytovatel služeb“* předměty ochrany *„propaguje, a to bez ohledu na povahu prostředků, které k tomu použije.“* Dojít k tomu může již v rámci rozhodnutí ve věci YouTube, kde je dotazováno, zda provozovatel služby provádí sdělování předmětů ochrany veřejnosti, pokud

„provádí na této platformě úpravu výsledků vyhledávání v podobě seznamů uspořádaných podle hodnocení a rubrik uspořádaných podle příslušného obsahu a registrovaným uživatelům zobrazuje přehled doporučených videí sestavený na základě videí, která uživatelé shlédli v minulosti.“[84]

2.3.7 ÚČEL ZISKU

Recitál 62 odůvodnění DSM směrnice uvádí, že PSSOO umožňují nahrávat a sdílet velké množství obsahu chráněného autorským právem *„za účelem přímého či nepřímého dosahování zisku.“* Bod 46 odůvodnění rozhodnutí SDEU ve věci Pirate Bay dovozuje, že provozování a správa dané platformy *„jsou uskutečňovány za účelem dosahování zisku, neboť tato platforma je zdrojem značných příjmů z reklamy.“* Tento aspekt tak nalezneme jak u služby YouTube, tak u služby Ulož.to.[85] Pro českou implementaci zde může být problematickým odlišení zisku od hospodářského či obchodního prospěchu, kterýžto termín používá český autorský zákon. Analýzou užité terminologie v legislativě EU lze dospět k tomu, že hospodářský prospěch odpovídá anglickému pojmu *„economic benefit“*,[86] popř. *„economic or commercial advantage.“*[87] Termín *„profit“* je tak skutečně překládán jako „zisk“. Tyto termíny je tak třeba odlišit, neboť hospodářský či obchodní

---

[83] K otázce našeptávačů viz např. KARAPAPA, Stavroula; BORGHI, Maurizio. Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm. *International Journal of Law and Information Technology* [online]. [cit. 13. 12. 2019] 2015, Vol. 23, Issue 3. s. 261-289. Dostupné z: https://doi.org/10.1093/ijlit/eav009.

[84] Viz shrnutí žádosti o rozhodnutí o předběžné otázce ze dne 13. 9. 2018 ve věci C-682/18, LF proti Google LLC a další („věc YouTube“).

[85] Viz např. Ceník reklamy na Ulož.to poskytované společností rootmedia platný od 1. 1. 2019. *rootmedia.cz* [online]. rootmedia [cit. 13. 12. 2019]. Dostupné z: https://rootmedia.cz/dokumenty/cenik_ulozto.pdf.

prospěch může kromě finančního plnění spočívat v plněních naturálních, v prominutí dluhu, v získání soutěžní výhody apod.[88] Termín zisk je tak zřejmě orientován pouze na finanční příjem platformy. Pokud poté vezmeme v potaz recitál 11 odůvodnění směrnice 2006/115/ES a rozhodnutí SDEU ve věci Pirate Bay, můžeme dospět k tomu, že účelem zisku bychom měli rozumět i situaci, kdy platforma skončí ve ztrátě, ačkoliv generuje příjmy z užití předmětů ochrany. Oproti tomu o obchodní či hospodářský prospěch by nemělo jít v případě, kdy úplata, kterou provozovatel přijme, pouze pokryje provozní náklady, či je ještě nižší. Podstatný je tu účel zisku, nikoliv kladná účetní závěrka.

2.4 PIRÁTSKÉ SLUŽBY

Dle recitálu 62 odůvodnění DSM směrnice by se mechanismus výjimek z odpovědnosti stanovený touto směrnicí „*neměl vztahovat na poskytovatele služeb, jejichž hlavním účelem je provádět nebo usnadňovat pirátství v oblasti autorských práv*.“ Jde o zřejmý projev rozhodnutí SDEU ve věci Pirate Bay. Provozovatelé služby Pirate Bay totiž „*byli informováni o skutečnosti, že tato platforma, kterou poskytují uživatelům a kterou spravují, umožňuje přístup k dílům zveřejněným bez svolení nositelů práv, a jednak to, že titíž provozovatelé na blozích a fórech dostupných na uvedené platformě výslovně uvádějí, že jejich cílem je zpřístupnit chráněná díla uživatelům, a tyto uživatele podněcují k pořízení rozmnoženin těchto děl*.“ K tomu SDEU dodal, že provozovatelé Pirate Bay nemohli nevědět, že „*tato platforma umožňuje přístup k dílům zveřejněným bez svolení nositelů práv*,“ a to s ohledem na skutečnost, že „*značná část souborů torrent nacházejících se na online*

[86] Viz překlady pojmu hospodářský prospěch ze služby Linguee. Hospodářský prospěch. *linguee.com* [online]. Linguee [cit. 13. 12. 2019]. Dostupné z: https://www.linguee.com/english-czech/search?source=czech&query=hospod%C3%A1%C5%99sk%C3%BD+prosp%C4%9Bch.

[87] Viz bod 11 odůvodnění směrnice Evropského parlamentu a Rady 2006/115/ES ze dne 12. prosince 2006 o právu na pronájem a půjčování a o některých právech v oblasti duševního vlastnictví souvisejících s autorským právem. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 13. 12. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/ALL/?uri=CELEX%3A32006L0115.

[88] TELEC, TŮMA, op. cit., s. 202.

platformě pro sdílení TPB odkazuje na díla zveřejněná bez svolení nositelů práv."[89]

Z toho lze dospět k tomu, že pro určení pirátského účelu takové služby by měla postačovat skutečnost, že většina obsahu služby obsahuje předměty ochrany, k jejichž sdělení nebylo uděleno svolení. Vlastní aktivní prohlášení služby o pirátském účelu by tudíž mělo působit jen jako podružný aspekt.

Z formulace recitálu 62, který mluví o „poskytovateli služeb", nikoliv o PSSOO, a z rozhodnutí ve věci Pirate Bay, které mluví o „online platformě pro sdílení" pak lze dovodit přímou odpovědnost jakékoliv služby informační společnosti spočívající ve sdílení obsahu bez svolení nositelů práv za sdělování a zpřístupňování předmětů ochrany veřejnosti. Taková platforma tudíž zřejmě nemusí naplnit všechny definiční prvky PSSOO.

Nabízí se tu však též ta úvaha, že ustanovení recitálu 62 je širší než popis pirátské služby v rozhodnutí Pirate Bay. O tomto svědčí formulace „služba, která provádí *nebo usnadňuje* pirátství." Osobně se však kloním k tomu, že přímou autorskoprávní odpovědnost těchto pirátských služeb lze zakotvit pouze v případě, kdy činnost této služby spočívá přímo v umožnění přístupu k obsahu chráněného autorským právem, ať už jej nahrávají uživatelé přímo na tuto službu, nebo služba slouží zejména k agregaci přístupových údajů k chráněnému obsahu (tj. zejména hyperlinky a hesla k uzamčeným či komprimovaným souborům uloženým na jiných službách).[90]

2.5 INDIVIDUÁLNÍ POSOUZENÍ PSSOO

DSM směrnice pro posouzení platformy jakožto PSSOO stanovuje v recitálu 63 odůvodnění směrnice korektiv individuálního posouzení služby v daném kontextu. Toto posouzení je ovšem vázáno pouze na prvky uchovávání velkého množství obsahu chráněného autorským právem a poskytování přístupu k tomuto obsahu veřejnosti. Z toho důvodu by například

[89] Bod 45 odůvodnění rozhodnutí ve věci Pirate Bay.

[90] Viz bod 62, první věta odůvodnění DSM směrnice.

posouzení hlavního účelu, propagace a organizace obsahu či účelu zisku mělo vycházet z objektivního posouzení, nikoliv případ od případu.

Při posouzení výše uvedených prvků definice je tak třeba „*zohledňovat kombinaci prvků, jako je cílové publikum služby a počet souborů obsahu chráněného autorským právem nahraných uživateli těchto služeb*.“[91] Cílové publikum i počet souborů již byly analyzovány výše. Důležité však je, že ze znění recitálu 63 vyplývá, že těchto prvků může být více a je tedy zřejmě i na úvaze členských států, zda explicitně zavedou další kritéria. Ačkoliv je tak ze strany YouTube či německé vlády uváděno, že je třeba výslovně implementovat otázku postavení na trhu a soutěže s ostatními platformami, tyto aspekty lze považovat spíše za specifický objektivní prvek samotné definice PSSOO, nikoliv za kritéria pro individuální posouzení toho, zda platforma uchovává velké množství obsahu chráněného autorským právem a poskytuje k němu přístup.

3. ZÁVĚR

Definice PSSOO obsahuje množství specifických aspektů a je třeba ji číst a rozebírat důsledně spolu s příslušnými recitály a judikaturou, na kterou nová směrnice navazuje. Ačkoliv jsou tak pochopitelné stížnosti některých subjektů na právní nejistotu spojenou s posouzením své vlastní činnosti, nezbývá než souhlasit s tím, že implementace v členských státech by se měla držet co nejvíce textace směrnice a nejednoznačná místa ponechat na soudní výklad. V případě definice PSSOO je tento požadavek klíčový, neboť PSSOO je nutno považovat za autonomní pojem práva EU. První vodítka by tak již mohla poskytnout rozhodnutí SDEU v probíhajících případech ve věci YouTube a Uploaded.net, čímž by již v době přijetí textu implementace směrnice mohla být snížena právní nejistota adresátů směrnice.

Lze shrnout, že nejobtížnějšími prvky definice k posouzení jsou velký počet předmětů ochrany uchovávaný platformou a propagace tohoto obsahu. S ohledem na vyžadovanou kumulativnost definičních prvků se totiž může stát, že určitá platforma bude na první pohled spadat pod definici PSSOO, avšak tímto jedním chybějícím či nejednoznačným prvkem

[91] Bod 63 odůvodnění DSM směrnice.

se na ni režim odpovědnosti dle čl. 17 nebude aplikovat. První uvedený aspekt bude zřejmě posouzen v rozhodnutí SDEU ve věci Uploaded.net, u druhého může napovědět rozhodnutí SDEU ve věci YouTube. Věc Uploaded.net pak může mít značné dopady na fungování českých uložišť typu Ulož.to a posouzení jejich odpovědnosti.[92]

Obdobně obtížným bude posouzení požadavku soutěže na trhu mezi platformami pro dané předměty ochrany jakožto kritéria pro aplikaci definice PSSOO, které je aktuálně propagováno ze strany platforem při implementačních jednáních v členských státech. I zde nezbývá než vyčkat judikaturních závěrů.

Ačkoliv bývá DSM směrnice kritizována (v případě některých legislativních opomenutí oprávněně), ztotožňuji se s prohlášením ředitele pro právní a legislativní záležitosti společnosti Seznam.cz Michala Feixe, jež pronesl na prvním implementačním jednání na Ministerstvu kultury ČR, tj. s tím, že směrnice má za cíl především narovnat postavení subjektů na trhu a vést k tomu, aby platformy založené na sdílení obsahu při své činnosti postupovaly zodpovědně a obezřetně. Pokud proto někdo založí svůj obchodní model na sdílení cizího obsahu, musí rovněž nést svoji odpovědnost a tomu přizpůsobit své chování.[93]

Aplikace článku 17 DSM směrnice nebude zprvu v praxi příliš jednoduchá, přičemž výše uvedený rozbor je důkazem toho, že již definice subjektů dotčených tímto článkem obsahuje množství neznámých proměnných. Domnívám se však, že komplexnost definice povede spíše k tomu, že množství subjektů bude moci stále vyloučit svoji odpovědnost dle E-Com směrnice. Režim odpovědnosti dle DSM směrnice se tak bude aplikovat jen na subjekty, které se specificky a ve větším rozsahu zaměřují na sdílení chráněného obsahu poskytnutého jejich uživateli, tj. zjevně těží z majetku třetích osob. Z toho důvodu považuji za vhodné upřít pozornost

[92] Viz bod 4 shrnutí žádosti ve věci Uploaded.net, které uvádí: „*Služba žalované je využívána jak pro zákonné účely, tak i způsobem, kterým je porušováno autorské právo třetích osob. Již v minulosti byla žalovaná ze strany poskytovatelů služeb pověřených nositeli práv mnohokrát upozorněna na dostupnost obsahů porušujících práva*.“ Podobnost se službou Ulož.to je zcela evidentní.

[93] Jednání pracovní skupiny č. IX k implementaci čl. 17 na Ministerstvu kultury ČR dne 11. 12. 2019.

aktuální debaty nad implementací DSM směrnice na samotnou definici subjektů, na které se nová úprava bude vztahovat. Rozbor provedený tímto článkem by tomu mohl být nápomocen.

4. POUŽITÉ ZDROJE

4.1 MONOGRAFIE

[1] HUSOVEC, Martin. *Zodpovednosť na internete podľa českého a slovenského práva*. 1. vyd. Praha: CZ.NIC, 2014, 230 s. ISBN 978-80-904248-8-3.

[2] ANDRUŠKO, Alena. Internet, informační společnost a autorské právo. 1. vyd. Praha: Wolters Kluwer ČR, 276 s. ISBN 978-80-7552-327-3.

[3] POLČÁK, Radim. *Internet a proměny práva*. 1. vyd. Praha: Auditorium, 2012, 392 s. ISBN 978-80-87284-22-3.

[4] POLČÁK, Radim a kol. *Právo informačních technologií*. 1. vyd. Praha: Wolters Kluwer, 2018, 656 s. ISBN 978-80-7598-045-8.

[5] TELEC, Ivo.; TŮMA, Pavel. *Autorský zákon: Komentář*. 2. vyd. Praha: C. H. Beck, 2019, s. 22. ISBN 978-80-7400-748-4.

4.2 ČLÁNKY

[6] HUSOVEC, Martin, QUINTAIS, J. P. *How to license Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms*. [online] 27 s. [cit. 27. 12. 2019]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3463011.

[7] MONTAGNANI, Maria Lillá; TRAPOVA, Alina. New Obligations for Internet Intermediaries in the Digital Single Market - Safe Harbors in Turmoil? *Journal of Internet Law* [online]. 2019, vol. 22, č. 7, s. 3-11 [cit. 15. 11. 2019]. Dostupné z: https://ssrn.com/abstract=3361073.

[8] VISSER, Dirk J.G. *Trying to understand the article formerly known as '13'*. [online] s. 3. [cit. 8. 12. 2019]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354494.

[9] LIEBOWITZ, Stan. *Economic Analysis of Safe Harbour Provisions* [online]. [cit. 13. 12. 2019]. Dostupné z: https://www.cisac.org/CISAC-University/Library/Studies-Guides/Economic-Analysis-of-Safe-Harbour-Provisions.

[10] KARAPAPA, Stavroula; BORGHI, Maurizio. Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm. *International Journal of Law and Information Technology* [online]. [cit. 13. 12. 2019] 2015, Vol. 23, Issue 3. s. 261-289. Dostupné z: https://doi.org/10.1093/ijlit/eav009.

4.3 JUDIKATURA

[11] Rozhodnutí Soudního dvora (velkého senátu) ze dne 12. července 2011 ve věci C-324/09, L'Oréal a další, ECLI:EU:C:2011:474.

[12] Rozhodnutí Soudního dvora (druhého senátu) ze dne 8. 9. 2016 ve věci C-160/15, GS Media, ECLI:EU:C:2016:644.

[13] Rozhodnutí Soudního dvora (druhého senátu) ze dne 14. 6. 2017 ve věci C-610/15, Stichting Brein, ECLI:EU:C:2017:456.

[14] Rozhodnutí Soudního dvora (pátého senátu) ze dne 2. 4. 2009 ve věci C-134/08, Hauptzollamt Bremen, ECLI:EU:C:2009:229.

[15] Stanovisko generálního advokáta Macieje Szpunara přednesené dne 30. dubna 2019 ve věci C-390/18, AIRBNB, ECLI:EU:C:2019:336.

[16] Žádost o rozhodnutí o předběžné otázce ze dne 13. 9. 2018 ve věci C-682/18, LF proti Google LLC a další. Dostupné z: http://curia.europa.eu/juris/showPdf.jsf?text=&docid=220171&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=576481.

[17] Žádost o rozhodnutí o předběžné otázce ze dne 6. 11. 2018 ve věci C-683/18, Elsevier Inc. proti Cyando AG. Dostupné z: http://curia.europa.eu/juris/showPdf.jsf?text=&docid=220297&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=576481.

[18] Rozhodnutí Městského soudu v Praze ze dne 25. 3. 2019, sp. zn. 32 C 41/2014.

[19] Rozhodnutí Městského soudu v Praze ze dne 22 .2. 2019, sp. zn. 34 C 5/2017.

[20] Rozhodnutí Bundesgerichtshof ze dne 12. 7. 2012, sp. zn. I ZR/18/11. *dejure.org* [online] Dejure, 2013 [cit. 10. 12. 2019]. Dostupné z: https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=12.07.2012&Aktenzeichen=I%20ZR%2018/11.

[21] Rozhodnutí Bundesgerichtshof ze dne 15. 8. 2013, sp. zn. I ZR/79/12. *dejure.org* [online] Dejure, 2013 [cit. 10. 12. 2019]. Dostupné z: https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=15.08.2013&Aktenzeichen=I%20ZR%2079/12.

4.4 INTERNETOVÉ ZDROJE

[22] Voice over Internet Protocol. *wikipedia.org* [online]. Wikipedia [cit. 25. 11. 2019]. Dostupné z: https://cs.wikipedia.org/wiki/Voice_over_Internet_Protocol.

[23] Implementatiewetsvoorstel Richtlijn auteursrecht in de digitale eengemaakte markt. *overheid.nl* [online]. Overheid [cit. 1. 12. 2019]. Dostupné z: https://www.internetconsultatie.nl/auteursrecht/reacties.

[24] We do not support the EU Copyright Directive in its current form. Here's why you shouldn't either. *wikimediafoundation.org* [onlince]. Wikimedia Foundation [cit. 1. 12. 2019]. Dostupné z: https://wikimediafoundation.org/news/2019/02/28/we-do-not-support-the-eu-copyright-directive-in-its-current-form-heres-why-you-shouldnt-either/.

[25] Podmínky poskytování služeb. *youtube.com* [online]. YouTube [cit. 12. 12. 2019]. Dostupné z https://www.youtube.com/static?gl=CZ&template=terms.

[26] Všeobecné smluvní podmínky užívání služeb poskytovaných společností Uloz.to cloud a.s. (mimo jiné) na stránkách uloz.to. *uloz.to* [online]. Ulož.to [cit. 12. 12. 2019]. Dostupné z: https://uloz.to/podminky/vseobecne-smluvni-podminky.

[27] Stanoviska členských států ke konečnému textu směrnice o autorském právu na jednotném digitálním trhu publikovaná pod č. 7986/19 ADD 1 REV 2 dne 15. 4. 2019. *data.consilium.europa.eu* [online]. Rada EU [cit. 13. 12. 2019]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-7986-2019-ADD-1-REV-2/en/pdf.

[28] Webhosting. *forpsi.com* [online]. Forpsi [cit. 8. 11. 2019]. Dostupné z: https://www.forpsi.com/webhosting/.

[29] Informace. *příručka.ujc.cas.cz* [online]. Ústav pro jazyk český Akademie věd ČR [cit. 8. 11. 2019]. Dostupné z: http://prirucka.ujc.cas.cz/?slovo=informace.

[30] Ceník reklamy na Ulož.to poskytované společností rootmedia platný od 1. 1. 2019. *rootmedia.cz* [online]. rootmedia [cit. 13. 12. 2019]. Dostupné z: https://rootmedia.cz/dokumenty/cenik_ulozto.pdf.

[31] Hospodářský prospěch. *linguee.com* [online]. Linguee [cit. 13. 12. 2019]. Dostupné z: https://www.linguee.com/english-czech/search?source=czech&query=hospod%C3%A1%C5%99sk%C3%BD+prosp%C4%9Bch.

[32] Music Listening 2019. *ifpi.org* [online]. IFPI [cit. 28. 5. 2020]. Dostupné z: https://www.ifpi.org/downloads/Music-Listening-2019.pdf.

[33] Youtube is generating $32k every minute – but how much of that money is being driven by music? *musicbusinessworldwide.com* [online]. Music Business Worldwide [cit. 28. 5. 2020]. Dostupné z: https://www.musicbusinessworldwide.com/youtube-is-generating-32k-every-minute-but-how-much-of-that-money-is-being-driven-by-music/.

[34] Prezentace společnosti Seznam ze 4. jednání dialogu Evropské komise k čl. 17 ze dne 16. 12. 2019. Dostupné z: https://ec.europa.eu/digital-single-market/en/news/fourth-meeting-stakeholder-dialogue-article-17-directive-copyright-digital-single-market.

4.5 PRÁVNÍ PŘEDPISY

4.5.1 PRÁVNÍ PŘEDPISY ČR

[35] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů. In: Beck-online [online právní informační systém]. Nakladatelství C. H. Beck [cit. 1. 12. 2019]. Dostupné z: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=onrf6mrqgay

f6mjsgewtema&groupIndex=2&rowIndex=0.

4.5.2 PRÁVNÍ PŘEDPISY EU

[36] Nařízení Evropského parlamentu a Rady (EU) 2015/2120 ze dne 25. listopadu 2015, kterým se stanoví opatření týkající se přístupu k otevřenému internetu a mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací a nařízení (EU) č. 531/2012 o roamingu ve veřejných mobilních komunikačních sítích v Unii. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 23. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32015R2120.

[37] Směrnice Evropského Parlamentu a Rady 98/34/ES ze dne 22. června 1998 o postupu při poskytování informací v oblasti norem a technických předpisů. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 17. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A31998L0034.

[38] Směrnice Evropského parlamentu a Rady 98/48/ES ze dne 20. července 1998, kterou se mění směrnice 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 17. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX%3A31998L0048.

[39] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 15. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32000L0031.

[40] Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. 5. 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 22. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32001L0029&from=EN.

[41] Směrnice Evropského parlamentu a Rady 2006/115/ES ze dne 12. prosince 2006 o právu na pronájem a půjčování a o některých právech v oblasti duševního vlastnictví souvisejících s autorským právem. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 13. 12. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/ALL/?uri=CELEX%3A32006L0115.

[42] Směrnice Evropského parlamentu a Rady 2014/26/EU ze dne 26. 2. 2014 o kolektivní správě autorského práva a práv s ním souvisejících a udělování licencí pro více území k právům k užití hudebních děl online na vnitřním trhu. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 12. 12. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32014L0026&from=EN.

[43] Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 17. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=uriserv:OJ.L_.2015.241.01.0001.01.CES.

[44] Směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 23. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/uri=uriserv:OJ.L_.2018.321.01.0036.01.

CES&toc=OJ:L:2018:321:TOC.

[45] Směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 15. 11. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN-CS/TXT/?uri=CELEX:32019L0790&from=cs.

[46] Návrh směrnice Evropského parlamentu a Rady o autorském právu na jednotném digitálním trhu ze dne 14. 9. 2016, publikováno pod COM(2016) 593 final. In: EUR-Lex [právní informační systém]. Úřad pro publikace Evropské unie [cit. 13. 12. 2019]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52016PC0593&from

=EN.

4.6 OSTATNÍ ZDROJE

[47] Jednání pracovní skupiny č. IX k implementaci čl. 17 na Ministerstvu kultury ČR dne 11. 12. 2019.

[48] Informace autora z jednání tzv. Madrid Group, pracovní skupiny právníků evropských kolektivních správců sdružených v organizaci GESAC („*Groupement Européen des Sociétés d'Auteurs et Compositeurs*“).

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

---

https://doi.org/10.5817/RPT2020-1-6

PROKAZOVÁNÍ PŘÍČINNÉ SOUVISLOSTI U ŠKOD ZPŮSOBENÝCH PROPOJENÝMI AUTONOMNÍMI VOZIDLY

VERONIKA ŽOLNERČÍKOVÁ[1]

ABSTRAKT

Dnešní silniční doprava funguje díky komplexní sadě pravidel. Klíčovým prvkem je fyzická osoba za volantem, která ovládá vozidlo. Pokud místo fyzické osoby vozidlo kontroluje autonomní systém, může se rozhodovat podobně jako člověk. Zároveň ale komunikuje s dalšími vozidly a okolní infrastrukturou. Představený technologický posun je natolik zásadní, že je potřeba revidovat některé základní právní principy a ujistit se, že budou použitelné i pro autonomní technologie.

Takovou revizi vyžaduje například princip prokazování příčinné souvislosti. Stanovení civilněprávní odpovědnosti za škodu způsobenou provozem dopravního prostředku předpokládá prokázání příčinné souvislosti mezi jednáním určité osoby (řidiče) a škodným následkem. U autonomních vozidel by logicky neměla být příčinná souvislosti prokazována ve vztahu k řidiči, ale k jiné osobě (výrobci, provozovateli, programátorovi). Nicméně i tak přetrvává obtíž, že škoda nikdy nebude způsobena jedním jediným vozidlem. Podíl budou do určité míry nést i další vozidla či infrastruktura v kooperativním systému.

Článek se zabývá právě touto málo prozkoumanou oblastí a klade si za otázku jakým způsobem prokazovat příčinnou souvislost u multikauzálních škod v kooperativním silničním systému. Článek analyzuje s přihlédnutím k relevantní judikatuře dosavadní přístup k prokazování příčinné souvislosti v českém právu.

[1] Mgr. Veronika Žolnerčíková, prezenční doktorská studentka na Ústavu práva a technologií Masarykovy univerzity, e-mail: veronika.zolnercikova@law.muni.cz.

Následně se zabývá otázkou, zdali by vůbec bylo možné za stávající právní úpravy dosáhnout prokázání příčinné souvislosti v kooperativním systému.

KLÍČOVÁ SLOVA

AI, příčinná souvislost, multikauzální újma, autonomní vozidlo, kooperativní inteligentní silniční systém

ABSTRACT

Today's road traffic system functions because of a complex set of rules. The key factor is a physical person sitting in the driver's seat and controlling the vehicle. If instead of a physical person there is an autonomous system in charge of the vehicle, it is capable of a human-like decision making. Furthermore, it is communicating with other vehicles and with the surrounding infrastructure. This technological shift is so significant that it is necessary to revise fundamental legal principles and make sure that they will be applicable for autonomous technologies as well.

One of the principles requiring revision is the proof of causal nexus. For establishing legal liability for damage caused in a road traffic accident, it is first needed to prove the causal nexus between the conduct of a specific person (the driver) and the damage caused. When talking about autonomous vehicles, causality should not be proven between the conduct of the driver and the damage, but between conduct of another person (manufacturer, operator, programmer) and the damage. Nevertheless, there is still the problem that the damage will never be caused by one single vehicle. Other vehicles and infrastructure connected in the cooperative system will all held their part of responsibility.

This article focuses precisely on this road less travelled in AI legal research. The question is how to prove causality for multicausal damage in cooperative road-traffic systems. The article contains an analysis of current approach towards proving causal nexus in Czech law within relevant case law. Furthermore, it answers the question, whether it would be possible to prove causal nexus in cooperative systems while using the current legislation.

KEYWORDS

AI, causal nexus, multicausal damage, autonomous vehicle, cooperative intelligent transportation system

1. ÚVOD

Článek se zabývá specifickým problémem, který představuje prokazování příčinné souvislosti mezi jednáním a škodným následkem v kooperativním silničním systému s autonomními vozidly. Příčinná souvislost je jednou z podmínek, která musí být naplněna, aby mohlo dojít k přičitatelnosti odpovědnosti určité osobě (škůdci) a vyvození sekundární právní povinnosti, která vzniká porušením právem chráněného zájmu. Princip prokazování příčinné souvislosti neboli také kauzality nalezneme jak v civilním, tak i správním a trestním právu. Jedná se o nezbytnou podmínku přičitatelnosti odpovědnosti vedle existence právně relevantního jednání a následku určité kvality. Čtvrtá podmínka, zavinění, pak není vyžadována vždy. Výjimkou je tzv. objektivní neboli striktní odpovědnost, která nevyžaduje nedbalostní zavinění ani úmysl na straně škůdce.

Ačkoliv se jedná o obecnou podmínku pro aplikaci odpovědnostních institutů, předmět zkoumání je v tomto textu zúžen na civilněprávní odpovědnost podle občanského zákoníku, konkrétně na skutkové podstaty civilní deliktní odpovědnosti za porušení zákona. V případě těchto druhů deliktů se pro vznik povinnosti nahradit škodu vyžaduje, aby byla jednáním škůdce porušena jeho povinnost a zároveň aby došlo k porušení práv poškozeného.[2]

Současný diskurs v České republice nedošel k jednoznačnému názoru, jaké skutkové podstaty jsou aplikovatelné i na autonomní systémy, jako jsou autonomní vozidla, která se dokáží rozhodovat a jednat bez lidského zásahu. Jsou diskutovány možnosti úpravy odpovědnosti za škodu způsobenou vadou výrobku podle § 2939 a násl. zákona č. 89/2012 Sb., občanského zákoníku ve znění pozdějších předpisů (dále jen „občanský zákoník“ či „ObčZ“) a § 2927 a násl. ObčZ o odpovědnosti za škodu

[2] MELZER, Filip. Corpus delicti aneb obrana úpravy deliktního práva v návrhu občanského zákoníku. *Bulletin advokacie*, 2011. 3/2011. 24-27.

způsobenou z provozu dopravního prostředku, či použití § 2924 o škodě způsobené provozní činností.[3] Debata je intenzivně vedena i na celounijní úrovni.[4]

Předmětem debaty pak je zejména jak určit osobu odpovědnou za jednání, ze kterého právo vyvozuje povinnost k náhradě škody. Důvodem je omezená možnost ovládat autonomní systém, jakmile je uveden do provozu. Pokud je systém schopný strojového učení, mění se jeho chování v čase a je do určité míry nepředvídatelné po jeho uvedení na trh.[5] Proto je otázkou, která osoba má odpovědnost za jeho chování nést, zdali výrobce, provozovatel, vlastník či uživatel. Podstata zodpovězení této otázky tkví v nutnosti určit, který z těchto subjektů má největší možnost riziko omezit a chování systému během jeho životního cyklu ovlivnit. Zatímco výrobce má největší kontrolu nad systémem v době jeho uvedení na trh, provozovatel či vlastník mohou jeho chování ovlivnit v době jeho užívání.

Zmíněné problémy však nejsou nepřekonatelné. Autonomní vozidlo bývá z důvodu omezené možnosti ovládat jeho provoz přirovnáváno ke zvířeti, které se rovněž rozhoduje samostatně nehledě na vůli jeho majitele, který je však za jeho chování odpovědný podle § 2933 a násl. ObčZ.[6] Současné civilní právo zná rovněž odpověď na situaci, ve které je za škodu odpovědno více škůdců najednou, přičemž zakládá jejich společnou a nerozdílnou odpovědnost s možností modifikace podle míry zavinění toho kterého škůdce (§§ 2915–2919 ObčZ).[7]

---

[3] KRAUSOVÁ, Alžběta et al. *Výzkum potenciálu rozvoje umělé inteligence v České republice, Analýza právně-etických aspektů rozvoje umělé inteligence a jejích aplikací v ČR*. Praha: Vláda ČR, 2018. Dostupné z: https://www.vlada.cz/assets/evropske-zalezitosti/aktualne/AI-pravne-eticka-zprava-2018_final.pdf.

[4] Evropská komise. *Pracovní dokument Odpovědnost za vznikající digitální technologie, doprovázející dokument Sdělení Komise Evropskému parlamentu, Evropské Radě, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů ze dne 25.4.2018 Umělá inteligence pro Evropu*. Brusel, 2018. Dostupné z: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137.

[5] LIM, Hannah YeeFen. *Autonomous Vehicles and the Law: Technology, Algorithms and Ethics*. Cheltenham: Edward Elgar Publishing, 2018. S. 88.

[6] POLČÁK, Radim. Odpovědnost umělé inteligence a informační útvary bez právní osobnosti. *Bulletin advokacie*, 2018. No. 11. 23 -26. S. 25.

[7] Tamtéž.

Méně je již řešeno, že ať už dojde ke změně ustanovení o odpovědnosti za škodu v občanském zákoníku či ne[8], překážkou pro odškodnění poškozených bude nutnost prokazování příčinné souvislosti. Jak již bylo řečeno, jedná o nezbytnou podmínku pro uplatnění kterékoliv ze skutkových podstat. To představuje komplikaci ze dvou důvodů.

První je, že jednání autonomního vozidla bude zcela řízeno počítačovým programem, a pokud nebude kauzalita mezi jednáním vozidla a škodným následkem zjevná (srovnejme případ kdy autonomní vozidlo poškodí jiné vozidlo zaparkované u cesty a případ, kdy narazí dvě autonomní vozidla do sebe), prokazování bude vyžadovat zpětné rozklíčování chování autonomního systému. Je však těžké (až nemožné) zjistit, jaké faktory mají na svědomí, že se systém choval daným způsobem, vyjma očividné programátorské chyby. Defaultně je potřeba počítat s určitou nevyhnutelnou chybovostí autonomního vozidla způsobenou propojením softwaru a hardwaru, kdy chyba softwaru může zapříčinit i chybu mechanickou.[9]

Druhou komplikací je zapojení autonomních vozidel do tzv. kooperativních inteligentních silničních systémů (dále jen „C-ITS“ z anglického *cooperative – intelligent transportation system*), ve kterém budou vozidla mezi s sebou sdílet data a podílet se na výpočtu společné trajektorie.[10] Pro fungování takového systému je klíčové, aby si všechna vozidla „rozuměla“, byla kompatibilní a pracovala správně, protože chyba

---

[8] Stejný problém pak nastává i ve správním právu v případě přestupků spáchaných autonomním systémem, které představují porušení úpravy zákona č. 361/2000 Sb., o provozu na pozemních komunikacích a o změnách některých zákonů (zákon o silničním provozu), ve znění pozdějších předpisů, který ve své současné úpravě přikazuje řidiči provádět všechny kritické funkce řízení vozidla (§ 5 odst. 1 písm. b) zákona o silničním provozu) a vylučuje tak autonomní řízení.

[9] NOVOTNÁ, Marianna; ADAMOVÁ, Zuzana. Deliktná zodpovednosť za ujmu, ktorá vznikla při využívání systémov umelej inteligencie. In: *Právo, obchod, ekonomika IX*. Košice: Univerzita P. J. Šafárika v Košiciach, 2019. 445 – 455. S. 447.

[10] Ministerstvo dopravy. *Základní informace o C-ITS*. Praha, 2018. Dostupné z: https://c-road-s.cz/?page_id=275 [cit. 1. 4. 2019], Ministerstvo dopravy. *Akční plán rozvoje inteligentních dopravních systémů (ITS) v ČR do roku 2020 (s výhledem do roku 2050)*. Praha, 2016. Dostupné z: https://www.czechspaceportal.cz/3-sekce/its---inteligentni-dopravni-systemy/strategicke-dokumenty-a-legislativni-akty/akcni-plan-rozvoje-its/ S. 83.

jednoho může negativně ovlivnit chování všech vozidel zapojených v systému.[11]

Jelikož výpočetní řešení nachází vozidla společně, identifikovat původce selhání může být problematické. Schopnost určit odpovědnou jednotku v systému je však hlavním předpokladem pro alokaci právní odpovědnosti v rámci kooperativního systému a uplatnění odpovědnosti podle §§ 2915–2919 ObčZ. Kvůli neustálým datovým přenosům uvnitř systému může dojít k situaci, kdy havarující vozidlo nenese stoprocentní podíl na následku. Jeho chybný manévr mohl být způsobem špatnou informací poskytnutou jiným vozidlem či inteligentní infrastrukturou (např. varováním před překážkou na cestě), chybou geolokačních služeb či výpadkem internetového připojení.[12]

Zákon v takovém případě vyžaduje, aby došlo k určení míry podílu jednotlivých pachatelů na škodném následku s určitou mírou pravděpodobnosti – podle toho bude případně modifikována jejich povinnost k náhradě škody stejným dílem společně a nerozdílně s dalšími škůdci. V důsledku je potřeba prokázat příčinnou souvislost mezi škodným následkem a jednáním jednotlivých subjektů. Takové prokazování bude spočívat v určení, zdali příčinná souvislost mezi jednáním a následkem vůbec existuje, a pokud ano, jaký podíl má konkrétní jednání na způsobeném následku.

Popisovaná situace je v právní teorii označována jako tzv. *multikauzální újma*, a jedná se o komplexní problém, který není, stejně jako příčinná souvislost jako taková, adresován v rámci legislativy. Otázka, co chápeme pod pojmem multikauzální újma, a jak přistupovat k jejímu prokazování, je tak ponechána k zodpovězení soudní praxi.[13] Je to právě soud, který při posuzování otázky odpovědnosti zjišťuje, zdali byla naplněna podmínka příčinné souvislosti.[14]

---

[11] ŽOLNERČÍKOVÁ, Veronika. Homologation of Autonomous Machines from a Legal Perspective. In: *Proceedings of the EXplainable AI in Law Workshop co-located with the 31st International Conference on Legal Knowledge and Information Systems (JURIX 2018)*. CEUR Workshop Proceedings, 2019. S. 51-52.

[12] Více viz LIM, Hannah YeeFen. *Autonomous Vehicles and the Law: Technology, Algorithms and Ethics*. Cheltenham: Edward Elgar Publishing, 2018. S. 31.

Jak je představeno v úvodu, článek se zabývá touto málo prozkoumanou oblastí dokazování příčinné souvislosti u multikauzální újmy v kooperativním silničním systému. V druhé kapitole poskytuje úvod kooperativních inteligentních silničních systémů, na které budou následně aplikovány poznatky z dalších kapitol. Ve třetí kapitole článek shrnuje s přihlédnutím k relevantní judikatuře dosavadní přístup k prokazování příčinné souvislosti v českém právu. Reflexe výsledků zkoumání je součástí třetí kapitoly. V závěru odpovídá článek na otázku, zda by za stávající právní úpravy šlo dosáhnout prokázání příčinné souvislosti v kooperativním systému, a jaká alternativní řešení jsou k dispozici.

2. CHARAKTERISTIKA KOOPERATIVNÍCH INTELIGENTNÍCH SILNIČNÍCH SYSTÉMŮ

C-ITS dále rozšiřují v současnosti užívané inteligentní dopravní systémy (ITS). Aby se jednalo o kooperativní (C-ITS) systém, musí se jednat o komunikaci oboustrannou, tzn. každé zařízení či vozidlo musí být schopno jak příjmu, tak vysílání informací.[15]

Základem kooperativního inteligentního dopravního systému jsou vozidla schopná vzájemné komunikace. V současnosti nejsou běžné manuálně řízené automobily vybaveny zařízeními umožňujícími komunikovat spolu s ostatními účastníky provozu. Jsou nicméně povinně vybavena jinými prostředky komunikace, a to výstražnými světelnými

---

[13] Viz NOVÁK, David. Odraz příčinné souvislosti dle Principů evropského deliktního práva v české právní úpravě. *Bulletin advokacie*, 2019. 10/2019. S. 41, HAMANOVÁ, Lucie. Prokazování příčinné souvislosti ve sporech o náhradu škody na zdraví způsobenou postupem lékaře non lege artis. *Časopis zdravotnického práva a bioetiky*, 2011. 1/2011. S. 61, DOLEŽAL, Adam; DOLEŽAL, Tomáš. Uplatnění PETL při řešení složitých kauz v oblasti příčinné souvislosti v medicínskoprávních sporech. *Soudní rozhledy*, 2013. 7-8/2013. S. 242.

[14] HAMANOVÁ, Lucie. Prokazování příčinné souvislosti ve sporech o náhradu škody na zdraví způsobenou postupem lékaře non lege artis. *Časopis zdravotnického práva a bioetiky*, 2011. 1/2011. S. 61.

[15] Evropská komise. *Sdělení Komise Evropskému parlamentu, Evropské Radě, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů Evropská strategie týkající se spolupracujících inteligentních dopravních systémů, milník na cestě ke spolupracující, propojené a automatizované mobilitě.* Brusel, 2016. S. 3 Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0766.

a zvukovými zařízeními.[16] Tyto prostředky sice umožňují vzájemnou interakci, ne však kooperaci.

Předpokládá se, že autonomní vozidla budou vybavena různými senzory[17] o mnohem větší citlivosti, než jaké jsou vlastní lidským smyslům člověka, který řídí automobil bez inteligentních systémů. Stejně tak se dá předpokládat, že se autonomní automobil pomocí senzorů dokáže v neočekávané situaci zorientovat a pomocí dat, kterými disponuje z testování a provozu, patřičně zareagovat i bez nutnosti datové komunikace se svým okolím.[18] Propojení jednotlivých agentů je tak volitelnou možností. Nicméně, kvůli výhodám, které přináší, bavíme-li se o autonomní mobilitě, má se za to, že budou součástí systémů propojených,[19] kde jsou vozidla propojena pomocí datových přenosů a společně vypočítávají nejvhodnější řešení dané dopravní situace, a to v reálném čase.

Do svého výpočtu zároveň zahrnují i vstupy pocházející z vnější, jako jsou pokyny uživatele (destinace) nebo okolní podmínky (terén, počasí). Ostatní účastníci provozu, tedy chodci, řidiči, cyklisté, stejně jako jiné prvky ve vozovce, např. zvěř, se tak z pohledu autonomních automobilů, které společně komunikují, stávají jednou z okolních podmínek, na kterou musí reagovat.

Vozidlo, které je v reálném čase datově propojené s okolními vozidly nebo okolní infrastrukturou označujeme jako *datově propojené* (angl.

---

[16] Viz Příloha č. 2 k Vyhlášce č. 341/2014, o schvalování technické způsobilosti a o technických podmínkách provozu vozidel na pozemních komunikacích.

[17] MAURER, Markus, et al. Autonomous driving. *Springer Berlin Heidelberg, Berlin, Germany*, 2016. S. 355.

[18] LIM, Hannah YeeFen. *Autonomous Vehicles and the Law: Technology, Algorithms and Ethics*. Cheltenham: Edward Elgar Publishing, 2018. S. 23 – 25.

[19] Expertní skupina Gear 2030. *Roadmap – discussion*. Brusel, 2016. Dostupné z: https://circabc.europa.eu/sd/a/a68ddba0-996e-4795-b207-8da58b4ca83e/Discussion%20Paper%C2%A0-%20Roadmap%20on%20Highly%20Automated%20Vehicles%2008-01-2016.pdf.

connected).[20] V závislosti na druhu propojení rozlišujeme mezi *Vehicle-to-Infrastructure* (zkráceně V2I) a tzv. *Vehicle-to-Vehicle* (V2V) propojením.

V rámci C-ITS je možné identifikovat vícero subjektů, kteří mohou ovlivnit fungování systému. Kromě provozovatelů a výrobců autonomních vozidel se jedná provozovatele elektronických komunikací, co se týče rádiového spojení a internetového připojení, poskytovatele služeb informační společnosti, co se týče aplikací používaných vozidly a infrastrukturou, a pochopitelně i všechny, kdo mají na starost správu pozemních komunikací a přilehlé infrastruktury. Obrovský vliv bude mít též zmiňovaná kompatibilita jednotlivých komponentů. I bezvadný výrobek může chybovat, když je propojen s výrobkem jiným – takovému problému však nelze předcházet jinak než nastavením testovacích a certifikačních mechanismů.

Nežádoucím výsledkem plurality subjektů poskytujících data, technologie a služby je, je, že v případě škodného následku si nebude muset právo poradit s prokázáním příčinné souvislosti. Výsledek potenciálního soudního řízení, kde by se vyžadovala aplikace objektivní škody podle § 2924 ObčZ o škodě způsobené provozní činností či § 2937 ObčZ o škodě způsobené vadou výrobku apod. na autonomní vozidla v rámci C-ITS, je tak nepředvídatelný.[21] Následující kapitola se situaci pokusí trochu osvětlit analýzou dosavadního přístupu soudů k prokazování příčinné souvislosti u odpovědnosti za škodu v několika vybraných komplexních případech.

3. KONCEPT MULTIKAUZÁLNÍ ÚJMY V ČESKÉM PRÁVU

Prokazování příčinné souvislosti se v komplexních případech odpovědnosti za škodu jeví jako problematické i nyní.[22] Stejně jako to činí zákon č. 40/2009 Sb., trestní zákoník, občanský zákoník nevymezuje příčinnou souvislost a ponechává to právní vědě a praxi[23], ačkoliv byla taková úprava původně součástí novely občanského zákoníku. Podoba navrhovaného

[20] Ministerstvo dopravy. *Vize autonomní mobility*. Praha, 2017. Str. 4 Dostupné z: https://www.czechspaceportal.cz/3-sekce/its---inteligentni-dopravni-systemy/strategicke-dokumety/vize-rozvoje-autonomni-mobility/.

[21] POLČÁK, Radim. Odpovědnost umělé inteligence a informační útvary bez právní osobnosti. *Bulletin advokacie*, 2018. No. 11. 23 -26, S. 25.

ustanovení měla následující textaci: „*Konání, opomenutí nebo jiná událost je příčinnou škody, jestliže by ke škodě jinak nedošlo.*“ Navazující ustanovení pak zahrnovala i alternativní pravidla příčinné souvislosti.[24]

Podobně předchůdce občanského zákoníku, zákon č. 40/1964 Sb., občanský zákoník (dále jen „OZ64“) a jeho úprava v § 420 a § 420a pojem příčinná souvislost nepoužíval. Místo toho předmětná ustanovení pojednávala o „způsobení škody porušením právní povinnosti“ a „o škodě způsobené jinému provozní činností“.[25]

Důsledkem je rozmanitá judikatura na téma příčinné souvislosti, která slouží vedle teoretických právních textů jako hlavní zdroj informací o tom, jak je v praxi prokazována příčinná souvislost.

3.1 JUDIKATURA TÝKAJÍCÍ SE PROKAZOVÁNÍ MULTIKAUZÁLNÍ ÚJMY

Hlavní otázkou při tvorbě tohoto textu bylo, jak vyfiltrovat judikaturu, která bude relevantní pro dokazování příčinné souvislosti v kooperativních systémech v civilněprávních sporech. Prvním kritériem bylo, že se musí jednat o prokazování příčinné souvislosti u škody, kterou zapříčinilo vícero faktorů vedoucích v důsledku ke škodnému následku (respektive soud musel zkoumat, zdali tomu tak bylo). Jako druhé kritérium bylo stanoveno, že z takové judikatury musí vyplývat obecné závěry, které lze dále analyzovat. Třetím kritériem pak bylo, aby se jednalo o judikaturu dostupnou. Toto kritérium předmět zkoumání zúžilo na judikaturu

---

[22] Viz TICHÝ, Luboš; HRÁDEK, Jiří. Deliktní právo v návrhu občanského zákoníku. *Právní fórum*, 2012. 1, 6-21 a MELZER, Filip. Corpus delicti aneb obrana úpravy deliktního práva v návrhu občanského zákoníku. *Bulletin advokacie*, 2011. 24-27. a DOLEŽAL, Tomáš; DOLEŽAL, Adam. Proof of causation in medical malpractice cases in the Czech republic. *The Lawyer quarterly*, 2015. 5.3.

[23] MELZER, Filip. Corpus delicti aneb obrana úpravy deliktního práva v návrhu občanského zákoníku. *Bulletin advokacie*, 2011, 24-27.

[24] TICHÝ Luboš; HRÁDEK, Jiří. Deliktní právo v návrhu občanského zákoníku. *Právní fórum*, 2012, 1, 6-21.

[25] DOLEŽAL, Tomáš; DOLEŽAL, Adam.Proof of causation in medical malpractice cases in the Czech republic. *The Lawyer quarterly*, 2015. 5.3.

Nejvyššího a Ústavního soudu s přihlédnutím k předchozím rozhodnutím nižších soudů ve věci, byla-li dostupná.

Komplexní problematiku podle prvního kritéria představují zejména zdravotnické spory, kde je v případě neúspěchu zdravotnického postupu a způsobení újmy na životě či zdraví potřeba zvážit mnoho možných příčin nežádoucího následku.[26] Za příčinu problému s prokazováním profesního pochybení ve zdravotnictví (v angličtině úderněji *medical malpractice*) je dokonce označována existence tzv. černé schránky (anglicky *black box*), shodně jako u autonomních systémů. Zatímco u autonomního systému je černou schránkou kód řídícího softwaru, jeho „umělá inteligence", u zdravotnického pochybení je jím lidské tělo. U umělé inteligence je nám znám výchozí stav a konečný stav, ale nejsme schopni s jistotou rozklíčovat, co se děje uvnitř.[27] To u zdravotnických sporů úplně neplatí – máme prostředky pro určení, zda se podílelo na následku pochybení zdravotníka, nepředvídatelná komplikace (např. alergie na medikament) či diagnóza pacienta. Co však neumíme, je vyčíslit, v jaké míře se ta která příčina podílela na škodném následku. V tomto směru je lidské tělo skutečně do určité míry záhadou a potřeba práva mít jistotu v příčinné souvislosti mezi jednáním a škodným následkem nám uplatnění odpovědnosti a odškodnění poškozených komplikuje.

Z důvodu podobné míry složitosti prokazování kauzality u těchto dvou skutkově zcela odlišných situací – újmy na zdraví v důsledku lékařského zákroku a havárii autonomního vozidla C-ITS – je možné v otázce prokazování kauzality přihlížet k judikatuře vztahující se ke způsobení újmy na zdraví důsledkem profesního pochybení lékaře. Nicméně se jedná o analogii fungující jenom na základě komplikovanosti uplatnění odpovědnosti za škodu. Ostatní aspekty případů, včetně aplikace konkrétních skutkových podstat deliktní odpovědnosti, jsou odlišné.

Další oblastí, kde dochází k multikauzálním újmám, jsou silniční havárie. Zde se analogie nabízí více, protože dochází k posuzování odpovědnosti za škodu podle ustanovení § 2927 a násl. ObčZ o škodě

[26] Tamtéž.

[27] Tamtéž.

z provozu dopravního prostředku, které je potenciálně uplatnitelné i na autonomní vozidla. Problémem v tomto případě je, že vyhodnocování, zdali je dána příčinná souvislost, je prováděno jinak, než tomu bude v případě autonomních vozidel. Nyní jde o zkoumání vnějšího fyzického chování stroje, u autonomní mobility bude potřeba rozklíčovat, co se událo uvnitř systému vozidla. Zda, v případě nežádoucí události, došlo pochybení uvnitř výše zmíněné černé schránky, kdo měl kontrolu nad vozidlem, zda systém upozorňoval řidiče (uživatele) na závadu.[28]

3.2 PŘEHLED DOSTUPNÉ JUDIKATURY

Podmínka prokázání příčinné souvislosti („*conditio sine qua non*“) je naplněna v případě, že je zřejmé, že nebylo-li by v řetězci určité události, škoda by nevznikla.[29] Je to právě požadavek zřejmosti provázanosti jednání se škodným následkem, který v soudní praxi činí potíže.

Usnesení Ústavního soudu ze dne 12. 8. 2008 sp. zn. I. ÚS 1919/08 potvrzuje všechny přednesené problémy u prokazování kauzality v nejednoduchých případech, kdy potenciální škůdce vstupuje do celého řetězce příčin a následků a dalších procesů. Toto usnesení se týká lékařského zásahu. Ústavní soud shrnuje, že náhled dosavadní judikatury na nutnost 100% prokázání příčinné souvislosti je problematický, obzvláště v případech, kdy je obtížné posoudit, zda mohly ke konečnému následku přispět další příčiny.[30]

Následující tři soudní případy byly vybrány tak, aby co nejlépe prezentovaly základní problémy s prokazováním příčinné souvislosti. Cílem je tyto, řekněme, nedostatky podrobně popsat a v následující kapitole navrhnout řešení situace tak, aby v případě zapojení autonomních vozidel

[28] LIM, Hannah YeeFen. *Autonomous Vehicles and the Law: Technology, Algorithms and Ethics*. Cheltenham: Edward Elgar Publishing, 2018. S. 110.

[29] NOVÁK, David. Odraz příčinné souvislosti dle Principů evropského deliktního práva v české právní úpravě. *Bulletin advokacie*, 2019. 10/2019. S. 41.

[30] DOLEŽAL, Adam; DOLEŽAL, Tomáš. Uplatnění PETL při řešení některých složitých kauz prokazování příčinné souvislost v medicínskoprávních sporech. *Soudní rozhledy,* 2013. *7-8/2013*. S. 242.

a implementace C-ITS nedošlo k nemožnosti uplatňování odpovědnosti za škodu.

3.3 K POJMU PŘÍČINNÉ SOUVISLOSTI A PRÁVNÍMU DOPADU MÍRY PODÍLU NA ÚJMĚ

Jedním z klíčových rozhodnutí pro pochopení konceptu příčinné souvislosti je nález Ústavního soudu sp. zn. III. ÚS 3067/13, který se zabývá otázkou, zdali určení míry podílu na vzniklé újmě, které je z hlediska právní odpovědnosti relevantní, je skutkovou či právní otázkou.[31] Ústavní soud rozhodoval ve věci snížení šance na přežití pacientky v důsledku lékařského zásahu. Ústavní soud polemizoval ve svém nálezu s rozhodnutím Nejvyššího soudu ve věci. Nejvyšší soud v něm uváděl, že podstatou sporu je tzv. teorie ztráty šancí, kterou je potřeba posuzovat jako otázku příčinné souvislosti.[32] Rozhodnutí Ústavního soudu má faktický dopad do roviny, s jakou pravděpodobností musí být prokázáno, že jednání konkrétní osoby přispělo ke škodlivému následku. Tedy zda musí být prokázáno na 100 % (s absolutní jistotou), že příčinná souvislost mezi jednáním a následkem existují, nebo zda postačuje míra pravděpodobnosti 51 %, která vychází z ustálené soudní praxe u medicínsko-právních sporů (tzv. „*but-for principle*“).

Stěžovatelé i krajský a vrchní soud se přikláněli k tomu, že se jedná o otázku právní, kdy příčinná souvislost a nutná míra jejího prokázání není definována v zákoně, a proto nic nebrání jejímu přehodnocení soudní judikaturou.[33] V rozhodnutí Ústavního soudu jsou vypořádávány i různé národní přístupy (např. německý, anglický) k této otázce. V závěru Ústavní soud dospívá k tomu, že otázka míry na vzniklé újmě je otázkou právní a nikoliv skutkovou[34], nicméně poznamenává, že tato otázka nemá

[31] Rozhodnutí Ústavního soudu ze dne 20. 12. 2016 sp. zn. III. ÚS 3067/13.

[32] Rozhodnutí Ústavního soudu ze dne 20. 12. 2016 sp. zn. III. ÚS 3067/13. Bod 40.

[33] Shodně viz Usnesení Ústavního soudu ze dne 12. 8. 2008 sp. zn. I. ÚS 1919/08.

[34] Rozhodnutí Ústavního soudu ze dne 20. 12. 2016 sp. zn. III. ÚS 3067/13. Bod 37.

v obecné rovině význam, protože v praxi často příčinná souvislost, její faktické souvislosti a právní konsekvence splývají.[35]

Rozhodnutí Ústavního soudu je (prozatím) posledním článkem dlouhodobé debaty na dané téma. Předchozí judikatura se přikláněla k názoru, že se jedná o otázku skutkovou, viz usnesení Nejvyššího soudu sp.zn. 25 Cdo 2440/2005 či rozsudek Nejvyššího soudu sp.zn. 21 Cdo 300/2001, se kterými se nález Ústavního soudu vypořádává.[36] Nicméně v minulosti pro změnu převládal názor, že se jedná o otázku právní, viz rozhodnutí Nejvyššího soudu ČSSR sp. zn. 7 Cz 111/68, [R 66/1969 civ.].[37]

Vzhledem k tomu, jak dlouho převládala soudní praxe, že se jedná o skutkovou právní otázku, je tímto přístupem ovlivněna i většina teoretické literatury k otázkám příčinné souvislosti.

3.4 KE SPOLUZAVINĚNÍ ŠKODY POŠKOZENÝM

V rozsudku Nejvyššího soudu sp. zn. 25 Cdo 4199/2013, [NS 1747/2014] se jako dovolací soud zabýval otázkou, zdali spoluzavinění újmy na zdraví samotným poškozeným vylučuje aplikaci ustanovení o odpovědnosti za škodu zcela, popřípadě zda budou poškozený a žalovaný společně odpovědní za následek, a pokud ano, v jakém poměru. Rozsudek ve věci dopravní nehody je zajímavý v tom, že se pokouší překlenout legislativní vakuum a stanovit, zdali je příčinná souvislost mezi jednáním a následkem způsobilá založit odpovědnost k náhradě škody, i když není 100 % a nelze s určitostí stanovit míru podílu jednotlivých subjektů. Skutkovou podstatou sporu poškozených s pojišťovnou je, že kromě zavinění intoxikovaného řidiče, který nehodu způsobil, lze určitou míru odpovědnosti spatřovat i na straně dalších poškozených, kteří, taktéž intoxikovaní, v autě jeli nepřipoutáni, převyšovali počtem kapacitu vozidla a v neposlední řadě řidiče neodradili od toho, aby sednul za volant.[38]

---

[35] Rozhodnutí Ústavního soudu ze dne 20. 12. 2016 sp. zn. III. ÚS 3067/13. Bod 29.

[36] Rozhodnutí Ústavního soudu ze dne 20. 12. 2016 sp. zn. III. ÚS 3067/13. Bod 34.

[37] DOLEŽAL, Adam; DOLEŽAL, Tomáš. Problematika prokazování příčinné souvislosti v medicínsko-právních sporech. *Právník*, 2013. 6/2013. S. 577.

[38] Rozsudek Nejvyššího soudu ze dne sp. zn. 25 Cdo 4199/2013, [NS 1747/2014].

Nejvyšší soud odkazuje na svou ustálenou rozhodovací praxi, podle které míra podílu na způsobené škodě spolujezdcem může dosáhnout až jedné poloviny, pokud ví o tom, že je řidič pod vlivem alkoholu (viz rozhodnutí Nejvyššího soudu sp. zn. 5 Cdo 1054/2007). Ve věci prokazování příčinné souvislosti pak dále odkazuje na rozsudek Nejvyššího soudu ze dne 19. 3. 2008, sp. zn. 25 Cdo 657/2006 a usnesení Nejvyššího soudu ze dne 15. 7. 2008, sp. zn. 25 Cdo 1500/2006.

Nejvyšší soud zrušil rozhodnutí odvolacího soudu, který stanovil, že si cestující způsobili škodu na 80 %, když vědomě absolvovali cestu s řidičem pod vlivem omamných látek a nebyli náležitě připoutáni. Své rozhodnutí odůvodnil tím, že byť se jedná o relevantní důvody, odvolací soud nedoložil, že právě nepřipoutání poškozených vedlo při havárii k úrazu jednotlivých poškozených, popřípadě že vedlo ke zhoršení důsledků a v jakém rozsahu.

Rozhodnutí bylo posuzováno podle úpravy OZ64 s přihlédnutím k jeho ustanovení § 441, nikoliv podle ustanovení §§ 2915–2919 ObčZ.

3.5 KE KUMULACI JEDNÁNÍ, JEJICHŽ VÝSLEDKEM JE VZNIK ŠKODY

Nejvyšší soud rozhodoval v kuriózním případě souběhu jednání jednotlivých subjektů, které až v konečném důsledku vedly ke způsobené škodě v rozhodnutí vedeném pod sp. zn. 25 Cdo 3925/2013, [NS 1305/2015] ze dne 18. 3. 2015. Jeden ze žalovaných se pokusil o spáchání pojistného podvodu tím, že odstavil své vozidlo na vlakových kolejích. Žalovaný do kolejiště zabočil úmyslně se záměrem poškodit podvozek vozidla. Z kolejiště se mu však již nepodařilo vyjet. O této skutečnosti zpravil policii, která o situaci uvědomila České dráhy. V důsledku pochybení pracovníka Českých drah však bylo uzavření koleje provedeno na jiném úseku a v místě, kde byl odstaven automobil, došlo ke srážce s vlakovou soupravou. V důsledku vznikla škoda jak na automobilu, tak na vlakové soupravě. Civilněprávní řízení zahájené žalobcem, Českými drahami a.s., bylo vedeno proti 5 žalovaným zároveň. Rozhodnutí je kromě věcné zajímavosti významné z hlediska přístupu ke kumulativní kauzalitě.

Rozhodnutí cituje rozsudek Nejvyššího soudu ze dne 19. 12. 2012, sp. zn. 25 Cdo 1474/2011, kde soud judikoval, že *„…i kdyby nějaká další skutečnost (…) mohla přispět ke vzniku škody, příčinná souvislost mezi škodnou událostí a způsobenou škodou se nepřerušuje, pokud původní škodná událost zůstává tou základní skutečností, bez níž by k následku nedošlo. K přerušení příčinné souvislosti dochází jen za situace, kdy nová okolnost působila jako rozhodující příčina, která způsobila vznik škody bez ohledu na původní škodnou událost.*"

Kvůli zajímavosti rozhodnutí cituji i větší úsek konečného rozhodnutí ve věci sp. zn. 25 Cdo 3925/2013: „*Názor žalovaného 1)* [pojišťovna]*, že škoda byla způsobena protiprávním jednáním (trestným činem) žalovaných 2), 3) a 4)* [provozovatel vozidla a spolupachatelé pojistného podvodu]*, a nešlo tak o škodu způsobenou zvláštní povahou provozu, nelze přijmout. Selhání nebo nedostatek činnosti osob použitých v provozu (v daném případě řidiče vozidla – žalovaného 2) představuje okolnost mající původ v provozu … Selháním řidiče je pak nutno rozumět jakékoli volní i mimovolní chování, jež je v příčinné souvislosti se vznikem škody, od úmyslného jednání (sebevražedný pokus, útok vozidlem, záměrné poškození vozidla), přes nedbalostní jednání (běžné nehody způsobené porušením pravidel silničního provozu), až po nezaviněná jednání (nezvládnutí složité dopravní situace, zdravotní indispozice). Okolnost, že osoba použitá v provozu spáchala v souvislosti s provozem vozidla trestný čin, tedy nemá za následek vyloučení odpovědnosti provozovatele či vyloučení závěru, že šlo o škodu způsobenou zvláštní povahou provozu. Provoz vozidla je objektivní skutečností. Případný úmysl řidiče konkrétního vozidla jej provozovat či neprovozovat je irelevantní za stavu, kdy se z objektivních okolností podává, že vozidlo je v okamžiku nehody v provozu. V tomto směru jsou tudíž nadbytečné úvahy obou soudů a také argumentace účastníků, zda bylo úmyslem žalovaného 2) vozidlo dále (ne)provozovat.*"

4. APLIKACE SOUČASNÉHO PŘÍSTUPU K PROKAZOVÁNÍ KAUZALITY NA C-ITS

Judikatura, která by se zabývala multikauzálními škodami a prokazováním příčinné souvislosti v takových případech není bohatá. Co se týče

medicínsko-právních sporů, existuje řada rozhodnutí, které jsou relevantní z hlediska komplexního posuzování složitých případů, nicméně ne všechna mohou posloužit pro vytvoření obecných úvah o příčinné souvislosti, které by byly aplikovatelné pro případ autonomní mobility.[39]

Tři rozhodnutí, která byla vybrána výše, včetně rozhodnutí, na která je v nich odkazováno, však představují základní pilíře problematiky. První rozhodnutí a vývoj judikatury ve věci pravidel prokazování příčinné souvislosti hovoří jasně. Příčinná souvislost, jakožto právní pojem používaný doktrínou a judikaturou, nikoliv však zákonem, není jasně definována co do všech svých aspektů. Ačkoliv se může zdát, že se jedná o čistě teoretický problém, dovolím si nesouhlasit.

Nález Ústavního soudu sp. zn. III. ÚS 3067/13 má dalekosáhlé důsledky do práv a povinností osob, když říká, že je prokazování příčinné souvislosti právní otázkou a nikoliv skutkovou. Tímto rozhodnutím totiž otevírá nové možnosti opravných prostředků ve sporech, jejichž součástí je složitá otázka prokazování příčinné souvislosti. Dokud byla příčinná souvislost považována za skutkovou otázku, vztahovala se na ní koncentrace řízení a nebylo možné v dalších instancích soudního řízení doplňovat důkazy. Možnosti účastníků řízení před a po rozhodnutí Ústavního soudu jsou tak diametrálně odlišné.

Druhé rozhodnutí, rozsudek Nejvyššího soudu sp. zn. 25 Cdo 4199/2013, zase poukazuje na to, že příčinná souvislost mezi právně relevantní skutečností a následkem je obtížně prokazatelná a sama o sobě může být příčinou vleklých sporů. Zároveň je díky absenci přesně stanovených pravidel posouzení odvislé od právního uvážení jednotlivých soudů a není harmonizováno. Současná judikaturní praxe vyžadující 100% prokázání příčinné souvislost i v případech, které nejsou až tak komplikované, zabraňuje v některých případech uplatnění odpovědnosti za škodu. Jak však zmiňuje usnesení Ústavního soudu ze dne 12. 8. 2008 sp. zn. I. ÚS 1919/08, díky tomu, že není příčinná souvislost legislativně

[39] Více k prokazování příčinné souvislosti v medicínském právu viz TICHÝ, Luboš; HRÁDEK, Jiří. *Prokazování příčinné souvislosti multikauzálních škod*. Praha: Centrum právní komparatistiky, Právnická fakulta UK, 2010.

zakotvena, je tuto praxi možno změnit. Touto cestou se ostatně některé státy již vydaly.[40]

Třetí rozhodnutí Nejvyššího soudu, rozsudek sp. zn. 25 Cdo 3925/2013, stanovuje s odkazem na předchozí judikaturu pravidla pro to, jaký vliv má, respektive nemá, na posouzení příčinné souvislosti to, že byl v jejím průběhu spáchán trestný čin, či že ke konečnému výsledku přispěla další osoba. Analýzou tohoto rozhodnutí bohužel opět dospíváme k závěru, že s některými druhy kauzality se stávající právo obtížně vypořádává. Jednu z příčin je možné vidět v tom, že české civilní právo nerozlišuje mezi druhy příčin vedoucích ke škodnému následku (druhy kauzality) a pohybuje se pouze v omezených možnostech modifikace společné a nerozdílné odpovědnosti (v současném právu podle § 2915 ObčZ).

Nelze než usoudit, že současný právní stav není pro provoz kooperativních systémů vhodný. Lze předpokládat, že kumulativní kauzalita, která je popsána v třetím rozhodnutí, bude mnohem častějším jevem, než je dnes. Je též nutné připomenout, že autonomní technologie se vyvíjí s předpokladem, že je bude možné používat i za hranicemi státu (stejně jako současná vozidla), proto není ideální, že je v každém jednotlivém státě příčinná souvislost upravena odlišně a podléhá jiné rozhodovací soudní praxi.

Lze namítnout, že již v současnosti nejsme schopni předvídat všechny okolnosti na straně řidiče, a v případě havárie vozidla není vždy jasné, z jakého důvodu vozidlo následovalo trajektorii, která zapříčinila nehodu. Nevíme, zda řidič zachoval patřičnou opatrnost nebo pochybil, popřípadě zda nedošlo k neočekávané zdravotní komplikaci na straně řidiče nebo zda neselhala dopravní infrastruktura, například semafor. Přesto jsme většinou schopni aplikovat odpovědnost za škodu způsobenou silniční havárií.

V čem se liší předestřená situace od havárie v rámci C-ITS? Proč v budoucnu může přístup k prokazování příčinné souvislosti činit potíže, podobně jako nyní činí v medicínském právu, když v současných soudních

[40] DOLEŽAL, Adam; DOLEŽAL, Tomáš. Problematika prokazování příčinné souvislosti v medicínsko-právních sporech. *Právník*, 2013. 6/2013. S. 577.

sporech týkajících se silniční dopravy problém činí pouze v ojedinělých případech?

V dnešním silničním provozu určujeme zdravotní způsobilost řidiče a testujeme jeho schopnost zachovávat pravidla silničního provozu. Při soudním rozhodování se vychází z obecné dlouholeté zkušenosti, jak průměrný řidič reaguje v případě neočekávané situace na vozovce. Víme, jaký je průměrný reakční čas, jak daleko vidí zdravý člověk. U autonomního vozidla řidiče nahradí software, člověkem vytvořená věc. Zatímco průměrné vlastnosti a schopnosti řidiče jsou dané, vše, co se týká autonomního software, je věcí lidského rozhodnutí. Jakou může mít maximální míru chybovosti? Jak citlivé musí být jeho senzory? Jak jej naprogramovat pro případ havárie? Má vozidlo dát přednost informaci pocházející z jeho vlastních senzorů nebo z dopravní infrastruktury, která je součástí C-ITS? Na rozdíl od člověka, jehož chování je do značné míry instinktivní, software se stihne rozhodnout, jakou akci zvolí. Chyby, které mohou nastat při provozu autonomního programu, nejsou předmětem zkušenosti ani ustálené rozhodovací praxe soudů.

Rozdíly mezi současnými haváriemi a potenciálními haváriemi autonomních vozidel jsou tak značné. Je zjevné, že autonomní vozidla nemohou být vůbec uvedena do provozu, aniž by zmíněné aspekty jejich provozu nebyly předem ošetřeny po právní i technické stránce. Nicméně to neodstraní všechny problémy. Pokud už v současnosti víme, že nefunguje něco tak fundamentálního, jako je přičitatelnost odpovědnosti za škodu, má podle mého názoru smysl se takovým problémem zabývat. A to i z toho důvodu, že se nejedná o problém postihující pouze budoucí technologie, ale i současné soudní případy, například v oblasti zdravotnického práva.

Jedním z řešení navrhovaných v oblasti zdravotnického práva je, aby se české soudy při rozhodování řídily podle nezávazných *Principů evropského deliktního práva* („*PETL*“), souboru pokynů sestavených Evropskou skupinou pro deliktní právo jako prostředku pro harmonizaci evropského deliktního

práva.[41] PETL se zabývá například obecnou přičitatelností škody, když stanoví, že je odpovědný ten, kdo a) ji způsobil svým zaviněným chováním, b) jehož abnormálně nebezpečná činnost způsobila škodu nebo c) jehož pomocník škodu způsobil v rozsahu svého úkolu.[42]

Hlava III PETL je pak věnována právě jednotlivým druhům kauzality. Je stanovena obecná kauzalita, jako *condition sine qua non*, která je definována velmi podobně, jako byla v návrhu občanského zákoníku. Článek 3:101 zní: „*Jednání nebo opomenutí (dále jen jednání) je příčinnou škody poškozeného, jestliže by při neexistenci takového jednání škoda nevznikla.*" Další články jsou pak věnovány pravidlům pro stanovení podílů jednotlivých subjektů na odpovědnosti za škodu ve speciálních případech kauzality. Těmi jsou: konkurenční příčiny, alternativní příčiny, potenciální příčiny, neurčitá dílčí kauzalita a příčina ve sféře poškozeného (čl. 3:102–106 PETL).

Pravidla stanovená PETL by byla potenciálně použitelná i na kooperativní autonomní vozidla. Minimálně by jejich využití naplnilo požadavek právní jistoty pro strany soudních sporů. Je to ostatně právě transparentnost a předvídatelnost právní regulace, po čem volají investoři do autonomních technologií. Konkrétní podoba právní úpravy pro ně není až tak relevantní.[43]

Dalším řešením by samozřejmě bylo rovněž výslovné zakotvení pravidel pro posuzování kauzality přímo do občanského zákoníku. Takové řešení by zabránilo nepředvídatelnosti ještě více. Jako negativní důsledek by se dalo očekávat zablokování flexibilního rozhodování soudů v případech, které by právem nebyly předvídány. Typickým následkem mohou být nespravedlivá soudní rozhodnutí.

Ještě lepším řešením se jeví přijít s konceptem deliktní odpovědnosti, který prokazování příčinné souvislosti nevyžaduje vůbec. Jednu z takových

---

[41] DOLEŽAL, Adam; DOLEŽAL, Tomáš. Uplatnění PETL při řešení složitých kauz v oblasti příčinné souvislosti v medicínskoprávních sporech. *Soudní rozhledy*, 2013. 7-8/2013. S. 242.

[42] Evropská skupina deliktního práva. *Principy evropského deliktního práva*. 2015. Dostupné z: http://www.egtl.org/index.html Čl. 1: 101.

[43] POLČÁK, Radim. Odpovědnost umělé inteligence a informační útvary bez právní osobnosti. *Bulletin advokacie*, 2018. No. 11. 23 -26. S. 25.

inovativních možností představuje tzv. *no-fault compensation scheme*, které funguje v kanadské provincii Quebec.[44] Takový koncept vyžaduje zavedení systému speciálního povinného pojištění nebo zřízení fondu financovaného například z daní z výdělků z provozu či prodeje autonomních vozidel. Získané peníze zajistí finanční kompenzaci pro poškozené. Princip takového systému je, že všechny subjekty zapojené do určité činnosti (v tomto případě do provozu C-ITS) přispívají na pojištění či do fondu, ze kterého je náhrada škody hrazena bez zkoumání, které subjekty se jakou mírou podílely na vzniku škody. Výhodou tohoto systému je rychlost odškodění poškozených, nevýhodou určitá demotivace subjektů k minimalizaci rizika vzniku škod, pokud je systém nastaven chybně. Toto řešení považuji za nejlépe realizovatelné i vzhledem k tomu, že není až tak daleko od našeho současného systému pojištění odpovědnosti za provoz vozidla.

5. ZÁVĚR

Cílem tohoto článku bylo zjistit, zdali současný přístup k prokazování příčinné souvislosti v případech multikauzální újmy dokáže pojmout i nehody způsobené autonomními kooperativními systémy. Analýzou právních textů a judikatury dospívám k názoru, že C-ITS systémy, ve kterých figuruje mnoho subjektů a příčinná souvislost bude těžko prokazatelná, nemohou fungovat za stávajících pravidel. Důsledkem by bylo zamezení přístupu poškozených k odškodnění za způsobenou újmu, popřípadě průtahy při soudním řešení těchto sporů. Kromě právních překážek pak současné řešení naráží i na překážky technické.

Nabízí se tři možnosti řešení. Prvním je iniciovat legislativní změnu a inkorporovat definici a pravidla pro složitější případy prokazování kauzality do občanského zákoníku. Druhou možností je tlačit na sjednocení rozhodovací praxe soudů, například za pomocí prosazování využívání Principů evropského deliktního práva. Třetí cestou pak je pro autonomní mobilitu, a potenciálně i pro jiná odvětví, kde je prokazování příčinné souvislosti složité, zavést alternativní pravidla deliktní odpovědnosti, která

[44] SCHELLEKENS, Maurice. No-fault compensation scheme for self-driving vehicles. *Law, Innovation and Technology*, 2018. 2/10. S. 314 -333.

nebudou vyžadovat prokazování příčinné souvislosti vůbec. Poslední řešení se zdá nejpragmatičtější. Praktickým příkladem takového řešení je zavedení speciálního povinného pojištění pro všechny provozovatele autonomních vozidel. Důraz je potřeba klást zejména na transparentnost a předvídatelnost způsobu, jakým bude odpovědnost za škodu způsobenou autonomním vozidlem uplatňována.

6. SEZNAM ZDROJŮ

6.1 LITERATURA

[1] DOLEŽAL, Adam; DOLEŽAL, Tomáš. Problematika prokazování příčinné souvislosti v medicínsko-právních sporech. *Právník*, 2013. 6/2013.

[2] DOLEŽAL, Adam; DOLEŽAL, Tomáš. Uplatnění PETL při řešení složitých kauz v oblasti příčinné souvislosti v medicínskoprávních sporech. *Soudní rozhledy*, 2013. 7-8/2013.

[3] DOLEŽAL, Tomáš; DOLEŽAL, Adam. Proof of causation in medical malpractice cases in the Czech republic. *The Lawyer quarterly*, 2015, 5.3.

[4] HAMANOVÁ, Lucie. Prokazování příčinné souvislosti ve sporech o náhradu škody na zdraví způsobenou postupem lékaře non lege artis. *Časopis zdravotnického práva a bioetiky*, 2011. 1/2011.

[5] KRAUSOVÁ, Alžběta et al. *Výzkum potenciálu rozvoje umělé inteligence v České republice, Analýza právně-etických aspektů rozvoje umělé inteligence a jejích aplikací v ČR*. Praha: Vláda ČR, 2018. Dostupné z: https://www.vlada.cz/assets/evropske-zalezitosti/aktualne/AI-pravne-eticka-zprava-2018_final.pdf.

[6] LIM, Hannah YeeFen. *Autonomous Vehicles and the Law: Technology, Algorithms and Ethics*. Cheltenham: Edward Elgar Publishing, 2018.

[7] MAURER, Markus, et al. Autonomous driving. *Springer Berlin Heidelberg, Berlin, Germany*, 2016.

[8] MELZER, Filip. Corpus delicti aneb obrana úpravy deliktního práva v návrhu občanského zákoníku. *Bulletin advokacie*, 2011. 3/2011. 24-27.

[9] NOVÁK, David. Odraz příčinné souvislosti dle Principů evropského deliktního práva v české právní úpravě. *Bulletin advokacie*, 2019. 10/2019.

[10] NOVOTNÁ, Marianna; ADAMOVÁ, Zuzana. Deliktná zodpovednosť za ujmu, ktorá vznikla při využívání systémov umelej inteligencie. In: *Právo, obchod, ekonomika IX*. Košice: Univerzita P. J. Šafárika v Košiciach, 2019. 445 – 455.

[11] POLČÁK, Radim. Odpovědnost umělé inteligence a informační útvary bez právní osobnosti. *Bulletin advokacie*, 2018. No. 11. 23 -26.

[12] SCHELLEKENS, Maurice. No-fault compensation scheme for self-driving vehicles. *Law, Innovation and Technology*, 2018. 2/10. 314 -333.

[13] TICHÝ, Luboš; HRÁDEK, Jiří. Deliktní právo v návrhu občanského zákoníku. *Právní fórum*, 2012. 1, 6-21.

[14] TICHÝ, Luboš; HRÁDEK, Jiří. *Prokazování příčinné souvislosti multikauzálních škod*. Praha: Centrum právní komparatistiky, Právnická fakulta UK, 2010.

[15] ŽOLNERČÍKOVÁ, Veronika. Homologation of Autonomous Machines from a Legal Perspective. In: *Proceedings of the EXplainable AI in Law Workshop co-located with the 31st International Conference on Legal Knowledge and Information Systems (JURIX 2018)*. CEUR Workshop Proceedings, 2019. 51-52.

6.2 PRÁVNÍ PŘEDPISY

[16] Zákon č. 89/2012 Sb., občanský zákoník.

[17] Zákon č. 40/1964 Sb., občanský zákoník.

[18] Příloha č. 2 k Vyhlášce č. 341/2014, o schvalování technické způsobilosti a o technických podmínkách provozu vozidel na pozemních komunikacích.

6.3 SOUDNÍ ROZHODNUTÍ

[19] Rozhodnutí Nejvyššího soudu ČSSR ze dne 27. 9. 1968 sp. zn. 7 Cz 111/68, [R 66/1969 civ.].

[20] Rozhodnutí Nejvyššího soudu ze dne 21. 2. 2002 sp.zn. 21 Cdo 300/2001.

[21] Rozhodnutí Nejvyššího soudu ze dne 23. 2. 2006 sp. zn.25 Cdo 2440/2005.

[22] Rozhodnutí Nejvyššího soudu ze dne 19. 3. 2008, sp. zn. 25 Cdo 657/2006.

[23] Rozhodnutí Nejvyššího soudu ze dne 15. 7. 2008, sp. zn. 25 Cdo 1500/2006.

[24] Rozhodnutí Ústavního soudu ze dne 12. 8. 2008 sp. zn. I. ÚS 1919/08.

[25] Rozhodnutí Ústavního soudu ze dne 12. 8. 2008 sp. zn. I. ÚS 1919/08.

[26] Rozhodnutí Nejvyššího soudu ze dne 28. 5. 2009 sp. zn. 5 Cdo 1054/2007.

[27] Rozhodnutí Nejvyššího soudu ze dne 19. 12. 2012 sp. zn. 25 Cdo 1474/2011.

[28] Rozhodnutí Nejvyššího soudu ze dne 27. 3. 2013 sp. zn. 25 Cdo 4199/2013, [NS 1747/2014].

[29] Rozhodnutí Nejvyššího soudu ze dne 18. 3. 2015 sp. zn. 25 Cdo 3925/2013, [NS 1305/2015].

[30] Rozhodnutí Ústavního soudu ze dne 20. 12. 2016 sp. zn. III. ÚS 3067/13.

[31] Rozhodnutí Ústavního soudu ze dne 20. 12. 2016 sp. zn. III. ÚS 3067/13.

[32] Rozhodnutí Ústavního soudu ze dne 20. 12. 2016 sp. zn. III. ÚS 3067/13.

6.4 NELEGISLATIVNÍ DOKUMENTY

[33] Evropská komise. *Pracovní dokument Odpovědnost za vznikající digitální technologie, doprovázející dokument Sdělení Komise Evropskému parlamentu, Evropské Radě, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů ze dne 25.4.2018 Umělá inteligence pro Evropu.* Brusel, 2018. Dostupné z: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137.

[34] Evropská komise. *Sdělení Komise Evropskému parlamentu, Evropské Radě, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů Evropská strategie týkající se spolupracujících inteligentních dopravních systémů, milník na cestě ke spolupracující, propojené a automatizované mobilitě.* Brusel, 2016. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0766.

[35] Evropská skupina deliktního práva. *Principy evropského deliktního práva*. 2005. Dostupné z: http://www.egtl.org/index.html.

[36] Expertní skupina Gear 2030. *Roadmap – discussion.* Brusel, 2016. Dostupné z: https://circabc.europa.eu/sd/a/a68ddba0-996e-4795-b207-8da58b4ca83e/Discussion%20Paper%C2%A0-%20Roadmap%20on%20Highly%20Automated%20Vehicles%2008-01-2016.pdf.

[37] Ministerstvo dopravy. *Akční plán rozvoje inteligentních dopravních systémů (ITS) v ČR do roku 2020 (s výhledem do roku 2050).* Praha, 2016. Dostupné z: https://www.czechspaceportal.cz/3-sekce/its---inteligentni-dopravni-systemy/strategicke-dokumenty-a-legislativni-akty/akcni-plan-rozvoje-its/.

[38] Ministerstvo dopravy. *Vize autonomní mobility*. Praha, 2017. Str. 4 Dostupné z: https://www.czechspaceportal.cz/3-sekce/its---inteligentni-dopravni-systemy/

strategicke-dokumety/vize-rozvoje-autonomni-mobility/.

[39] Ministerstvo dopravy. *Základní informace o C-ITS.* Praha, 2018. Dostupné z: https://c-roads.cz/?page_id=275 [cit. 1. 4. 2019].

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

---

https://doi.org/10.5817/RPT2020-1-7

GOOGLE, PRÁVO BÝT ZAPOMENUT A LISTINA ZÁKLADNÍCH PRÁV EU[1]

JAROMÍR FRONC[2]

Soud:	Spolkový ústavní soud
Věc:	1 BvR 276/17
Datum:	6. 11. 2019
Dostupnost:	bundesverfassungsgericht.de

1. ÚVOD

Právo být zapomenut se v poslední dekádě stalo oblíbeným postmoderním právně-technologickým tématem. Vše odstartoval rozsudek Soudního dvora EU ve věci *Google Spain*, který v poměrech tehdejší směrnice 95/46/ES[3] dovodil povinnost provozovatele vyhledávače na žádost vymazat z výsledku vyhledávání provedeného na základě jména osoby odkazy na webové stránky zveřejněné třetími osobami obsahující informace týkající se této osoby.[4] Závěry SDEU byly následně zapracovány do čl. 17 obecného nařízení o ochraně osobních údajů,[5] který garantuje právo na výmaz.

Právem být zapomenut se loni zabýval německý Spolkový ústavní soud ve dvou rozhodnutích vydaných ve stejný den. Ta přinesla nejen určitou

---

[1] Tento příspěvek vznikl v rámci plnění projektu Specifického vysokoškolského výzkumu (SVV) Univerzity Karlovy č. 260 494 *„Integrující úloha lidských práv v současném právu“*.

[2] Jaromír Fronc, magisterský student Právnické fakulty Univerzity Karlovy. Kontaktní e-mail: jaromir.fronc@gmail.com.

[3] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

[4] Rozsudek SDEU (velkého senátu) ze dne 13. 5. 2014, ve věci C-131/12, Google Spain (dále jen „*Google Spain*“).

korekci judikatury SDEU, ale i obecnější závěry ohledně vztahu unijního a německého práva.

V prvním usnesení (*„Recht auf Vergessen I“*)[6] se stěžovatel domáhal toho, aby byly z webových stránek novin *Der Spiegel* odstraněny články z let 1982 a 1983, které pojednávaly o jeho odsouzení pro trestný čin vraždy. Tento případ je specifický pro zvláštní ochranu, která je národním ústavním pořádkem přiznána médiím. Vzhledem k většímu komparativnímu přínosu pro českého čtenáře proto níže rozeberu usnesení druhé (*„Recht auf Vergessen II“*), ve kterém bylo aplikováno výhradně unijní právo.

2. SKUTKOVÝ STAV

Televizní kanál *Norddeutscher Rundfunk* odvysílal 21. 1. 2010 díl pořadu *Panorama s* názvem *Výpověď: Odporné triky zaměstnavatelů*. V pořadu bylo zmíněno i jméno pozdější stěžovatelky (v rozhodnutí anonymizováno), která byla obviněna z nespravedlivého chování vůči zaměstnanci. Stěžovatelka pořadu poskytla rozhovor, ve kterém se k případu vyjádřila. Díl byl dostupný v online archivu *NDR a* zobrazoval se ve výsledcích vyhledávání Google při vyhledání jména stěžovatelky.

3. PROCESNÍ HISTORIE

Poté, co Google odmítl odkaz odstranit, se stěžovatelka obrátila na Zemský soud v Lüneburgu, který žalovanému rozsudkem z 22. 4. 2016 zakázal na stránku odkazovat, a to s odkazem na občanský zákoník,[7] na právo na důstojnost a ochranu osobnosti podle Základního zákona,[8] a také na § 35 zákona o ochraně osobních údajů,[9] který prováděl směrnici 95/46/ES, s přihlédnutím k rozsudku *Google Spain*.

---

[5] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) [dále jen „GDPR“].

[6] Usnesení BVerfG ze dne 6. 11. 2019, sp. zn. 1 BvR 16/13.

[7] *Bürgerliches Gesetzbuch*, BGBl. I 2002, s. 42. Znění německých předpisů čerpám z beck-online.de.

[8] *Grundgesetz*, BGBl. I 1949, s. 1.

[9] *Bundesdatenschutzgesetz*, BGBl. I 2003, s. 66.

Vyšší zemský soud v Celle k odvolání žalovaného 29. 12. 2016 po provedení vážení zájmů rozsudek změnil tak, že se žaloba zamítá. Proti tomuto rozhodnutí žalobkyně podala ústavní stížnost ke Spolkovému ústavnímu soudu, jehož první senát rozhodl usnesením z 6. 11. 2019 tak, že se stížnost zamítá.

4. APLIKOVATELNOST LZPEU

Spolkový ústavní soud konstatoval, že právní úprava je plně harmonizovaná unijním právem.[10] Citoval judikaturu SDEU, podle kterého směrnice 95/46/ES nepředstavuje minimální harmonizaci, nýbrž vyžaduje jednotné provedení a aplikaci v rámci EU,[11] což bylo později potvrzeno i přijetím GDPR.[12] V takové situaci pro soud nejsou referenčním kritériem základní práva vyplývající z národního ústavního pořádku, nýbrž základní práva vyplývající z unijního práva.[13] Při výkladu unijního práva nelze ke Základnímu zákonu ani přihlížet, mj. proto, že takový výklad by mohl být mylně považován za správnou interpretaci i pro ostatní členské státy EU.[14]

Ustanovení směrnice 95/46/ES musí být v rozsahu, v němž upravují zpracování osobních údajů, které může představovat zásah do základních svobod, a zejména práva na soukromí, nutně vykládána ve světle základních práv, která jsou nyní zakotvená v LZPEU.[15,16] Tato práva se uplatní nejen ve vztazích mezi jednotlivcem a státem, ale i ve vztazích horizontálních.[17]

---

[10] Bod 33 anotovaného rozhodnutí.

[11] Bod 39 anotovaného rozhodnutí. K metodám harmonizace viz KRÁL, Richard. *Směrnice EU z pohledu jejich transpozice a vnitrostátních účinků*. 1. vydání. Praha: C. H. Beck, 2014, s. 66–72.

[12] Bod 40 anotovaného rozhodnutí.

[13] Body 42–43 anotovaného rozhodnutí.

[14] Bod 45 anotovaného rozhodnutí.

[15] Listina základních práv Evropské unie, uznaná čl. 6 odst. 1 Smlouvy o Evropské unii jako součást primárního práva EU.

[16] Bod 95 anotovaného rozhodnutí odkazující se mj. na *Google Spain*, bod 68.

[17] Bod 96 anotovaného rozhodnutí.

5. VÁŽENÍ ZÁJMŮ

Soud se následně věnoval samotnému porovnání jednotlivých konkurujících si práv a zájmů. Na straně stěžovatelky došlo k zásahu do práva na respektování soukromého a rodinného života (čl. 7 LZPEU) a práva na ochranu osobních údajů (čl. 8 LZPEU).[18] Tato práva spolu úzce souvisí,[19] což platí obzvlášť při zpracování osobních údajů prováděném provozovatelem vyhledávače.[20]

To nejsou nijak převratné závěry, mnohem zajímavější však je, co soud položil na opačnou misku vah. Primárně tu je žalovaná společnost Google, které svědčí svoboda podnikání (čl. 16 LZPEU).[21] Svoboda projevu (čl. 11 LZPEU) se na ni zde však nevztahuje, neboť byť výsledky vyhledávání nejsou obsahově neutrální a mohou ovlivnit mínění uživatelů, vyhledávač není určen k šíření konkrétních názorů a sám se popisuje jako nezávislá služba, která se snaží co nejvíce uspokojit potenciální zájmy uživatelů.[22]

Při poměřování však musí být zohledněna práva třetí osoby – tvůrce obsahu.[23] Pokud je totiž zákaz zobrazování výsledku vyhledávání vydán vůči konkrétnímu obsahu, tvůrce je tím připraven o důležité médium pro jeho rozšiřování, které by jinak měl k dispozici, čímž se omezuje jeho svoboda projevu.[24]

Stejně tak musí být zváženy i informační zájmy uživatelů. Zde se nicméně nejedná o práva jednotlivých uživatelů, nýbrž o obecný princip svobody informací podle čl. 11 LZPEU.[25] Přičemž zatímco ekonomickým

---

[18] Bod 98 anotovaného rozhodnutí.

[19] Bod 99 anotovaného rozhodnutí odkazující se mj. na rozsudek SDEU (velkého senátu) ze dne 9. 11. 2010 ve spojených věcech C-92/09 a C-93/09, Volker und Markus Schecke GbR a Hartmut Eifert, bod 47.

[20] Bod 99 anotovaného rozhodnutí odkazující se mj. na *Google Spain*, bod 80.

[21] Body 103–104 anotovaného rozhodnutí.

[22] Bod 105 anotovaného rozhodnutí.

[23] Body 108–109 anotovaného rozhodnutí.

[24] Takto argumentovala již KATSIREA, Irini. Search Engines and Press Archives Between Memory and Oblivion. *European Public Law*. 2018, roč. 24, č. 1, s. 128–129.

[25] Bod 110 anotovaného rozhodnutí odkazující se mj. na *Google Spain*, bod 81.

zájmům provozovatele vyhledávání soud nepřiznal velkou důležitost,[26] na informační zájmy veřejnosti a práva tvůrců klade větší důraz.[27] Stěžejním východiskem vážení zájmů pak je, že se nevychází z domněnky přednosti osobnostních práv; konkurující si práva musí být spravedlivě porovnána.[28]

Při aplikaci výše uvedených postulátů na konkrétní případ Spolkový ústavní soud zdůraznil, že odvysílaný pořad se nezabýval čistě soukromým životem stěžovatelky, nýbrž otázkami, které byly předmětem veřejného zájmu a stále jsou (byť se snižující se intenzitou). V prostředí Internetu ovšem určitému překryvu mezi osobním a profesním životem nelze zabránit.[29] Pro soud bylo také důležité, že sama stěžovatelka souhlasila s poskytnutím rozhovoru, aniž by k tomu byla jakkoliv dotlačena či donucena.[30] Název odvysílaného dílu (*Odporné triky zaměstnavatelů*) byl přípustným hodnotícím soudem, což platí i pro další rozšiřování tohoto kritického titulku prostřednictvím Internetu.[31] Pokud jde o faktor času, pro soud bylo rozhodné, že stěžovatelka do nynějška působí jako jednatelka a stále existuje veřejný zájem ohledně tématu pořadu – v tomto ohledu není období 7 let excesivní.[32] Došel tedy k závěru, že Google nemá povinnost odkaz odstranit.

6. DISKUSE

Anotované rozhodnutí vzbudilo poměrně bouřlivé ohlasy, které se však primárně zabývaly otázkou vztahu ústavního a unijního práva. Spolkový německý soud totiž dosud se základními právy Evropské unie v podstatě neoperoval. Jeho rozhodnutí k právu být zapomenut tak přinesla dva podstatné závěry: soud se jednak přihlásil k tomu, že bude sám LZPEU aplikovat, jednak provedl „jednoznačný řez“, kdy tak bude činit. Rozlišil na

---

[26] Shodně *Google Spain*, bod 81.

[27] Bod 120 anotovaného rozhodnutí.

[28] Bod 121 anotovaného rozhodnutí.

[29] Bod 128 anotovaného rozhodnutí.

[30] Bod 129 anotovaného rozhodnutí.

[31] Bod 130 anotovaného rozhodnutí.

[32] Bod 134 anotovaného rozhodnutí. Soud zde má zřejmě na mysli období do rozhodnutí odvolacího soudu.

jedné straně situaci, na kterou dopadá přímo použitelný předpis EU (případně prováděcí předpis, při jehož přijímání však německý zákonodárce neměl prostor pro uvážení) – a referenční rámcem přezkumu je tak výhradně LZPEU – a na druhé straně aplikaci národního práva, které nepodléhá plné unijní harmonizaci – a referenční rámcem je tudíž primárně Základní zákon. Německá jurisprudence závěry rozhodnutí v zásadě kvitovala, byť si také povšimla, že si tím soud zároveň ve vlastním zájmu vytvořil podmínky k tomu, aby nebyl opomíjen při interpretaci a aplikaci stále narůstajícího objemu unijní právní regulace.[33]

Čtenář si tak zřejmě nejprve položí otázku, zda by měl podobný řez učinit také český Ústavní soud. Ten sice s LZPEU operuje, ale žádný jednoznačný návod pro její použití v judikatuře nenalezneme, přičemž obecně je akcentována především povinnost eurokonformního výkladu.[34] Setkáváme se spíše se syntetickou metodou, kdy Ústavní soud ověřuje, že bylo dosaženo standardu ochrany podle všech relevantních lidskoprávních dokumentů. Metoda jistě logická a pochopitelná, ale obtížněji použitelná ve chvíli, kdy je třeba poměřovat proti sobě stojící základní práva. Ústavní soud svůj postoj příliš nevyjasnil ani v nedávném nálezu, kde anotované rozhodnutí výslovně citoval.[35] Z jeho odůvodnění se totiž nepodává, že by byl připraven rozhodovat čistě na základě LZPEU, nýbrž se zde opět mluví pouze o (eurokonformním?) výkladu práva.

Pro naše potřeby je ovšem použití LZPEU v anotovaném rozhodnutí užitečné především tím, že soudu umožnilo dospět k závěrům ve věci samé, které – pokud můžeme Spolkovému ústavnímu soudu věřit, že se oprostil

---

[33] BREUER, Marten. Wider das Recht auf Vergessen … des Bundesverfassungsgerichts! In: *Verfassungsblog* [online]. 2. 12. 2019. [cit. 31. 3. 2020]. Dostupné z: https://verfassungsblog.de/wider-das-recht-auf-vergessen-des-bundesverfassungsgerichts/. KARPENSTEIN, Ulrich, KOTTMANN, Matthias. Vom Gegen- zum Mitspieler – Das BVerfG und die Unionsgrundrechte. *Europäische Zeitschrift für Wirtschaftsrecht.* 2020, roč. 31, č. 5, s. 185–189.

[34] Srov. BOHÁČEK, Lukáš. Součástí referenčního rámce a kritériem přezkumu Spolkového ústavního soudu bude do budoucna rovněž Listina základních práv Evropské unie. *Bulletin oddělení analytiky a srovnávacího práva.* [online]. 2019, roč. X, č. 4, s. 5–7. [cit. 31. 3. 2020]. Dostupné z: http://www.nsoud.cz/judikatura/ns_web.nsf/0/A127C1166CE3E527C12584E1003BC6BD/$file/Bulletin%20%5B2019%5D%204.pdf.

[35] Nález Ústavního soudu ze dne 11. 2. 2020, sp. zn. Pl. ÚS 4/17, bod 109.

od německého práva – mohou být použitelné i pro ostatní členské státy EU, a to i pro v současnosti účinný čl. 17 GDPR. To ovšem s výhradou, že konečný výsledek poměřování se v různých členských státech může beztak lišit.[36]

Rozsudek *Google Spain* v závěru postuluje, že osobnostní práva podle čl. 7 a 8 LZPEU převládají *„v zásadě nejen nad hospodářským zájmem provozovatele vyhledávače, ale rovněž nad zájmem veřejnosti nalézt uvedenou informaci při vyhledávání prováděném na základě jména subjektu údajů.“*[37] Anotované rozhodnutí v zásadě jde v těchto šlépějích, avšak zároveň přináší určité posuny. Na rozdíl od judikatury SDEU výslovně zmiňuje čl. 11 a 16 LZPEU a nově uvádí i nutnost zohlednit práva tvůrce. Pokud tedy dotčené osoby tvrdí, že provozovatel webového vyhledávání by měl přestat poskytovat informace o určitém obsahu Internetu a odkazovat na něj, musí se osobnostní práva dotčených osob poměřit se základními právy příslušných tvůrců obsahu a informačními zájmy uživatelů Internetu, a to v rámci svobody podnikání provozovatelů vyhledávání.

Zároveň však zdůrazňuje, že přípustnost zveřejnění samotného obsahu a přípustnost odkazování na něj ve výsledcích vyhledávání musí být poměřovány v samostatných testech.[38] Nadále tedy platí, že provozovateli vyhledávače může být v některých případech zakázáno odkazovat na obsah, jehož zveřejnění na odkazované stránce je samo o sobě v souladu se zákonem.[39]

Z výše uvedené citace SDEU by se také mohlo zdát, že osobnostní práva dotčených osob mají *prima facie* navrch a nutnosti výsledky odstranit se tak dá vyhnout jen s poukazem na specifické okolnosti případu. Rozhodnutí z Karlsruhe je tak třeba ocenit i proto, že explicitně stanoví povinnost

---

[36] Rozsudek SDEU (velkého senátu) ze dne 24. 9. 2019, ve věci C-507/17, Google LLC v. CNIL, bod 67.

[37] *Google Spain*, bod 99.

[38] Body 112–119 anotovaného rozhodnutí. K této dvojkolejnosti viz též NONNEMANN, František. Základní analýza rozhodnutí Soudního dvora EU ve věci internetového vyhledávače Google. *Právní rozhledy*. 2014, roč. 22, č. 13-14, s. 484–485.

[39] Srov. *Google Spain*, bod 88.

konkurující si základní práva porovnat bez jakýchkoliv předsudečných úvah.

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

---

https://doi.org/10.5817/RPT2020-1-8

NIKDO NESMÍ VLASTNIT PRÁVO[1]

JAKUB HARAŠTA[2]

Soud:	Nejvyšší soud USA / Supreme Court of the United States
Věc:	No. 18-1150
Datum:	27. 4. 2020
Dostupnost:	https://www.supremecourt.gov/opinions/19pdf/18-1150_new_d18e.pdf (vč. disentů)

1. PŘEDMĚT SPORU

V dubnu 2020 se Nejvyšší soud USA (dále jen „SCOTUS“) vyjádřil k autorskoprávní ochraně anotovaných textů zákonů státu Georgia, které jsou shromážděné v *Official Code of Georgia Annotated* (dále jen „OCGA“). SCOTUS dospěl k závěru, že autorskoprávní ochrana tomuto dokumentu (a jemu podobným) nepřísluší s tím, že se jedná o materiál publikovaný při výkonu zákonodárné moci. Je proto z autorskoprávní ochrany vyloučen. Na první pohled relativně jednoduchý a logický závěr prezentovaný majoritou prošel poměrem 5-4. Názor majority i disentní stanoviska přinášejí zajímavou argumentaci, která se, jako je u tohoto soudního tělesa zvykem, věnuje problému z různých stran a snaží se „domyslet“ důsledky rozhodnutí do konce.

Stát Georgia zveřejňuje OCGA. OCGA zahrnuje text každého aktuálně účinného zákona, který je pak doprovázen také podpůrnými materiály ve formě anotací. Tyto anotace zahrnují shrnutí soudních rozhodnutí, seznam

[1] Zpracováno v rámci specifického výzkumu Masarykovy univerzity, projekt Právo a technologie VIII (MUNI/A/0989/2019).

[2] JUDr. Mgr. Jakub Harašta, Ph.D., odborný asistent na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. E-mail: jakub.harasta@law.muni.cz

relevantní článků v amerických *law reviews* nebo odkazy na historický původ konkrétních norem (např. identifikovanou sémantickou podobností s dřívějšími soudními rozhodnutími). OCGA je sestavováno tzv. *Code Revision Commission* (dále jen „Komise"). Většina z 15 členů této Komise jsou představitelé zákonodárné moci státu Georgia. Činnost Komise jako celku je pak financována v rámci rozpočtové kapitoly určené na činnost zákonodárné moci. Komise nesestavuje OCGA sama, ale skrze smlouvu platí za sestavování textů a vytváření anotací jedné z divizí společnosti LexisNexis – texty nicméně Komise schvaluje. Smlouva specifikovala, že práva náleží státu Georgia, který jedná skrze Komisi. Neanotované texty musí dát zhotovitel k dispozici veřejně a online, požívá nicméně exkluzivního práva anotované texty publikovat a distribuovat. Kopie OCGA stojí více než 400 USD a v současné době zahrnuje 54 svazků.

2. PROCESNÍ HISTORIE

Public.Resource.Org (dále jen „PRO") se jako nezisková organizace věnuje zpřístupňování právních zdrojů a podobných záznamů veřejnosti. PRO zveřejnila OCGA na několika internetových stránkách a přes výzvy ze strany orgánů státu Georgia od svého jednání neupustila. Vše tak skončilo před soudem. První stupeň[3] (*District Court for the Northern District of Georgia*, dále jen „DC"*)* dospěl k názoru, že anotace a poznámky obecně mohou být předmětem ochrany autorského práva. Nejsou totiž vyloučeny, protože se nejedná o texty, které by měly jakoukoli právní sílu. Druhý stupeň[4] (*United States Court of Appeals for the Eleventh Circuit*, dále jen „CoA") prvostupňové rozhodnutí nicméně zrušil s tím, že celý materiál není předmětem ochrany. OCGA musí být, dle názoru CoA, přístupný všem, protože má zcela jasně autoritativní váhu – anotace sice nemají právní sílu, ale jsou zcela nedílnou součástí práva státu Georgia.

[3] Text prvostupňového rozhodnutí je dostupný na https://www.leagle.com/decision/inadvfdco171222000293.

[4] Text druhostupňového rozhodnutí je dostupný na https://www.leagle.com/decision/infco20181019244.

3. POSOUZENÍ NEJVYŠŠÍM SOUDEM USA

SCOTUS se nakonec vůbec nezabýval tím, zda je možné, aby byly anotace a poznámky v textu OCGA předmětem ochrany autorským právem (což bylo jádrem rozhodnutí DC). Podobně jako CoA se SCOTUS soustředil na to, zda není důvod pro vyloučení OCGA z ochrany. SCOTUS dospěl k závěru, že OCGA nemá žádného autora, který by k němu byl způsobilý nést a vykonávat autorská práva. K tomuto závěru však dospěl jinými cestami, než CoA. SCOTUS totiž explicitně uvedl, že tento závěr je platný bez ohledu na to, zda mají anotace v OCGA autoritativní povahu. Tedy ať už jsou či nejsou nedílnou součástí práva státu Georgia. OCGA není možné podrobit autorskoprávní ochraně z důvodu, že členové Komise, kteří se na jeho tvorbě podíleli, tak činili v rámci svojí oficiální činnosti. Není tedy nutné přezkoumávat, zda je materiál nebo jeho části nadán právní silou.

SCOTUS k tomuto názoru dospěl posunem své předcházející rozhodovací praxe. Ve věci *Wheaton v. Peters*[5] *a* ve věci *Banks v. Manchester*[6] SCOTUS uvedl, že soudci nemohou držet práva ke svým výtvorům. Toto platí bez ohledu na to, zda se jedná o přípravu závazného majoritního stanoviska nebo disentu. Jakmile soudce vykonává svoji činnost, jeho materiály jsou v režimu *public domain.* Osoba zpracovávající rozhodovací praxi do podoby přehledových *reports* může držet práva k poznámkám, nadpisům a dalším podpůrným materiálům, ale to pouze za předpokladu, že není soudcem (*Callaghan v. Myers*[7]). Majorita tuto praxi shrnula do pravidla, které označila za přímočaré: Protože je soudce nadán mocí tvořit a interpretovat právo, nemůže být autorem u děl, která připravuje v rámci této činnosti. Činnost je pak nutno chápat široce a zahrnuje kromě závazných materiálů i ty nezávazné (nadpisy, shrnutí).[8] Pokud nemohou být představitelé soudní moci, kteří vytvářejí a interpretují právo, autory,

---

[5] Rozhodnutí *Supreme Court of the United States* ve věci Wheaton v. Peters (1834) dostupné na https://www.leagle.com/decision/noyr62433us5911564.

[6] Rozhodnutí *Supreme Court of the United States* ve věci Banks v. Manchester (1888) dostupné na https://www.leagle.com/decision/1888372128us2441346.

[7] Rozhodnutí *Supreme Court of the United States* ve věci Callaghan v. Myers (1888) dostupné na https://www.leagle.com/decision/1888745128us6171675.

[8] Anotované rozhodnutí, s. 7.

pak jimi nesmí být ani představitelé moci zákonodárné.[9] Toto pravidlo se opět vztahuje i na nezávazné materiály, jako jsou proslovy, zprávy různých komisí nebo návrhy zákonů.[10]

Jako faktickou otázku tak SCOTUS musel vyhodnotit, zda má OCGA původ v zákonodárné moci.[11] Stát Georgia potvrdil, že za autora je nutné považovat Komisi. Komise je, jak již bylo zmíněno, součástí zákonodárné moci státu Georgia (je financována z rozpočtové kapitoly určené pro zákonodárnou moc) a většinově se skládá z příslušníků zákonodárného sboru.[12] Majorita proto konstatovala, že OCGA má původ v zákonodárné moci a není způsobilá k autorskoprávní ochraně. Stát Georgia se v rámci svých podání k možnosti takového závěru vyjadřoval negativně – což je stěží překvapivé – a argumentoval zejména tím, že vyloučení z autorskoprávní ochrany přinese těžkosti při hledání smluvních partnerů, kteří by pro stát a pro Komisi anotace zpracovávali. SCOTUS ve svém rozhodnutí poznamenal, že toto je otázka politiky nastavené pro zpracování OCGA a zpřístupňování právních informací, a jako takovou ji nepřísluší soudu hodnotit nebo se k ní vyjadřovat.[13]

4. DISENTNÍ STANOVISKA

Leitmotivem celého rozhodnutí bylo, že *„nikdo nesmí vlastnit právo.“*[14] Přirozeně se tak předmětem diskuze v disentech stala otázka, co právem vlastně je. Majorita k tomu přistoupila extenzivně a uvedla, že jakkoli jsou nezávazné věci neprávem, jsou produktem subjektu, který právo tvoří a/nebo vykládá. V opačném případě, uvedla majorita, by bylo možné, aby jednotlivé státy vybíraly poplatky za přístup k nezávazným, ale přesto

[9] Anotované rozhodnutí, s. 8.

[10] Anotované rozhodnutí, s. 9.

[11] Srov. rozhodnutí *Supreme Court of Georgia* ve věci Harrison Co. v. Code Revision Commission (1979), dostupné na https://www.leagle.com/decision/1979569244ga325 1433: *„In our view, however, the work of the Commission; i.e., selecting a publisher and contracting for and supervising the codification of the laws enacted by the General Assembly, including court interpretations thereof, is within the sphere of legislative authority.“* (s. 244 Ga. 330)

[12] Anotované rozhodnutí, s. 16.

[13] Anotované rozhodnutí, s. 14-15.

[14] Anotované rozhodnutí, s. 7.

podstatným materiálům (návrhy zákonů, zprávy komisí). Soudce Thomas (částečně se k němu připojil i Breyer) se ve svém disentu s takto dalece narýsovanou paralelou mezi mocí soudní a zákonodárnou nespokojil. Soudce Thomas uvedl, že moc zákonodárnou je pro účely vylučování z autorskoprávní ochrany nutné chápat restriktivně. Zatímco soudní moc musí být chápána extenzivně, protože disentní stanoviska demonstrují potenciální aplikační problémy a celkově jsou součástí kritické diskuze závěrů soudů[15], zákonodárná moc je kvalitativně odlišná. Nezávazné materiály totiž takovýto kritický vhled nemusí nutně poskytovat.

K podobnému závěru ve svém disentu dospěla soudkyně Ginsburg (připojil se Breyer) – zákonodárné anotace dle ní nejsou součástí zákonodárné činnosti.[16] Rozlišila mezi nezávaznými dokumenty, které jsou součástí legislativního procesu, a nezávaznými dokumenty, které jsou vytvářeny až po okamžiku účinnosti zákona. Zatímco ty první mají být vyloučeny z autorskoprávní ochrany, dokumenty ve druhé kategorii nikoli.[17] Anotace v OCGA jsou deskriptivní a nikoli preskriptivní – jsou neutrálním popisem reality právních informací. Nejsou přípravnými dokumenty, které formují dojmy a názory zákonodárců.[18]

Disenty Thomase i Ginsburg lze tak dle mého chápat tak, že části OCGA by měly být předmětem autorského práva a část nikoli. Troufám si tvrdit, že zde mohl mít na názor majority vliv *amicus curiae* podaný CaseLaw Access Project (Harvardova univerzita), kde byl klíčovým právě argument, že rozlišování mezi částmi materiálu činí problematickou jak digitalizaci, tak i zpracování právních informací v rozsahu v jakém se to děje například v rámci projektu digitalizace historických rozhodnutí.[19] I majorita totiž uvedla, že se s přiznáním autorskoprávní ochrany musí nakládat opatrně. Není žádoucí, aby se uživatelé museli spoléhat například na výjimky,

---

[15] Disent soudce Thomase (částečně Breyer), s. 13-14.

[16] Disent soudkyně Ginsburg (Breyer), s. 2.

[17] Disent soudkyně Ginsburg (Breyer), s. 2-3.

[18] Disent soudkyně Ginsburg (Breyer), s. 3-4.

[19] *Amicus curiae* CaseLaw Access Project na https://www.supremecourt.gov/DocketPDF/18/18-1150/119213/20191016161938490_Cyberlaw%20Clinic_Georgia%20%20Public.Resource_Amicus%20Brief.pdf.

protože tyto jsou extrémně závislé na faktech a často nemohou být plně využity bez rozhodnutí soudu.[20] Majorita tak vlastně uzavřela, že namísto individuálního vyhodnocování, zda má daná anotace sílu díla či nikoli, je vhodné, aby nastoupilo posouzení, zda je dokument připraven zákonodárnou mocí.

Soudce Thomas však ve svém disentu majoritu právě za neúspěch při zjednodušování tvrdě kritizuje – dle mého názoru zcela oprávněně. Majorita sice vypsala seznam faktorů, které vstupují do rozhodování, zda je dokument připraven mocí zákonodárnou či nikoli. Nijak nicméně, jak uvádí Thomas, nespecifikovala, zda jsou tyto faktory taxativní či demonstrativní a jaké jsou jejich individuální váhy při rozhodování o vyloučení z autorskoprávní ochrany.[21] Ve své snaze zajistit vyšší právní jistotu pro ty, kteří právní informace zpřístupňují a využívají, tak SCOTUS bohužel jen pokračuje ve vytváření standardů, které jsou citlivé na fakta konkrétního případu. V podstatě tak odpadá jeden z hlavních důvodů pro existenci celého rozhodnutí. Velké riziko také Thomas spatřuje v tom, že se státům jednoduše nevyplatí přehledy zpracovávat. OCGA se dá prostřednictvím LexisNexis pořídit za již zmíněných cca 400 dolarů. Konkurenční produkt od West Publishing však stojí více než šestinásobek.[22] Rozhodnutí majority tak může být kontraproduktivní – namísto toho, aby existoval de facto dotovaný zdroj, který si ale nebude moci dovolit každý, tento zdroj přestane existovat úplně a dostupnost informací se výrazně sníží (okruh osob, které si ho budou moci dovolit, bude výrazně nižší).

5. ZÁVĚR

V rámci anotace jsem se snažil vynechávat konkrétní úvahy na téma dopadu konkrétních norem a konkrétních precedentů – rozhodnutí je jich, pochopitelně, plné, ale pro nás mají jen malou váhu. Snažil jsem se soustředit na ústřední myšlenku. *„Nikdo nesmí vlastnit právo“* je na první pohled velmi jednoduchá maxima pro rozhodování. Realita má ale, jako

[20] Anotované rozhodnutí, s. 18. Podobně *amicus curiae* CaseLaw Access Project, s. 9-11.

[21] Disent soudce Thomase (částečně Breyer), s. 16.

[22] Disent soudce Thomase (částečně Breyer), s. 17.

ostatně ve všem, ke každému A své B. Pozitivní dle mého názoru je, že existuje značný potenciál, že toto rozhodnutí usnadní digitalizaci a zpřístupňování existujících právních informací. Odvrácenou stranou mince je pak oprávněná kritika soudce Thomase. Nadpoloviční většina členů Komise je tvořena členy zákonodárného sboru. Bude stačit, když se sníží jejich počet? Bude stačit, když nebude činnost Komise hrazena z rozpočtové kapitoly určené zákonodárné činnosti? Do budoucna je tak situace nejistá. Těžko říct, nakolik bude ovlivněna kreativními snahami jednotlivých institucí zachovat autorskoprávní ochranu pro anotované texty předpisů a další podobné zdroje.

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

---

https://doi.org/10.5817/RPT2020-1-9

PŘEHLED AKTUÁLNÍ JUDIKATURY I/2020

DOMINIKA COLLETT, FRANTIŠEK KASL, JAKUB KLODWIG, IVANA KUDLÁČKOVÁ, PAVEL LOUTOCKÝ, JAKUB MÍŠEK, ANNA STÁRKOVÁ, JAN SVOBODA, PETRA VYDROVÁ, VERONIKA ŽOLNERČÍKOVÁ

1. SLUŽBY INFORMAČNÍ SPOLEČNOSTI

AIRBNB JAKO SLUŽBA INFORMAČNÍ SPOLEČNOSTI

Soud: Soudní dvůr Evropské unie
Věc: C-390/18 (Airbnb Ireland)
Datum: 19. 12. 2019
Dostupnost: curia.europa.eu

Společnost Airbnb Ireland UC[1] provozuje online platformu, která slouží ke zprostředkování ubytovacích prostor za úplatu mezi hostitelem (a to ať už soukromým, tak i profesionálním) a osobami, které dané ubytování vyhledávají. Tato společnost nadto poskytuje pronajímatelům další služby, např. pojištění občanskoprávní odpovědnosti či volitelný nástroj pro odhad ceny pronájmu. Francouzské sdružení Association pour un hébergement et un tourisme professionnels nepovažovalo činnost Airbnb Ireland UC za prostou zprostředkovatelskou činnost a podalo trestní oznámení s návrhem na přiznání náhrady škody v adhezním řízení z důvodu, že daná činnost je vykonávána bez profesního povolení nutného pro činnosti související se správou a pronájmem nemovitostí.

[1] K přesnější charakterizaci předmětné služby a specifickému propojení jednotlivých obchodních společností vlastněných americkou Airbnb Inc. Více viz bod 18 a násl. anotovaného rozhodnutí.

Daným případem se zabýval Tribunal de grande instance de Paris, který vznesl na SDEU dvě předběžné otázky. První bylo to, jestli by služba poskytovaná společností Airbnb Ireland UC měla být kvalifikována jako „služba informační společnosti“ ve smyslu směrnice o elektronickém obchodu.[2] Druhou pak bylo to, jestli tato směrnice brání použití příslušného zákona stanovujícího povinnost ke zřízení povolení pro správu nemovitostí a tedy jestli daná směrnice nebrání uplatnění trestní odpovědnosti společnosti Airbnb Ireland UC za nesplnění zákonných podmínek[3].

SDEU vedl poměrně rozsáhlou argumentaci, ze které je patrné, že se chtěl jednoznačně vyhnout připodobnění dané služby k předešlým rozhodnutím souvisejícím se službami v oblasti dopravy.[4] SDEU v této věci především argumentoval, že spojovat činnost s ubytovacími službami je problematické a v případě služeb v oblasti dopravy se jedná o zcela jinou oblast navíc pokrytou čl. 58 odst. 1 SFEU.[5] Nadto zdůraznil, že u činnosti společnosti Airbnb Ireland UC nemůže být prokázána existence rozhodujícího vlivu na ubytovací služby (na rozdíl od společnosti Uber). Tato společnost tak neposkytuje ubytovací služby, zprostředkovává spíše možnost uzavřít související smlouvy. Důležitější než detailní argumentace,[6] je fakt, že SDEU zde (ač nebyl přímo dotazován) argumentuje ve smyslu omezeného vlivu na ubytovací služby společností Airbnb Ireland UC (i přesto, že tato společnost poskytuje i doplňkové služby související s ubytováním). Směr argumentace je tak odlišný oproti potenciálně srovnatelnému rozhodnutí Uber Spain.

SDEU konstatoval, že službu poskytovanou společností Airbnb Ireland UC je nutno považovat za službu informační společnosti.[7] Tím tak soud zdůraznil, že se jedná „jen“ o službu poskytovanou na dálku, elektronicky

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

[3] Bod 26 anotovaného rozhodnutí.

[4] Především rozhodnutí ze dne 20. prosince 2017 ze dne 20. prosince 2017 SDEU ve věci Uber Spain, C-434/15.

[5] Bod 66 anotovaného rozhodnutí.

[6] Ta je obsažena v bodě 52 a násl. anotovaného rozhodnutí.

[7] Jedná se o odpověď na první předběžnou otázku.

a na individuální žádost příjemce;[8] odlišuje ji tak zcela od ubytovacích služeb. V obdobném kontextu argumentoval i v souvislosti s druhou položenou otázkou; závěrem však konstatuje, že záleží na právu každého členského státu a soud nemůže vyloučit možnost zahájení trestního řízení s návrhem na přiznání náhrady škody v adhezním řízení.

Na rozhodnutí je dle našeho názoru patrná snaha o korekci předešlého rozhodování v obdobných případech a snaha o limitaci faktorů omezujících fungování služeb sdílené ekonomiky. Soud se totiž (oproti předešlým rozhodnutím) mnohem více věnoval argumentaci nastavující mantinely fungování dané služby informační společnosti a ve svém odůvodnění se snažil naznačit, že ne každá činnost nutně musí podléhat příslušným registracím a vnitrostátním limitům (i díky několikerému zdůraznění, že veškerá činnost společnosti Airbnb Ireland UC nemůže být vnímána jinak, než jako zprostředkovatelská). Toto rozhodnutí tak může mít i dalekosáhlé dopady související s daňovými otázkami, na charakter podnikání, ochranu spotřebitele a může dále ovlivňovat ubytovací standardy. Otázkou zůstává, jestli jednotlivé členské státy budou ochotny respektovat potenciálně větší benevolenci k regulaci služeb sdílené ekonomiky a sdílet výše nastíněný problematický názor soudu.

Autor: PL

ODPOVĚDNOST ZA VÝROBKY USKLADNĚNÉ ONLINE TRŽIŠTĚM

Soud: Soudní dvůr Evropské unie
Věc: C-567/18 (Coty Germany)
Datum: 2. 4. 2020
Dostupnost: curia.europa.eu

Společnost Coty distribuující parfémy je držitelkou licence k evropské ochranné známce DAVIDOFF. Společnost Amazon je online tržištěm, které umožňuje na stránkách uživatelům umisťovat výrobky k prodeji. Společnost Amazon rovněž nabízí k využití své sklady pro uskladnění výrobků.

[8] Bod 5 anotovaného rozhodnutí.

Společnost Coty si jako testující kupující pořídila parfém „Davidoff“ (konkrétní druh) a zjistila, že nebyl na evropský trh uveden v souladu s právem. Po komunikaci se společností Amazon došlo k zaslání těchto „vadných“ výrobků společnosti Coty, ta ale navíc požadovala, aby se společnost Amazon do budoucna zdržela jakéhokoli skladování těchto výrobků chráněných ochrannou známkou.

Německý Spolkový soudní dvůr posléze v souvislosti s evropským nařízením o OZ[9] formuloval předběžnou otázku k SDEU zaměřující se na pojem užití ochranné známky.

SDEU se zabýval otázkou, jestli „*osoba, která pro třetí stranu uskladňuje výrobky porušující práva z ochranné známky, aniž o tomto porušení ví, tyto výrobky za účelem jejich nabízení nebo uvádění na trh* [skladuje]*, jestliže úmysl nabízet tyto výrobky nebo je uvádět na trh nemá tato osoba, ale pouze třetí strana?*“[10]

Hlavní otázkou bylo, jestli nařízení o OZ upravuje užívání ochranné známky v daném kontextu, a co zahrnuje její užití. Soud s odkazem na předchozí rozhodnutí[11] zdůraznil, že užití znamená „*aktivní jednání a přímou či nepřímou kontrolu nad aktem představujícím užívání.*“[12] „*Pouze třetí osoba, která má přímou či nepřímou kontrolu nad aktem představujícím užívání, je skutečně schopna toto užívání ukončit.*“[13] SDEU dále zdůrazňuje, že „*k tomu, aby uskladnění výrobků označených označeními totožnými nebo podobnými s ochrannými známkami mohlo být kvalifikováno jako „užívání“, je ještě třeba […], aby hospodářský subjekt provádějící toto uskladnění sám sledoval cíl […], který spočívá v nabízení výrobků nebo jejich uvádění na trh.*“[14]

Na základě výše řečeného tedy SDEU shrnul, že osoba, která pro třetí stranu uskladňuje výrobky porušující práva z ochranné známky, aniž

[9] Nařízení Evorpského parlamentu a Rady (EU) 2017/1001 ze dne 14. června 2017 o ochranné známce Evropské unie.

[10] Bod 18 anotovaného rozhodnutí.

[11] Bod 37 anotovaného rozhodnutí.

[12] Tamtéž.

[13] Bod 38 anotovaného rozhodnutí.

[14] Bod 45 anotovaného rozhodnutí.

o tomto porušení ví (a sama takový cíl nesleduje), neužívá ve smyslu dané legislativy příslušnou ochrannou známku.

Toto rozhodnutí je dobrou zprávou pro online tržiště a mimo jiné (a co je asi nejzajímavější) se zde ukazuje inspirace limitací odpovědností ISP a využití bezpečného přístavu. Argumentace využitá v anotovaném rozhodnutí je totiž nápadně podobná konceptu omezení odpovědnosti ISP a bezpečného přístavu. Je tak patrné, jak regulace otázek spadajících čistě do oblasti práva informačních technologií zpětně začínají ovlivňovat i „klasičtější“ problematiku.

Autor: PL

2. PRÁVO DUŠEVNÍHO VLASTNICTVÍ

ODCHYLKY OD USTANOVENÍ, PODLE NICHŽ MOHOU BÝT VYUŽÍVÁNA DÍLA VÝKONNÝCH UMĚLCŮ

Soud:	Soudní dvůr Evropské unie
Věc:	C-484/18 (Spedidam, PG, GF proti Institut national de l'audiovisuel)
Datum:	14. 11. 2019
Dostupnost:	curia.europa.eu

Institut national de l' audiovisuel (dále jen „INA“) je veřejnoprávní institucí v oblasti audiovizuálního dědictví asistující při využívání archivů audiovizuálních výrobců. PG a GF jakožto právní nástupci zemřelého hudebníka ZV podali vůči INA žalobu za účelem získání náhrady za údajný zásah do práv výkonných umělců, kterých se INA měla dopustit nabízením videozáznamů a zvukových záznamů vystoupení hudebníka ZV bez svolení PG a GF. Kasační soud vznesl následující předběžnou otázku.

Soudní dvůr byl tázán, zda čl. 2 písm. b) a čl. 3 odst. 2 písm. a) směrnice 2001/29 (o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti) musí být vykládány v tom smyslu, že brání vnitrostátním právním předpisům, které v oblasti

využívání audiovizuálních archivů orgánem určeným k tomuto účelu stanoví vyvratitelnou domněnku svolení výkonného umělce se záznamem a užíváním jeho výkonu, pokud se tento výkonný umělec podílí na nahrávání audiovizuálního díla pro účely jeho vysílání.[15]

V souladu s cílem vysoké úrovně ochrany práv výkonných umělců je třeba vnímat preventivní povahu práv, která výkonným umělcům zaručujíčl. 2 písm. b) a čl. 3 odst. 2 písm. a) směrnice 2001/29, a to v tom smyslu, že každé rozmnožení či zpřístupnění záznamů jejich výkonů veřejnosti vyžaduje jejich předchozí svolení.[16] Z tohoto výkladu tedy plyne, že s výhradou výjimek a omezení, které jsou taxativně uvedeny v článku 5 předmětné směrnice, musí být každé užití takových předmětů ochrany třetí osobou bez předchozího svolení považováno za zásah do práv majitele.[17] Předmětné články směrnice ale již dále neupřesňují způsob, jakým musí být předchozí svolení výkonného umělce vyjádřeno, je tedy umožněno i vyjádření implicitní formou.[18]

Soudní dvůr v této souvislosti uvedl, že výkonný umělec, který se sám podílí na výrobě audiovizuálního díla pro účely jeho vysílání státními vysílacími společnostmi, a který se tak nachází na místě nahrávání takového díla k těmto účelům, jednak ví o zamýšleném užití svého výkonu a jednak svůj výkon realizuje pro účely takového užívání.[19] Je tedy možné mít za to, neexistuje-li důkaz v opačném smyslu, že v důsledku této účasti dal svolení se záznamem uvedeného výkonu, jakož i s jeho užíváním.[20] Francouzská právní úprava ovšem umožňuje prokázání nesouhlasu s pozdějším užíváním výkonu, předmětná domněnka má tedy vyvratitelnou povahu.[21]

V odpovědi na předběžnou otázku Soudní dvůr uvedl, že čl. 2 písm. b) a čl. 3 odst. 2 písm. a) směrnice 2001/29 nebrání vnitrostátním právním

[15] Srov. bod 34 anotovaného rozhodnutí.

[16] Srov. body 38 a 39 anotovaného rozhodnutí.

[17] Srov. bod 38 anotovaného rozhodnutí.

[18] Srov. bod 40 anotovaného rozhodnutí.

[19] Srov. bod 42 anotovaného rozhodnutí.

[20] Srov. bod 42 anotovaného rozhodnutí.

[21] Srov. bod 43 anotovaného rozhodnutí.

předpisům stanovit vyvratitelnou domněnku svolení výkonného umělce se záznamem a užíváním jeho výkonu, pokud se tento výkonný umělec podílí na nahrávání audiovizuálního díla pro účely jeho vysílání.[22]

Autorka: IK

PŘEKRYTÍ STAVBY REKLAMOU JAKO ZÁSAH DO ROZMNOŽENINY AUTORSKÉHO DÍLA

Soud: Vrchní soud v Praze
Věc: 3 Co 89/2019–66
Datum: 2. 12. 2019
Dostupné z: na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím

Vrchní soud v Praze rozhodoval o odvolání ve věci žalobce Jana H., architekta domu v ulici Boženy Němcové na Praze 2, proti žalované JIZERA INVEST s.r.o., vlastníci domu, na němž je umístěn billboard a reklamní obrazovka překrývající celé průčelí.[23]

Městský soud v Praze jako soud prvního stupně zamítnul nárok na odstranění reklamních panelů a zaplacení zadostiučinění žalobci z důvodu zásahu do jeho autorských práv.[24] Žalobce se odvolal v celém rozsahu.[25]

Žalobce tvrdil, že umístěním reklamy byla snížena hodnota díla a porušeno právo na jeho nedotknutelnost (§ 11 odst. 3 autorského zákona[26] („AZ“)).[27] Dům je ceněn odbornou veřejností zejména kvůli tzv. střešní frontě na průčelí, nyní zakryté.[28] Žalobce se na základě § 40 odst. 1

[22] Srov. bod 46 anotovaného rozhodnutí.

[23] Bod 2 anotovaného rozhodnutí.

[24] Bod 1 anotovaného rozhodnutí.

[25] Bod 12 anotovaného rozhodnutí.

[26] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů.

[27] Body 2 a 12 anotovaného rozhodnutí.

[28] Bod 2 anotovaného rozhodnutí.

písm. d) AZ domáhal nápravy s tím, že k úpravě neposkytnul souhlas a jeho renomé je dlouhodobě poškozováno komolením díla.[29]

Prvoinstanční soud žalobě nevyhověl[30], z důvodu, že dle něj dílo nedošlo k úhoně, pouze není vidět.[31] Žalobce totiž neprokázal, že reklamní plocha je fyzicky spjata s průčelím.[32] Prvoinstanční soud také nepovažoval úpravy stavby za zásah do rozmnoženiny díla podle § 40 odst. 1 písm. d) AZ.[33] Odvolací však se závěry soudu prvního stupně nesouhlasil. Stavba dle něj může představovat rozmnoženinu,[34] a navíc překrytí díla může snížit jeho hodnotu. Odvolací soud dále konstatoval, že soud prvního stupně nedostatečně zkoumal způsob upevnění reklamy.[35]

Odvolací soud změnil výrok prvoinstančního soudu a nařídil žalované odstranění obrazovky i billboardu z průčelí budovy.[36] Výrok týkající se zadostiučinění zrušil a vrátil k rozhodnutí soudu prvního stupně z důvodu chybějícího posouzení narušení průčelí upevněním reklamy.[37]

Rozsudek konstatuje, že překrytí budovy reklamní plochou, jejíž umístění autor neodsouhlasil, konstituuje zásah do autorského díla – architektonické stavby. Žalovaná nicméně podala dovolání k Nejvyššímu soudu. Zároveň podala návrh na odklad vykonatelnosti povinnosti odstranit reklamu. Nejvyšší soud návrh na odklad zamítl.[38]

Autorka: VŽ

---

[29] Tamtéž.

[30] Rozhodnutí Městského soudu v Praze ze dne 22. 5. 2019, sp. zn. 23 C 34/2017-44.

[31] Bod 10 anotovaného rozhodnutí.

[32] Bod 9 anotovaného rozhodnutí.

[33] Bod 10 anotovaného rozhodnutí.

[34] Bod 14 anotovaného rozhodnutí.

[35] Tamtéž.

[36] Bod 15 anotovaného rozhodnutí.

[37] Bod 16 anotovaného rozhodnutí.

[38] Rozhodnutí Nejvyššího soudu České republiky ze dne 26. 5. 2020, sp. zn. 27 Cdo 1079/2020.

ZNAMENÁ NEOPRÁVNĚNÁ ZMĚNA POČÍTAČOVÉHO PROGRAMU TAKÉ PORUŠENÍ SMLOUVY?

Soud: Soudní dvůr Evropské unie
Věc: C-666/18 (IT Development SAS proti Free Mobile SAS)
Datum: 18. 12. 2019
Dostupnost: curia.europa.eu

Společnost IT Development poskytla společnosti Free Mobile licenci a došlo k uzavření smlouvy o údržbě počítačového programu ClickOnSite. Následně společnost IT Development podala proti společnosti Free Mobile žalobu pro porušení práv k počítačovému programu, v níž se s poukazem na licenční smlouvu domáhala náhrady škody z důvodu neoprávněné změny tohoto programu v podobě vytvoření nových formulářů. Soud prvního stupně označil nároky založené na deliktní odpovědnosti za nepřípustné. Odvolací soud poukázal na zásadu zákazu souběhu, kdy nemůže být založena smluvní odpovědnost a zároveň deliktní odpovědnost za tytéž činy a též je deliktní odpovědnost vyloučena ve prospěch smluvní odpovědnosti v případě existence platné smlouvy. Z důvodu působnosti směrnice 2004/48 o dodržování práv duševního vlastnictví, jež má být aplikována na jakékoli porušení práv duševního vlastnictví bez rozlišení, zda k porušení došlo v důsledku nesplnění smlouvy, či nikoli, se odvolací soud rozhodl vznést předběžnou otázku.

Soudní dvůr byl tázán, zda musí být směrnice 2004/48 o dodržování práv duševního vlastnictví a 2009/24 o právní ochraně počítačových programů vykládány v tom smyslu, že porušení ustanovení licenční smlouvy k počítačovému programu týkající se práv duševního vlastnictví nositele autorských práv k tomuto programu spadá pod pojem „porušení práv duševního vlastnictví“ ve smyslu směrnice 2004/48, a že tudíž musí mít uvedený nositel možnost požívat záruk stanovených touto směrnicí, bez ohledu na režim odpovědnosti použitelný podle vnitrostátního práva.[39]

[39] Srov. bod 30 anotovaného rozhodnutí.

Soudní dvůr v této souvislosti uvedl, že zákaz změny zdrojového kódu počítačového programu patří k autorským právům k počítačovému programu a ochrana takového práva je přiznána jakékoli osobě podle ustanovení vnitrostátních právních předpisů o autorském právu k těmto dílům.[40] Směrnice 2009/24 tedy neváže ochranu práv nositele autorských práv k počítačovému programu na otázku, zda tvrzené porušení těchto práv spadá pod porušení licenční smlouvy, či nikoli.[41] Taktéž i směrnice 2004/48 se vztahuje na jakékoli porušení práv duševního vlastnictví, tedy i na porušení, jež vyplývají z nesplnění smluvní podmínky týkající se využívání práva duševního vlastnictví, včetně práva autora počítačového programu.[42]

Soudní dvůr dospěl k závěru, že porušení ustanovení licenční smlouvy k počítačovému programu spadá pod pojem „porušení práv duševního vlastnictví“ ve smyslu směrnice 2004/48 o dodržování práv duševního vlastnictví.[43] Soudní dvůr též uvedl, že určení odpovědnostního režimu použitelného v případě porušení autorských práv k počítačovému programu nabyvatelem licence k tomuto programu spadá do pravomoci členských států.[44] Nositeli autorských práv ale musí být umožněno požívat záruk stanovených směrnicí 2004/48 o dodržování práv duševního vlastnictví bez ohledu na režim odpovědnosti použitelný podle vnitrostátního práva členských států.[45]

Autorka: IK

[40] Srov. bod 32 anotovaného rozhodnutí.

[41] Srov. bod 33 anotovaného rozhodnutí.

[42] Srov. bod 36 anotovaného rozhodnutí.

[43] Srov. bod 42 anotovaného rozhodnutí.

[44] Srov. bod 46 anotovaného rozhodnutí.

[45] Srov. bod 49 anotovaného rozhodnutí.

JE ON-LINE SLUŽBA SPOČÍVAJÍCÍ VE VIRTUÁLNÍM TRHU S „POUŽITÝMI“ ELEKTRONICKÝMI KNIHAMI SDĚLOVÁNÍ VEŘEJNOSTI?

Soud: Soudní dvůr Evropské unie
Věc: C-263/18 (Nederlands Uitgeversverbond a Groep AlgemeneUitgevers)
Datum: 19. 12. 2019
Dostupnost: curia.europa.eu

Skupina vydavatelů pověřila sdružení Nederlands Uitgeversverbonda Groep Algemene Uitgevers (dále jen „žalobci“), aby zajistili ochranu autorských práv, jež jim udělili nositelé těchto práv prostřednictvím výhradních licencí. Společnost Tom Kabinet Holding je jediným akcionářem společnosti Tom Kabinet Uitgeverij, která vydává knihy, elektronické knihy a databáze, a společnosti Tom Kabinet, spravující internetové stránky, na kterých začala nabízet on-line službu spočívající ve virtuálním trhu s „použitými“ elektronickými knihami. Následně Tom Kabinet nabízené služby nahradila tzv. „Toms Leesclub“, kde vystupuje jako obchodník s elektronickými knihami. Toms Leesclub svým členům nabízí po zaplacení finanční částky „použité“ elektronické knihy, které Tom Kabinet zakoupila nebo ji byly bezplatně věnovány.[46]

Žalobci podali na základě nizozemského zákona o autorském právu proti uvedeným společnostem návrh na předběžné opatření. Rechtbank Amsterdam jejich návrh zamítl. Žalobci se proti tomuto rozhodnutí odvolali u Gerechtshof te Amsterdam, který uvedené rozhodnutí potvrdil a současně Tom Kabinet zakázal nabízet on-line službu umožňující prodej protiprávně stažených elektronických knih. Žalobci následně podali u Rechtbank Den Haag žalobu, kterou se domáhali zákazu porušování autorských práv svých členů.

Nizozemský soud se obrátil na Soudní dvůr s předběžnými otázkami. Soudní dvůr se zabýval zejména otázkou, zda poskytnutí elektronické knihy

[46] Bod 24 anotovaného rozhodnutí.

k trvalému užívání prostřednictvím stažení spadá pod pojem „sdělování veřejnosti“ ve smyslu čl. 3 odst. 1 směrnice 2001/29[47], nebo pod pojem „veřejné rozšiřování“ uvedený v čl. 4 odst. 1 této směrnice a zda se případně uplatní právo na vyčerpání dle čl. 4 odst. 2 této směrnice.

Soudní dvůr uvedl, že je nesporné, že Tom Kabinet zpřístupňuje dotčená díla každé osobě, která se zaregistruje na internetových stránkách čtenářského klubu, s tím, že má k těmto dílům přístup z místa a v době, které si zvolí, takže poskytování takové služby je nutno považovat za sdělování díla ve smyslu čl. 3 odst. 1 směrnice 2001/29, přičemž není nutné, aby uvedená osoba této možnosti využila a skutečně elektronickou knihu z těchto internetových stránek získala.[48] Vzhledem k tomu nemůže být řeč ani o vyčerpání práv k dílu. Soudní dvůr tak opětovně potvrdil, že k vyčerpání práv při online distribuci dochází jen ve vztahu k počítačovým programům.[49]

Autorka: DC

JE UŽITÍ KONKRÉTNÍHO TETOVÁNÍ V POČÍTAČOVÉ HŘE PORUŠENÍM AUTORSKÉHO PRÁVA?

Soud:	District Court Southern District of New York
Věc:	Solid Oak Sketches v. 2K Games
Datum:	26. 3. 2020
Dostupnost:	https://www.documentcloud.org/documents/6819709-SolidOak.html

Take-Two Interactive Software, Inc. (dále jen „žalovaní“) je hlavní vývojář, vydavatel a prodejce video her, které vydává prostřednictvím svých dceřiných společností 2KGames, Inc. a Rockstar Games, Inc. Žalovaní každoročně vydávají upravenou verzi video hry simulující basketbalové

[47] 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.

[48] Bod 65 anotovaného rozhodnutí.

[49] Srovnej rozhodnutí SDEU ze dne 3. 7. 2012 ve věci UsedSoft, C-128/11.

utkání s realistickým zobrazením jednotlivých týmů a hráčů NBA, které mimo jiné zahrnuje i zobrazení případných tetování jednotlivých hráčů. Solid Oak (dále jen „žalobce“) tvrdí, že žalování porušili jeho autorské právo veřejným vystavením jeho děl[50] v rámci vydání upravených verzí hry 2K14, 2K15, 2K16. Jednotlivý hráči dali NBA svolení k udílení licence na vyobrazení jejich podoby třetím stranám. NBA tuto licenci udělila žalovaným.

Žalobce podal žalobu u District Court Southern District of New York (dále jen „District Court“) pro porušení ustanovení 101 a násl. amerického autorského zákona.[51] Tento návrh byl zamítnut, kdy následně žalobce doplnil svůj návrh, kdy současně žalovaní podali protinávrh. District Court návrhu žalobce opětovně nevyhověl a zamítl také obranu žalovaných v rámci řízení.

District Court se ve svém následném rozsudku zabýval zejména: a) žalobcovým návrhem týkajícím se porušení autorských práv, b) vyhověním návrhu ve prospěch žalovaných na základě výjimky z autorského práva, tzv. fair use a aplikace užití minimálního rozsahu, tzv. pravidla de minimis.

Soud řešil otázkou, zda může případné autorské právo autora tetování omezit možnost následného zachycení podoby daného člověka s tímto tetováním. Soud v rozhodnutí došel k závěru, že případná práva k tetování nemohou omezit osobu, která tetování má, v možnosti následného zachycení a zobrazení jejich podoby na veřejnosti, v televizi nebo při jiných příležitostech a že se tak jedná o implicitní licenci, pokud si toto smluvní strany dopředu nevyloučí.[52] Soud v rozsudku mimo jiné vzal v potaz, že zobrazená tetování ve video hře dosahovala od 4,4 % do 10,96 % jejich skutečné velikosti.[53] Zároveň soud rozhodl, že užití tetování ze strany žalovaných bylo v souladu s výjimkou fair use.[54]

Autorka: DC

---

[50] Jednalo se o 5 tetování, které byly vyobrazeny na hráčích Eric Bledsoe, LeBron James a Kenyon Martin.

[51] Copyright Act of 1976, 17 U.S.C.

[52] Viz str. 16 anotovaného rozhodnutí.

[53] Viz str. 13 anotovaného rozhodnutí.

[54] Viz str. 23 anotovaného rozhodnutí.

3. OSOBNÍ ÚDAJE A SOUKROMÍ

ZABAVENÍ NOSIČŮ S DATY, CHRÁNĚNÝMI ADVOKÁTNÍM TAJEMSTVÍM

Soud: Evropský soud pro lidská práva
Věc: 14704/12 (Kirdök a další proti Turecku)
Datum: 3. 12. 2019
Dostupnost hudoc.echr.int

Trojice tureckých advokátů si stěžovala na zabavení jejich elektronických dat soudním příkazem, vydaným v souvislosti s trestním stíháním jiného advokáta, se kterým trojice sdílela kancelář. Data byla okopírována z počítače, který advokáti společně používali a také z hard disku jednoho z advokátů. Advokáti požadovali vydání nebo výmaz okopírovaných dat, jelikož byla chráněna advokátním tajemstvím a nepatřila obviněnému, proto podle nich Istanbulský soudní dvůr neměl oprávnění advokátní tajemství takto omezit. Istanbulské státní zastupitelství namítalo, že ještě nebyl proveden přepis sporných dat, a tudíž není možné určit komu data patřila. Istanbulský soudní dvůr zamítl vznesený požadavek, protože předmětný soudní příkaz byl vydán v souladu se zákonem, a to ačkoli byl soud povinen podle tureckého práva neprodleně posoudit zabavené údaje a vrátit data, která jsou advokátním tajemstvím chráněna.

Stěžovatelé se proto obrátili na Evropský soud pro lidská práva (*ESLP*), aby určil, zda mohla být zabavena také data chráněná advokátním tajemstvím a zda Istanbulský soudní dvůr, i přes absenci mechanismu k filtrování elektronických důkazů, splnil svoji povinnost pečlivě ověřovat nezbytnost omezení advokátního tajemství mezi advokátem a jeho klientem.

ESLP posuzoval, zda je předmětný případ a relevantní turecké právo v souladu s čl. 8 Evropské úmluvy o ochraně lidských práv a svobod (EULP), stanovující, že každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.

ESLP shledal, že zabavení předmětných dat neodpovídalo naléhavé sociální potřebě, nebylo úměrné sledovaným legitimním cílům a nebylo nutné v demokratické společnosti, jelikož předmětná data přímo nesouvisela s podezřelým advokátem. Istanbulský soudní dvůr dále přezkumem žádosti advokátů nesplnil svoji povinnost zajistit zvláště pečlivé ověření nezbytnosti opatření údajů, které jsou chráněné advokátním tajemstvím, a proto došlo k porušení čl. 8 (právo na soukromí) a čl.13 (právo na účinný prostředek nápravy) EULP.

Autor: JK

ZÁKONNOSŤ MONITOROVANIA REZIDENČNÝCH DOMOV PROSTREDNÍCTVOM KAMIER

Soud: Soudní dvůr Evropské unie
Věc: C-708/18 (Asociaţia de Proprietari bloc M5A-ScaraA)
Datum: 11. 12. 2019
Dostupnost: curia.europa.eu

TK ako vlastník bytu v rezidenčnej budove podal žalobu na spoločenstvo vlastníkov bytov, ktoré do rezidenčnej budovy nainštalovalo viacero kamier na video monitorovanie. Kamery boli nainštalované na popud ďalších obyvateľov z dôvodu lepšieho dohľadu nad priestormi v budove, nakoľko v nej už došlo k viacerým vlámaniam a krádežiam a tiež z dôvodu, že predchádzajúce opatrenia, napr. zavedenie bezpečnostného systému vstupu do budovy, nezabránili trestným činom.[55] TK v žalobe predloženej rumunskému súdu tvrdil, že kamery porušujú jeho právo na rešpektovanie súkromného života a tiež povinnosti spoločenstva v oblasti ochrany osobných údajov.[56]

Vnútroštátny rumunský súd následne inicioval konanie o predbežnej otázke pred Súdnym dvorom EÚ.

[55] Body 19 a 20 anotovaného rozhodnutia.

[56] Bod 16 anotovaného rozhodnutia.

Aj keď rumunský súd položil SDEÚ viacero otázok, SDEÚ zhrnul, že všetky smerujú k otázke, či bránia čl. 7 f) Smernice o ochrane osobných údajov[57] a čl. 7 a 8 Charty tomu, aby vnútroštátne právo umožnilo video monitorovaniev spoločných priestoroch rezidenčných budov bez súhlasu dotknutých osôb, a to s cieľom chrániť oprávnený záujem spočívajúci v ochrane osôb a majetku.[58]

SDEÚ následne primárne analyzoval nadväzujúce ustanovenie čl. 7 f) Smernice o ochrane osobných údajov týkajúce sa legitímneho záujmu prevádzkovateľa a definoval tri podmienky jeho uplatnenia ako požiadavky zákonnosti spracovania osobných údajov bez súhlasu. Po prvé, legitímny záujem musí byť v čase spracovania aktuálny, nie hypotetický. Táto podmienka je v predmetnom prípade jednoznačne splnená, aj keď SDEÚ zdôraznil, že nie je nevyhnutné, aby už v minulosti muselo dôjsť k zásahu do majetku osôb aby išlo o aktuálny záujem[59]. Po druhé, pri aplikácii legitímneho záujmu je nevyhnutné posúdiť, či spracovanie bolo nevyhnutné a či jeho účel nebolo možné dosiahnuť použitím menej invazívnych prostriedkov a spracovaním menšieho množstva údajov. Aj tu SDEÚ skonštatoval zohľadnenie tejto podmienky, nakoľko menej invazívne prostriedky v uvedenom prípade už boli bezvýsledne použité a nakoľko kamery snímajú len relevantné priestory.[60] Po tretie je nevyhnutné vyvažovať legitímny záujem proti právam dotknutých osôb, vždy však samostatne v každom jednotlivom prípade.

SDEÚ napokon skonštatoval, že vnútroštátne právo umožňujúce video monitorovanie v rezidenčných budovách bez súhlasu dotknutých osoba účelom ochrany osôb a majetku nie je v rozpore s právom EÚ, ak toto monitorovanie spĺňa požiadavky čl. 7 f) Smernice o ochrane osobných údajov. Posúdenie splnenia týchto podmienok je však úlohou vnútroštátneho súdu.

Autorka: PV

---

[57] Smernica Európskeho parlamentu a Rady 95/46/EHS z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov.

[58] Bod 33 anotovaného rozhodnutia.

[59] Body 44 a 45 anotovaného rozhodnutia.

[60] Body 46 - 51 anotovaného rozhodnutia.

ZÁKONNOST UŽITÍ TECHNOLOGIÍ FACE RECOGNITION PŘI VSTUPU DO ŠKOL

Soud: Tribunal Administratif de Marseille
Věc: N° 1901249 (La Quadrature du Net et Autres)
Datum: 27. 2. 2020
Dostupnost: forum.technopolice.fr

Francouzský region Provence-Alpes-Côte d'Azur („PACA“) schválil testování přístupového systému založeného na technologii rozpoznávání obličejů (tzv. face recognition) na dvou středních školách.

Učinil tak, aniž by takové rozhodnutí spadalo do mezí jeho působnosti. La Quadrature du Net a další sdružení na ochranu práv proto podala správní žalobu proti zákonnosti tohoto rozhodnutí, o které rozhodoval soud prvního stupně.

PACA zdůvodňoval použití technologie face recognition zájmem na zvýšení bezpečnosti studentů a zaměstnanců školy a zjednodušení přístupu do školních prostor. Technologie totiž umožňovala přístup nejen osobám, jejichž biometrické údaje rozpoznala, ale také osobám neznámým, jejichž pohyb po prostorách následně sledovala.[61] Zákonnost takového zpracování byl opírán o právní základ souhlasu subjektů údajů,[62] přičemž pro tuto operaci zpracování nebylo získáno předchozí povolení dozorového úřadu ani nebylo provedeno posouzení vlivu na ochranu osobních údajů.

Soud měl vedle zákonnosti samotného rozhodnutí posoudit rovněž zákonnost zpracování biometrických údajů ve světle výjimek čl. 9 odst. 2 ve spojení s čl. 4 a 7 Nařízení (EU) 2016/679.[63]

Ve svém rozhodnutí soud poukázal na to, že technologie face recognition zpracovávala biometrické údaje zranitelných osob, především nezletilých, jimž je náleží nejvyšší možná ochrana. Vzhledem k nerovnému postavení stran nebyly splněny podmínky svobodného a informovaného

[61] Bod 8 anotovaného rozhodnutí.

[62] Bod 12 anotovaného rozhodnutí.

[63] Body 9-11 anotovaného rozhodnutí.

souhlasu.[64] Zlepšení bezpečnosti a přístupu do škol rovněž nelze považovat za významný veřejný zájem, jelikož takové zpracování není přiměřené.[65]

Soud na základě výše uvedených argumentů rozhodl o nezákonnosti testování technologie face recognition a napadené rozhodnutí PACA zrušil.

Autorka: AS

ODPOVĚDNOST OBJEDNATELE OBCHODNÍCH SDĚLENÍ

Soud: Městský soud v Praze
Věc: 14 A 242/2018
Datum: 7. 4. 2020
Dostupnost: nssoud.cz

Žalobce uzavřel se svým obchodním partnerem smlouvu o marketingové spolupráci – o pořádání kampaně v žalobcův prospěch.[66] V rámci této kampaně byla šířena obchodní sdělení jejich zasláním na elektronické adresy.[67] Partner byl smluvně zavázán k dodržování právních předpisů a žalobci potvrdil, že disponuje potřebnými souhlasy.[68] Úřad pro ochranu osobních údajů, v anotovaném rozsudku již v pozici žalovaného, vydal příkaz, v němž shledal žalobce vinným ze spáchání přestupku podle § 11 odst. 1 písm. a) bod 1 a 2 zákona č. 480/2004 Sb., o některých službách informační společnosti (dále jen „ZNSIS“). Žalobce se tedy podle žalovaného dopustil hromadného nebo opakovaného šíření obchodních sdělení i) bez souhlasu adresáta a těch, která ii) nebyla jasně a zřetelně označena jako obchodní sdělení. Na tomto nic nezměnil ani odpor[69] a následný rozklad.[70]

---

[64] Bod 12 anotovaného rozhodnutí.

[65] Bod 13 anotovaného rozhodnutí.

[66] Bod 52 anotovaného rozhodnutí.

[67] Srov. bod 6 anotovaného rozhodnutí.

[68] Srov. bod 15 anotovaného rozhodnutí.

[69] Bod 5 anotovaného rozhodnutí.

[70] Body 6-8 anotovaného rozhodnutí.

Žalobce v rámci své správní žaloby mimo jiné uvedl, že nebyl šiřitelem nebo odesílatelem obchodních sdělení a že není odpovědný za jednání partnera, neboť mu žádný právní předpis neukládá ověřovat to, zda jeho partner disponuje potřebnými souhlasy.[71] Soud tedy posuzoval, zda je možné za šiřitele nebo odesílatele obchodních sdělení považovat i objednatele marketingové kampaně, ačkoli nebyl jejich přímým odesílatelem.[72]

Podmínky šíření obchodních sdělení elektronickými prostředky upravuje § 7 ZNSIS a v návaznosti na něj jsou pak v § 11 stanoveny přestupky.

Soud s ohledem na smysl a účel zákona uvedl, že je za osobu, která šíří obchodní sdělení, možné považovat i tu, která toto šíření pouze iniciovala,[73] to navíc s poukazem na to, že žalobce fakticky určuje účely a prostředky zpracování osobních údajů adresátů obchodních sdělení a jako správce osobních údajů za toto tedy nese odpovědnost.[74] Klíčovou roli osoby, která zasílání iniciovala, pak soud dovodil i z čl. 13 odst. 4 směrnice č. 2002/58/ES.[75] Dále shledal, že nebyl naplněn liberační důvod ve smyslu § 21 zákona č. 250/2016 Sb. o odpovědnosti za přestupky, neboť žalobce nevynaložil veškeré možné úsilí, aby přestupku předešel.[76]

Úřad pro ochranu osobních údajů již v minulosti uvedl, že za šíření obchodních sdělení je odpovědný nejen rozesílatel, ale i jejich objednatel.[77] Anotovaný rozsudek toto staví najisto. Zároveň nijak nebrání uplatnění regresního nároku objednatele vůči rozesílateli.

Autor: JS

---

[71] Bod 15 anotovaného rozhodnutí.

[72] Body 40 a 49 anotovaného rozhodnutí.

[73] Bod 43-45 anotovaného rozhodnutí.

[74] Body 53-55 anotovaného rozhodnutí.

[75] Body 46 a 48 anotovaného rozhodnutí.

[76] Bod 60 anotovaného rozhodnutí.

[77] ÚOOÚ. *Za šíření obchodních sdělení je odpovědný nejen rozesílatel, ale i objednatel* [online]. 5. 5. 2017 [cit. 1. 6. 2020]. Dostupné z: https://www.uoou.cz/za-sireni-obchodnich-sdeleni-je-odpovedny-nejen-rozesilatel-ale-i-objednatel/d-23490

4. OSTATNÍ

FINANČNÍ PŘÍSPĚVEK NA PROGRAMY ÚSPOR A ENERGETICKÉ ÚČINNOSTI JAKO POVINNOST VEŘEJNÉ SLUŽBY

Soud: Soudní dvůr Evropské unie

Věc: C-523/18 (Engie Cartagena)

Datum: 19. 12. 2019

Dostupnost: curia.europa.eu

Předběžná otázka se týkala sporu o povahu příspěvku, který musí hradit podniky vyrábějící elektrickou energii pro účely financování národního akčního programu pro úsporu energie a energetickou účinnost, mezi společností Engie Cartagena SL a španělským Ministerio para la Transición Ecológica.

Společnost podala v roce 2014 žalobu k Audiencia Nacional (Vrchní soud s celostátní působností, Španělsko) na zrušení vyhlášky zakládající daný příspěvek. Zpochybňována byla především výše za období 2008-2012.[78] Daná vyhláška podle ní nesplňovala kritéria a zásady formulované rozsudky Soudního dvora ohledně ukládání povinnosti veřejné služby.[79] Sporný předpis byl přijat v reakci na tarifní deficit v odvětví elektřiny a měl zamezit tomu, aby financování těchto nákladů dopadalo na celou elektrickou síť.[80] Audiencia Nacional přitom konstatovala, že v rozporu s požadavky vyplývajícími z čl. 3 odst. 2 směrnice 2009/72 neuvádí nařízení s mocí zákona 14/2010 žádné upřesnění ohledně kritéria použitého pro stanovení částek povinného příspěvku.[81]

Předběžná otázka Soudnímu dvoru se týkala toho, zda uložený povinný příspěvek představuje povinnost veřejné služby ve smyslu čl. 3 odst. 2 směrnic 2003/54 a 2009/72, a pokud ano, zda je jasně vymezená, transparentní, nediskriminační a ověřitelná?[82]

---

[78] Bod 20 anotovaného rozhodnutí.

[79] Bod 21 anotovaného rozhodnutí, odkazující na rozsudky SDEU ze dne 20. 4. 2010 ve věci Federutility a další, C-265/08, a ze dne 7. 9. 2016 ve věci ANODE, C-121/15.

[80] Bod 22 anotovaného rozhodnutí.

[81] Bod 27 anotovaného rozhodnutí.

[82] Bod 29 anotovaného rozhodnutí.

Členské státy mohou uložit z důvodů obecného hospodářského zájmu podnikům působícím v elektroenergetice povinnosti veřejné služby, které se mohou týkat bezpečnosti, jakož i ochrany životního prostředí.[83] Pojem povinnosti veřejné služby, je autonomní pojem unijního práva.[84] Čl. 106 odst. 2 SFEU směřuje k nalezení rovnováhy mezi zájmem členských států využít některé podniky jako nástroje hospodářské nebo sociální politiky a zájmem Unie na dodržování pravidel hospodářské soutěže a zachování jednotnosti společného trhu.[85] Povinnost veřejné služby je v souladu se systémem zavedeným směrnicí 2009/72.[86] Povinný příspěvek neukládá dotyčným podnikům žádný požadavek (např. aby byly dodávaly určité zboží nebo poskytovaly určité služby), který by omezoval jejich svobodu jednat na trhu s elektřinou, nemůže tudíž spadat pod pojem povinnosti veřejné služby ve smyslu čl. 3 odst. 2 směrnice 2009/72.[87] Pouhá okolnost, že příjmy z povinného příspěvku jsou převáděny do fondu spravovaného IDAE, který je pověřen prováděním opatření v rámci akčního programu v oblasti úspor a energetické účinnosti, neznamená, že je uložena povinnost veřejné služby ve smyslu uvedeného ustanovení.[88]

Soudní dvůr tudíž uzavřel, že čl. 3 odst. 2 směrnice 2009/72 musí být vykládán v tom smyslu, že finanční příspěvek uložený některým podnikům vyrábějícím elektrickou energii za účelem financování programů úspor a energetické účinnosti spravovaných orgánem veřejné správy nepředstavuje povinnost veřejné služby spadající pod toto ustanovení.[89]

Autor: FK

---

[83] Bod 33 anotovaného rozhodnutí.

[84] Bod 34 anotovaného rozhodnutí, odkazující na rozsudky SDEU ze dne 21. 2. 2008 ve věci Tele2 Telecommunication, C-426/05, bod 26, a ze dne 9. 11. 2016 ve věci Wathelet, C-149/15, bod 29.

[85] Bod 40 anotovaného rozhodnutí, odkazující na rozsudky SDEU ze dne 21. 9. 1999 ve věci Albany, C-67/96, bod 103, a ze dne 7. 9. 2016 ve věci ANODE, C-121/15, bod 43.

[86] Bod 46 anotovaného rozhodnutí.

[87] Bod 51 anotovaného rozhodnutí.

[88] Bod 52 anotovaného rozhodnutí.

[89] Bod 57 anotovaného rozhodnutí.

PŘÍSTUP K INFORMACÍM ČHMÚ

Soud: Nejvyšší správní soud
Věc: 5 As 231/2018 - 77
Datum: 20. 1. 2020
Dostupnost: nssoud.cz

Datový novinář Jan Cibulka žádal od Českého hydrometeorologického ústavu („ČHMÚ“) informace o průměrné denní teplotě a srážkách ve všech měřicích stanicích za dobu, po kterou ČHMÚ tyto informace má. ČHMÚ aplikoval zákon č. 106/1999 Sb., o svobodném přístupu k informacím a odmítl informaci poskytnout s argumentem, že v omezeném rozsahu jsou již požadované informace pro veřejnost online k dispozici. V plném požadovaném rozsahu je jejich poskytnutí možné jen za úplatu, protože zdarma jsou jen pro subjekty veřejné správy. Předmětná data a databáze navíc dle ČHMÚ tvoří nehmotný majetek ve smyslu zákona č. 219/2000 Sb. Rozhodnutí ČHMÚ bylo napadeno u Městského soudu v Praze, který s interpretací zákona č. 106/1999 Sb. provedenou ČHMÚ nesouhlasil, zejména na základě argumentu, že " *informace o vývoji počasí v ČR, … mají veřejnoprávní charakter. … Úplné informace o vývoji počasí, musí být ze své podstaty přístupné na vyžádání bezplatně už jen proto, že přístup k jejich obsahu nemůže být závislý na finančních příjmech a sociálním statusu jednotlivce. … Dotčení ekonomických zájmů činnosti [ČHMÚ] nemůže být důvodem pro odepření poskytnutí informací.*"[90] Městský soud rozhodnutí správního orgánu zrušil, ten nicméně podal kasační stížnost.

NSS se však ve svém rozsudku otázce možnosti poskytnout předmětné informace vůbec nevěnoval, protože se ve svých úvahách zastavil na otázce, podle jakého zákona je celou kauzu třeba posuzovat. Právní otázkou anotovaného rozhodnutí tak je, zda mají být informace o počasí poskytovány v režimu zákona č. 106/1999 Sb., nebo v režimu zákona č. 123/1998 Sb., o právu na informace o životním prostředí.

[90] Bod 6 anotovaného rozhodnutí.

NSS zmínil ustanovení Aarhuské úmluvy, směrnici 2003/4/ES a zákon č. 123/1998 Sb. a uvedl poměrně široké vymezení, že informace o životním prostředí jsou jakékoli informace o stavu složek životního prostředí.[91] Vyžádané informace do tohoto širokého vymezení spadají.[92] Z toho důvodu je dle NSS nezbytné dodržet přísné rozdělení věcné působnosti obou informačních zákonů,[93] a to i přes jejich zjevnou podobnost.[94] NSS v závěru konstatuje, že jak ČHMÚ, tak Městský soud postupovaly podle nesprávného zákona a z toho důvodu všechna předchozí rozhodnutí ve věci zrušil a věc vrátil ČHMÚ k dalšímu řízení.

Anotované rozhodnutí je věcně zajímavé, byť nikterak nepomohlo zodpovědět otázku poskytování předmětných informací. Relativně striktní přístup NSS ukázal, že přísné rozlišování mezi zákony 106/1999 Sb. a 123/1998 Sb. je i nadále nezbytné.

Autor: JM

NEZÁKONNOST PAUŠÁLNÍHO POŽADAVKU NA ZASLÁNÍ DOKUMENTACE O ZADÁVACÍM ŘÍZENÍ V ORIGINÁLE

Soud:	Krajský soud v Brně
Věc:	31 Af 24/2018
Datum:	29. 4. 2020
Dostupnost:	na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím

Úřad pro ochranu hospodářské soutěže, v anotovaném rozsudku v pozici žalovaného, ve svém rozhodnutí shledal postup veřejného zadavatele, zde v pozici žalobce, v řízení o přezkoumání úkonů zadavatele před uzavřením smlouvy nezákonným. To konkrétně z důvodu, že žalobce žalovanému v daném řízení nezaslal dokumentaci o zadávacím řízení (konkrétně se jednalo o části zadávací dokumentace) na dotčenou veřejnou zakázku

[91] Body 25 a 26 anotovaného rozhodnutí.

[92] Bod 27 anotovaného rozhodnutí.

[93] Bod 29 anotovaného rozhodnutí.

[94] Bod 31 anotovaného rozhodnutí.

v požadované podobě. Žalobce zaslal žalovanému předmětné části dokumentace pouze v kopii, což však žalovaný vyhodnotil jako nedostatečné pro splnění zákonných podmínek uvedených v § 252 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ"). Předseda žalovaného v řízení o rozkladu výše uvedené rozhodnutí potvrdil a rozklad zamítl.[95]

Žalobce ve své správní žalobě především namítal, že je zaslání kopie dokumentace o zadávacím řízení pro účely řízení o přezkoumání úkonů zadavatele dostačující, neboť zákonná úprava požadavek originálu nestanovuje.[96] Soud se tak v anotovaném rozsudku zabýval tím, zda v řízení o přezkoumání úkonu zadavatele žalovaný může a *priori* vždy vyžadovat originály (nebo podobu jim postavenou na roveň).[97]

Ustanovení § 252 odst. 1 ZZVZ stanovuje, že je zadavatel povinen žalovanému doručit své vyjádření k obdrženému návrhu na zahájení řízení o přezkumu úkonů zadavatele, a to do 10 dnů od jeho doručení. Společně s tímto vyjádřením má být žalovanému zaslána dokumentace o zadávacím řízení nebo soutěži o návrh. Nejvyšší správní soud se pak v minulosti vyjádřil, že nevidí důvod pro neakceptace kopie listin, které mají sloužit jako důkazní prostředky před správními orgány.[98]

Soud uvedl, že forma uchovávané dokumentace není v ZZVZ nijak definována.[99] Dále poukázal na to, že pouze z důvodu, že dotčené ustanovení neobsahuje výslovné umožnění zaslat kopii, nelze usuzovat na povinnost zaslat originál,[100] a to i s odkazem na enumerativnost veřejnoprávních pretenzí.[101] Dále uvedl, že znak vysoké formalizovanosti se vztahuje pouze na zadávací řízení a není možné se na něj paušálně odvolávat i při dalších souvisejících úkonech žalovaného.[102] Z výše

[95] Body 1-5 anotovaného rozhodnutí.

[96] Viz body 6-12 anotovaného rozhodnutí.

[97] Bod 35 anotovaného rozhodnutí.

[98] Rozsudek Nejvyššího správního soudu ze dne 22. 11. 2018, č. j. 7 Azs 399/2018-34.

[99] K tomu viz blíže bod 47 anotovaného rozhodnutí.

[100] Bod 52 anotovaného rozhodnutí.

[101] Bod 54 anotovaného rozhodnutí.

[102] K tomu viz blíže bod 55 anotovaného rozhodnutí.

uvedených důvodů a s odkazem na předcházející judikaturu[103] soud označil paušální požadavek žalovaného na zasílání dokumentů ve smyslu § 252 odst. 1 ZZVZ vždy v originále (nebo podoby mu postavené na roveň) za nezákonný.[104]

Z anotovaného rozsudku vyplývá, že je dlouhotrvající praxe žalovaného, která je deklarovaná i na jeho webových stránkách,[105] v rozporu se zákonem.[106]

Autor: JS

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

---

[103] Bod 59 anotovaného rozhodnutí.

[104] Bod 61 anotovaného rozhodnutí.

[105] Úřad pro ochranu hospodářské soutěže. *V jaké podobě předávat ÚOHS dokumentaci o zadávacím řízení, je-li postup zadavatele napaden?* [online] [cit. 15. 6. 2020]. Dostupné z: https://www.uohs.cz/cs/verejne-zakazky/obrana-proti-nespravnemu-postupu-zadavatele/navrh-na-prezkoumani-ukonu-zadavatele/pozadavky-uohs-na-podobu-predkladane-dokumentace-o-zadavacim-rizeni.html.

[106] Proti anotovanému rozhodnutí byla dne 9. 6. 2020 podána kasační stížnost.

MICHNA, LUKÁŠ. PROGRAMOVÁNÍ PRO PRÁVNÍKY. PRÁVNÍKŮV PRŮVODCE MOŽNOSTMI, JAK SI SE ZNALOSTÍ ZÁKLADŮ PROGRAMOVÁNÍ USNADNIT PRÁCI A ZPŘÍJEMNIT ŽIVOT

JAN SVOBODA[1]

MICHNA, Lukáš. *Programování pro právníky. Právníkův průvodce možnostmi, jak si se znalostí základů programování usnadnit práci a zpříjemnit život.* Praha: Wolters Kluwer ČR, 2019. 176 str. ISBN 978-80-7598-659-7.

JUDr. Lukáš Michna, LL.M., Ph.D., je autorem se vzděláním v právu. Jak vyplývá nejen z tématu recenzované publikace, ale i ze strany „O autorovi" v předmětné monografii, věnuje se rovněž programování.[2]

Autor se pro sepsání této knihy vydané u nakladatelství Wolters Kluwer ČR v roce 2019 dle svého vyjádření rozhodl na základě svých zkušeností z praxe, kdy se setkával s potřebou programování.[3] Recenzovaná publikace má pojednávat o propojení programování s právnickými činnostmi a o přínosu programování pro právní praxi. Má rovněž popisovat možnosti použití webových technologií pro tvorbu aplikací.[4] Pro zhodnocení toho,

---

[1] Mgr. Jan Svoboda je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity v Brně. Vedle toho působí v mezinárodní advokátní kanceláři PricewaterhouseCoopers Legal. Kontaktní email je jan.svoboda@mail.muni.cz.

[2] Viz str. XI knihy.

[3] Viz str. XV knihy.

[4] Tamtéž.

zda kniha naplňuje v předmluvě vzbuzená očekávání, se nejdříve podívejme na její obsah a způsob zpracování.

Kniha od začátku první kapitoly čítá 159 stran a je členěna do sedmi obecných kapitol, které jsou děleny na řadu podkapitol a dalších dílčích celků. Byť takováto četnost dělení, zvláště u kratších publikací, text nezřídka spíše tříští, než aby přispívala k jeho přehlednosti, u recenzované publikace je toto členění, s ohledem na její technické zaměření, bezesporu vhodné. Recenzovaná publikace je z jazykového hlediska na poměrně dobré úrovni. Kladně lze hodnotit užívání jednoduchých obratů, kterým porozumí i laik.

Předmětná monografie obecně neobsahuje poznámky pod čarou, či obdobný způsob uvádění citací, jak bývá u jiných právnických publikací zvykem.[5] Toto je veskrze pochopitelné, neboť spíše než odborným pojednáním je kniha převážně návodem či příručkou. Seznam použité literatury a zdrojů (vč. právních předpisů, které jsou však v textu zmíněny spíše namátkou[6]), nepřesahuje jednu stranu.[7] I to je s ohledem na zaměření publikace možné očekávat. Rezervu lze nicméně spatřovat v tom, že webové stránky, které tvoří většinu zdrojů, jsou v knize zapsány pouze formou webové adresy, tedy bez dalších informací, jakými může být např. název stránky nebo datum citace. Čtenář tak nejen že nemusí mít při pohledu na daný odkaz představu, ke které stránce bude přistupovat, ale v případě, že byl její obsah změněn nebo přesunut pod jiné doménové jméno, může mít značné potíže toto zjistit či předmětný obsah dohledat.

První kapitola s názvem „Právníci, nebojte se programování!“[8] pojednává obecně o programování,[9] o tom, proč by měli právníci umět programovat,[10] dále mimo jiné o volbě programovacího jazyka[11]

[5] Recenzovaná publikace je na obálce označována jako právní monografie.

[6] Viz zejména str. 141, 145 a 151 knihy.

[7] Viz str. 156 knihy.

[8] Viz str. 3-16 knihy.

[9] Viz str. 3 knihy.

[10] Viz str. 5-7 knihy.

[11] Viz str. 11-14 knihy.

a o doporučených editorech kódu.[12] Její podkapitolu s názvem „Proč by měl umět právník programovat!“[13] pak považuji za nejzajímavější pasáž celé monografie. Autorova úvaha o programování jakožto jedné ze základních kompetencí budoucnosti, která je srovnatelná např. se znalostí cizího jazyka, je bezpochyby smysluplná a její zařazení do publikace si určitě zaslouží pozitivní hodnocení.

Michna právníkovu znalost programování spojuje zejména s možností řešení rutinních úkolů.[14] Dále uvádí, že znalost programování napomáhá porozumění činnosti používaných softwarových nástrojů a rozvoji analytického myšlení.[15] Byť lze s tímto obecně souhlasit, je možné se domnívat, že výše uvedené výhody umění programovat mohou být převáženy jinou, která v publikaci přímo uvedena není. Konkrétně se jedná o výhodu spojenou s lepším pochopením toho, čeho se v dnešní době týká velké množství právních rad, tedy počítačového programu, respektive softwaru. Právní poradenství se v dané oblasti může týkat např. licencování počítačového programu jakožto literárního autorského díla[16] nebo třeba zpracování osobních údajů automatizovaným způsobem.[17] Pochopení základů programování totiž bezpochyby může přispět k lepšímu pochopení toho, co počítačový program je a jakým způsobem k němu právně přistoupit. Je tedy škoda, že se autor v recenzované publikaci této myšlence nijak nevěnuje, neboť ta by pro řadu právníků, kteří běžně poskytují poradenství v oblasti softwarového práva (např. i jen z pohledu vkladu licence do základního kapitálu společnosti), mohla přinejmenším motivovat ke snaze o pochopení základů zdrojových kódů a souvisejících prvků.

---

[12] Viz str. 15 knihy.

[13] Viz str. 5-7 knihy.

[14] Tamtéž.

[15] Viz str. 7 knihy.

[16] Viz § 65 a násl. zákona č. 121/2000 Sb., autorský zákon.

[17] Viz čl. 2 odst. 1 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Autor se v publikaci věnuje třem základním programovacím jazykům, a to HTML[18], CSS a JavaScript.[19] Tuto volbu lze pro knihu pojednávající o základech programování, kterou recenzovaná publikace bezpochyby je, považovat za vhodnou. To nejen pro snadnou propojitelnost těchto jazyků, ale i pro jejich rozšířenost vycházející zejména z využívání těchto u webových aplikací. Při popisu volby programovacích jazyků naráží Michna na rozdíl mezi programováním a skriptováním. Čtenáři však tento rozdíl blíže nespecifikuje a zůstává u pouhého konstatování, že skriptování je *„čímsi méně vznešeným“*. Lze přitom usuzovat, že nemalá část právníku by vysvětlení rozdílu mezi těmito pojmy v recenzované publikaci ocenila.

Za velký klad publikace, který se neprojevuje jen v první kapitole, nýbrž je charakteristický pro celou knihu, lze označit konkrétní doporučení řady nástrojů[20] a rovněž uvádění zejména těch, které jsou kromě operačního systému Windows dostupné i pro MacOS a Linux.[21]

Druhá kapitola je věnována jazyku HTML,[22] třetí CSS[23] a čtvrtá základům JavaScriptu.[24] Všechny tyto kapitoly pojednávají o základech programování v daném programovacím jazyce, vč. popisu způsobu jejich vzájemného provázání. Autor ve výkladu postupuje logicky dle základních prvků daného jazyka a kromě úvodů do dané problematiky poskytuje i příklady v podobě konkrétního kódu. Lze ocenit zejména skutečnost, že autor všechny příklady kódů umístil v editovatelné podobě na webové stránky. Čtenář je tedy v rámci testování nemusí pracně přepisovat z knihy. Otázkou však zůstává, zdali by tuto skutečnost nebylo vhodné čtenáři sdělit dříve, než v samém závěru knihy. Poctivý čtenář, který se publikaci věnuje stránku po stránce, totiž může tuto informaci objevit až poté, co řadu kódů přepsal. Příklady uvedené v kapitolách dva až pět jsou vesměs určeny pro pochopení základů programování v předmětných jazycích, nikoli přímo

[18] HTML je značkovací jazyk.

[19] Viz str. 11-14 knihy.

[20] Viz např. str. 15, 16, 127 nebo 133-135 knihy.

[21] Viz např. str. 135 knihy.

[22] Viz str. 19-40 knihy.

[23] Viz str. 43-62 knihy.

[24] Viz str. 65-108 knihy.

zaměřené na právnické prostředí. Vyzdvihnout lze zejména podkapitolu pět kapitoly čtvrté, která se věnuje funkcím, vč. jejich deklarace a volání. Autor v ní danou problematiku velmi stručně shrnuje způsobem, díky kterému se čtenář v této zbytečně neztrácí.[25]

Pátá kapitola je věnována algoritmizaci,[26] šestá pokročilým možnostem programování[27] (vč. třeba využití uživatelského rozhraní Bootstrap,[28] serverového prostředí Node.js[29] či prostředí Electron[30]).

Sedmá kapitola je věnována řešení vybraných právních problémů programovou cestou a obsahuje některé výpočty s časem a výpočty týkající se financí. Tato kapitola se rozkládá na str. 141-153, přičemž jedna ze stran je prázdná a další prázdná z většiny (prázdné strany jsou v textu recenzované publikace používány pro oddělení jednotlivých celků z důvodu přehlednosti). Daná kapitola je přitom, společně s již zmíněnou třístránkovou podkapitolou nesoucí název „Proč by měl umět právník programovat?“ (str. 5-7), výjimkou v tom smyslu, že je skutečně zaměřena na právnické prostředí.

Vraťme se nyní k výše popsaným očekáváním vzbuzených na základě předmluvy a k posouzení toho, zda byla naplněna. Z výše uvedeného v této recenzi je patrné, že daná kniha popisuje využití webových technologií pro tvorbu aplikací. To navíc činí přehlednou a stručnou formou. O propojení programování s právnickými činnostmi a o přínosu programování pro právní praxi kniha sice pojednává rovněž, avšak jen v její menší části. Na tomto místě je vhodné upozornit na titul i podtitul knihy. Obojí nasvědčuje tomu, že provázání programování a právnické praxe bude v textu věnován značný prostor. Uvědomíme-li si však, že po odstranění stran 5-7 a 141-153 nám v ruce zůstane publikace, která by mohla nést název „Základy programování v HTLM, CSS a JavaScript“, je nasnadě konstatovat, že

[25] Viz str. 77-82 knihy.

[26] Viz str. 111-115 knihy.

[27] Viz str. 119-137 knihy.

[28] Viz str. 121-125 knihy.

[29] Viz str. 127-131 knihy.

[30] Viz str. 133-136 knihy.

předmětná monografie svůj potenciál vyplývající již z jejího názvu v určitých směrech nenaplňuje.

Je možné shrnout, že recenzovaná publikace je dobrým úvodem do programování. Stejně tak je třeba vyzdvihnout, že veškeré v ní uvedené informace týkající se právnického prostředí jsou věcné, podnětné a bezesporu užitečné. Lze však doporučit, aby autor v následujícím vydání knihy, neboť ta své místo na trhu nepochybně – stejně jako její případné následující vydání – má, obohatil nejen o další části věnující se úvahám o tom, proč je pro právníky dovednost programování užitečnou (bez zajímavosti přitom nejsou ani možnosti regulace kódem[31]), ale i o další příklady konkrétních kódů, které lze právníky v rámci praxe využít. Zajímavé by mohlo být představit např. způsoby pro automatické předvyplňování určitých typizovaných podání (např. vzdání se práva na odvolání pro řízení u rejstříkového soudu) na základě údajů z veřejných seznamů. Autorovi pak v každém případě patří díky za upozornění na dané téma formou knihy tohoto druhu u právnického nakladatelství a především pak v českém jazyce.

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

---

[31] Srov. LESSIG, Lawrece. *Code.* V.2. New York: Basic Books: 2006, 410 str.

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 www.revue.law.muni.cz.

RECOMMENDED EXTENT OF THE CONTRIBUTIONS:

Topic section:	30 – 80 standard pages
Discussion section:	5 – 30 standard pages
Case annotation:	2 – 10 standard pages
Book review:	1 – 5 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: 31st March

For the winter issue: 30th September

The Review of Law and Technology is a gold open access journal.

The journal and contributions are available on the journal website at www.journals.muni.cz/revue under the terms of public license Creative Commons Attribution-ShareAlike 4.0 International (Available at: http://creativecommons.org/licenses/by-sa/4.0/legalcode).

Contributions are included into respective electronic legal information systems operated by Wolters Kluwer ČR, a. s. (ASPI), Nakladatelství C. H. BECK, s. r. o. (beck-online.cz) and ATLAS consulting spol. s r. o. (CODEXIS).

Detailed information about the publication process, structure and format of the contributions, the review process and copyright are available in the “For the authors” section at www.revue.law.muni.cz. Further information is available upon request addressed to editorial staff (contact e-mail revue@law.muni.cz).

REVIEW OF LAW AND TECHNOLOGY

VOLUME 11 | YEAR 2020 | NUMBER 21

DISCUSSION

Martin Eliášek, Jakub Kól, Miloš Švaňa: Automatic Classification of Semantic Units in Case Law 3

Adam Jareš: Cryptocurrencies and Civil Law 21

Ivana Kudláčková: Cyber Weapon: Approaches to its Definition 47

Pavel Mates: Right to Digital Services 73

Rostislav Sliwka: Online Content-Sharing Service Provider according to Directive (EU) 790/2019 91

Veronika Žolnerčíková: Proving Causal Nexus for Damage Caused by Connected Autonomous Vehicles..... 129

ANNOTATION

Jaromír Fronc: Google, the Right to Be Forgotten and the EU Charter of Fundamental Rights 153

Jakub Harašta: No One Can Own the Law 161

D. Collett, F. Kasl, J. Klodwig, I. Kudláčková, P. Loutocký, J. Míšek, A. Stárková, J. Svoboda, P. Vydrová, V. Žolnerčíková: Overview of the Current Case Law I/2020 169

BOOK REVIEW

Jan Svoboda: Michna, Lukáš. Programování pro právníky: Právníkův průvodce možnostmi, jak si se znalostí základů programování usnadnit práci a zpříjemnit život 195

Review of Law and Technology
Peer-reviewed scientific journal for technological areas of law and jurisprudence, listed in the List of non-impact peer-reviewed journals published in the Czech Republic and ERIH PLUS database.
Only the contributions submitted for the Discussion and Topic sections are peer-reviewed.
Published bi-annually. This issue was published on 30th June 2020.
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. Matěj Myška, Ph.D., Institute of Law and Technology, Faculty of Law, Masaryk University, Veveří 70, 611 80 Brno, Czech Republic, tel: +420 549494751, fax: +420 541210604, e-mail: revue@law.muni.cz | www.revue.law.muni.cz
Deputy editor-in-chief: Ing. Mgr. František Kasl
Editorial Staff: JUDr. Mgr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek, Ph.D.
Editorial Secretary: Anna Blechová
Editor: Anna Blechová
Editorial Board: doc. 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, doc. 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., 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, 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 VIII“, MUNI/A/0989/2019.
Journal © Masaryk University, 2020

KARLOVARSKÉ PRÁVNICKÉ DNY

PRESTIŽNÍ CENA 2020

pro nejlepší právnický časopis v České a Slovenské republice

Anketní lístek

	Časopis Recenzované časopisy (R)		Vydavatel		Hodnoťte 1-10 úroveň ---------- Odborná/informační	
1	Acta Iuridica Olomucensia	(R)	Univerzita Palackého v Olomouci	ČR		
2	Ad Notam		Notářská komora ČR	ČR		
3	Ars notaria		Notárska komora SR	SR		
4	Bulletin advokacie/Advokátní deník	(R)	Česká advokátní komora	ČR		
5	Bulletin slovenskej advokácie	(R)	Slovenská advokátska komora	SR		
6	Bulletin Stavební právo		Česká společnost pro stavební právo	ČR		
7	Časopis pro právní vědu a praxi	(R)	Masarykova univerzita, Brno	ČR		
8	International and Comparative Law Review	(R)	Univerzita Palackého v Olomouci	ČR		
9	Jurisprudence	(R)	Wolters Kluwer ČR, a. s., a PF UK	ČR		
10	Justičná revue	(R)	Ministerstvo spravodlivosti SR	SR		
11	Kriminalistika	(R)	Ministerstvo vnitra ČR	ČR		
12	Obchodní právo	(R)	Wolters Kluwer ČR, a. s.	ČR		
13	Obchodněprávní revue	(R)	C. H. Beck	ČR		
14	Právněhistorické studie	(R)	PF Univerzita Karlova v Praze	ČR		
15	Právní rádce		Economia, a. s.	ČR		
16	Právní rozhledy	(R)	C. H. Beck	ČR		
17	Právník	(R)	Ústav státu a práva AV ČR	ČR		
18	Právny obzor	(R)	Ústav štátu a práva SAV	SR		
19	Právo a rodina		Wolters Kluwer ČR, a. s.	ČR		
20	Soukromé právo		Wolters Kluwer ČR, a. s.	ČR		
21	Revue církevního práva	(R)	Společnost pro církevní právo	ČR		
22	Revue pro právo a technologie	(R)	Masarykova univerzita Brno	ČR		
23	Soudce		Soudcovská unie ČR	ČR		
24	Soudní rozhledy	(R)	C. H. Beck	ČR		
25	Správní právo	(R)	Ministerstvo vnitra ČR	ČR		
26	Státní zastupitelství	(R)	Wolters Kluwer ČR, a. s.	ČR		
27	Súkromné právo		Wolters Kluwer SR s. r. o.	SR		
28	Trestněprávní revue	(R)	C. H. Beck	ČR		
29	Trestní právo	(R)	Wolters Kluwer ČR, a. s.	ČR		
30	Zo súdnej praxe	(R)	Wolters Kluwer SR s. r. o.	SR		
31	Zpravodaj Jednoty českých právníků		Jednota českých právníků	ČR		
32	Epravo		EPRAVO.CZ, a. s.	ČR		
33	Právní prostor		ATLAS consulting spol. s r. o.	ČR		
34	Jiné právo		Kolektiv autorů (blog)	ČR		

Hodnoťte výlučně na základě osobní znalosti a srovnání, není nutné hodnotit každý časopis. Zvlášť hodnoťte odbornou a informační úroveň přidělením bodů od 1 do 10, kdy 1 bod představuje dle Vás nejnižší možnou úroveň a 10 nejvyšší úroveň.
Současně Vám lze navrhnout pravomocný rozsudek publikovaný v období od 1. 5. 2019 do 28. 2. 2020 na cenu Pocta judikátu:
Soud…….…….. sp. zn. …….. ze dne…….……

Anketní lístek prosíme zaslat poštou nejpozději do 20.10. 2020, per e-mail do 14:00 hod. 23.10.2020 na adresu casopis@kjt.cz, případně vyplnit na www.kjt.cz, zde je zveřejněn i Statut této ceny. Obdržené anketní lístky do 30.9. 2020 budou slosovány o věcné ceny (právnickou literaturu, včetně i účasti na XXVIII. Konferenci či na vyhlášení ceny na slavnostní recepci v rámci konference).

Podpisem či odesláním souhlasím s uchováním těchto údajů po dobu dvou let společností výlučně pro účely zpracování a hodnocení ankety a zároveň prohlašuji, že jsem anketní lístek vyplnil/a osobně dle svého nejlepšího přesvědčení.

Jméno, příjmení, titul…….Profese……..….
Adresa sídla……Tel……..E-mail……..….....

Podpis……..

Při el. vyplnění (bez vlastního podpisu) zašlete ze svého vlastního e-mailu uvedeného ve Vašich veřejných kontaktech.

MUNI
LAW

LL.M. v právu informačních a komunikačních technologií

Moderní odborné vzdělávání, atraktivní zaměření

Mezinárodně uznávaný program LL.M. v právu informačních a komunikačních technologií je úzce zaměřené dvouleté postgraduální studium určené pro zájemce o právní aspekty informačních a komunikačních technologií. Cílovou skupinou programu jsou praktikující právníci všech právních profesí se zájmem o informační a komunikační technologie. Díky volitelnému propedeutickému modulu je program určen též zájemcům bez právnického vzdělání - IT specialistům, manažerům v oboru ICT, bezpečnostním expertům, vedoucím pracovníkům veřejné správy aj.

Elitní pracoviště a odborníci s mezinárodním renomé – předpoklad kvalitního vzdělávání

Program LL.M. je odborně zajišťován a garantován **Právnickou fakultou Masarykovy univerzity** a za jeho realizaci odpovídá **Ústav práva a technologií**. Tento ústav byl na Právnické fakultě zřízen v roce 2010 jako první odborné pracoviště v České republice zaměřené na výzkum a výuku v oblastech právní úpravy pokročilých technologií. Během své existence si ústav vybudoval v oboru práva informačních a komunikačních technologií mezinárodní renomé a stal celoevropsky uznávanou institucí. Vedle vědecké a pedagogické činnosti ústav úzce spolupracuje s českými a evropskými justičními orgány, bezpečnostními sbory, státními orgány, špičkovými advokátními kancelářemi a poradenskými společnostmi.

Povinné moduly

- Akademické psaní a právní kontext
- Normativní systémy v kyberprostoru
- Soukromé právo ICT
- Veřejné právo ICT
- Ochrana soukromí a osobních údajů
- Duševní vlastnictví on-line
- Elektronické důkazy
- Softwarové právo
- Kyberkriminalita
- Právo e-commerce
- Informační technologie v právní praxi

Volitelné moduly

- Kryptografie a bezpečnostní technika
- Právo kybernetické bezpečnosti
- On-line řešení sporů
- eGovernment a eJustice
- Evropské a mezinárodní právní informační systémy

Další informace

Podrobné informace o programu naleznete na **www.llm.law.muni.cz**, případně je poskytne

Mgr. Lenka Sochorová (Lenka.Sochorova@law.muni.cz)

Obsah a zaměření programu – moderní informační a komunikační technologie a jejich právní aspekty, úzká specializace

Právo informačních a komunikačních technologií se dotýká řady oblastí soukromého a veřejného práva. Neopomenutelný je též jeho evropský a mezinárodní rozměr. Moduly studijního programu jsou zaměřeny tak, aby reflektovaly aktuální praktické problémy právní regulace vývoje a použití pokročilých informačních a komunikačních technologií. Cílem programu je předat maximum znalostí a praktických dovedností z tohoto vysoce specializovaného oboru.

Personální zabezpečení

Odborným garantem programu je **Radim Polčák**, vedoucí Ústavu práva a technologií. Výuku v programu zajišťují členové Ústavu práva a technologií a zástupci dalších odborných pracovišť Právnické fakulty a Fakulty informatiky Masarykovy univerzity. Na výuce se ve značné míře podílejí též špičkoví odborníci z právní praxe. Mezi lektory programu jsou: **Josef Donát** (ROWAN LEGAL), **Jaroslav Fenyk** (PrF MU), **Tomáš Gřivna** (PrF UK), **Jan Hajný** (VUT), **Jakub Harašta** (PrF MU) **František Korbel** (Havel & Holásek), **Josef Kotásek** (PrF MU), **Zdeněk Kučera** (Baker & McKenzie), **Matěj Myška** (PrF MU) a další.

Cena

Cena za semestr je stanovena následovně:

- pro absolventy právnických fakult: 37 500 Kč (bez DPH)
- pro ostatní zájemce: 40 500 Kč (bez DPH) – cena zahrnuje odborný kurs propedeutického základu pro neprávníky

Diskuze

Martin Eliášek, Jakub Kól, Miloš Švaňa: **Automatická klasifikace významových celků v judikatuře**

Adam Jareš: **Kryptoměny a občanské právo**

Ivana Kudláčková: **Kybernetická zbraň: Přístupy k její definici**

Pavel Mates: **Právo na digitální služby**

Rostislav Sliwka: **Poskytovatel služeb sdílení obsahu online dle směrnice (EU) 790/2019**

Veronika Žolnerčíková: **Prokazování příčinné souvislosti u škod způsobených propojenými autonomními vozidly**

Anotace

Jaromír Fronc: **Google, právo být zapomenut a Listina základních práv EU**

Jakub Harašta: **Nikdo nesmí vlastnit právo**

D. Collett, F. Kasl, J. Klodwig, I. Kudláčková, P. Loutocký, J. Míšek, A. Stárková, J. Svoboda, P. Vydrová, V. Žolnerčíková: **Přehled aktuální judikatury I/2020**

Recenze

Jan Svoboda: **Michna, Lukáš. Programování pro právníky: Právníkův průvodce možnostmi, jak si se znalostí základů programování usnadnit práci a zpříjemnit život**

MUNI PRESS