25

REVUE PRO PRÁVO A TECHNOLOGIE

Ústav práva a technologií Právnické fakulty Masarykovy univerzity

Ročník 13 / Rok 2022 / Číslo 25

Revue.law.muni.cz

XIV. národní konference | 15. - 16. září 2022, Právnická fakulta, MUNI, Brno

České právo a informační technologie 2022

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

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

Pořadatel konference vyzývá zájemce o aktivní účast, aby hlásili své příspěvky do některé z odborných sekcí. Rozšířený abstrakt v rozsahu 1-2 stran obsahující strukturu příspěvku, výzkumnou otázku a zásadní myšlenky, které budou v prezentaci představeny, posílejte do **31. 7. 2022** na adresu **cpit@law.muni.cz**.
O přijetí příspěvku k prezentaci bude rozhodnuto do 15. 8. 2022.

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

Další informace na webu cpit.law.muni.cz

Předběžný program konference

Čtvrtek 15. září 2022

plenární panelová diskuse

Akt o umělé inteligenci (AI Act)

Moderuje: Radim Polčák
Panelisté: TBC

paralelní sekce

Aktuální otázky autorského práva

Moderuje: Matěj Myška
národní transpozice Směrnice o autorském právu na jednotném digitálním trhu; upload filtry; uživatelská práva; práva nakladatelů; text a data mining; digitalizace kulturního dědictví; e-learning; umělá inteligence a autorské právo; kolektivní správa práv; ochrana software; ochrana prostých dat; vymáhání autorských práv

Právní informatika

Moderuje: Jakub Harašta
experimenty s uživateli; právní informatika; strojové učení; získávání právních informací

Právní otázky autonomních systémů

Moderuje: Veronika P. Žolnerčíková
bezpečnost (safety & security); odpovědnost; připravované regulatorní rámce; transparentnost; neosobní data; vytěžování big data

Právní informační systémy

Moderuje: Tereza Novotná
novinky v právních informačních systémech

Pátek 16. září 2022

paralelní sekce

Ochrana osobních údajů a soukromí

Moderuje: Jakub Míšek
osobní údaje; e-privacy; GDPR; data protection by design & by default; princip odpovědnosti správce; hodnocení dopadů zpracování; oprávněný zájem správce údajů; policejní směrnice; přímé nároky

Elektronické důkazy

Moderuje: Václav Stupka
elektronické důkazy; mezinárodní spolupráce při zajišťování elektronických důkazů; data retention

Elektronizace státní správy, online soudnictví

Moderuje: Pavel Loutocký
elektronický spis; elektronická správa dat; online komunikace v rámci státní správy (asynchronní komunikace, videopřenosy apod.); moderní přístupy k rozhodování sporů; online platformy a ochrana práv; digitální služby; elektronický dokument; digitální obsah

Kybernetická bezpečnost a obrana

Moderuje: František Kasl
kybernetické bezpečnostní incidenty; certifikace; povinnost hlášení; kritické informační infrastruktury; odpovědnost státu; nestátní aktéři; přičitatelnost; protiopatření; kybernetické zbraně; použití síly; kybernetický útok; Talinský manuál

REVUE PRO PRÁVO A TECHNOLOGIE

ROČNÍK 13 | ROK 2022 | ČÍSLO 25

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. 2022.
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: doc. 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: JUDr. Ing. František Kasl, Ph.D.
Redakce: JUDr. Mgr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek, Ph.D.
Tajemnice redakce: Anna Blechová
Editoři: Anna Blechová, Martin Erlebach
Redakční rada: prof. JUDr. Radim Polčák, Ph.D. (čestný předseda), JUDr. Zuzana Adamová, Ph.D., prof. JUDr. Michael Bogdan, B.A., LL.M., jur. dr. (Lund), JUDr. Marie Brejchová, LL.M., JUDr. Jiří Čermák, 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., doc. JUDr. Matěj Myška, Ph.D., Mgr. Antonín Panák, LL.M., Mgr. Bc. Adam Ptašnik, Ph.D., JUDr. Danuše Spáčilová, JUDr. Eduard Szattler, Ph.D., JUDr. Tomáš Ščerba, Ph.D.
Grafická úprava: Mgr. Martin Loučka, doc. JUDr. Matěj Myška, Ph.D.
Tisk: POINT CZ, s.r.o., Milady Horákové 20, 602 00 Brno
Vydání tohoto čísla časopisu Revue pro právo a technologie bylo financováno z projektu „Právo a technologie X“, MUNI/A/1484/2021.

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 Diskuze:	5 – 30 normostran
Sekce Anotace:	2 – 10 normostran
Sekce Essays:	5 – 10 normostran
Sekce Recenze:	1 – 5 normostran
Sekce Téma:	30 – 80 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: 28. února

Do zimního čísla: 31. srpna

Časopis se hlásí k politice otevřeného přístupu realizovaného zlatou cestou.

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

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

Detailní informace ohledně publikačního procesu, struktury a formálních náležitostí příspěvků, recenzního řízení a autorských práv jsou dostupné v sekci „Pro autory“ na webu časopisu 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/RPT2022-1-1

KRIMINALISTICKÉ A TRESTNĚPRÁVNÍ ASPEKTY DETEKCE LŽÍ ANALÝZOU TZV. MIKROEXPRESÍ[1]

JAN PROVAZNÍK[2]

ABSTRAKT

Tento článek se zaměřuje na tzv. analýzu mikroexpresí a její použitelnost v trestním řízení. Nejprve představuje základy a vývoj této metody a současný stav poznání včetně rozdílů, které ohledně této metody přinesl rozvoj informačních technologií. Následně článek pokračuje ke srovnání této metody s fyziodetekčním vyšetřením (tj. standardní metodou založenou na využití detektoru lži) co do jejich podstat, právních omezení důkazní hodnoty jejich výstupů a jejich důvodů. Článek končí provedením vlastní analýzy použitelnost metody analýzy mikroexpresí v trestním řízení a podmínek, na kterých závěr o použitelnosti spočívá.

KLÍČOVÁ SLOVA

Mikroexprese; fyziodetekční vyšetření; zákaz donucení k sebeobvinění; důkazní použitelnost

[1] Tento článek vznikl v rámci projektu č. VJ01010084 Elektronické důkazy v trestním řízení realizovaného v programu Strategická podpora rozvoje bezpečnostního výzkumu ČR 2019-2025 (IMPAK-1).

[2] JUDr. Jan Provazník, Ph.D., je odborným asistentem na Katedře trestního práva Právnické fakulty Masarykovy univerzity, odborným asistentem Centra vzdělávání, výzkumu a inovací v informačních a komunikačních technologiích Fakulty informatiky Masarykovy univerzity a asistentem místopředsedy Ústavního soudu České republiky. Kontaktní e-mail: jan.provaznik@law.muni.cz. Tento článek nevyjadřuje oficiální stanovisko žádné z uvedených institucí a obsahuje toliko osobní názory autora.

ABSTRACT

This article focuses on a so-called micro-expression analysis and its applicability in a criminal procedure. At first, it presents foundations and development of this method and its current state of art, including the difference information technologies have made thereto. Then it proceeds to a comparison of the said method with a physio-detection examination (i.e. common lie detection method with the use of a lie detector) in the terms of their natures, legal limitations for the evidentiary value of their outcomes including their reasons. It finishes with an own analysis of applicability of the method of micro-expression analysis in criminal proceedings and conditions upon which the conclusion lies.

KEY WORDS:

Micro-expressions; Physio-detection Examination; Privilege Against Self-incrimination; Evidentiary Applicability

1. ÚVOD

Metoda detekce lži tzv. fyziodetekčním vyšetřením[3] je součástí kriminalistického instrumentária již několik desítek let,[4] byť její důkazní použitelnost v trestním řízení rozhodovací praxe soudů dlouhodobě a ustáleně vylučuje,[5] proto její výsledky lze využít toliko jako operativní informace, resp. jako součást operativně pátrací činnosti.[6] Tento nekompromisní přístup soudů je odůvodňován jednak jistou skepsí ohledně spolehlivosti této metody,

[3] Srov. DOHNALOVÁ, Zuzana; ŠTĚPÁNKOVÁ, Dana; NĚMEC, Miroslav. In: NĚMEC, Miroslav a kol. Teorie a metodologie kriminalistiky pro magisterské studium II II. Praha: Abook, 2019, s. 17.

[4] NĚMEC a kol. (2019), *op. cit.*, s. 22nn.

[5] Srov. např. rozhodnutí Nejvyššího soudu České republiky ze dne 25. 3. 1992, sp. zn. 6 To 12/92 (publ. na s. 26 pod č. Rt 8/1993 v č. 1-2 roč. 1993 Sbírky soudních rozhodnutí a stanovisek Nejvyššího soudu), usnesení Nejvyššího soudu České republiky ze dne 1. 7. 2009, sp. zn. 3 Tdo 737/2009, usnesení Nejvyššího soudu ze dne 14. 4. 2020, sp. zn. 6 Tdo 347/2020, usnesení Ústavního soudu ze dne 10. 3. 2015, sp. zn. II. ÚS 3651/13, usnesení Vrchního soudu v Olomouci ze dne 8. 12. 2011, sp. zn. 6 To 100/2011, usnesení Nejvyššího soudu ze dne 31. 10. 2018, sp. zn.8 Tdo 993/2017, usnesení Nejvyššího soudu ze dne 5. 8. 2020, sp. zn. 7 Tdo 749/2020, aj.

jednak obavou o její slučitelnost s ochranou základních lidských práv osoby, která ji je podrobena.[7]

V posledních letech však díky technologickému rozmachu automatického zpracování dat došlo k podstatnému posunu ve vývoji metod detekce lži, spočívající v analýze tzv. mikroexpresí, tedy drobných, lidskými smysly téměř nepozorovatelných změn ve výrazu tváře či jiných vnějších projevů pozorované osoby, které nejsou vůlí ovladatelné.

Moderní informační technologie umožnily zkoumání těchto mikroexpresí s nebývalou důkladností a podrobností zcela nemožnou v dobách prvních polygrafů, nadto se oproti nim podstatně změnil i způsob, jímž zasahují do osobní sféry vyšetřované osoby. Nabízí se tedy otázka, zda z hlediska důkazní využitelnosti výstupů této metody v trestním řízení k usvědčení pachatele (ale, což nelze opomíjet, i k očištění nevinného obviněného) bude na místě přidržet se závěrů platných pro fyziodetekční vyšetření, či zda se zde otevírá prostor k odlišnému přístupu.

Cílem tohoto článku je představit metodu detekce lži analýzou mikroexpresí z pohledu kriminalistického a trestněprávního (důkazního), k čemuž bude zapotřebí věnovat se hned třem dílčím celkům. Prvý bude obsahovat shrnutí relevantních závěrů odborné literatury o podstatě této metody a její spolehlivosti, druhý rozbor využitelnosti dosavadně užívaných metod detekce lži (tedy tzv. fyziodetekčního vyšetření) a třetí přinese polemiku o tom, zda tato metoda nemůže narušit mnoholeté doktrinální dogma o nepoužitelnosti výstupů z detektoru lži jakožto důkazu v trestním řízení (přinejmenším ve stadiu řízení před soudem).

2. PODSTATA METODY ANALÝZY MIKROEXPRESÍ

Podstata této metody je vcelku jednoduše pochopitelná. Je notorietou, že lidé při interakci s vnějším světem vysílají řadu různých signálů

[6] Srov. např. usnesení Ústavního soudu České republiky ze dne 10. 3. 2015, sp. zn. II. ÚS 3651/13; usnesení Ústavního soudu České republiky ze dne 23. 8. 2016, sp. zn. II. ÚS 265/16, bod 11; či usnesení Nejvyššího soudu ze dne 14. 4. 2020, sp. zn. 6 Tdo 347/2020, bod 38.

[7] Srov. např. MUSIL, Jan; KONRÁD, Zdeněk; SUCHÁNEK, Jaroslav. Kriminalistika. 2. přepracované vydání. Praha: C. H. Beck, 2004, s. 106.

prostřednictvím vnějších projevů svého těla (zpravidla pohyby, ale např. i změna barvy v důsledku změny prokrvenosti drobných povrchových cév, změna v pachu vyvolaná intenzivním pocením, rozšíření zornic, úsměv atd.), které mají určitou komunikační hodnotu (je v nich obsažena informace užitečná z hlediska interakce s jinými lidmi) a jsou dekódovatelné třetí osobou,[8] přičemž ne všechny z nich podléhají volní kontrole osoby, která je vysílá.[9] Některé tyto signály pak rovněž nelze bez pomoci vnímat pouhým pozorováním,[10] či dokonce ani žádným jiným lidským smyslem bez (a to jak pro původce, tak pro toho, kdo je přijímá).[11]

Celá metoda analýzy mikroexpresí tak stojí na postulátu, že existují takové signály, které doprovází lidský komunikační akt a zároveň splňují podmínky, že:

- jsou běžnými lidskými smysly postřehnutelné jen velmi obtížně či zcela nepostřehnutelné;
- je lze spolehlivě rozpoznat, zachytit, zaznamenat a vyhodnotit s použitím speciální snímací a výpočetní technologie;
- osoba, která je vysílá, je volně nedokáže kontrolovat ani ovlivnit či je toho schopna jen s mimořádnými obtížemi;
- mají výpovědní hodnotu ohledně pravdivosti sdělení komunikačního aktu, který doprovází.[12]

Jinými slovy, tato metoda počítá s tím, že lidé doprovází svou řeč či jinou přímou komunikaci (např. gesta, posunky atd.) drobnými, velmi krátkými pohyby v obličeji (případně v jiných částech těla, primárně však tuto

[8] Tak např. vztyčí-li na nás někdo palec směrem nahoru, zatímco zbytek prstů je stále pokrčen v pěst, registrujeme tento pohyb a připisujeme mu význam gesta značícího souhlas či ocenění, pokryje-li něčí tvář či dekolt ruměnec, je to pro nás postřehnutelná a rozlišitelná změna vizáže, kterou považujeme za projev studu, nervozity atd.

[9] Např. pocení či zvýšený svalový tonus, v některých případech i tremor.

[10] Např. zrychlení tepu v důsledku radosti či napětí.

[11] Např. změna v okysličení krve v očekávání nějaké okamžité fyzické akce při pocitu ohrožení, zvýšení krevního tlaku v důsledku iritace atd.

[12] Srov. např. LI, Xiaobai; HONG, Xiaopeng; MOILANEN, Antti; HUANG, Xiaohua; PFISTER, Tomas; ZHAO, Guoying; PIETIKÄINEN, Matti. Towards Reading Hidden Emotions: A Comparative Study of Spontaneous Micro-Expression Spotting and Recognition Methods. In: IEEE Transactions on Affective Computing, 2019, roč. 9, č. 4, s. 565nn.

metodu zajímá právě obličejová část hlavy), které se stabilně a spolehlivě liší podle toho, zda daná osoba mluví pravdu, mlží, či dokonce přímo lže.

2.1 PODSTATA MIKROEXPRESÍ

Mikroexprese (mikrovýrazy) jsou velmi krátká vyjádření emocí v obličeji člověka, která se objevují mimo jiné tehdy, když mluvčí musí lhát v situacích, v nichž mu jde o hodně (tzv. *high stakes situation*).[13] Pouhým okem jsou mikroexprese postřehnutelné jen s vynaložením velkého úsilí, neboť trvají zlomky vteřiny (v různých zdrojích se uvádí pohyby kratší než 1/5, 1/4, 1/3 či dokonce i 1/2 vteřiny[14] (tedy 200, 250, 333 či 500 ms), což je v porovnání s makroexpresemi (normálním výrazem emoce v obličeji), trvajícími cca 3/4 s až 2 s (750 až 2000 ms),[15] velice krátký interval. Podrobnější zkoumání délky mikroexpresí pak přineslo závěry, že vhodnějším pojetím není pouhé „zastropování" délky pohybu, ale stanovení intervalu, konkrétně cca 170 - 500 ms (tedy cca 1/6 až 1/2 s) celkové délky, či dokonce jen 65-260 ms (tedy cca 1/15 až 1/4 s) délky nástupu mikroexprese (tj. při rozlišování fází mikroexprese na nástup – *onset*, vrchol – *apex* a ústup – *offset*).[16]

Rozdíl mezi makroexpresemi a mikroexpresemi přitom v zásadě není ve způsobu vyjádření emoce, ale právě v délce jeho trvání. I mikroexprese tedy představuje plnohodnotný projev dané emoce „se vším všudy" (byť se uvádí, že jde o vyjádření s nedostatečnou svalovou kontrakcí) se specifickými pohyby v určitých místech obličeje, zejména v oblasti očí, obočí, nosu

[13] Jde spíše o předpoklad, že v takovýchto situacích se tento jev vyskytuje častěji, což má forenzně značný potenciál. Srov. např. HURLEY, Carolyn M.; ANKER, Ashley E.; FRANK, Mark G.; MATSUMOTO, David; HWANG, Hyisung C. Background Factors predicting accuracy and improvement in micro expression recognition. In: Motivation and Emotion. 2014, roč. 38, č. 5, s. 701.

[14] K přehledu zdrojů srov. YAN, Wen-Jing; WU, Qi, LIANG, Jing; CHEN, Yu-Hien; FU, Xiaolan. How Fast are the Leaked Facial Expressions: The Duration of Micro-Expressions. In: Journal of Nonverbal Behavior. 2013, roč. 37, s. 218.

[15] TAKALKAR, Madhumita; XU, Min; WU, QUIANG; CHACZKO, Zenon. A survey: facial micro-expression recognition. In: Multimedia Tools and Applications, 2018, roč. 77, s. 19302.

[16] YAN, WU, LIANG a CHEN, (2013), s. 229.

a úst,[17] jen se tak děje na mnohem kratší dobu než u makroexprese (tedy normálního vyjádření emoce tak, jak jsme na ně v běžné komunikaci zvyklí).[18] Jelikož projevy základních emocí (překvapení, strach, znechucení, pohrdání, hněv, radost, smutek) jsou v zásadě univerzální a ustálené,[19] zachycení mikroexprese dokáže odhalit nesoulad mezi obsahem sdělení a emocionálním stavem komunikátora (osoby, která dané sdělení činí), který mu neodpovídá.

Celá metoda analýzy mikroexpresí vychází ze závěrů práce dvojice psychologů Paula Ekmana a Wallace V. Friesena představené již koncem 60. let 20. století, podle níž při snaze ovládnout projevy emocí zračících se v obličeji, potlačit je či zamaskovat člověku unikají na velice krátké časové úseky mikrovyjádření jeho skutečných emocí, které při dostatečném tréninku lze pozorovat.[20] Na svém počátku tak tato metoda počítala s předpokladem, že mikroexprese budou zachytávat a analyzovat zvlášť vyškolení odborníci svými vlastními smysly, tedy využití informačních technologií se nepředpokládalo. To představuje stěžejní rozdíl mezi začátky této metody a současností, v níž se naopak analýza mikroexpresí stala doménou umělé inteligence a strojového učení.

Vysvětlení tohoto jevu zmíněnou autorskou dvojicí lze velmi zjednodušeně shrnout tak, že již v nejranějším stádiu vývoje lidského jedince si osvojujeme určitý způsob vyjádření emocí doprovázející naše snahy o uspokojení základních potřeb (ukojení hladu atd.). Tato prvotní vyjádření emocí jsou časem potlačena a zůstávají z nich jen určitá rezidua, která již neplní svou původní funkci, ale stále v našem chování na zlomek vteřiny

[17] Srov. ZHAO, Yue; XU, Jiancheng. An Improved Micro-Expression Recognition Method Based on Necessary Morphological Patches. In: Symmetry. 2019, roč. 11, č. 4, s. 498.

[18] EKMAN, Paul. Telling Lies. Clues to Deceit in the Marketplace, Politics and Marriage. Londýn, New York: W. W. Norton & Company, 1991, s. 129.

[19] Srov. např. ALEXA, Gianina; ANDELIN, Emanuel; FEHER, Tiberiu. The Importance of Facial Micro-Expressions and Nonverbal Behavior in Psychological Evaluation. In: European Review of Applied Sociology. 2013, roč. 6, č. 7, s. 52nn.

[20] EKMAN Paul; FRIESEN, Wallace V. Nonverbal Leakage and Clues to Deception. In: Psychiatry. Journal for the Study of Interpersonal Processes. 1969, roč. 32, č. 1, s. 97.

probleskávají, vyjadřujeme-li základní emoce, s nimiž jsou spojené, a to mimoděk, neboť si je ani neuvědomujeme, resp. se na ně nezaměřujeme.[21]

Kromě toho, že si některá vyjádření některých emocí (štěstí, strach, hněv, znechucení, smutek a tíseň[22]) neuvědomujeme, jsou navíc i mimovolní, takže je nedokážeme ovládnout na povel. Stejně tak některé obličejové svaly prakticky nelze volně ovládat (nebo jen s mimořádným obtížemi), přičemž některé z nich se mimovolně aktivují při určité emoci (např. svěšení koutků dolů bez pohnutí svalů brady je prý téměř nemožné bez stovek hodin cviku, automaticky k němu však dochází, pociťuje-li člověk smutek, lítost či žal).[23]

Možnosti člověka ovládat různé obličejové svaly při předstírání určitých emocí, či naopak jejich mimovolní aktivaci při pocítění skutečné odpovídající emoci byla věnována pozornost i v dalších desetiletích a dřívější poznatky v podstatě byly potvrzeny, např. na podkladě výzkumu osob předstírajících zmizení svých blízkých, které ve skutečnosti usmrtily, vs. osob skutečně zoufalých z pohřešování svých příbuzných.[24]

S tím souvisí i zdůvodnění, proč lze očekávat od analýzy těchto jevů spolehlivost při určování, zda pozorovaná osoba lže. Člověk, který lže, se totiž nachází ve vědomém nesouladu mezi tím, co skutečně sděluje, a tím, co by sdělovat měl, resp. s tím, co tvrdí, že sděluje. Protože je s tímto nesouladem spojeno vyjádření odpovídající emoce ve shora nastíněném smyslu, mluvčí, který chce lhát a předstírat přitom, že mluví pravdu, musí volně toto vyjádření potlačit, či naopak vytvořit vyjádření takové emoce, která by byla namístě (např. musí potlačit hněv, že vyšetřující disponuje přesnými informacemi od jeho komplice, který slíbil, že jej nikdy nezradí, či vyvolat dojem překvapení, jestliže předstírá, že nějaká informace je pro něj úplně nová).[25]

---

[21] EKMAN, FRIESEN (1969), s. 97nn.

[22] EKMAN (1991), s. 124.

[23] EKMAN (1991), s. 132nn.

[24] Srov. TEN BRINKE, Leanne; PORTER, STEPHEN; BAKER, ALYSHA. Darwin the Detective: Observable facial muscle contractions reveal emotional high-stakes lies. In: Evolution and Human Behavior. 2012, roč. 33, s. 414.

Protože obličej jako část těla, která slouží k primární výměně informací při komunikaci, vysílá signály velice rychle, mikroexprese odhalující pravou emoci komunikátora mu může uniknout ještě předtím, než ji stihne volně potlačit, pozměnit, vytvořit atd. Tato hypotéza byla na počátku odůvodňována tím, že mikroexpresí si obyčejně při komunikaci jiní lidé nevšímají, takže ani sám komunikátor si je ani na nevědomé úrovni nehlídá, neboť nedostává zpětnou vazbu, že by si je hlídat měl, protože mohou v úspěšnosti komunikace hrát roli.[26]

V zásadě tak existují tři mechanismy úniku skutečné emoce u komunikátora, který lže – mikroexprese coby velmi krátká úplná zobrazení skutečně pociťovaných emocí, která komunikátor „neuhlídá", mikroexprese následně volně potlačené a ty prvky výrazu určité emoce, které jsou ovládány svaly, jejichž aktivitu nelze volně potlačit.[27]

Původní myšlenky Ekmana a Friesena stály na více různých příčinách, proč lidé selhávají ve snaze při svém komunikačním aktu klamat (např. někteří mohou ve skutečnosti chtít, aby jejich klam byl odhalen, jiní vysílají úmyslně protichůdné signály, čímž se snaží snížit svoji odpovědnost za obsah sdělení atd.), pro předmět tohoto textu je však podstatná hypotéza (později všeobecně přijatá jako výchozí předpoklad metody analýzy mikroexpresí[28]), že lidé při komunikaci volně některé formy nonverbální komunikace prostě neovládají.[29]

Není bez zajímavosti, že původně bylo zkoumání v této oblasti zaměřeno i na další části těla, v nichž bylo možno sledovat určité projevy nonverbální komunikace, zejména ruce a nohy. Ekman a Friesen dokonce považovali ruce, a ještě více pak nohy za spolehlivější zdroj informací o skutečných emocích komunikátora než obličej, neboť podle jejich zjištění se

[25] Ekman v této souvislosti nemluví o mikroexpresích, ale o potlačených expresích. Srov. EKMAN (1991), s. 131. Protože však jde o velmi podobný mechanismus s prakticky stejným postupem detekce i významem, pro jednoduchost budu i v dalším textu souhrnně užívat pojmu mikroexprese pro „skutečné" mikroexprese i pro potlačené exprese, nebude-li výslovně uvedeno jinak.

[26] EKMAN, FRIESEN (1969), s. 98.

[27] EKMAN (1991), s. 140.

[28] Tak s ní pracuje drtivá většina dalších studií uvedená v tomto článku.

[29] EKMAN, FRIESEN (1969), s. 104.

komunikátorova vůle při potlačování či skrývání emocí na tyto části těla zaměřuje podstatně méně než na výraz obličeje.[30] V pozdějších obdobích se však pozornost zaměřila primárně (téměř výlučně) právě na obličej. Dlužno však zdůraznit, že v těchto „pionýrských dobách" se metoda odhalování mikroexpresí stále opírala o přímé pozorování člověka člověkem, tedy toliko o využití lidských smyslů bez pomoci výpočetní techniky.

2.2 ÚSKALÍ ZKOUMÁNÍ MIKROEXPRESÍ

Již od počátku Ekman varoval, že pátrání po mikroexpresích a vyvozování závěrů z jeho výsledku má mnoho úskalí, neboť např. ne každý lhář vždy mikroexprese vysílá (lze říci, že neexistuje mikroexprese odpovídající přímo lži, jen odpovídající skutečnému emocionálnímu rozpoložení komunikátora). Jen sama skutečnost, že nebyly v komunikačním aktu zjištěny, tedy neznamená ještě, že komunikátor mluví pravdu (můžeme si představit např. komunikátora, který vyjadřuje vztek, který skutečně cítí, protože vyšetřující odhalil nějakou jeho chybu při zametání stop, ale tento vztek může být vnějškově připisován rozhořčení, že byl údajně falešně nařčen, rozhořčení z chování vyšetřujícího atd.).

Naopak i komunikátor, který mluví pravdu, může v důsledku stresu a obav, že by mohl být považován za lháře, vykazovat mikroexprese emocí, které jsou v rozporu s tím, jak se snaží navenek jevit – Ekman to nazývá Othellovým efektem.[31] Stejně tak si lze osvojit umění znovuvybavit si určitou emoci v potřebném okamžiku, jak je typické např. pro tzv. Stanislavského metodu herectví – v takovém případě mikroexprese mohou rovněž klamat, protože odráží skutečně pociťovanou emoci, byť uměle vyvolanou a dané situaci neodpovídající; stejná situace nastává tehdy, když lhář sám sobě vsugeruje, že mluví pravdu.[32]

Obdobné výhrady ke spolehlivosti mikroexpresí coby indikátoru lži vznáší i někteří jiní autoři a autorky. Např. Judee K. Burgoon upozorňuje, že je třeba rozlišovat mezi prožívanou emocí (to, co komunikátor skutečně

[30] EKMAN, FRIESEN (1969), s. 99nn.

[31] EKMAN (1991), s. 132.

[32] EKMAN (1991), s. 140.

prožívá), pociťovanou emocí (to, jak to na něj působí) a jejím zobrazením (to, jak to dává navenek najevo), přičemž tyto tři kategorie si nemusí vždy odpovídat.[33] Byť uznává, že některé projevy některých pociťovaných emocí nejsou pod komunikátorovou kontrolou, tyto nemusí vždy odpovídat skutečně prožívaným emocím.[34] Výskyt mikroexpresí navíc nedoprovází každou lež, naopak jde podle některých studií o jev spíše řídký (alespoň tak, jak je pojímá Ekman).[35]

Spolehlivost mikroexpresí jakožto kritéria pro odhalení lží tedy byla relativně dlouhou dobu brána s rezervou. Studie opakovaně prokazovaly, že schopnost člověka rozpoznat lež i při náležitém tréninku není příliš vysoká. Jedna metastudie zabývající se studiemi úspěšnosti odhalování lži prostým pozorováním (tedy bez specifického zaměření na analýzu mikroexpresí, ale všech možných metod k odhalení lži prostým okem, poslechem atd.) uvádí, že úspěšnost je v průměru 54 %,[36] přičemž se prakticky neliší úspěšnost laiků a expertů (profesionálů, u nichž odhalování lží představuje součást jejich každodenní činnosti, jako jsou policisté, soudci atd.).[37]

Specifické výzkumy již byly ovšem zaměřeny i zcela konkrétně na výsledky skupiny podrobené výcviku v rozpoznávání mikroexpresí vytvořeného přímo na základě Ekmanových poznatků. Tato skupina byla porovnávána se skupinou podrobenou domnělému (fiktivnímu) výcviku a skupinou nepodrobenou žádnému výcviku, přičemž i zde byly výsledky velmi neuspokojivé – statisticky relevantní rozdíly mezi jednotlivými skupinami neexistovaly a jejich úspěšnost (tedy včetně „vycvičené“ skupiny) se pohybovala pod hranicí prosté náhody (byla nižší než 50 %).[38] I zde opakuji, že šlo

[33] BURGOON, Judee K. Microexpressions Are Not the Best Way to Catch a Liar. In: Frontiers in Psychology. 2018, roč. 9, čl. č. 1672, s. 1nn.

[34] BURGOON, *op. cit.*, s. 2.

[35] Srov. např. PORTER, Stephen; TEN BRINKE, Leanne. Reading Between the Lies. Identifying Concealed and Falsified Emotions In Universal Facial Expressions. In: Psychological Science. 2008, roč. 19, č. 5, s. 511.

[36] HARTWIG, Maria; BOND, Charles F. Jr. Why do Lie-Catchers Fail? A Lens Model Meta-Analysis of Human Lie Judgments. In: Psychological Bulletin. 2011, roč. 137, č. 4, s. 644.

[37] BOND, Charles F.; DEPAULO, Bella M. Accuracy of Deception Judgments. In: Personality and Social Psychology Review. 2006, roč. 10, č. 3, s. 229.

stále o dobu, v níž se výcvik opíral toliko o pozorovací schopnosti daných jednotlivců bez pomoci vyspělé techniky.

Takto neoslnivé výsledky mají dle mého názoru své jednoduché opodstatnění v povaze lidského vnímání a komunikace – pro člověka je užitečná jak schopnost sám při komunikaci klamat, neboť to vede zpravidla přinejmenším ke krátkodobému prospěchu, tak schopnost klam v komunikačním aktu jiné osoby odhalit, neboť její prospěch získaný klamem je zpravidla na úkor komunikačního partnera. Jelikož se při dvoustranné komunikaci obě tyto schopnosti střetávají, není překvapivé, že vývoj člověka (ať už z evolučního hlediska či z hlediska sociálního učení) dospěl do bodu, že výsledek tohoto střetu (odhalení klamu vs. úspěšný klam) je v průměru v zásadě 50:50, tedy že se rovnoměrně vyvinula schopnost klamat i klam odhalit, neboť obě jsou člověku při komunikaci stejně prospěšné.

Mohlo by se tedy zdát, že velká očekávání od mikroexpresí v souvislosti s odhalováním lží se dodnes nenaplnila a že se jednalo o slepé rameno cesty za svatým grálem kriminalistiky – jednoznačným a spolehlivým určením, zda vyslýchaný lže, či nikoliv. Přesto výzkum nonverbálních náznaků klamu opuštěn až do dnešních dní nebyl, neboť se stále očekává, že by nějaké takové dosud neodhalené náznaky klamu ještě objeveny být mohly.[39]

Dlužno zde však znovu připomenout, že starší práce zejména Ekmanovy v podstatě počítaly s osobním prováděním analýzy mikroexpresí, tedy s vytrénováním odborníků tak, aby sami vlastními silami byli schopni tuto metodu provádět vlastním přímým pozorováním bez technické pomoci. V posledních letech se však objevují až nebezpečně slibné (byť prozatím jen velmi omezené a předběžné) výsledky výzkumů počítačové analýzy mikroexpresí (a dalších pozorovatelných vnějších projevů) při odhalování lží.

---

[38] JORDAN, Sarah; BRIMBAL, Laura; WALLACE, Brian D. KASSIN, Saul M. HARTWIG, Maria; STREET, Chris N. H. A test of the micro-expressions training tool: Does it improve lie detection? In: Journal of Investigative Psychology and Offender Profiling. 2019, roč. 16, č. 3, s. 231.

[39] VRIJ, Aldert; FISHER, Ronald P.Unraveling the Misconception About Deception and Nervous, Behavior. In: Frontiers in Psychology. 2020, roč. 11, čl. č. 1377, s. 5.

2.3 VYUŽITÍ INFORMAČNÍCH TECHNOLOGIÍ PŘI ANALÝZE MIKROEXPRESÍ

Rozmach výpočetní techniky v posledních desetiletích obecně a technologií rozpoznávání obličejů zvláště totiž vnesl i do oblasti zkoumání nonverbálních projevů člověka nové obzory. Metoda obličejových analýz včetně analýz mikroexpresí tak mohla vstoupit z fáze lidského pozorování, jež se ukázalo jako nespolehlivé, do fáze počítačové analýzy, která přináší podstatně nadějnější výsledky.

Postupně byly vyvinuty různé metody počítačové analýzy mikroexpresí na videonahrávkách osob, resp. analýzy expresí obličeje, neboť zpravidla daná metoda zohledňuje jak mikroexprese, tak makroexprese. Navrhována je dokonce i integrace dalších sledovaných údajů, např. propojení s analýzou hlasu či srdečního tepu,[40] tedy v podstatě integrace analýzy mikroexpresí (resp. obecně analýzy obličeje) do fyziodetekčního vyšetření. Na takové úvahy je však prozatím patrně ještě brzy. Metoda počítačové analýzy mikroexpresí musí být nejprve dostatečně spolehlivě rozvinuta sama o sobě.

Velmi zhruba lze tyto analýzy rozlišovat do dvou hlavních skupin – statické, které každý snímek nahrávky vyhodnocují samostatně, a dynamické, které extrahují z každého snímku nezávisle příznaky (*features*) za účelem vymodelování vývoje exprese v čase.[41] Každá tato metoda opírající se o umělou inteligenci musí již při samotném vyhledávání mikroexpresí v záznamu vyřešit dva problémy – vytěžení příznaků z nahrávky a jejich klasifikaci.

Vytěžení příznaků vyžaduje nalezení a zachycení takových informací ve videozáznamu obličeje, které jsou relevantní pro popis mikroexpresí, přičemž sledovány jsou v zásadě dvě skupiny příznaků – geometrické (*geometric*), tedy rozložení částí obličeje jako jsou oči, nos atd., a vzhledové (*appea-*

[40] Např. ZHOU, Ling; SHAO, XIUYAN; MAO, Qirong. A survey of micro-expression recognition. In: Image and Vision Computing. 2021, roč. 105, článek č. 104043, DOI: https://doi.org/10.1016/j.imavis.2020.104043 [online]. Citováno 19. 1. 2021, s. 9.

[41] Srov. např. KULKARNI, Kaustubh; CORNEANU, Ciprian; OFODILE, Ikechukwu a kol. Automatic Recognition of Facial Displays of Unfelt Emotions. In IEEE Transactions on Affective Computing [online], doi: 10.1109/TAFFC.2018.2874996, cit. 19. 1. 2021, s. 3.

rance), tedy změny v textuře obličeje při pohybu.[42] Klasifikace (*classification*) pak spočívá ve využití takto získaných informací pro identifikaci sekvencí mikroexpresí v záznamu.[43]

Často se tak využívá v zásadě tříkrokový proces – předzpracování (*preprocessing*), dynamická analýza příznaků (*dynamic feature analysis*) a klasifikace (*classification*). V prvém kroku je po rozpoznání obličeje (*face detection*) a lokalizace významných bodů obličeje (*facial landmark localization*) na základě antropometrického modelu zkoumaný obličej rozložen do dílčích oblastí. Při dynamické analýze jsou ze všech dílčích obličejových oblastí sbírány exprese, které indikují klam, z nichž je vytvořen vektor popisu chování obličeje (*facial behavior description vector*). Klasifikace je pak provedena tzv. metodou náhodných lesů (*Random Forest*),[44] tedy metodou strojového učení využívající více rozhodovacích stromů, z jejichž výsledků (výsledků jednotlivých klasifikací) se vytvoří medián.

Výsledkem by tedy mělo být zjištění, zda osoba na záznamu vypovídá pravdu, či nikoliv, resp. zda mikroexprese odpovídají obsahu sdělení a volně kontrolovaným projevům emocí, či zda je zde rozpor.

Exprese indikující klam byly vybrány na základě dřívějších poznatků o tom, které pohyby v obličeji je nejobtížnější simulovat (resp. u kterých to prakticky není možné),[45] a to ať už šlo o mikroexprese. nebo o makroexprese. Počítačové zpracování informací zde využívá tzv. hlubokého učení (*deep learning*), tedy jednu z metod strojového učení. Při té vychází z dat obsažených v databázích (nahrávky reálných lidských výpovědí), která vyhodnocuje a nesmírně složitými výpočetními postupy srovnává s videem obsahujícím právě analyzovanou výpověď.

Vcelku příznivé výsledky přineslo použití podkladového materiálu v podobě reálných videí osob, které buď skutečně pohřešovaly někoho

---

[42] WANG, Yandan; SEE, John; OH, Yee-Hui; a kol. Effective recognition of facial micro-expressions with vide motion magnification. In: Multimedia Tools and Applications, 2017, roč. 76, s. 21669.

[43] např. ZHAO, XU, s. 499.

[44] SU, Lin; LEVINE, Martin. Does „Lie to me" lie to you? An evaluation of facial clues to high-stakes deception. In: Computer Vision and Image Understanding. 2016, roč. 147, s. 53.

[45] SU, LEVINE, *op. cit.*, s. 55.

blízkého, s jehož zmizením neměly nic do činění, nebo které byly následně bezpečně usvědčeny z opaku (zpravidla oběť samy usmrtily). Výzkumníci dosáhli výsledku 76,92 % přesnosti[46] v určení, zda dotyčná osoba projevuje upřímnou emoci, či zda lže, a to přesto, že použitá videa představovala relativně omezený vzorek, byla různé kvality a zkoumané osoby často měly část obličeje blokovánu brýlemi, vousy, vlasy atd.[47]

Byť výsledek 76,92 % rozhodně není dostatečný proto, aby opravňoval nárok na uznání této metody jako spolehlivé pro potřeby praktického využití v kriminalistice, natož aby mohly její výsledky být uznány jako důkaz v trestním řízení, je třeba si uvědomit, že celá tato metoda je dosud takříkajíc v plenkách.

Nadšení zchladí již jen skutečnost, že úspěšnost učení umělé inteligence tzv. hlubokým učením závisí především na velikosti databáze vzorků a jejich rozmanitosti,[48] přičemž do současnosti existuje takových databází jen několik[49] a vzorky v nich se počítají nejvýše na řády nízkých stovek,[50] zpravidla pocházejících od nízkých desítek sledovaných osob, často navíc s relativně malou etnickou různorodostí.[51] Jednotlivé databáze se přitom liší nejen způsobem snímání videozáznamů, ale i kategoriemi mikroexpresí,

[46] *Accuracy*, tedy vyjádření celkové úspěšnosti. Toto procento tedy vypovídá o tom, jaký podíl celkových pokusů vedl k úspěšné identifikaci bez zohlednění úspěšnosti v jednotlivých zkoumaných kategoriích (jednotlivých prvcích či proměnných, které počítač analyzoval). Tato hodnota tak má nepopiratelně obecnou vypovídací hodnotu, ovšem je třeba ji korigovat bližším zkoumáním jednotlivých analyzovaných kategorií z hlediska preciznosti (*precision* – úspěšnost v konkrétní specifické kategorii) a úplnosti (*recall* – celkový počet případů, kdy se určitou kategorii podařilo správně určit). Vysoká přesnost totiž nevylučuje, že u určitých specifických kategorií umělá inteligence přináší podstatně horší výsledky, což u tak komplikovaného procesu s tak velkým množstvím proměnných jako je analýza mikroexpresí, může být dost zásadní.

[47] SU, LEVINE, *op. cit.*, s. 67.

[48] Srov. ZHAO, Xu, *op. cit.*, s. 498.

[49] Srov. např. WANG, SEE, OH a kol., *op. cit.*, s. 21670.

[50] OH, Yee-Hui; SEE, John; NGO, Anh Cat Le; PHAN, Raphael C.-W.; BASKARAN, Vishnu M. A Survey of Automatic Facial Micro-Expression Analysis: Databases, Methods and Challenges. In: Frontiers in Psychology. 2018, roč. 9, čl. č. 1128, s. 3.

[51] Srov. např. DAVIDSON, Adrian K.; LANSLEY, Cliff; COSTEN, Nicholas; TAN, Kevin a YAP. Moi Hoon. SAMM: A Spontaneous Micro-Facial Movement Dataset. In: IEEE Transactions on Affective Computing. 2018, roč. 9, č. 1, s. 118.

které nabízí (zejména které emoce jsou ve sbírkách zpracovány).[52] Stále tedy hovoříme o výsledcích dosažených ve velmi omezených „laboratorních" podmínkách s velmi limitovanými datovými soubory. Tento současný stav je tedy propastně vzdálen tomu, aby na jeho základě bylo možno činit závěry o jeho obecné úspěšnosti v reálném životě kriminalistické praxe. Ta vyžaduje spolehlivost metody v těch zcela nejtěžších – z hlediska vzhledu a specifik zkoumaného subjektu v podstatě zcela nahodilých – podmínkách. Vytvoření dostatečně naplněných databází co do kvantity (celkový počet dat), tak kvantity (rozmanitost zkoumaných subjektů a jejich projevů), sjednocení základních požadavků na způsob jejich sběru a vyhodnocování tak, aby byly výsledky alespoň částečně zobecnitelné, si tak vyžádá ještě obrovské množství úsilí, prostředků a času.

Z předchozích řádek tedy plyne, že metoda analýzy mikroexpresí není v současném stavu svého vývoje ještě dostatečně otestovanou a spolehlivou, aby se mohla stát účinnou součástí palety kriminalistických metod. Dosud se nachází ve svém „batolecím období"[53] a teprve budoucnost ukáže, zda při postupném zdokonalování studia lidského obličeje a podstatném rozšíření databází obličejových videí bude schopna dosáhnout bodu, v němž její výsledky budou obdobně spolehlivé jako např. při daktyloskopii či forenzní srovnávací analýze DNA, tedy na takové úrovni, aby o ně bylo možno opřít vyšetřování, či dokonce meritorní rozhodnutí v trestním řízení. Má však značný potenciál, a to zejména je-li doprovozena a podpořena i analýzou makroexpresí, což je u počítačové verze této metody zcela běžné.

Dosud provedená zkoumání byla vždy zejména co do počtu vzorku záznamů obličejů a emocí v nich vyjádřených dosti omezená a odpovídala specifickým podmínkám. Byť výsledky některých výzkumů naznačují, že např. osvětlení, kvalita videa, úhel snímání, překrytí části obličeje vlasovým porostem či vousy atd. žádnou nepřekonatelnou překážku využitelnosti této metody nevytváří,[54] jistě bude úspěšnost metody třeba testovat

[52] Srov. např. ZHOU, SHAO, MAO a kol., *op. cit.*, s. 2nn.

[53] Srov. např. WANG, SEE, OH a kol., *op. cit.*, s. 21665.

[54] SU, LEVINE, *op. cit.*, s. 66.

i ve vztahu k nahodilým nestandardním situacím jako je výpověď vyšetřovaného, který prodělal parézu obličeje či trpí některou z nemocí, mezi jejichž symptomy patří tremor obličejové části hlavy, kortikální myoklonus, dystonie v obličeji (např. blefarospazmus, oromandibulární dystonie atd.), prochází botulotoxinovou terapií či je pohyb jeho obličejových svalů nějakým jiným způsobem výrazně modifikován.

Stejně tak bude muset tato metoda ještě být vystavena zkoušce schopnosti lidí naučit se cíleně klamat při znalosti způsobu jejího fungování, neboť dosud je testována v podstatě v laboratorních podmínkách či na základě videozáznamů, u nichž aktéři nepředpokládali, že jejich výpověď bude této metodě vystavena, a tedy se na ni specificky nezaměřovali.

Zcela specifickým problémem pak bude zkoumání relevance závěrů této analýzy, tedy do jaké míry (s jakou spolehlivostí) bude možno na základě (byť bezpečně zjištěných) dílčích nesouladů mezi skutečnými a znázorňovanými emocemi vyslýchané osoby vyvozovat závěr o tom, že lže. Ani kdyby totiž počítačová analýza mikroexpresí dosáhla úrovně spolehlivosti umožňující bezpečné forenzní využití, nelze zapomínat na to, že nejde o metodu detekce lži, ale pouze o metodu odhalení disonance mezi projevovanými a pociťovanými emocemi, která však stále citelně vyžaduje interpretaci případného rozporu, tedy mezi níž a mezi závěrem o tom, zda daná osoba lže, je ještě velmi dlouhý kauzální řetěz. Jinými slovy nelze ze zřetele ztrácet to, co je vlastně výstupem analýzy mikroexpresí, tedy že jím není závěr o tom, zda zkoumaný subjekt lže, či nikoliv, ale pouze to, že pociťuje jinou emoci, než kterou projevuje, resp. že pociťovanou emoci potlačuje. Jediným vysvětlením toho, proč tak činí, přitom totiž nemusí být to, že lže (viz výše sub 2.2).

Ačkoliv tedy i jen zvažování hypotetického nasazení metody počítačové analýzy mikroexpresí pro kriminalistické účely, či dokonce pro rozhodování o věci samé v trestním řízení je třeba dnes považovat za hudbu budoucnosti, rozmach výpočetních technologií v posledních desetiletích i pozornost, která je této metodě věnována v posledních letech, svědčí o tom, že tato budoucnost nemusí být natolik vzdálená, aby bylo možno nechat úvahy o ní s klidným svědomím až na generace našich vnuků či pravnuků.

Bude proto užitečné sledovat další pokroky na tomto poli a s předstihem se zamýšlet nad tím, jaké místo potenciálně tato metoda může v naší kriminalistické či právněaplikační praxi zaujmout.

3. SROVNÁNÍ S FYZIODETEKČNÍM VYŠETŘENÍM

Nabízí se premisa, že byla-li by někdy u nás zavedena do policejní praxe metoda počítačové analýzy mikroexpresí, měl by se vůči ní uplatňovat stejný právní přístup jako vůči metodě fyziodetekčního vyšetření. Tato premisa jistě poučenému čtenáři přijde na mysl jako první, neboť metoda počítačové analýzy mikroexpresí je *de facto* jen jinou metodou usilující o usnadnění odhalení lži ve výpovědi vyšetřované osoby,[55] a tedy by s ní *de iure* mělo být zacházeno stejně jako s metodou fyziodetekčního vyšetření.

Jak budu níže demonstrovat, domnívám se, že věc není tak snadná, jak na první pohled vypadá. I když konečný závěr nakonec může vyznít ve prospěch stejného přístupu, nebude po mém soudu založen na tomto apriorním srovnání, ale bude k němu třeba vyvinout specifickou argumentaci. Mezi metodami fyziodetekčního vyšetření a analýzy mikroexpresí existují totiž při bližším zkoumání rozdíly, které se prizmatem shora popsaných důvodů pro odmítnutí důkazní použitelnosti první zmíněné metody mohou jevit jako dosti podstatné a ospravedlňující odlišný přístup ke druhé zmíněné metodě v právní praxi.

K tomu však bude nejprve nutno podrobněji zmapovat přístup právněaplikační praxe k metodě fyziodetekčního vyšetření a důvodů, které k němu vedou.

3.1 METODA FYZIODETEKČNÍHO VYŠETŘENÍ VE SVĚTLE PRÁVA

Právní názory českých soudů o mezích využitelnosti metody fyziodetekčního vyšetření, korelující v zásadě i s přístupy jiných evropských soudů, determinují i domácí kriminalistickou a trestněprávní aplikační praxi. Jak již bylo nastíněno v úvodu tohoto textu, domácí rozhodovací praxe setrvale

[55] Pro jednoduchost mějme dále za to, že vyšetřovanou osobou je vždy obviněný, nebude-li uvedeno jinak. Pojmy „vyšetřovaný“, „vyšetřovaná osoba“, „obviněný“ a „osoba, proti níž se řízení vede“, budu nadále užívat *promiscue*, avšak samozřejmě s vědomím, že v terminologii kriminologie a trestního práva procesního odpovídají různým postavením.

uplatňuje právní názor, že výsledky fyziodetekčního vyšetření nejsou použitelným důkazem v trestním řízení.

Byť u nás neplatí absolutní zákaz jeho použití v trestním řízení, je možné jej nasadit jen s písemným souhlasem zkoumané osoby[56] a jeho výsledky lze použít jen pro usměrňování taktiky vyšetřování (v kriminalistickém slova smyslu), tedy v zásadě jen ve fázi prověřování (tj. před zahájením trestního stíhání), výjimečně i poté, ovšem bez toho, aby na základě výsledků vyšetření bylo možno založit konečné (ale v podstatě ani jakékoliv jiné) rozhodnutí ve věci. Fyziodetekční vyšetření tak může posloužit kriminalistům v podstatě jen jako jedna z indicií potvrzující, či naopak vylučující některou vyšetřovací verzi, což může vést k efektivnějšímu a rychlejšímu vyřízení věci (zejména tím, že se rychle vyloučí osoby, které jsou mimo podezření).

Sluší se podotknout, že ačkoliv přístup evropských států v této otázce není uniformní, právní názor o úplné důkazní nepoužitelnosti metody fyziodetekčního vyšetření či o její jen velmi omezené použitelnosti je rozšířený i v řadě jiných států (Belgie, Nizozemí, Německo, skandinávské státy atd.).[57]

Pro účely další analýzy je nanejvýše žádoucí si alespoň ve stručnosti přiblížit, proč (nejen) domácí soudy vůči metodě fyziodetekčního vyšetření zastávají takto restriktivní postoj. Ten se opírá nejen o dlouhodobá odborná stanoviska o nedostatečné spolehlivosti fyziodetekčního vyšetření, ale rovněž o argumenty právní,[58] spočívající v porušení základních lidských práv osoby, proti níž se řízení vede. Jde zde zejména o zákaz donucení k sebeobvinění (vyjadřovaného latinskou sentencí *nemo tenetur se ipsum accusare* či *nemo tenetur se ipsum prodere*), který je jedním z požadavků na ochranu práva na obhajobu osoby, proti níž se trestní řízení vede, jejž sdílejí prakticky všechny civilizované státy světa.

[56] NĚMEC a kol (2019)., *op. cit.*, s. 25.

[57] Srov. CANTER, ŽUKAUSKIENE, *op. cit.*, s. 41-45.

[58] Srov. např. MEIJER, Ewout H; VAN KOPPEN, Peter J. In: CANTER, David; ŽUKAUSKIENE, Rita Psychology and Law: Bridging the Gap. Routhledge: Abingdon, New York: 2008, s. 31.

3.2 STRUČNĚ K ZÁKAZU DONUCENÍ K SEBEOBVINĚNÍ

V členských státech Rady Evropy (tedy i u nás) vtiskává základní parametry jakož i limity tomuto zákazu judikatura Evropského soudu pro lidská práva (dále jen „ESLP“). Ta primárně spatřuje podstatu zákazu donucení k sebeobvinění v povinnosti orgánů činných v trestním řízení postupovat tak, aby vina byla prokázána bez využití metod nátlaku či útisku popírajících vůli osoby, proti níž se řízení vede.[59] Primárně samozřejmě tato ochrana směřuje proti vynucování doznání mučením či jeho pohrůžkami,[60] avšak tím se nevyčerpává.

Osobě, proti níž se řízení vede, nesmí být ani procesními předpisy uložena povinnost s orgány činnými v trestním řízení spolupracovat, např. jim poskytovat pravdivé a úplné informace o svém duševním stavu a motivech svých činů,[61] vydat jim dokumenty, které ji usvědčují, a o nichž orgány činné v trestním řízení neví, kde se nachází, [62] poskytnout výpověď o svém přesném pohybu v určité inkriminované době[63] atd.

Zákaz donucení k sebeobvinění pak nesmí být v situacích, v nichž osoba, proti níž se řízení vede, nijak při vyšetřování nespolupracuje a zůstává zcela pasivní, obcházen ani nepřímo tím, že by se z její pasivity usuzovalo na její vinu,[64] nebo že by tato osoba nebyla o svém právu mlčet a ničím k svému obvinění nepřispívat poučena, tedy že by vyšetřující spoléhal na

[59] Srov. např. rozsudek velkého senátu ESLP ze dne 17. 12. 1996 ve věci Saunders proti Spojenému království, stížnost č. 19187/91, bod 68.

[60] Srov. např, rozsudek velkého senátu ESLP ze dne 1. 6. 2010 ve věci Gäfgen proti Německu, stížnost č, 22978/05, bod 178.

[61] Srov. např. rozsudek velkého senátu ESLP ze dne 4. 12. 2018 ve věci Ilnseher proti Německu, stížnosti č. 10211/12 a 27505/14, bod 115.

[62] Srov. např. rozsudek ESLP ze dne 25. 2. 1993 ve věci Funke proti Francii, stížnost č. 10828/84, bod 44.

[63] Srov. např. rozsudek velkého senátu ESLP ze dne 21. 12. 2000 ve věci Heaney a McGuinness proti Irsku, stížnost č. 34720/97, bod 55.

[64] Srov. např. rozsudek velkého senátu ESLP ze dne 8. 2. 1996 ve věci John Murray proti Spojenému království, stížnost č. 18731/91, bod 47. – dlužno podotknout, že ESLP v tomto případě rovněž „jedním dechem“ doplnil, že je přípustné činit na vrub osoby, proti níž se řízení vede, nepříznivé závěry, jestliže mlčí v situaci, která si zjevně žádná její vysvětlení. V domácích podmínkách je takový přístup značně limitován, avšak lze si jej představit např. v odůvodnění rozsudku, že soud uvěřil určitému skutkovému zjištění proto, že bylo objektivně důkazně podloženo a sám obviněný jej nijak nezpochybnil.

to, že z neznalosti poskytne důkaz sama proti sobě v mylném domnění, že tak učinit musí.[65]

V domácích podmínkách je právo obviněného mlčet vykládáno poměrně široce. Nevyprazdňuje se jen tím, že na vůli osoby, proti níž se řízení vede, závisí to, zda vypovídat vůbec bude, či nikoliv, ale i to, jak bude vypovídat, zejména zda uvede pravdu či zda bude lhát, jakož i to, v jakém rozsahu bude vypovídat, zda a případně v jakém rozsahu bude odpovídat na otázky atd.[66] Stručně řečeno, obviněný je tedy pánem své vlastní výpovědi a jen jemu náleží rozhodnutí o tom, co učiní jejím obsahem, v jakém rozsahu a jakým způsobem.

Není tím však vyloučeno, aby jako důkaz posloužily výsledky donucovacích pravomocí orgánů činných v trestním řízení, jichž bylo použito k získání materiálu, který existuje nezávisle na vůli osoby, proti níž se řízení vede, např. k dokumentům odňatým při domovní prohlídce, k snímání dechu, odebírání krve, slin či vlasů pro potřeby metody analýzy DNA atd.[67]

Zákaz donucení k sebeobvinění tedy samozřejmě nezapovídá jakýkoliv způsob získání důkazů ve sféře osoby, proti níž se řízení vede, které by se dělo proti její vůli. Opak by v mnoha případech vyšetřování naprosto paralyzoval a byl by ve zcela zřejmém rozporu se samotnou podstatou činnosti orgánů činných v trestním řízení, které se nutně musí dostávat do situací, kdy s jejich aktivitou osoba, proti níž se řízení vede, nesouhlasí a odmítá dobrovolně spolupracovat, ačkoliv úplné a řádné prošetření věci v souladu se zásadou materiální pravdy vyžaduje vyhledávání a zajišťování důkazů i v její soukromé či zcela osobní sféře.[68]

Judikatura ESLP jakož i našich domácích soudů se tak v zásadě vytvarovala do podoby, v níž demarkační linii mezi ještě přípustnými metodami

[65] Srov. např. rozsudek velkého senátu ESLP ze dne 9. 11. 2018 ve věci Beuze proti Belgii, stížnost č. 71409/10, bod 130.

[66] Srov. např. FENYK, Jaroslav; PROVAZNÍK, Jan. In: FENYK, Jaroslav; GŘIVNA, Tomáš; CÍSAŘOVÁ, Dagmar, a kol. Trestní právo procesní. 7. vydání. Praha: Wolters Kluwer, 2019, s. 378.

[67] Srov. např. rozsudek velkého senátu ESLP ze dne 11. 7. 2006 ve věci Jalloh proti Německu, stížnost č. 54810/00, bod 102.

[68] Srov. např. nález Ústavního soudu České republiky sp. zn. III. ÚS 528/06 ze dne 11. 10. 2007 (N 159/47 SbNU 75).

získávání důkazů přímo od osoby, proti níž se řízení vede, a již nepřípustným porušením zásady zákazu donucení k sebeobvinění představuje to, zda sama musí nějak k poskytnutí důkazu proti sobě aktivně přispět, či nikoliv. Jestliže je k získání důkazu zapotřebí, aby osoba, proti níž se řízení vede, jen pasivně strpěla provedení úkonu ze strany orgánů činných v trestním řízení (např. odebrání tzv. bukálního stěru pro účely metody analýzy DNA, stěr potu pro účely metody pachové identifikace, pouhé postavení se mezi figuranty při rekognici atd.), výsledek nelze považovat za získaný v rozporu se zákazem donucení k sebeobvinění.

Pokud naopak tato osoba musí k výsledku sama aktivně přispět (např. poskytnout vzorek hlasu či ručního písma, udělat při rekognici nějaké gesto, označit místo, kam ukryla usvědčující důkaz atd.), zákaz donucení k sebeobvinění bude porušen, nedá-li k tomuto svému aktivnímu přispění dobrovolný souhlas při náležitém pochopení skutečnosti, že k tomu není povinna.[69]

Vezmeme-li v potaz tato právní východiska, pak rozpor metody fyziodetekčního vyšetřní a zákazu nucení k sebeobvinění lze spatřovat v tom, že v zásadě úplně vylučuje vůli vyslýchaného,[70] neboť ten se v průběhu vyšetření nemůže kvalifikovaně rozhodnout, zda využije svého práva nevypovídat, či nikoli,[71] ani jaké informace vyšetřujícím poskytne tak, jak by mohl učinit při „běžném“ výslechu. Celá tato metoda je ostatně postavena právě na tom, že sbírá a vyhodnocuje o vyšetřovaném data na základě mimovolných procesů, které z podstaty věci nedokáže ovládnout, na rozdíl od obsahu svých řečových aktů.

Kromě toho by bylo možno uvažovat i tom, zda zákaz donucení k sebeobvinění zde není porušen již jen způsobem, jakým je metoda fyziodetekčního vyšetření realizována. Ta pro své řádné provedení vyžaduje

[69] Srov. zejména stanovisko pléna Ústavního soudu České republiky sp. zn. Pl.ÚS-st. 30/10 ze dne 30. 11. 2010 (ST 30/59 SbNU 595; 439/2010 Sb.), nález Ústavního soudu České republiky sp. zn. II. ÚS 2369/08 ze dne 9. 12. 2010 (N 244/59 SbNU 489) či PÚRY, František. In: ŠÁMAL, Pavel a kol. Trestní řád. Komentář. 7. vydání. Praha: C. H. Beck, 2013, s. 1348nn.

[70] Srov. např. JELÍNEK, Jiří. In: JELÍNEK, Jiří a kol. Trestní právo procesní. 2. aktualizované vydání. Praha: Leges, 2011, s. 364.

[71] Srov. např. FENYK, GŘIVNA, CÍSAŘOVÁ a kol., *op. cit.*, s. 349.

sledování hned čtyř biologických procesů (doprovázejících vegetativní funkce) prostřednictvím přístrojů, které musí být přiloženy pevně k tělu vyšetřovaného (snímání kožního odporu kůže, krevního tlaku, tepové frekvence a dechu[72]).

Jelikož však žádný ze senzorů těchto biologických procesů nevyžaduje volní vědomou aktivitu vyšetřovaného, ale snímá pouze to, co vyšetřovaný produkuje nezávisle na své vůli, snese jistě z tohoto ohledu metoda fyziodetekčního vyšetření srovnání s praktikami, které rozhodovací soudní praxe pozitivně potvrdila jako nestojící v rozporu se zákazem donucení k sebeobvinění (např. bukální stěr či dechová zkouška).

Jednoznačně v rozporu se zákazem donucení k sebeobvinění by však byl poslední snímaný proces, jímž je hlas vyšetřované osoby zachycovaný analyzátorem hlasu jakožto nedílná součást fyziodetekčního vyšetření.[73] Právě poskytnutí vzorku hlasu je totiž jedním z typických příkladů úkonů který představuje aktivní jednání osoby, jenž jej poskytuje, a který je tedy chráněn zákazem donucení k sebeobvinění.

Je tedy zřejmé, že i kdyby domácí rozhodovací praxe změnila na spolehlivost metody fyziodetekčního vyšetření názor a zvažovala změnu názoru i na důkazní přípustnost jejích výsledků, tato by i tak byla nadále podmíněna naprostou dobrovolností osoby, proti níž se řízení vede. Alespoň tedy, nedošlo-li by ke změně kompozice sledovaných procesů.

4. METODA POČÍTAČOVÉ ANALÝZY MIKROEXPRESÍ A ZÁKAZ DONUCENÍ K SEBEOBVINĚNÍ

Závěry ohledně důvodů důkazní nepoužitelnosti výsledků metody fyziodetekčního vyšetření poslouží jako odrazový můstek k analýze možných přístupů právněaplikační praxe k důkazní využitelnosti výsledků metody analýzy mikroexpresí, pokud by někdy v budoucnu bylo zvažováno její praktické využití i domácími orgány činnými v trestním řízení.

Domnívám se, že si lze představit relevantní a přesvědčivou argumentaci k oběma základním možnostem – že by tato metoda měla stejný „právní

[72] Srov. NĚMEC a kol. (2019), *op. cit.*, s. 18-20.

[73] Srov. NĚMEC a kol. (2019), *op. cit.*, s. 20.

osud“ jako metoda fyziodetekčního vyšetření, a že by na rozdíl od ní byla připuštěna (resp. její výsledky) jako důkaz v trestním řízení. Existují totiž nepochybně společné i rozdílné charakteristiky obou metod. Pokusím se proto představit obě možné základní argumentační linie.

4.1 ARGUMENTY PROTI VZTAŽENÍ STÁVAJÍCÍHO PRÁVNÍHO NÁZORU I NA METODU ANALÝZY MIKROEXPRESÍ

Nejprve se zaměřím na argumentaci ve prospěch závěru, že metoda analýzy mikroexpresí by byla právně do všech důsledků nazírána totožně jako metoda fyziodetekčního vyšetření. Takový závěr je totiž na první pohled pravděpodobně přijatelnější. Podporuje jej hned několik závažných důvodů.

Za prvé, přes nadšení vědců zavádějících tuto metodu i předběžné výsledky prezentované v odborné literatuře nelze dosud bezpečně uzavřít, že metoda analýzy mikroexpresí je natolik spolehlivá, aby mohla být obecně v trestním řízení důkazně akceptována. Metoda fyziodetekčního vyšetření byla vyvinuta před desítkami let a po celou dobu byla neustále zdokonalována, přesto až dosud přetrvává ohledně její spolehlivosti značná skepse.

Metoda počítačové analýzy mikroexpresí je relativně nová, je využívána teprve několik let, a to ještě navíc zhusta vůbec nejde o praxi orgánů činných v trestním řízení, ale především o experimentální vědeckou sféru. Přes nadějné dosavadní výsledky proto nelze vyloučit, že delší a intenzivnější využívání této metody odhalí její nedostatky, které dosud známy nebyly a jimž nic nenasvědčovalo.

Se spolehlivostí metody, která jde ruku v ruce s její ověřitelností, se pojí i další svízel – oslnivý úspěch, který mnohé vědce ohledně této metody vede k optimismu, je postaven především na využití neuronových sítí k „učení“ příslušných programů. Tento proces lze přirovnat ke koncentrování zkušenosti několika desítek, stovek atd. expertů (dle velikosti sítě odborníků) do jedné umělé inteligence. Když tato umělá inteligence dospěje k určitému závěru, jde sice stále o výsledek přesného, sofistikovaného matematického výpočtu (umělá inteligence stále žije jen ve světě „jedniček

a nul“), ale nikoliv abstraktního, nýbrž toliko uplatňujícího agregované zkušenosti, kterou má umělá inteligence uložena a s níž dokáže pracovat.

Jinými slovy, ví, že určitá kombinace mikroexpresí nasvědčuje tomu, že mluvčí lže, protože je srovnává s obrovským množstvím podobných situací, v nichž tato kombinace doprovázela lež. Tím se celá metoda přibližuje spíše intuici (byť až mrazivě robustnější, než čeho je schopen člověk), než přesné vědecké metodě.

Jistě i dosud uznávanými vědeckými metodami bude možno spolehlivost této metody ověřovat a pro kriminalistickou i justiční praxi bude v zásadě postačující, bude-li bezpečně statisticky prokázáno, že se umělá inteligence ve svých závěrech nemýlí, bez ohledu na to, že v budoucnu již možná kriminalisté a soudci ani nebudou schopni vůbec pojmout, jak ke svým závěrům dospěla.

Celý tento způsob však již stojí na hraně samostatného lidského pochopení, a čím úspěšnější bude, tím více bude třeba spoléhat na to, že se umělá inteligence nespletla, protože sami nebudeme schopni její postup pro přílišnou složitost ověřit. Již jen toto hledisko může v očích konzervativní justiční praxe převážit nad pragmatickým hlediskem statistické úspěšnosti.

Za druhé, tato metoda se v mnohém podobá metodě fyziodetekčního vyšetření, jejíž výsledky jako důkaz nejsou přijímány nejen pro určitou skepsi ohledně její spolehlivosti, ale i pro rozpor se zákazem donucení k sebeobvinění. I kdyby tak časem metoda analýzy mikroexpresí byla uznána za spolehlivou, neznamená to, že by již jen proto měla být důkazně připuštěna bez důkladného vypořádání se s tím, zda a případně jak vážný představuje problém z hlediska ochrany základních lidských práv vyšetřovaného.

Metoda fyziodetekčního vyšetření podléhá zákazu donucení k sebeobvinění přesto, že (s výjimkou hlasu, viz výše) nevyžaduje žádnou aktivní participaci ze strany vyšetřovaného a toliko pasivně snímá výsledky jeho biologických procesů, jež vyšetřovaný svou vůlí neovládá. Přesto, že zákaz donucení k sebeobvinění se z logiky věci neuplatní tam, kde osoba, proti níž se řízení vede, dá k určitému postupu svůj dobrovolný souhlas, a poskytnutí vzorku hlasu je typickým příkladem takového postupu, zákaz donucení k sebeobvinění brání důkazní použitelnosti výstupů fyziodetekčního vyšet-

ření i tehdy, když se mu vyšetřovaný podrobil dobrovolně. To nasvědčuje tomu, že soudní praxe považuje i mezi ostatními postupy podléhajícími zákazu donucení k sebeobvinění fyziodetekční vyšetření za něco mimořádného, co natolik oslabuje práva vyšetřované osoby, že to důkazně nelze připustit ani tam, kde výsledky jiných takových postupů by připuštěny byly.

Důvodem zde je nepochybně značná intenzita, jíž tato metoda působí na vůli vyšetřovaného. Ten nemůže své sledované biologické procesy ovládat ani dávkovat, tyto přitom mají pro vyšetřující v podstatě stejný, ne-li větší význam než to, co je obsahem jeho výpovědi, již tyto procesy doprovází. Tím lze opodstatnit i rozdíl mezi sběrem dat o těchto procesech a sběrem biologického materiálu vyšetřovaného či sběrem jiných informací z jeho sféry bez nutnosti jeho aktivního přispění.

Bylo by totiž možno namítat, že přeci biologické procesy jako je odpor kůže, dech, tep či krevní tlak existují nezávisle na vůli vyšetřovaného stejně jako jeho sliny či krev a vyšetřující je pouze pasivně sbírají. Přesto je však mezi těmito dvěma skupinami nositelů informací dosti podstatný rozdíl, který spočívá v jejich informační hodnotě. Ta je u sběru různých druhů biologického materiálu absolutní, neboť nevyžaduje žádný slovní či jiný doprovod ze strany vyšetřovaného, a byť jde o absolutnost jen v tomto kontextu, neboť jinak přináší analýza biologického materiálu cenné informace toliko při srovnání s jiným zajištěným biologickým materiálem, jde po celou dobu o proces, který je objektivní a nevyžaduje, aby se do něj vyšetřovaný jakkoliv dále zapojil.

Oproti tomu informační hodnota údajů zjištěných při fyziodetekčním vyšetření je relativní, neboť tyto údaje nejsou pro vyšetřující zajímavé samy o sobě ani ve srovnání s jiným objektivně existujícím materiálem, ale jen a pouze pro svůj verifikační potenciál ve vztahu k obsahu výpovědi vyšetřovaného, respektive pro svůj autoverifikační potenciál (potenciál nespočívá v tom, že by umožňoval zjištění objektivní pravdivosti výpovědi, ale jen v tom, že umožňuje zjištění subjektivního přesvědčení vyšetřovaného o tom, že mluví pravdu). S ním jsou tak neoddělitelně spjaty a tvoří jeho nedílnou součást. Lze to vyjádřit i tak, že do obsahu výpovědi přidávají další dílčí komunikační prvky, byť nonverbální podoby, které bychom si

však pracovně mohli přepsat i do verbální podoby, jako kdyby např. za každou větou vyšetřovaného byla do závorky připsána douška *„teď lžu/mluvím pravdu/si nejsem jistý“* atd.

Výpověď obviněného je přitom jeho výsostným právem, k jehož využití nesmí být i při pro orgány činné v trestním řízení nejvelkorysejším a nejbenevolentnějším výkladu mezí zákazu donucení k sebeobvinění nijak nucen. Jestliže tedy při fyziodetekčním vyšetření dochází k tomu, že vyšetřovaný nemá pod kontrolou část obsahu své výpovědi, je to v rozporu se zásadou, že jako obviněný si může svobodně a zcela podle své vůle vybrat, co učiní obsahem své výpovědi a v jakém rozsahu (viz výše).

V této argumentační linii je tak třeba tento závěr vztáhnout i na počítačovou analýzu mikroexpresí, neboť situace je zde v podstatných okolnostech stejná. Zkoumání a vyhodnocování mikroexpresí má stejný účel jako zkoumání a vyhodnocování uvedených biologických procesů u metody fyziodetekčního vyšetření, tedy (auto)verifikovat obsah výpovědi vyšetřovaného, a to zkoumáním projevů, které jsou nerozlučně spojeny s aktem poskytování této výpovědi a nad nimiž nemá vyšetřovaný prakticky žádnou volní kontrolu.

Lze tedy shrnout, že i kdyby v budoucnu metoda počítačové analýzy mikroexpresí byla uznána za spolehlivou, její podobnost metodě fyziodetekčního vyšetření by z hlediska právních garancí zákazu donucení k sebeobvinění svědčila pro závěr, že by měla podléhat zcela stejným právním limitacím. Pokud by tento argument byl uznán, počítačové analýze mikroexpresí by *pro futuro* bylo vyčleněno místo toliko při sběru operativních informací, a to pouze za předpokladu naprosté dobrovolnosti participace vyšetřovaného.

4.2 ARGUMENTY PRO DŮKAZNÍ PŘÍPUSTNOST VÝSLEDKŮ METODY ANALÝZY MIKROEXPRESÍ

Byť výše uvedené argumenty proti změně stávajícího právního názoru odpovídají dlouhodobému způsobu výkladu zákazu donucení k sebeobvinění v případě fyziodetekčního vyšetření i jeho podobnosti s metodou počítačové analýzy mikroexpresí v právně relevantních ohledech, domnívám se,

že lze argumentovat celkem přesvědčivě i pro opačné řešení, a to z důvodů níže nastíněných.

Předesílám, že v této části nemá valnějšího smyslu argumentovat pro spolehlivost metody počítačové analýzy mikroexpresí, neboť je zřejmé, že veškeré úvahy o praktické využitelnosti této metody v kriminalistické a právněaplikační praxi jsou na bezpečném prokázání této spolehlivosti zcela závislé. Dosud je ještě příliš brzy na činění konečných závěrů, tedy všechny dále následující úvahy jsou činěny *in eventum* pro možný budoucí vývoj, v němž tato spolehlivost bezpečně prokázána bude.

Onen podstatný rozdíl spočívá v tom, že při analýze mikroexpresí není vůbec žádným způsobem zasahováno do fyzické integrity vyšetřovaného, a to ani zcela neinvazivní formou připojením sensorů odporu kůže, tepu, krevního tlaku, dechu či analyzátoru hlasu, jako je tomu u metody fyziodetekčního vyšetření. Potenciálně až děsivá efektivita metody počítačové analýzy mikroexpresí spočívá v možnosti (auto)verifikace obsahu výpovědi na základě snímání pouhých vnějších vizuálních projevů vyšetřovaného, tedy v podstatě jen s využitím přímého pozorování.

Tento rozdíl by se z pohledu výše učiněných závěrů o mezích zákazu donucení k sebeobvinění mohl zdát jako nepodstatný. Ani u metody fyziodetekčního vyšetření nespočívalo z hlediska možného konfliktu s tímto zákazem jádro problému v tom, že by tato metoda byla příliš invazivní ve smyslu zásahu do fyzické integrity, ale v popření rozhodnosti vůle vyšetřovaného a znemožnění mu volní kontroly nad tím, které všechny informace učiní součástí své výpovědi.

Proti tomu se však nabízí argument, jehož důležitost nelze podceňovat. Ona kontrola vyšetřovaného nad obsahem jeho výpovědi totiž není a nikdy nebyla bezbřehá. Orgánům činným v trestním řízení nikdy nebylo zapovězeno přihlížet k těm informacím, které vyšetřovaný poskytuje při své výpovědi nonverbálně, byť by tak činil i nevědomky nebo dokonce v rozporu se svou vůlí jednoduše proto, že je nebyl schopen dobře kontrolovat.

Ba právě naopak, orgány činné v trestním řízení v moderní době nikdy nebyly při hodnocení pravdivosti výpovědi vyšetřovaného odkázány toliko na její obsah (a jeho konfrontaci s jinými důkazy, hodnocení vnitřní

koherence výpovědi atd.), ale vždy bylo jejich doménou analyzovat i nonverbální projevy, které ji doprovází[74] (pocení, blednutí, rudnutí, chvějící se hlas, uhýbání očnímu kontaktu atd.).

Na tom, že výpověď svědka či obviněného je tvořena komplexem informačního obsahu sdělení, ale i způsobu, jakým je tento podán, a okolností na straně vyslýchané osoby, které takové podání doprovází, je ostatně postavena i veledůležitá zásada trestního práva procesního – zásada bezprostřednosti. Ta vyžaduje, aby soud přihlédl pouze k těm důkazům, které před ním byly provedeny, tedy aby si na ně názor utvářel pod bezprostředním dojmem z řízení, v němž byly provedeny,[75] a to v případě výpovědí právě i s přihlédnutím k celkovému kontextu jejich podávání (jistota či nejistota, nervozita či klid atd.) a s náležitou péčí o vysvětlení jeho příčin.[76] S ní se pojí i zásada volného hodnocení důkazů, která mírou důkazu činí vnitřní přesvědčení příslušného orgánu činného v trestním řízení.

Snad ani neexistuje vážně míněný názorový proud, který by dnes tvrdil, že na hodnocení nonverbálních projevů vyslýchané osoby by kriminalisté či z procesního hlediska všechny orgány činné v trestním řízení nesměly brát zřetel a otrocky se musely držet jen toho, co taková osoba explicitně říká. Z hlediska zákazu donucení k sebeobvinění je tato triviální skutečnost ospravedlnitelná tím, že jde o nonverbální projevy, které tvoří přirozenou součást každého verbálního řečového aktu, bez níž by nebyl ani reálně možný (tedy *ad absurdum* kdyby jen pro ně nebyl výslech obviněného přípustným důkazním prostředkem pro rozpor se zákazem k donucení k sebeobvinění, obviněnému by bylo znemožněno ústně vypovídat vůbec a byl nutný návrat k toliko písemnému trestnímu procesu), a které jsou nadto vnímatelné jen prostým okem samotným přímým pozorováním.

Na pouhém přímém pozorování je přitom založena i metoda počítačové analýzy mikroexpresí. Byť se zaměřuje na detaily, které pouhým okem

[74] NĚMEC, Miroslav. Kriminalistická taktika pro policisty a studenty Policejní akademie České republiky v Praze. Praha: ABOOK, 2017, s. 364.

[75] Srov. např. MULÁK, Jiří. Základní zásady trestního řízení a právo na spravedlivý proces. Praha: Leges, 2019, s. 255.

[76] Srov např. MUSIL, Jan. In: ŠAMAL, Pavel; MUSIL, Jan; KUCHTA, Josef a kol. Trestní právo procesní. 4. přepracované vydání. Praha: C. H. Beck, 2013, s. 115.

nejsou zpravidla seznatelné, nejde vlastně o nic jiného než o vylepšení dosud jinak zcela běžné obecné kriminalistické metody, tvořící základ i pro hodnocení důkazů soudem v trestním řízení. Pozice počítačové analýzy mikroexpresí je zde tedy z hlediska možného konfliktu se zákazem donucení k sebeobvinění mnohem silnější než pozice fyziodetekčního vyšetření. Pro potenciální závěr o porušení zmíněného zákazu jen pro samotnou podstatu metody počítačové analýzy mikroexpresí by tak muselo být argumentováno tím, že z přípustné obecné metody (přímé pozorování) činí nepřípustnou proto, že ji posouvá za práh toho, čeho je schopen člověk bez technické pomoci jen s bezprostředním využitím vlastních smyslů.

Tento argument však není příliš přesvědčivý, neboť celý obor kriminalistické techniky (který je rovněž celospolečensky i právně uznáván a jeho výstupy jsou obecně přípustnými důkazy v trestním řízení) vlastně nedělá nic jiného, než že s využitím vědeckotechnických postupů rozšiřuje poznávací schopnosti člověka nad limit toho, čeho by byl schopen dosáhnout s pomocí toliko vlastních smyslů.

4.3 VLASTNÍ STANOVISKO

Ačkoliv předestřené argumenty umožňují ponechat konečný verdikt na čtenáři, předkládám i vlastní stanovisko, bez nějž bych tento text nepovažoval za úplný. Shora jsem opakovaně připomínal problematiku spolehlivosti zde rozebírané metody, která bude bezpochyby alfou i omegou úvah o její praktické využitelnosti.

Osobně se domnívám, že bude-li tato metoda vysoce spolehlivá, nic nebude překážet její důkazní použitelnosti v trestním řízení. Za rozhodující považuji právě její neinvazivnost v kombinaci se shora nastíněným problémem vyhodnocování lži na základě prostého lidského pozorování, na kterém je založena zásada bezprostřednosti a volného hodnocení důkazů. Jestliže i v současné době *de lege lata* i *de lege aplicata* závisí hodnocení výpovědí svědků i obviněných na vnitřním přesvědčení soudu, přičemž, jak uvedeno výše, ani u trénovaného profesionála se úspěšnost odhalení nepravdy při přímém pozorování v podstatě nepohybuje nad hranicí prosté náhody, pak jakýkoliv postup, který tuto praxi nahradí spolehlivým

určením s nejvyšší prakticky dosažitelnou mírou pravděpodobnosti (jako např. u srovnávací analýzy DNA), bude představovat zlepšení a zkvalitnění současného stavu. Byla-li by tak tato metoda s dostatečnou spolehlivostí dostupná orgánům činným v trestním řízení, jistě by to bylo způsobilé podstatně zvýšit jistotu orgánů činných v trestním řízení a snížit míru výskytu justičních omylů.

Obávám se však, že by to současně předznamenávalo novou éru ve vývoji společnosti. Tato metoda by totiž určitě nezůstala toliko v hájemství orgánů činných v trestním řízení, ale došla by i svého komerčního využití. Možnost zjišťovat pouhým vylepšeným přímým pozorováním skutečné emoce např. spotřebitelů sledujících určitou reklamu či vystavené zboží, obchodních partnerů při zvlášť důležitých vyjednáváních, zaměstnanců při zjišťování nedostatků v chodu podniku atd. by jistě nezůstala nepovšimnuta a do posledního halíře nezužitkována nejen velkými nadnárodními obchodními korporacemi. Taktéž dopad schopnosti rychle a pohodlně (např. aplikací ve speciálních inteligentních brýlích, které se již někteří technologičtí giganti pokouší zavést do každodenního života) ověřit pravdivost informací do sféry soukromého či přímo intimního života si pak snadno lze představit.

Jsem přesvědčen, že na možnost bezpečného odhalení každé přetvářky, každého klamu či lži není naše společnost připravena, byť neustále deklaruje svou inklinaci k myšlenkám transparentnosti a upřímnosti. Nezbývá tak než doufat, že kdyby se tato hrůzná představa měla realizovat, přinese řešení problému ten samý zdroj, který jej i zapříčinil – masivní rozvoj technologií, který bude schopen přinést možnost, jak užívání této metody v běžném každodenním životě eliminovat. Pokud by tomu tak bylo a potenciálně v budoucnu spolehlivá metoda počítačové analýzy mikroexpresí by zůstala rezervována jen činnosti orgánů činných v trestním řízení a její použitelnost v každodenním životě by byla vyloučena, bylo by takový výsledek jistě možno považovat za optimální. Tyto představy jsou však již za hranicí spíše vědeckotechnických fantazií, než že by šlo o střízlivý odhad možného budoucího vývoje.

Nebude-li naopak z jakéhokoliv důvodu spolehlivost této metody ani v budoucnu vysoká, je prognóza mnohem jednodušší. Dokazování v trestním řízení by se o ni opírat nemohla. V takovém případě by bylo optimální zařazení metody počítačové analýzy mikroexpresí do fyziodetekčního vyšetření jako jedné z jeho složek. Sdílela by tak s ním i jeho právní režim, tedy mohla by jej obohatit coby potenciálně cenný prostředek získávání relevantních operativních informací, odkázaný na souhlas vyšetřované osoby, avšak důkazní použitelnost pro rozhodování v trestním řízení by byla vyloučena.

5. ZÁVĚR

Vzhledem k současné dosud brzké fázi vývoje metody počítačové analýzy mikroexpresí nelze již bezpečně usuzovat na to, zda půjde o revoluci v kriminalistice a bezpečnostně-právních oborech, nebo o jednu z mnoha slepých vývojových větví vědeckých snah zdokonalit odhalování a vyšetřování trestné činnosti či regulaci jiných sociálně patologických jevů. Jde však nepochybně o metodu slibně vypadající, jejíž další pokroky bude záhodno sledovat. Na jakékoliv závěry tak bude třeba si počkat, a i na prognózy eventuálního možného využití metody počítačové analýzy mikroexpresí v kriminalistické či dokonce rozhodovací praxi je tak ještě mnoho času a je možné, že na ně ani nedojde.

V každém případě se domnívám, že již dnes není na škodu nastínění základních mantinelů, v nichž by se tyto prognózy měly pohybovat. Právě to bylo jedním z cílů tohoto textu. Ten na svém počátku představil metodu analýzy mikroexpresí, vysvětlil její podstatu a výsledky jejího dosavadního vývoje. Ten se nachází spíše na počátku možných úvah o nějaké budoucí praktické aplikovatelnosti v kriminalistické či trestněprávní praxi.

V další části se tento text zamýšlí nad tím, jakou roli za předpokladu, že by tato metoda v budoucnu byla vypracována k forenzně relevantní spolehlivosti, by mohla hrát v současném instrumentáriu kriminalistických metod a jak by na ni mohly pohlížet soudy z důkazního hlediska. Za referenční kritérium bylo zvoleno fyziodetekční vyšetření, neboť mezi oběma metodami lze nalézt v relevantních aspektech podobné znaky. Text tak

pokračoval představením fyziodetekčního vyšetření ve světle práva a vyústil v předložení argumentů, proč by eventuálně při svém osvědčení se a zavedení do praxe metoda analýzy mikroexpresí měla podléhat stejnému právnímu režimu jako fyziodetekční vyšetření, jakož i argumentů, proč by její výsledky na rozdíl od ní mohly být použitelným důkazem pro rozhodnutí v trestním řízení. K tomu předkládám vlastní stanovisko.

Dospěl jsem tedy k závěru, že metoda analýzy mikroexpresí s využitím umělé inteligence vybavené *deep learningem* je zajímavým a slibně se rozvíjejícím projektem, jehož potenciál slibuje usnadnit vyhodnocování pravdivosti výpovědí, avšak ve svém současném stavu je však ještě dosti vzdálený reálnému využití v kriminalistické praxi, neboť v současném stavu je analýza mikroexpresí prováděna s využitím velmi obecných databází, neposkytujících ani dostatečnou kvantitu, ani dostatečnou kvalitu dat na to, aby výsledky byly zobecnitelné pro nahodilé prostředí. Přikláním se k důkazní použitelnosti této metody jenom tehdy, bude-li v budoucnu (patrně vzdáleném) robustním testováním prokázána její vysoká spolehlivost v nahodilých podmínkách.

6. POUŽITÉ ZDROJE

6.1 ODBORNÁ LITERATURA

[1] ALEXA, Gianina; ANDELIN, Emanuel; FEHER, Tiberiu. The Importance of Facial Micro-Expressions and Nonverbal Behavior in Psychological Evaluation. In: European Review of Applied Sociology. 2013, roč. 6, č. 7.

[2] BOND, Charles F.; DEPAULO, Bella M. Accuracy of Deception Judgments. In: Personality and Social Psychology Review. 2006, roč. 10, č. 3.

[3] BURGOON, Judee K. Microexpressions Are Not the Best Way to Catch a Liar. In: Frontiers in Psychology. 2018, roč. 9, čl. č. 1672.

[4] CANTER, David; ŽUKAUSKIENE, Rita Psychology and Law: Bridging the Gap. Routhledge: Abingdon, New York: 2008.

[5] DAVIDSON, Adrian K.; LANSLEY, Cliff; COSTEN, Nicholas; TAN, Kevin a YAP. Moi Hoon. SAMM: A Spontaneous Micro-Facial Movement Dataset. In: IEEE Transactions on Affective Computing. 2018, roč. 9, č. 1.

[6] EKMAN Paul; FRIESEN, Wallace V. Nonverbal Leakage and Clues to Deception. In: Psychiatry. Journal for the Study of Interpersonal Processes. 1969, roč. 32, č. 1.

[7] EKMAN, Paul. Telling Lies. Clues to Deceit in the Marketplace, Politics and Marriage. Londýn, New York: W. W. Norton & Company, 1991.

[8] FENYK, Jaroslav; GŘIVNA, Tomáš; CÍSAŘOVÁ, Dagmar, a kol. Trestní právo procesní. 7. vydání. Praha: Wolters Kluwer, 2019.

[9] HARTWIG, Maria; BOND, Charles F. Jr. Why do Lie-Catchers Fail? A Lens Model Meta-Analysis of Human Lie Judgments. In: Psychological Bulletin. 2011, roč. 137, č. 4.

[10] HURLEY, Carolyn M.; ANKER, Ashley E.; FRANK, Mark G.; MATSUMOTO, David; HWANG, Hyisung C. Background Factors predicting accuracy and improvement in micro expression recognition. In: Motivation and Emotion. 2014, roč. 38, č. 5.

[11] JELÍNEK, Jiří a kol. Trestní právo procesní. 2. aktualizované vydání. Praha: Leges, 2011.

[12] JORDAN, Sarah; BRIMBAL, Laura; WALLACE, Brian D. KASSIN, Saul M. HARTWIG, Maria; STREET, Chris N. H. A test of the micro-expressions training tool: Does it improve lie detection? In: Journal of Investigative Psychology and Offender Profiling. 2019, roč. 16, č. 3.

[13] KULKARNI, Kaustubh; CORNEANU, Ciprian; OFODILE, Ikechukwu a kol. Automatic Recognition of Facial Displays of Unfelt Emotions. In IEEE Transactions on Affective Computing [online], doi: 10.1109/TAFFC.2018.2874996

[14] LI, Xiaobai; HONG, Xiaopeng; MOILANEN, Antti; HUANG, Xiaohua; PFISTER, Tomas; ZHAO, Guoying; PIETIKÄINEN, Matti. Towards Reading Hidden Emotions: A Comparative Study of Spontaneous Micro-Expression Spotting and Recognition Methods. In: IEEE Transactions on Affective Computing, 2019, roč. 9, č. 4.

[15] MULÁK, Jiří. Základní zásady trestního řízení a právo na spravedlivý proces. Praha: Leges, 2019.

[16] MUSIL, Jan; KONRÁD, Zdeněk; SUCHÁNEK, Jaroslav. Kriminalistika. 2. přepracované vydání. Praha: C. H. Beck, 2004.

[17] NĚMEC, Miroslav a kol. Teorie a metodologie kriminalistiky pro magisterské studium II. Praha: Abook, 2019.

[18] NĚMEC, Miroslav. Kriminalistická taktika pro policisty a studenty Policejní akademie České republiky v Praze. Praha: ABOOK, 2017.

[19] OH, Yee-Hui; SEE, John; NGO, Anh Cat Le; PHAN, Raphael C.-W.; BASKARAN, Vishnu M. A Survey of Automatic Facial Micro-Expression Analysis: Databases, Methods and Challenges. In: Frontiers in Psychology. 2018, roč. 9, čl. č. 1128.

[20] PORTER, Stephen; TEN BRINKE, Leanne. Reading Between the Lies. Identifying Concealed and Falsified Emotions In Universal Facial Expressions. In: Psychological Science. 2008, roč. 19, č. 5.

[21] SU, Lin; LEVINE, Martin. Does „Lie to me“ lie to you? An evaluation of facial clues to high-stakes deception. In: Computer Vision and Image Understanding. 2016, roč. 147.

[22] ŠÁMAL, Pavel a kol. Trestní řád. Komentář. 7. vydání. Praha: C. H. Beck, 2013.

[23] ŠÁMAL, Pavel; MUSIL, Jan; KUCHTA, Josef a kol. Trestní právo procesní. 4. přepracované vydání. Praha: C. H. Beck, 2013.

[24] TAKALKAR, Madhumita; XU, Min; WU, QUIANG; CHACZKO, Zenon. A survey: facial micro-expression recognition. In: Multimedia Tools and Applications, 2018, roč. 77.

[25] TEN BRINKE, Leanne; PORTER, STEPHEN; BAKER, ALYSHA. Darwin the Detective: Observable facial muscle contractions reveal emotional high-stakes lies. In: Evolution and Human Behavior. 2012, roč. 33.

[26] VRIJ, Aldert; FISHER, Ronald P.Unraveling the Misconception About Deception and Nervous, Behavior. In: Frontiers in Psychology. 2020, roč. 11, čl. č. 1377.

[27] WANG, Yandan; SEE, John; OH, Yee-Hui; a kol. Effective recognition of facial micro-expressions with vide motion magnification. In: Multimedia Tools and Applications, 2017, roč. 76.

[28] YAN, Wen-Jing; WU, Qi, LIANG, Jing; CHEN, Yu-Hien; FU, Xiaolan. How Fast are the Leaked Facial Expressions: The Duration of Micro-Expressions. In: Journal of Nonverbal Behavior. 2013, roč. 37.

[29] ZHAO, Yue; XU, Jiancheng. An Improved Micro-Expression Recognition Method Based on Necessary Morphological Patches. In: Symmetry. 2019, roč. 11, č. 4.

[30] ZHOU, Ling; SHAO, XIUYAN; MAO, Qirong. A survey of micro-expression recognition. In: Image and Vision Computing. 2021, roč. 105, článek č. 104043, DOI: https://doi.org/10.1016/j.imavis.2020.104043 [online].

6.2 SOUDNÍ ROZHODNUTÍ

[31] Stanovisko pléna Ústavního soudu České republiky sp. zn. Pl.ÚS-st. 30/10 ze dne 30. 11. 2010 (ST 30/59 SbNU 595; 439/2010 Sb.)

[32] Nález Ústavního soudu České republiky sp. zn. III. ÚS 528/06 ze dne 11. 10. 2007 (N 159/47 SbNU 75).

[33] Rozhodnutí Nejvyššího soudu České republiky ze dne 25. 3. 1992, sp. zn. 6 To 12/92 (publ. na s. 26 pod č. Rt 8/1993 v č. 1-2 roč. 1993 Sbírky soudních rozhodnutí a stanovisek Nejvyššího soudu)

[34] Rozsudek ESLP ze dne 25. 2. 1993 ve věci Funke proti Francii, stížnost č. 10828/84.

[35] Rozsudek velkého senátu ESLP ze dne 8. 2. 1996 ve věci John Murray proti Spojenému království, stížnost č. 18731/91.

[36] Rozsudek velkého senátu ESLP ze dne 17. 12. 1996 ve věci Saunders proti Spojenému království, stížnost č. 19187/91.

[37] Rozsudek velkého senátu ESLP ze dne 21. 12. 2000 ve věci Heaney a McGuinness proti Irsku, stížnost č. 34720/97.

[38] Rozsudek velkého senátu ESLP ze dne 11. 7. 2006 ve věci Jalloh proti Německu, stížnost č. 54810/00.

[39] Usnesení Nejvyššího soudu České republiky ze dne 1. 7. 2009, sp. zn. 3 Tdo 737/2009.

[40] Rozsudek velkého senátu ESLP ze dne 1. 6. 2010 ve věci Gäfgen proti Německu, stížnost č. 22978/05.

[41] Usnesení Ústavního soudu České republiky ze dne 10. 3. 2015, sp. zn. II. ÚS 3651/13.

[42] Usnesení Ústavního soudu České republiky ze dne 23. 8. 2016, sp. zn. II. ÚS 265/16.

[43] Rozsudek velkého senátu ESLP ze dne 9. 11. 2018 ve věci Beuze proti Belgii, stížnost č. 71409/10.

[44] Rozsudek velkého senátu ESLP ze dne 4. 12. 2018 ve věci Ilnseher proti Německu, stížnosti č. 10211/12 a 27505/14.

[45] Usnesení Nejvyššího soudu ze dne 14. 4. 2020, sp. zn. 6 Tdo 347/2020.

[46] Nález Ústavního soudu České republiky sp. zn. II. ÚS 2369/08 ze dne 9. 12. 2010 (N 244/59 SbNU 489).

---

https://doi.org/10.5817/RPT2022-1-2

PRÁVO NA PŘÍSTUP K INTERNETU: SOUČASNÝ POSTOJ ORGANIZACE SPOJENÝCH NÁRODŮ A EVROPSKÉ UNIE[1]

MICHAELA PRUCKOVÁ[2]

ABSTRAKT

Dopad internetu na vykonávání lidských práv je nesporný. Představuje nástroj a platformu, skrz kterou jsou uplatňována některá z práv, jež nazýváme jako základní lidská práva (např. právo na informace, svobodu projevu, právo na vzdělání). Příspěvek se věnuje tématu práva na přístup k internetu, které zužuje na dvě jednotky (mezinárodní a nadnárodní) a lidsko-právní kontext. Jeho cílem je určit, jakou pozici zaujímá právo na přístup k internetu na úrovni těchto jednotek ve vztahu k základním lidským právům.

KLÍČOVÁ SLOVA

Právo na přístup k internetu, lidská práva, základní práva, internet, Organizace spojených národů, Evropská unie, společnost, cenzura, hard law, soft law

ABSTRACT

The impact of the Internet is indisputable. It serves as a tool and a platform through which some of the fundamental human rights are executed (right to information, freedom of expression, right to education etc.). This article deals

[1] Příspěvek vznikl jako soutěžní práce do Studentské vědecké a odborné činnosti v akademickém roce 2020/2021, který autorka obhajovala ve fakultním i česko-slovenském kole.

[2] Mgr. Michaela Prucková je studentkou magisterského studijního programu Právo a právní věda na Právnické fakultě Masarykovy univerzity. Kontaktní e-mail: 471380@mail.muni.cz.

with the topic of the right to Internet access while narrowing it to two units (international and transnational) and human rights context. Its goal is to determine the position of the right to Internet access according to those units in the designated context.

KEY WORDS

Right to the Internet Access, Human Rights, Fundamental Rights, Internet, United Nations, European Union, Society, Cenzorship, Hard Law, Soft Law

1. ÚVOD

Internetové připojení a přístup k internetovému obsahu se staly nedílnou součástí moderní společnosti. Internet je nástrojem, který společnost pomáhá utvářet i měnit. Médiem, pomocí něhož lidé komunikují, zjišťují a sdílí informace, vzdělávají se, pracují. Platformou, skrze kterou se formuje občanská společnost i sám jedinec. A prostorem pro uplatňování mnoha práv, včetně těch, která označujeme jako *základní lidská práva*.

Zároveň ale může být místem s negativními dopady. Nástrojem represe, cenzury, vyvolávání strachu; médiem pro šíření dezinformací,[3] misinformací,[4] nepřátelské propagandy; platformou pro omezování občanské společnosti a jedinců; obecně prostorem pro omezování práv. Proto se nabízí otázka, jak k internetu přistupují ti, kdo nastavují standardy současného světa. Tento příspěvek je věnuje právu na přístup k internetu; tématu, o němž by se dalo pojednávat obšírně, ať už v rámci polemiky, zda vůbec existuje, nebo diskuse o jeho obsahu. Proto je téma zúženo na dvě úrovně a lidsko-právní problematiku.

Vybranými úrovněmi jsou mezinárodní a nadnárodní. Mezinárodní scéna nastavuje standardy a minima, která by měla být dodržována. Ovšem v rovině konkrétních dopadů na národní státy (jako např. Českou republiku) je často nedostačující. Mezinárodní úroveň v článku reprezentuje Organizace spojených národů (OSN). Ačkoli existuje více mezinárodních or-

[3] Úmyslně lživá či falešná informace.

[4] Nezáměrně nepravdivá či falešná informace.

ganizací řešících lidská práva,[5] je to právě OSN se 193 členskými státy, kdo má největší potenciál zapojit do debaty téměř všechny aktéry.

Nadnárodní úroveň představuje Evropská unie (EU). Od mezinárodní se liší menším počtem členů (27 po odchodu Velké Británie), geografickým vymezením (primárně Evropský kontinent) a právním statusem. EU je svým členům ve vymezených oblastech působnosti nadřazena[6] a disponuje vlastním právním systémem. Proto má přímější dopad na národní legislativy členských zemí.

Lidsko-právní zúžení tématu vychází z premisy, že právo na přístup k internetu je posuzováno ve vztahu k základním lidským právům jako nástroj a platforma, skrz kterou jsou mnohá z těchto práv uplatňována.

Článek je postaven na kvalitativním způsobu zkoumání čili orientuje se na popis jevů, jejich objevování a odkrývání. Kvalitativní výzkum má vysvětlující charakter, přináší mnoho informací o malém počtu jevů za použití induktivního přístupu[7] a jeho smyslem je dosáhnout zobecnitelných tvrzení.[8] Přestože se článek zabývá skutečným stavem věcí (*de lege lata*), zabředává práce i do roviny *de lege ferenda*, jelikož polemizuje nad budoucím vývojem.

Jak píšou Dobinson a Johns,[9] kvalitativní právní výzkum by měl začínat určením cíle, jehož má být dosaženo. Cílem zde je popsat současnou pozici práva na přístup k internetu v kontextu lidsko-právního odvětví na úrovni mezinárodní a nadnárodní organizace; čímž vznikla výzkumná otázka: *Jakou pozici na úrovni Organizace spojených národů a Evropské unie zastává právo na přístup k internetu ve vztahu k základním lidským právům?*

K jejímu zodpovězení dojde na základě analýzy dvou typů dokumentů – hlavního lidsko-právního dokumentu dané úrovně a existujícího souvisejí-

---

[5] Např. Rada Evropy, Organizace pro bezpečnost a spolupráci v Evropě.

[6] Na rozdíl od mezinárodních organizací, jež členským státům nadřazeny nejsou.

[7] Vyvozování obecných závěrů z dílčích poznatků.

[8] HENDL, Jan a REMR, Jiří. *Metody výzkumu a evaluace*. 1. vydání. Praha: Portál, 2017.

[9] DOBINSON, Ian a JOHNS, Francis. Legal Research as Qualitative Research. In: MCCONVILLE, Mike a CHUI, Wing Hong. (eds.). *Research Methods for Law*. 2. vydání Edinburgh: Edinburgh University Press, 2007, s. 36.

ho právního předpisu, které budou konfrontovány se skutečným dopadem a stavem věcí a souvisejícími okolnostmi.

2. KONCEPTUALIZACE POJMŮ

2.1 ZÁKLADNÍ LIDSKÁ PRÁVA

Základní práva označují *lidská práva každého jedince*, která má od narození až do konce života, čistě z titulu, že je člověkem. Jsou od nich odvozena všechna ostatní lidská práva. Fungují na principu univerzálnosti, nezcizitelnosti, nedělitelnosti a vzájemné závislosti.[10] Z pohledu právní teorie představují *„závazná pravidla chování […] směřující k uskutečňování a reprodukci zvláště významných kvalit lidského života“*.[11]

2.1.1 GENERACE LIDSKÝCH PRÁV

Pro ucelenější pohled řadíme lidská práva (a svobody) do tzv. *generací* – skupin tvořených jednotlivými právy na základě jejich vývoje a obsahu. Generace se navzájem nevylučují ani si nekonkurují. Naopak na sebe navazují, překrývají se a mapují vývoj právního myšlení v otázkách, co je lidský jedinec zač, co potřebuje k (důstojnému) životu a co by mu mělo být garantováno.

Nabízených kategorizací je celá řada. Následující a jedno z nejčastěji používaných[12] dělení vychází z článku Karla Vašáka, který v roce 1977 v příspěvku A *30-year struggle: The sustained efforts to give force of law to the Universal Declaration of Human Rights* přišel se třemi generacemi:

[10] What are human rights? *United Nations Human Rights. Office of the High Commissioner* [online]. [cit. 17. 2. 2021]. Dostupné z: https://www.ohchr.org/en/issues/pages/whatarehumanrights.aspx

[11] BLAHOŽ, Josef. *Sjednocující se Evropa a lidská a občanská práva*. 1. vydání. Praha: ASPI, 2005, s. 12.

[12] DOMARADZKI, Spasimir a KHVOSTOVA, Margaryta a PUPOVAC, David. Karel Vasak's Generations of Rights and the Contemporary *Human Rights Discourse* [online]. 2019, č. 20. [cit. 20. 2. 2021]. s. 423-443.

1. Civilní a politická práva,
2. Ekonomická, sociální a kulturní práva,
3. Kolektivní a solidární práva.[13]

První generace odpovídá negativně vymezeným právům, jež vymezují sféru jedince, do níž stát nemá zasahovat. Druhá generace odpovídá pozitivně vymezeným právům, k jejichž naplnění je potřeba aktivní konání státu. Třetí generaci, která podle Vašáka v době psaní článku teprve vznikala, spojujeme se skupinami osob a mezinárodním systémem. Jedná se o pozitivně vymezená práva, objevující se v reakci na *„nesnáze moderního světa“*.[14] Konkrétně třetí generace obsahuje právo na rozvoj, právo na mír, právo na příznivé životní prostředí, právo na společné dědictví lidstva nebo právo na komunikaci.

Vašákovo má však dva hlavní nedostatky. Za prvé, opomíjí základní práva předcházející uvedeným – tzv. osobní práva, kam spadají právo na život, právo na osobní svobodu, vlastnické právo, právo na soukromí, svoboda myšlení nebo svoboda pobytu a pohybu.

A za druhé, je v podstatě zastaralé. V roce 1977 Vašák nemohl předvídat dnes nastoupivší a zatím nevyjasněnou čtvrtou generaci lidských práv. Dle různých výkladů do ní mohou patřit práva náležející lidstvu jako celku, práva související s kosmickým prostorem nebo práva související s genetickým inženýrstvím (bezpodmínečný zákaz některých aktivit).[15] Můžeme sem zařadit i právo na přístup k internetu, jakožto další právo, jež by mělo náležet celému lidstvu (pro důvody, jež jsou popsány dále v textu).

---

[13] VAŠÁK, Karel. A 30-year struggle: The sustained efforts to give force of law to the Universal Declaration of Human Rights. *The Unesco Courier* [online]. 1977 [cit. 20. 2. 2021], roč. 30, s. 29-31.

[14] HORŇÁČKOVÁ, Kristýna. *Rada pro lidská práva OSN a iniciativy v oblasti „nových lidských práv“* [online]. Brno, 2013. [cit. 17. 3. 2021]. Diplomová práce. Masarykova univerzita, Právnická fakulta, Katedra mezinárodního a evropského práva. Dostupné z: https://is.muni.cz/th/iubek/KH.pdf

[15] CORNESCU, Adrian Vasile. The Generations of Human's Rights. In: SEHNÁLEK, David a VALDHANS, Jiří a DÁVID, Radovan a KYNCL, Libor (eds.). *Dny práva – 2009 – Days of Law: the Conference Proceedings.* Brno: Masarykova univerzita, 2009. [cit. 17. 3. 2021]. Dostupné z: https://www.law.muni.cz/sborniky/dny_prava_2009/files/prispevky/tvorba_prava/Cornescu_Adrian_Vasile.pdf

Zároveň na úrovni OSN probíhá debata, zda čtvrtá generace nebude mít také za úkol modernizovat již existující lidská práva. S příchodem čtvrté průmyslové revoluce a moderních technologií je totiž těžší dostát závazkům z předchozích generací.[16] Ohroženo je právo na soukromí v důsledku užívání chytrých zařízení a shromažďování osobních informací o jedinci nebo právo na práci jako důsledek rušení pracovních pozic díky procesu digitalizace. Nemluvě o možnosti zneužít moderní technologie k cenzuře a narušení práva na svobodu projevu.

2.2 INTERNET

Podle Nového akademického slovníku cizích slov je internet *„celosvětová počítačová síť sloužící jako komunikační médium.“*[17] Konkrétnější a techničtější definici nabízí Výkladový slovník kybernetické bezpečnosti, podle něhož internet znamená *„globální systém propojených počítačových sítí, které používají standardní internetový protokol… Je to síť sítí, která se skládá z milionů soukromých, veřejných, akademických, obchodních a vládních sítí, s místním až globálním rozsahem, které jsou propojeny širokou škálou elektronických, bezdrátových a optických síťových technologií.“*[18]

V této počítačové síti jsou jednotlivá zařízení (počítače) propojená navzájem, díky čemuž si mohou vyměňovat informace (data). Informace se převádí na tzv. bity, které v podobě světelných nebo elektrických signálů putují do přijímacího zařízení, v němž jsou interpretována a tím se poskládá původní (odeslaná) informace.[19] Nic z toho by nefungovalo bez fyzických komponent – drátů, kabelů, infrastruktury, datových center, sítí procesorů aj.

---

[16] SOH, Changrok a CONNOLLY, Daniel a NAM, Seunghyun. Time for a Fourth Generation of Human Rights? *United Nations Research Institute for Social Development* [online]. 2018 [cit. 21. 2. 2021]. Dostupné z: https://www.unrisd.org/TechAndHumanRights-Soh-et-al

[17] KRAUS, Jiří (ed.). *Nový akademický slovník cizích slov*. 1. vydání, dotisk. Praha: Academia, 2009, s. 358.

[18] JIRÁSEK, Pavel a NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA, 2015, s. 59. [cit. 17. 3. 2021]. Dostupné z: https://www.cybersecurity.cz/data/slovnik_v310.pdf

[19] How does the Internet work? *Cloudfare* [online]. [cit. 19. 2. 2021]. Dostupné z: https://www.cloudflare.com/learning/network-layer/how-does-the-internet-work/

2.3 PRÁVO NA PŘÍSTUP K INTERNETU

Právo na přístup k internetu je tvořeno dvěma částmi – (1) právem na internetové připojení a (2) právem na přístup k internetovému obsahu.

Právo na internetové připojení označuje možnost se dostat k internetovému připojení. Je to stav, kdy je jedinec připojen a může prostřednictvím internetu vykonávat další práva. Skládá se z dílčích částí, jež dohromady dávají možnost se připojit. Internet – ač je virtuální doménou – funguje na reálné fyzické infrastruktuře. Osoba, která se chce připojit, musí vlastnit zařízení či mít přístup k zařízení, z něhož se připojí. Má-li to být z vlastního zařízení, potřebuje finance na toto zařízení i finance na zaplacení připojení. Toto není vyčerpávají výčet a nepokrývá všechny kroky potřebné k tomu, aby člověk mohl být připojen. Má pouze naznačit, že otázka internetového připojení není jen o tom, zda jedinec *má či nemá internet*.

Právo na přístup k internetovému obsahu je spojováno s výkonem práv na svobodu projevu a přijímání informací.[20] Jeho provedení je sice jednodušší než zajištění přístupu k internetu, na druhou stranu se ale dotýká citlivých (často politických) otázek. I proto se nabízí zmínit *cenzuru* – omezování, potlačování a zakazování informací určených ke zveřejnění,[21] projevující se na internetu jako blokování obsahu – jelikož toto právo není všeobecně respektováno a dodržováno.

Je třeba uvést, že termín *právo* v sobě nutně nenese *nárok* ve smyslu možnosti domáhat se ochrany jeho realizace.[22] Existencí práva na internetové připojení automaticky nevzniká někomu povinnost zajistit, aby bylo k dispozici všem. Uznáním práva na internetové připojení se deklaruje nový autonomní prostor jedince, do něhož by stát (či jiná entita) neměl zasahovat, případně by měl zásah co nejvíce omezit a provádět jen v rámci předem vytyčených a schválených mantinelů.

---

[20] FIALOVÁ, Eva. Právo na přístup k internetu. *Právník* [online]. 2018 [cit. 15. 2. 2021], roč. 157, č. 7, s. 545-557.

[21] KRAUS, Jiří (ed.). *Nový akademický slovník cizích slov*. 1. vydání, dotisk. Praha: Academia, 2009, s. 132.

[22] KNAPP, Viktor. *Teorie práva.* 1. vydání. Praha: C. H. Beck, 1999, s. 197.

Aby se neustále neopakovalo spojení *právo na přístup k internetu*, bude využíváno i dalších označení – právo na internet, právo k internetu, právo na (internetové) připojení, právo k internetovému přístupu. Nebude-li řečeno jinak, zahrnují pojmenování obě části dotčeného práva.

3. UKOTVENÍ ZÁKLADNÍCH LIDSKÝCH PRÁV

Následující kapitola představuje hlavní lidskoprávní dokument vybrané úrovně. U OSN je to Všeobecná deklarace lidských práv, u EU Listina základních práv Evropské unie. V obou dokumentech jsou hledána ustanovení, jež bychom mohli aplikovat i na právo na přístup k internetu.

3.1 ORGANIZACE SPOJENÝCH NÁRODŮ

Všeobecná deklarace lidských práv (VDLP) představuje základní a pravděpodobně nejznámější lidskoprávní dokument, z něhož vycházejí další dokumenty s lidskoprávní tematikou a katalogy lidských práv jednotlivých států. Byla přijata 10. prosince roku 1948, v den, který od roku 1950 oslavujeme jako *Den lidských práv*.

Skládá se z celkem 30 článků, pokrývající práva hospodářská, občanská, politická, sociální a kulturní, která jsou přiznána každému jedinci bez ohledu na státní útvary. Přestože se jedná o právně nezávazný dokument, je jeho částečná vynutitelnost zajištěna čl. 55 a 56 Charty OSN, která je sama považovaná za první závazný akt právního významu, který se zabývá lidskými a občanskými právy.[23]

V souladu s čl. 55 písm. c) mají členské státy OSN podporovat *„obecnou úctu k lidským právům a základním svobodám pro všechny bez rozdílu rasy, pohlaví, jazyka nebo náboženství a jejich zachovávání“*. Čl. 56 zavazuje státy ke konání, jež povede k dosažení cílů z čl. 55.[24] Na základě těchto ustanovení jsou minimálně členské státy povinny se zněním deklarace řídit.

[23] BLAHOŽ, Josef. *Sjednocující se Evropa a lidská a občanská práva*. 1. vydání. Praha: ASPI, 2005, s. 218.

[24] Členové se zavazují společně i jednotlivě jednat v součinnosti s Organizací, aby bylo dosaženo cílů stanovených v článku 55.

Následující demonstrativní výčet je zúžen na ustanovení související s právem na přístup k internetu.

Čl. 19	Každý má právo na svobodu přesvědčení a projevu; toto právo nepřipouští, aby někdo trpěl újmu pro své přesvědčení, a zahrnuje právo vyhledávat, přijímat a rozšiřovat informace a myšlenky jakýmikoli prostředky a bez ohledu na hranice.
Čl. 25	Každý má právo na takovou životní úroveň, která by byla s to zajistit jeho zdraví a blahobyt i zdraví a blahobyt jeho rodiny, počítajíc v to zejména výživu, šatstvo, byt a lékařskou péči, jakož i nezbytná sociální opatření [...].
Čl. 26	Každý má právo na vzdělání [...].
Čl. 27	Každý má právo svobodně se účastnit kulturního života společnosti, užívat plodů umění a podílet se na vědeckém pokroku a jeho výtěžcích.

Tabulka 1: Vybraná práva obsažená ve Všeobecné deklaraci lidských práv. Autor: Michaela Prucková, zdroj: Všeobecná deklarace lidských práv.

3.2 EVROPSKÁ UNIE

Základní lidská práva na úrovni EU jsou zaručena ústavami jednotlivých členských zemí a *Listinou základních práv Evropské unie* (2012/C 326/02).[25] Ta jakožto základní unijní lidskoprávní dokument obsahuje výčet základnách práv, jež jsou závazná pro orgány a instituce EU a jednotlivé státy, jejichž legislativa musí být s unijními pravidly v souladu. Inspirovaná je mj. Evropskou úmluvou o lidských právech (1950) a Evropskou sociální chartou (1989)[26] a některá její práva jsou stanovena i ve Smlouvě o Evropské unii.[27]

Práce na tvorbě unijní Listiny základních práv (LZP EU) začaly v roce 1999. Cílem Evropské rady, která si její vznik vyžádala, bylo sjednotit

[25] Někdy nazývaná jako Charta základních práv Evropské unie.

[26] Charta základních práv EU. *Euroskop.cz* [online]. [cit. 23. 2. 2021]. Dostupné z: https://euroskop.cz/627/sekce/charta-zakladnich-prav-eu/

[27] Konsolidované znění Smlouvy o Evropské unii a Smlouvy o fungování Evropské unie (2012/C 326/01).

základní práva na unijní úrovni do jediného dokumentu a zvýšit povědomí o jejich existenci.[28] Vytvoření nových práv mezi cíle nepatřilo. K deklaraci Listiny došlo 7. prosince 2000 na zasedání Evropské rady ve francouzském Nice. Tato verze nebyla právně závazná, přesto se členské státy zavázaly ji dodržovat.

Závaznou se LZP EU[29] stala po ratifikaci Lisabonské smlouvy, tedy 1. prosince 2009, poté, co ji podepsal poslední zbývající stát EU – Česká republika (ČR).[30] Oproti VDLP má výhodu v tom, že spadá do kategorie *hard law*.[31]

Skládá se z 54 článků rozdělených do preambule a sedmi hlav: (1) Důstojnost, (2) Svobody, (3) Rovnost, (4) Solidarita, (5) Občanská práva, (6) Soudnictví, (7) Obecná ustanovení upravující výklad a použití Listiny.

Následující demonstrativní výčet je zúžen na ustanovení související s právem na přístup k internetu.

[28] Charta základních práv EU. *Euroskop.cz* [online]. [cit. 23. 2. 2021]. Dostupné z: https://euroskop.cz/627/sekce/charta-zakladnich-prav-eu/

[29] Evropská unie. *Listina základních práv Evropské unie, 2012/C 326/02* [online]. [cit. 20. 2. 2021]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A12012P%2FTXT

[30] Lisabonská smlouva. *Ministerstvo vnitra České republiky* [online]. 2011 [cit. 25. 2. 2021]. Dostupné z: https://www.mvcr.cz/clanek/agenda-eu-na-mv-lisabonska-smlouva.aspx

[31] *Hard law* označuje právně závazná ustanovení. Naproti tomu *soft law* závaznost postrádá.

Čl. 11	Každý má právo na svobodu projevu. Toto právo zahrnuje svobodu zastávat názory a přijímat a rozšiřovat informace nebo myšlenky bez zasahování veřejné moci a bez ohledu na hranice.
Čl. 14	Každý má právo na vzdělání a přístup k odbornému a dalšímu vzdělávání.
Čl. 21	Zakazuje se jakákoli diskriminace založená zejména na pohlaví, rase, barvě pleti, etnickém nebo sociálním původu, genetických rysech, jazyku, náboženském vyznání nebo přesvědčení, politických názorech či jakýchkoli jiných názorech, příslušnosti k národnostní menšině, majetku, narození, zdravotním postižení, věku nebo sexuální orientaci.
Čl. 25	Unie uznává a respektuje práva starších osob na to, aby vedly důstojný a nezávislý život a podílely se na společenském a kulturním životě.

Tabulka 2: Vybraná práva obsažená v Listině základních práv Evropské unie. Autor: Michaela Prucková, zdroj: Listina základních práv Evropské unie (2012/C 326/02).

4. POSTOJE K PRÁVU NA PŘÍSTUP K INTERNETU

4.1 ORGANIZACE SPOJENÝCH NÁRODŮ

Ústředním článkem VDLP ve vztahu k otázce o právu k internetovému připojení je čl. 19:

„*Každý má právo na svobodu přesvědčení a projevu; toto právo nepřipouští, aby někdo trpěl újmu pro své přesvědčení, a zahrnuje právo vyhledávat, přijímat a rozšiřovat informace a myšlenky jakýmikoli prostředky a bez ohledu na hranice.*“

Z něj vychází právně nezávazná rezoluce OSN – *Podpora, ochrana a výkon lidských práv na internetu* A/HRC/32/L.20 z 27. června 2016,[32] okolo níž se debata točí.

[32] United Nations, General Assembly, Human Rights Council. *Oral Revisions of 30 June, no. A/HRC/32/L.20. The promotion, protection and enjoyment of human rights on the Internet* [online]. 27. 6. 2016 [cit. 4. 3. 2021]. Dostupné z: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

Přisouzení tématu k čl. 19 odpovídá tomu, že internet a přístup k němu představuje v moderních společnostech jeden ze základních nástrojů vyhledávání, přijímání a šíření informací (a myšlenek). Internetové připojení je prostředkem uvedeného skutečně *„bez ohledu na hranice“*. Šíření informací, přesvědčení a obecně jakéhokoliv projevu ztratilo díky internetu řadu předchozích omezení, a lze tak oslovit jedince a masy kdekoliv ve světě. Kromě čl. 19 lze v textu najít odkazy na další články, např. čl. 25 (právo na přiměřenou životní úroveň)[33] a čl. 26 (právo na vzdělání).[34]

Přístup k internetu ale není pro rezoluci hlavním tématem. Internet zde představuje nástroj, skrze který lze uplatňovat základní práva popsaná ve VDLP. Vydání rezoluce přitom provázely mediální výstupy, ohlašující vznik nového základního práva.[35] Nic takového se ale nestalo a právo na internet v rezoluci není popsáno jako základní lidské právo.[36] Naopak, rezoluce je psaná velmi opatrně a vyhýbá se tomu, aby přístup k internetu označovala jako *právo*. Jejím primárním cílem je deklarovat, že práva existující off-line nepozbývají v online světě platnosti a účinnosti, a že internet hraje základní roli při jejich uplatňování.[37] Snaží se nastavit mezinárodní standard v přístupu států k internetu, nikoli volat po odpovědnosti, aby byl zajištěn přístup pro všechny.[38]

Rezoluce shrnuje svá prohlášení do 15 bodů, v nichž mimo jiné...:

---

[33] Odst. 1. Každý má právo na takovou životní úroveň, která by byla s to zajistit jeho zdraví a blahobyt i zdraví a blahobyt jeho rodiny [...].

[34] Odst. 1. Každý má právo na vzdělání.

[35] Např. HOWELL, Catherine. a WEST, Darrell M. The internet as a human right. *Brookings.edu* [online]. 2016 [cit. 23. 2. 2021]. Dostupné z: https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/; SANDLE, Tim. UN thinks internet access is a human right. *Business Insider* [online]. 2016 [cit. 23. 2. 2021]. Dostupné z: https://www.businessinsider.com/un-says-internet-access-is-a-human-right-2016-7; HEICK, Terry. UN: Internet Access Is Now A Basic Human Right. *Teach Thought* [online]. 2016 [cit. 23. 2. 2021]. Dostupné z: https://www.teachthought.com/technology/un-internet-access-now-basic-human-right/

[36] SZOSZKIEVICZ, Łukasz. Internet Access as a New Human Right? State of the Art on the Threshold of 2020. *Adam Mickiewicz University Law Review* [online]. 2018 [cit. 4. 3. 2021], roč. 8, s. 50.

[37] Že svoboda projevu a další práva platí i online připomínají a opakují i další dokumenty OSN, např. Zpráva zvláštního zpravodaje o podpoře ochraně práva na svobodu názoru a projevu A/HRC/35/22.

Bod č. 1	Potvrzuje, že práva lidí off-line (ve fyzickém světě) musí být chráněna také na on-line (na internetu), s důrazem na svobodu projevu.
Bod č. 2	Uznává globální a otevřenou povahu internetu jakožto hybné síly pro urychlování pokroku, včetně dosahování cílů udržitelného rozvoje.
Bod č. 4	Uznává, že pro rozvoj je rozhodující kvalitní vzdělání, a proto vyzývá všechny státy, aby podporovaly digitální gramotnost a usnadňovaly přístup k informacím na internetu.
Bod č. 9	Jednoznačně odsuzuje porušování lidských práv (mučení, vyhošťování, zastrašování aj.) páchané na jedincích v reakci na výkon lidských práv a základních svobod na internetu, a vyzývá státy k přijetí odpovědnosti.
Bod č. 10	Jednoznačně odsuzuje opatření vedoucí k úmyslnému zabraňování nebo narušování přístupu na internet nebo šíření informací on-line a vyzývá státy, aby od takových opatření upustily.
Bod č. 12	Vyzývá státy, aby zvážily formulování a přijetí vnitrostátních politik týkajících se internetu, jejichž jádrem by bylo zajištění univerzálního přístupu a dodržování lidských práv.

Tabulka 3: Vybraná ustanovení rezoluce A/HRC/32/L.20 *Podpora, ochrana a výkon lidských práv na internetu*. Autor: Michaela Prucková, zdroj: United Nations, General Assembly, Human Rights Council.

4.1.1 DOPAD POSTOJE OSN

Účelem rezoluce je ukázat postoj mezinárodního společenství v oblasti lidských práv tak, aby nedocházelo k porušování VDLP. Problém představuje určitá *bezzubost*, kterou OSN v při použití tohoto formátu trpí. Jelikož rezoluce spadá do oblasti *soft law* a nevyvolává právní důsledky, postrádá

[38] BARRY, Jack J. COVID-19 exposes why access to the internet is a human right. *Open Global Rights* [online]. 2020 [cit. 20. 2. 2021]. Dostupné z: https://www.openglobalrights.org/covid-19-exposes-why-access-to-internet-is-human-right/

OSN mechanismus, kterým by státy od jednání, které je s ní v rozporu, odradila.

Problémem mohou být samotní členové OSN, pokud nerespektují a nedodržují postoje, principy a standardy, které organizace deklaruje. V případě této rezoluce se nabízí zaměřit se na cenzuru obsahu internetu jakožto konání, které je s ní v rozporu (bod č. 10).[39]

Přitom příkladem asi nejznámějšího státu cenzurujícího obsah na internetu je člen OSN – Turecká republika. Země, která stála u tvorby návrhu usnesení rezoluce a jen za rok 2019 zablokovala na svém území více než 400 tisíc webových stránek. Internetový obsah je v Turecku blokován od roku 2014, kdy byl upraven zákon o internetu. Obětí cenzury se staly mj. Facebook, Google Apps, Instagram, OneDrive, Twitter, Wikipedia nebo YouTube.[40]

Podobné restrikce uplatňuje Čínská lidová republika (ČLR), stálý člen Rady bezpečnosti OSN (RB OSN).[41] Ta se kromě webových stránek a sociálních sítí zaměřuje na zpravodajské servery, jejichž obsah nekoresponduje s oficiálním čínským narativem. Na území nefungují stránky BBC, CNN, New York Times nebo Wall Street Journal. Blokovány jsou např. Faceebok a Messenger, Google Apps, Instagram, Twitter, Wikipedie, YouTube, Reddit, Slack, Snapchat i Spotify.[42] Také Ruská federace (RF)[43] – další stálý člen RB OSN – je známá zasahováním do svobod k internetu i na internetu. Kromě blokování *škodlivého* obsahu se zaměřuje na kontrolu internetové infrastruktury. Roste i tendence úplně zemi izolovat od celosvětového systé-

[39] Rezoluce odsuzuje opatření vedoucí k úmyslnému zabraňování nebo narušování přístupu na internet nebo šíření informací online a vyzývá státy, aby od takových opatření upustily.

[40] EDWARDS, Luke. What websites and online services are blocked in Turkey – Facebook, Wikipedia and more. *Techradar.com* [online]. 2020 [cit. 15. 2. 2021]. Dostupné z: https://www.techradar.com/vpn/websites-online-services-blocked-turkey-facebook-wikipedia

[41] Jediný orgán OSN, jež může vydávat závazné rezoluce a jejich splnění vymáhat silou.

[42] FRENCH, Darcy. Which websites and online services are banned in China? In: *Techradar.com* [online]. 2020 [cit. 17. 2. 2021]. Dostupné z: https://www.techradar.com/vpn/which-websites-and-online-services-are-banned-in-china

[43] Příspěvek vznikl před válkou na Ukrajině a neobsahuje tedy informace o masivním a bezprecedentním omezování internetového přístupu, k němuž se Rusko uchyluje od března 2022. Na druhou stranu, o to aktuálnější tato debata nyní je.

mu prohlížení *World Wide Web*, což by pro ruské internetové uživatele znamenalo ztrátu on-line kontaktu s okolním světem.[44] Je otázkou, zda odříznutí od světového prohlížeče zasahuje do připojení ve smyslu, že internet nebude dostupný. Čistě ruský internet by dostupný byl, byť v omezeném rozsahu a na základě cenzury. Bezesporu by však bylo porušeno právo na internetový obsah.

Že vlády zasahováním do internetového připojení často nedodržují lidskoprávní standardy, uznává i OSN Zpráva zvláštního zpravodaje o podpoře ochraně práva na svobodu názoru a projevu A/HRC/35/22 z roku 2017, podle níž *„státy stále více uplatňují cenzuru prostřednictvím soukromého sektoru“*.[45] Tato zpráva, orientující se primárně na právo na přístup k internetovému obsahu, se nevěnuje pouze státním aktérům, ale i soukromým společnostem a jejich roli při ochraně nebo naopak podrývání lidských práv ve spojitosti s internetem. Ačkoli zpráva rámuje státy jako hlavní aktéry omezující práva na svobodu názoru a projevu online, přehazuje část odpovědnosti i na soukromý sektor, který by měl podle zvláštního zpravodaje při výkonu své (výdělečné) činnosti dodržovat lidskoprávní zásady.

Vrátíme-li se k rezoluci, z formálního pohledu splňuje všechny požadavky kladené na tento typ předpisu. Má však zásadní problém z materiálního pohledu. Postrádá vnitřní koherenci, což plyne mj. z toho, že jeden z nejznámějších cenzorů obsahu internetu (Turecká republika) stál za vznikem návrhu jejího znění, a dva stálí členové RB OSN (ČLR a RF), mající v OSN značný vliv, nedodržují prohlášení v ní obsažená.

4.2 EVROPSKÁ UNIE

Stěžejní dokument na úrovni EU o právu k internetu je v současnosti stále ještě nařízení EU 2015/2120 ze dne 25. listopadu 2015, kterým se stanoví

---

[44] Russia: Growing Internet Isolation, Control, Censorship. *Human Rights Watch* [online]. 2020 [cit. 20. 2. 2021]. Dostupné z: https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship

[45] United Nations, General Assembly, Human Rights Council. *A/HRC/35/22. Report of the Special Rapporteur on the promotion and Protection of the right to freedom of opinion and expression* [online]. 23. 6. 2017 [cit. 26. 8. 2021], s. 20. Dostupné z: https://www.ohchr.org/en/issues/freedomopinion/pages/sr2017reporttohrc.aspx

opatření týkající se přístupu k otevřenému internetu a mění směrnici 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 – zkráceně *nařízení o otevřeném přístupu k internetu*, platné od 30. dubna 2016.

Jako u OSN se nejedná o deklaraci práva na přístup k internetu ani jeho uznání za základní právo. Nařízení internetovému připojení přiznává důležitou roli v zajišťování fungování společnosti a vývoje, ale jeho účelem není lidskoprávní debata, nýbrž určení pravidel *„pro zajištění rovného a nediskriminačního nakládání s provozem při poskytování služeb přístupu k internetu“* a vytvoření mechanismu pro tvorbu *„maloobchodních cen za regulované roamingové služby na území Unie s cílem zrušit maloobchodní příplatky za roaming“* (čl. 1 odst. 1 a 2).

Internet je brán jako otevřená platforma, k níž mají mít koncoví uživatelé přístup, aniž by docházelo k blokování, diskriminování nebo naopak upřednostňování obsahu a služeb. V textu je přímo stanoveno, že EU respektuje zásadu technologické neutrality.[46] Dodržována je i zásada neutrality sítě,[47] přestože není výslovně zmíněna. Nařízení stanovuje povinnost státům, aby koncovým uživatelům umožnily požívání práva na přístup k informacím, obsahu a šíření tohoto obsahu podle vlastního výběru (čl. 3 odst. 1) a aby je nikdo pro tento výběr nemohl diskriminovat (ve smyslu zamezování nebo zpomalování toku odesílaných či přijímaných dat) (čl. 3 odst. 3). Co se roamingu týče, byl zrušen k 15. červnu 2017 ve všech členských státech EU.[48]

4.2.1 DOPAD POSTOJE EU

Nařízení o otevřeném internetu pomohlo nastavit jednotná pravidla fungování internetu a jedincům zaručilo, že nesmí docházet k porušování jejich

[46] *„Svoboda jednotlivců nebo organizací vybrat si nejvhodnější technologii, která nejlépe odpovídá jejich potřebám.“* Definováno ve výstupu Komise *Podpora telekomunikačních sítí a infrastruktur digitálních služeb v Evropě.*

[47] Zásada stejného nakládání se všemi internetovými daty ze strany poskytovatelů internetových služeb bez ohledu na jejich povahy, zdroj, destinaci.

[48] Čl. 7. Změny nařízení (EU) č. 531/2012 jako čl. 6a.

práva na svobodu projevu podle č. 11 LZP EU.[49] Unie považuje nařízení za svůj *„významný úspěch jednotného digitálního trhu“*.[50]

Tím, že zakazuje případnou diskriminaci obsahu a služeb, je zároveň v souladu s čl. 21 LZP EU o zákazu diskriminace. Navíc je internetové připojení považováno za *„univerzální službu“*, což znamená, že jedinci členských zemí musí mít možnost získat přístup k internetu za dostupnou cenu.[51] Ani tak ale předpis nereflektuje, že ne všichni obyvatelé mají prostředky se připojit. EU deklaruje důležitost internetu pro společnost a její vývoj, ale neřeší, jak zajistit připojení i pro ty, co si ho nemohou dovolit – 13 procent domácností v roce 2020.[52]

Že je přístup k internetu *„novým lidským právem“*, prohlásila předsedkyně Evropské komise (EK) Ursula von der Lyen na konci roku 2020 v projevu,[53] v němž dále řekla, že Unie zajistila, aby se mohl každý připojit k internetu a aby byl internetový provoz neutrální. Nastínila i přípravu nových pravidel, jejichž cílem bude bojovat proti dezinformacím nebo nelegálnímu zboží a obsahu na internetu.

Jedna z těchto budoucích restrikcí byla pod názvem *Návrh nařízení o jednotném trhu digitálních služeb (nařízení o digitálních službách)* představena v prosinci 2020 a v současnosti prochází schvalovacím procesem.[54] Cílem je mj. zavést povinnost transparentnosti modelu a algoritmu

---

[49] Každý má právo na svobodu projevu. Toto právo zahrnuje svobodu zastávat názory a přijímat a rozšiřovat informace nebo myšlenky bez zasahování veřejné moci a bez ohledu na hranice.

[50] Open Internet. *European Commission* [online]. [cit. 23. 2. 2021]. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/open-internet

[51] Používání internetu a přístup k němu. *Europa.eu* [online]. [cit. 23. 2. 2021]. Dostupné z: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/internet-access/index_cs.htm

[52] THORNHILL, John. Internet access is both a human right and a business opportunity. *Financial Times* [online]. 2020 [cit. 17. 2. 2021]. Dostupné z: https://www.ft.com/content/872dc219-d4d8-4896-92d3-7f9d45a5ce90

[53] Statement by President von der Leyen at the roundtable ‘Internet, a new human right' after the intervention by Simona Levi. *European Commission* [online]. 2020 [cit. 23. 2. 2021]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/statement_20_2001

[54] The Digital Services Act: ensuring a safe and accountable online environment. *European Commission* [online]. [cit. 25. 2. 2021]. Dostupné z: https://ec.europa.eu/info/digitalservices-act-ensuring-safe-and-accountable-online-environment_en

jednotlivým digitálním službám. Dále prochází schvalováním další dva předpisy – *návrh nařízení o spravedlivých trzích otevřených hospodářské soutěži v digitálním odvětví (nařízení o digitálních trzích)* a *Evropský akční plán pro demokracii*. Také ty souvisí s právem na internet a představují reakci EK na posun v potřebách evropské společnosti, které se z velké části přesunuly do online prostředí. Nařízení o digitálních trzích má za cíl zabránit silným hráčům na digitálních trzích zneužívat jejich sílu proti menším a slabším.[55]

Účelem Akčního plánu je posílení demokracie na základě priorit stanovených ve třech pilířích:

1. Propagace svobodných a spravedlivých voleb,
2. Posílení svobody a plurality sdělovacích prostředků,
3. Boj proti dezinformacím.

Ač se to na první pohled nemusí zdát, zaměření Akčního plánu směřuje k internetovému obsahu – jelikož ten bývá zdrojem rychle se šířích dezinformací a misinformací. Cílem je např. přepracovat kodex *„zásad boje proti dezinformacím na společný regulační rámec povinností a odpovědnosti online platforem v souladu s připravovaným aktem o digitálních službách“*.[56]

Všechny tři návrhy mají nastavit nová pravidla internetového obsahu a jeho zhodnocování, nikoli zavést cenzuru a kontrolu. Přesto je hranice velmi tenká a při nesprávné aplikaci by mohlo dojít k zásahům do práva na internetový obsah unijních uživatelů. Důležitost internetu je na půdě EU uznána, čímž se stává zdrojem pro nové regulace.

Ačkoli uznáním internetového přístupu jako nového lidského práva ústy předsedkyně EK nevzniká občanovi EU nebo jedinci pobývajícímu v EU nárok na přístup k internetu, snaží se unie nad rámec vlastních pravidel zajistit, aby přístupu požívalo co nejvíce osob. Konkrétním řešením je např. iniciativa WiFi4EU, jejímž cílem bylo do roku 2020 pokrýt bezdrátovým bezplatným internetovým přístupem veřejná prostranství, jako jsou parky, bu-

[55] The Digital Markets Act: ensuring fair and open digital markets. *European Commission* [online]. [cit. 3. 3. 2021]. Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

[56] European Democracy Action Plan: making EU democracies stronger. *European Commission* [online]. 2020 [cit. 3. 3. 2021]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250

dovy, náměstí či nemocnice ve státech EU.[57] WiFi4EU však může být účinná pouze za *normálního* stavu, nikoli v době, kdy je omezen volný pohyb osob a bezplatným připojení pokrytá místa jsou pro ty, co ho nejvíc potřebují, nedosažitelná.

4.3 SOUHRNNÁ DISKUSE NAD PŘÍSTUPY OSN A EU

Na úvod je třeba rozlišit mezi pozitivním a negativním právem a konsekvencemi, které takové rozlišení přináší. Jak zmiňuje Fialová,[58] pokud by právo na internet bylo formulováno jako pozitivní závazek, bylo by povinností pověřených entit přístup k internetu zajistit. Všem a celoplošně. Mezinárodní organizace, nadnárodní organizace nebo stát by na sebe vzaly odpovědnost za to, že připojit se budou moci všichni. Negativně formulované právo by zase entity zavazovalo, aby se vzdaly zásahu do tohoto práva.

Podle toho, jak je právo na internet posuzováno, může docházet ke dvojímu porušování práv– buďto je zasahováno do práva na připojení, nebo je porušování způsobeno cenzurou obsahu. Internetového připojení v současnosti požívá zhruba 50 procent lidské populace,[59] respektive na 5 miliard a 12 milionu osob k 15. srpnu 2021.[60] Zbytek k internetu nemá přístup. V Evropě nebylo v roce 2020 připojeno na 13 procent domácností, v Africe 82 procent.[61] Ačkoli je internet zprostředkovatelem mnoha práv (včetně práv základních), asi polovina obyvatel planety se na jejich uplatňování nedokáže podílet.

---

[57] WiFi4EU. *European Commission* [online]. [cit. 23. 2. 2021]. Dostupné z: https://digitalstrategy.ec.europa.eu/cs/activities/wifi4eu

[58] FIALOVÁ, Eva. Právo na přístup k internetu. *Právník* [online]. 2018 [cit. 15. 2. 2021], roč. 157, č. 7, s. 545-557.

[59] The Impact of Digital Technologies. *United Nations* [online]. [cit. 3. 3. 2021]. Dostupné z: https://www.un.org/en/un75/impact-digital-technologies#:~:text=Digital%20technologies%20have%20advanced%20more,can%20be%20a%20great%20equaliser

[60] Internet Users. *Internet Live Stats* [online]. [cit. 15. 8. 2021]. Dostupné z: https://www.internetlivestats.com/internet-users/

[61] THORNHILL, John. Internet access is both a human right and a business opportunity. *Financial Times* [online]. 2020 [cit. 17. 2. 2021]. Dostupné z: https://www.ft.com/content/872dc219-d4d8-4896-92d3-7f9d45a5ce90

Přitom závislost společností na internetovém připojení je vidět všude. EU měří užívání internetu za pomocí *Indexu digitální ekonomiky a společnosti* (DESI). Ze zmíněných 13 procent domácností, které k internetu v roce 2020 v unii neměly přístup, se podle DESI jedná o 15 procent unijních občanů.

Mezi nejčastější úkony na internetu na unijní úrovni patří konzumace online obsahu (hudby, filmů, televize, médií, her), komunikace (sociální média, video platformy) nebo transakční aktivity (online nakupování, online bankovnictví).[62] Mimo to internet slouží ke komunikaci s veřejnou správou, skrze tzv. e-government (elektronická veřejná správa), který např. Ministerstvo vnitra ČR definuje jako *„správu věcí veřejných za využití moderních elektronických nástrojů, díky kterým bude veřejná správa k občanům přátelštější, dostupnější, efektivnější, rychlejší a levnější“*.[63] V současnosti na úrovni EU využívá e-governmentu zhruba 67 procent unijních obyvatel.[64]

Na úrovni ČR je e-government tvořen hlavně kontaktními místy veřejné správy Czech POINT, datovými schránkami a systémem základních registrů. Některé státy unie jsou ale ještě dál. Estonsko jakožto průkopník online veřejné správy má na 99 procent veřejných služeb online a dovoluje svým občanům přes internet volit, platit daně, platit parkovné nebo získávat digitální občanství.[65] Což už pro jedince bez připojení může být omezující, zvláště, je-li využívání těchto služeb online preferováno.

Proto Reglitz zastává názor, že právo na přístup k internetu by mělo být základním lidským právem, a že každý by měl mít neomezený a nesledovaný přístup.[66] Vychází z teze, že bez internetu nelze prožít důstojný život. Takový názor podporují i výsledky studie University of Birmingham, podle kterých nepřipojený jedinec ztrácí v globálním světě možnost podílet

[62] Use of Internet and Online Activities. *European Commission* [online]. [cit. 3. 3. 2021]. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/desi-use-internet

[63] Co je to eGovernment? *Ministerstvo vnitra České republiky* [online]. [cit. 3. 3. 2021]. Dostupné z: https://www.mvcr.cz/clanek/co-je-egovernment.aspx

[64] Digital Public Services. *European Commission* [online]. [cit. 3. 3. 2021]. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/desi-digital-public-services

[65] E-estonia. *E-estonia.com* [online]. [cit. 3. 3. 2021]. Dostupné z: https://e-estonia.com/

[66] REGLITZ, Merten. The Human Right to Free Internet Access. *Journal of Applied Philosophy* [online]. 2019 [cit. 3. 3. 2021], roč. 37, č. 2, s. 314-331.

se na chodu světa; a tím ztrácí i způsob, jak ovládat vlastní život.[67] Reglitz jde ve své představě tak daleko, že navrhuje, aby připojení bylo zdarma pro ty, kdo si ho nemůžou dovolit z vlastních finančních prostředků. Už ale neříká, jak a kdo by za něj měl platit, ani jak zajistit spravedlivou distribuci připojení.

Deklarace i Listina stojí na odmítání diskriminace mj. ze sociálních či majetkových důvodů.[68] Není ale nemožnost zapojit se do společenského dění skrz internet formou diskriminace, vůči níž by měly entity bojovat, bez ohledu na to, zda je závazek negativní či pozitivní, čistě z pozice, že pasivitou porušují vlastní lidsko-právní katalogy? Kdybychom zašli ještě dál a drželi se představ, že bez internetu nelze prožít důstojný život a představuje kritický nástroj pro možnost podílet se na společenském dění, lze použít i další ustanovení:

- právo na přiměřenou životní úroveň (čl. 26 VDLP),
- právo na svobodnou účast na kulturním životě společnosti a podílení se na vědeckém pokroku a jeho výtěžcích (čl. 27 VDLP).

Jejich striktní aplikací lze polemizovat, zda OSN neporušuje vlastní Deklaraci a neměla by v zajišťování a ochrany internetového připojení konat více.

Také u EU se dá uvažovat o možném porušování Listiny, jejíž čl. 25 hovoří o *právu na důstojný a nezávislý život starších osob a jejich podílení se na společenském a kulturním životě*. Přitom právě starší osoby patří v unii mezi ty nejméně připojené. V roce 2016 bylo mezi pravidelnými internetovými uživateli jen 57 procent unijních obyvatel z věkové kategorie 55-74 let.[69] Pro přijetí pozitivního závazku zajišťovat lidem připojení k internetu, aby mohli být plnohodnotnou součástí společnosti a rozhodovat sami o sobě, hovoří také zkušenosti z celosvětové pandemie. Jak ukázal rok 2020

[67] University of Birmingham. Free Internet access should be a basic human right, study says. *Phys.org* [online]. 2019 [cit. 3. 3. 2021]. Dostupné z: https://phys.org/news/2019-11-free-internet-access-basic-human.html

[68] Čl. 2 VDLP, čl. 21 LZP EU.

[69] Archive: Internet access and use statistics – households and individuals. *Eurostat. Statistics Explained* [online]. 2018 [cit. 3. 3. 2021]. Dostupné z: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:Internet_access_and_use_statistics_-_households_and_individuals&oldid=379591

(a v podstatě i rok 2021), internet představuje za určitých okolností jediný nástroj, skrz který mohou lidé zůstat plnohodnotnou součástí společnosti v době lockdownu a restriktivních opatřeních.

Přesto představa pozitivního závazku spouští mnoho palčivých otázek. Jak by pověřené entity docílily, aby mohli práva požívat všichni? Existovaly by sankce? Nevznikla by další propast mezi chudými a bohatými státy a kontinenty?[70] A co ti, jež o přístup k internetu nestojí? Když by existovala možnost připojení pro všechny a většina společenské a státotvorné agendy by se přesunula od virtuálního prostředí, jaký postoj zaujmout k těm, kdo se nechtějí připojit nebo se neumí v internetovém prosředí pohybovat? Není proto překvapivé, že entity se přijetí pozitivního závazku brání.

5. ZÁVĚREM

Vliv internetu na vykonávání lidských práv, včetně těch základních, je nesporný. Internet jedincům umožňuje uplatňovat právo na informace, svobodu projevu, svobodu vyznání, právo na vzdělání aj. Stal se zároveň ukazatelem lidské důstojnosti a svobody, určité minimální životní úrovně, které chce ve společnosti participující jedinec dosáhnout.

Tuto roli internetu nezpochybňují OSN ani EU. Naopak, obě organizace se vymezily vůči omezování práv uživatelů na internetu. Na základě předchozích kapitol je možné odpovědět na zvolenou výzkumnou otázku: *Jakou pozici na úrovni Organizace spojených národů a Evropské unie zastává právo na přístup k internetu ve vztahu k základním lidským právům?*

OSN skrze svou rezoluci *Podpora, ochrana a výkon lidských práv na internetu* A/HRC/32/L.20 z 27. června 2016 deklarovala, že práva existující offline platí i v online světě a jejich přesun na internet neznamená, že mohou být porušována ze strany státních aktérů. Postoj OSN se tedy blíží závazku negativnímu, jelikož se soustředí na to, aby státy do práva přístupu k internetu nezasahovaly. Stále se však jedná o ochranu existujících zá-

[70] Lze předpokládat, že africké státy by měly s výstavbou infrastruktury a zařizováním internetové připojení pro všechny velké problémy finanční povahy.

kladních práv, nikoli právo přístupu k internetu ve své podstatě – a navíc pouze ve formě *soft law* a za absence vnitřní koherence.

Zkušenost OSN ukazuje, že deklarace lidských práv ne nutně znamená jejich dodržování a realizaci, a že tato práva mohou zůstat pouze na papíře podepsaném státy, jež je samy nedodržují a svým občanům je odpírají. Kdyby se OSN rozhodla zařadit právo na přístup k internetu do VDLP, bylo by třeba vyjasnit jeho obsah, implementaci a ochranu. Což nelze za stavu, kdy je právo na internet členy organizace porušováno, vidět jako proveditelné.

Na druhou stranu, už uznání důležitosti internetu jako nástroje pro vykonávání základních lidských práv na mezinárodní úrovni a půdě OSN lze považovat za úspěch. Základní práva se v čase vyvíjí. Ostatně proto existuje dělení do jednotlivých generací. I přes očekávatelné problémy s dodržováním se někteří domnívají, že mezinárodní společenství směřuje k zařazení práva na přístup k internetu do katalogu základních lidských práv.[71]

EU má z pohledu právního dopadu výhodnější postavení, byť na omezenější počet aktérů. Stěžejní předpis na úrovni EU je nařízení EU 2015/2120 o *otevřeném přístupu k internetu*. V něm je internet uznán jako otevřená platforma, k níž mají mít koncový uživatelé přístup, aniž by docházelo k blokování, diskriminování nebo naopak upřednostňování obsahu a služeb, za dodržování technologické a síťové neutrality.

Krom toho EU připravuje další tři předpisy se zásadním vlivem pro právo na přístup k internetu, hlavně k internetovému obsahu – nařízení o digitálních službách, nařízení o digitálních trzích, Akční plán pro demokracii.

Evropská unie v otázce práva na přístup k internetu zaujímá aktivnější postoj, přesto ani ona nepřijala právo na přístup k internetu za pozitivní závazek. Díky přenesení části suverenity členských zemí může nastavovat společná pravidla a určovat standardy, jimiž se ostatní musí řídit. To se například stalo zařazením internetového připojení mezi univerzální služby.

[71] SZOSZKIEVICZ, Łukasz. Internet Access as a New Human Right? State of the Art on the Threshold of 2020. *Adam Mickiewicz University Law Review* [online]. 2018 [cit. 4. 3. 2021], roč. 8, s. 49-62.

Zároveň se snaží pomoci svým občanům k internetu skrze dobrovolné iniciativy jako je představená iniciativa WiFi4EU.

Ačkoli předsedkyně EK Ursula von der Lyen označila přístup k internetu za *„nové lidské právo“,*[72] nezavázala se Unie oficiální cestou zajistit internetové připojení pro všechny občany unijních zemí. Právo na přístup k internetu tak oficiálně na úrovni EU – stejně jako na úrovni OSN – zůstává v režimu negativně formulovaného práva.

EU v zásadě leží na pomezí negativního a pozitivního závazku, kdy se skrze své právní předpisy snaží plnit negativní závazek (internet za dostupnou cenu, síťová neutralita, technologická neutralita, zákaz diskriminace), ale uznává existenci práva, které by měla zajišťovat pozitivně, chce-li doslovně dodržovat ustanovení vlastní Listiny a výroky své předsedkyně.

Na závěr můžeme zhodnotit, že se obě organizace více orientují na zajištění necenzurovaného internetového obsahu než na zajištění plošného přístupu. Tím však částečně ignorují otázku, v jaké pozici se ocitají jedinci, kteří si internetový přístup nedokážou sami zajistit.

EU navíc v současnosti zažívá další posun v oblasti práva na přístup k internetu, a to směrem k vyšší aktivitě ze strany národních/unijních orgánů a zásahům. Když se vrátíme k předkládaným návrhům EK (nařízení o digitálních službám, nařízení o digitálních trzích, Akční plán pro demokracii), lze si povšimnout posunu evropských představitelů ve vnímání internetu. Tyto návrhy stojí na premise, že internetový obsah je třeba regulovat. Snaží se přenastavit pravidla tak, aby uživatelé měli z internetového prostředí užitek, nebyli vystavování lžím a manipulacím, aniž by bylo internetové prostředí diskriminační, nerovné nebo v něm docházelo k porušování práv. Internet se stává na úrovni EU prostorem, jenž ukázal, že bezbřehá svoboda bez vynutitelných pravidel spolu s dosahem bez ohledu na hranice, může přinést více škody než užitku.

[72] Statement by President von der Leyen at the roundtable ‘Internet, a new human right' after the intervention by Simona Levi. *European Commission* [online]. 2020 [cit. 23. 2. 2021]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/statement_20_2001

6. POUŽITÉ ZDROJE

[1] Archive: Internet access and use statistics – households and individuals. *Eurostat. Statistics Explained* [online]. 2018 [cit. 3. 3. 2021]. Dostupné z: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Archive:Internet_access_and_use_statistics_households_and_individuals&oldid=379591

[2] BARRY, Jack J. COVID-19 exposes why access to the internet is a human right. *Open Global Rights* [online]. 2020 [cit. 20. 2. 2021]. Dostupné z: https://www.openglobalrights.org/covid-19-exposes-why-access-to-internet-is-human-right/

[3] Co je to eGovernment? *Ministerstvo vnitra České republiky* [online]. [cit. 3. 3. 2021]. Dostupné z: https://www.mvcr.cz/clanek/co-je-egovernment.aspx

[4] CORNESCU, Adrian Vasile. The Generations of Human's Rights. In: SEHNÁLEK, David a VALDHANS, Jiří a DÁVID, Radovan a KYNCL, Libor (eds.). *Dny práva – 2009 – Days of Law: the Conference Proceedings* [online]. Brno: Masarykova univerzita, 2009. [cit. 17. 3. 2021]. ISBN 978-80-210-4990-1. Dostupné z: https://www.law.muni.cz/sborniky/

dny_prava_2009/files/prispevky/tvorba_prava/Cornescu_Adrian_Vasile.pdf

[5] Digital Public Services. *European Commission* [online]. [cit. 3. 3. 2021]. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/desi-digital-public-services

[6] DOBINSON, Ian a JOHNS, Francis. Legal Research as Qualitative Research. In: MCCONVILLE, Mike a CHUI, Wing Hong. (eds.). *Research Methods for Law*. 2. vydání Edinburgh: Edinburgh University Press, 2007, s. 18-47. ISBN 978-1-4744-0321-4.

[7] DOMARADZKI, Spasimir a KHVOSTOVA, Margaryta a PUPOVAC, David. Karel Vasak's Generations of Rights and the Contemporary *Human Rights Discourse* [online]. 2019, č. 20, s. 423-443 [cit. 20. 2. 2021]. ISSN 1874-6306. Dostupné z: https://link.springer.com/article/10.1007/s12142-019-00565-x

[8] EDWARDS, Luke. What websites and online services are blocked in Turkey – Facebook, Wikipedia and more. *Techradar.com* [online]. 2020 [cit. 15. 2. 2021]. Dostupné z: https://www.techradar.com/vpn/websites-online-services-blocked-turkey-facebook-wikipedia

[9] E-ESTONIA. *E-estonia.com* [online]. [cit. 3. 3. 2021]. Dostupné z: https://e-estonia.com/

[10] European Democracy Action Plan: making EU democracies stronger. *European Commission* [online]. 2020 [cit. 3. 3. 2021]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250

[11] EVROPSKÁ UNIE. *Lisabonská smlouva pozměňující Smlouvu o Evropské unii a Smlouvu o založení Evropského společenství, podepsaná v Lisabonu dne 13. prosince 2007* [online]. [cit. 4. 3. 2021]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=LEGISSUM%3Aai0033#:~:text=Lisabonsk%C3%A1%20smlouva%20je%20z%20velk%C3%A9,%C5%99%C3%ADjna%202004%20v%20%C5%98%C3%ADm%C4%9B.

[12] EVROPSKÁ UNIE. *Listina základních práv Evropské unie, 2012/C 326/02* [online]. [cit. 20. 2. 2021]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A12012P%2FTXT

[13] FIALOVÁ, Eva. Právo na přístup k internetu. *Právník* [online]. 2018 [cit. 15. 2. 2021], roč. 157, č. 7, s. 545-557. ISSN 0231-6625. Dostupné z: https://www.ilaw.cas.cz/upload/web/files/pravnik/issues/2018/7/1.Fialov%C3%A1_545-557_7_2018.pdf

[14] FRENCH, Darcy. Which websites and online services are banned in China? In: *Techradar.com* [online]. 2020 [cit. 17. 2. 2021]. Dostupné z: https://www.techradar.com/vpn/which-websites-and-online-services-are-banned-in-china

[15] HEICK, Terry. UN: Internet Access Is Now A Basic Human Right. *Teach Thought* [online]. 2016 [cit. 23. 2. 2021]. Dostupné z: https://www.teachthought.com/technology/un-internet-access-now-basic-human-right/

[16] HENDL, Jan a REMR, Jiří. *Metody výzkumu a evaluace*. 1. vydání. Praha: Portál, 2017, 373 s. ISBN 978-80-262-1192-1.

[17] HORŇÁČKOVÁ, Kristýna. *Rada pro lidská práva OSN a iniciativy v oblasti „nových lidských práv"* [online]. Brno, 2013. [cit. 17. 3. 2021]. Diplomová práce. Masarykova univerzita, Právnická fakulta, Katedra mezinárodního a evropského práva. Dostupné z: https://is.muni.cz/th/iubek/KH.pdf

[18] How does the Internet work? *Cloudfare* [online]. [cit. 19. 2. 2021]. Dostupné z: https://www.cloudflare.com/learning/network-layer/how-does-the-internet-work/

[19] HOWELL, Catherine. a WEST, Darrell M. The internet as a human right. *Brookings.edu* [online]. 2016 [cit. 23. 2. 2021]. Dostupné z: https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/

[20] Charta základních práv EU. *Euroskop.cz* [online]. [cit. 23. 2. 2021]. Dostupné z: https://euroskop.cz/627/sekce/charta-zakladnich-prav-eu/

[21] Internet Users. *Internet Live Stats* [online]. [cit. 15. 8. 2021]. Dostupné z:https://www.internetlivestats.com/internet-users/

[22] JIRÁSEK, Pavel a NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti* [online]. Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA, 2015, 247 s. [cit. 17. 3. 2021]. Dostupné z : https://www.cybersecurity.cz/data/slovnik_v310.pdf

[23] KNAPP, Viktor. *Teorie práva*. 1. vydání. Praha: C. H. Beck, 1995, 247 s. ISBN 80-7179-028-1.

[24] KRAUS, Jiří (ed.). *Nový akademický slovník cizích slov*. 1. vydání, dotisk. Praha: Academia, 2009, 879 s. ISBN 978-80-200-1351-4.

[25] Lisabonská smlouva. *Ministerstvo vnitra České republiky* [online]. 2011 [cit. 25. 2. 2021]. Dostupné z: https://www.mvcr.cz/clanek/agenda-eu-na-mv-lisabonska-smlouva.aspx

[26] Open Internet. *European Commission* [online]. [cit. 23. 2. 2021]. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/open-internet

[27] ORGANIZACE SPOJENÝCH NÁRODŮ. *Charta Organizace spojených národů a Statut Mezinárodního soudního dvora* [online]. [cit. 4. 3. 2021]. Dostupné z: https://www.osn.cz/wp-content/uploads/Charta-OSN-2019.pdf

[28] ORGANIZACE SPOJENÝCH NÁRODŮ. *Všeobecná deklarace lidských práv* [online]. [cit. 4. 3. 2021]. Dostupné z: https://www.osn.cz/wp-content/uploads/2015/12/UDHR_2015_11x11_CZ2.pdf

[29] Podpora telekomunikačních sítí a infrastruktur digitálních služeb v Evropě. In: Evropská komise [online]. [cit. 20. 2. 2021]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=LEGISSUM:26030103_1

[30] Používání internetu a přístup k němu. *Europa.eu* [online]. [cit. 23. 2. 2021]. Dostupné z: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/internet-access/index_cs.htm

[31] Před třiceti lety byla FS ČSFR schválena Listina základních práv a svobod. *Advokátní online deník* [online]. 2021 [cit. 25. 2. 2021]. Dostupné z: https://advokatnidenik.cz/2021/01/08/pred-triceti-lety-byla-fs-csfr-schvalena-listina-zakladnich-prav-a-svobod/

[32] REGLITZ, Merten. The Human Right to Free Internet Access. *Journal of Applied Philosophy* [online]. 2019 [cit. 3. 3. 2021], roč. 37, č. 2, s. 314-331. ISSN 1468-5930. Dostupné z: https://onlinelibrary.wiley.com/doi/abs/10.1111/japp.12395

[33] Russia: Growing Internet Isolation, Control, Censorship. *Human Rights Watch* [online]. 2020 [cit. 20. 2. 2021]. Dostupné z: https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship

[34] SANDLE, Tim. UN thinks internet access is a human right. *Business Insider* [online]. 2016 [cit. 23. 2. 2021]. Dostupné z: https://www.businessinsider.com/un-says-internet-access-isa-human-right-2016-7

[35] SOH, Changrok a CONNOLLY, Daniel a NAM, Seunghyun. Time for a Fourth Generation of Human Rights? *United Nations Research Institute for Social Development* [online]. 2018 [cit. 21. 2. 2021]. Dostupné z: https://www.unrisd.org/TechAndHumanRights-Soh-et-al

[36] Statement by President von der Leyen at the roundtable 'Internet, a new human right' after the intervention by Simona Levi. *European Commission* [online]. 2020 [cit. 23. 2. 2021]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/statement_20_2001

[37] SZOSZKIEVICZ, Łukasz. Internet Access as a New Human Right? State of the Art on the Threshold of 2020. *Adam Mickiewicz University Law Review* [online]. 2018 [cit. 4. 3. 2021], roč. 8, s. 49-62. ISSN 2083-9782. Dostupné z: https://www.researchgate.net/publication/328290234_Internet_Access_as_a_New_Human_Right_State_of_the_Art_on_the_Threshold_of_2020

[38] The Digital Markets Act: ensuring fair and open digital markets. *European Commission* [online]. [cit. 3. 3. 2021]. Dostupné z: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

[39] The Digital Services Act: ensuring a safe and accountable online environment. *European Commission* [online]. [cit. 25. 2. 2021]. Dostupné z: https://ec.europa.eu/info/digital-services-act-ensuring-safe-and-accountable-online-environment_en

[40] The Impact of Digital Technologies. *United Nations* [online]. [cit. 3. 3. 2021]. Dostupné z: https://www.un.org/en/un75/impact-digital-technologies#:~:text=Digital%20technologies%20have%20advanced%20more,can%20be%20a%20great%20equaliser

[41] THORNHILL, John. Internet access is both a human right and a business opportunity. *Financial Times* [online]. 2020 [cit. 17. 2. 2021]. Dostupné z: https://www.ft.com/content/872dc219-d4d8-4896-92d3-7f9d45a5ce90

[42] UNITED NATIONS, GENERAL ASSEMBLY, HUMAN RUGHTS COUNCIL. *Oral Revisions of 30 June, no. A/HRC/32/L.20. The promotion, protection and enjoyment of human rights on the Internet* [online]. 27. 6. 2016 [cit. 4. 3. 2021]. Dostupné z: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

[43] UNITED NATIONS, GENERAL ASSEMBLY, HUMAN RUGHTS COUNCIL. *A/HRC/35/22. Report of the Special Rapporteur on the promotion and Protection of the right to freedom of opinion and expression* [online]. 23. 6. 2017 [cit. 26. 8. 2021]. Dostupné z: https://www.ohchr.org/en/issues/freedomopinion/pages/sr2017reporttohrc.aspx

[44] UNIVERSITY OF BIRMINGHAM. Free Internet access should be a basic human right, study says. *Phys.org* [online]. 2019 [cit. 3. 3. 2021]. Dostupné z: https://phys.org/news/2019-11-free-internet-access-basic-human.html

[45] Use of Internet and Online Activities. *European Commission* [online]. [cit. 3. 3. 2021]. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/desi-use-internet

[46] VAŠÁK, Karel. A 30-year struggle: The sustained efforts to give force of law to the Universal Declaration of Human Rights. *The Unesco Courier* [online]. 1977 [cit. 20. 2. 2021], roč. 30, s. 29-31. ISSN 0041-5278. Dostupné z: https://unesdoc.unesco.org/ark:/48223/pf0000074816/PDF/074816engo.pdf.multi.nameddest=48063

[47] What are human rights? *United Nations Human Rights. Office of the High Commissioner* [online]. [cit. 17. 2. 2021]. Dostupné z : https://www.ohchr.org/en/issues/pages/whatarehumanrights.aspx

[48] WiFi4EU. *European Commission* [online]. [cit. 23. 2. 2021]. Dostupné z: https://digital-strategy.ec.europa.eu/cs/activities/wifi4eu

https://doi.org/10.5817/RPT2022-1-3

PŘEHLED AKTUÁLNÍ JUDIKATURY I/2022

ANNA BLECHOVÁ, MARTIN ERLEBACH, VOJTĚCH JUŘIČKA,
ANEŽKA KARPJÁKOVÁ, FRANTIŠEK KASL, ANDREJ KRIŠTOFÍK,
PAVEL LOUTOCKÝ, SOFIE PETROVÁ, JAN SVOBODA,
JAKUB VOSTOUPAL, ONDŘEJ WOZNICA

1. PRÁVO DUŠEVNÍHO VLASTNICTVÍ A AUTORSKÉ PRÁVO

JE DŮLEŽITÉ MÍTI FILIPA?

Soud: Nejvyšší soud
Věc: 27 Cdo 2023/2019
Datum: 24. 3. 2021
Dostupnost: nsoud.cz

V roce 2012 byla Městskému soudu v Praze doručena žaloba na zdržení se užívání názvu českého překladu „Jak důležité je mít Filipa“ a užívání jména „Filip“ a obratu „mít filipa“ v textu českého překladu literárního díla spisovatele O.Wildea[1]. Žalobcem byl A. N, dědic a spolunositel autorských práv po zemřelém překladateli J. Z. N.[2] Spor mezi žalovaným a žalobcem tkvěl v tom, že žalovaný P. D. v roce 2012 vytvořil překlad slavné Wildeovy divadelní hry s názvem „Jak důležité je mít Filipa“ [v originále „The Importance of Being Earnest“], který byl šířen prostřednictvím internetových stránek, v rámci inscenace divadelní hry a zároveň i jako publikace

[1] Bod 1 anotovaného rozhodnutí.

[2] Bod 3 anotovaného rozhodnutí.

dostupná v knihkupectví.[3] Soud první instance žalobci vyhověl.[4] Následně se spor dostal před Vrchní soud v Praze, který na základě odvolání žalovaného rozhodnutí soudu první instance změnil tak, že žalobu zamítl.[5] V roce 2018 se pak celý spor dostal až k Nejvyššímu soudu.

Podstata sporu spočívala v tom, zda je překlad slovní hříčky názvu (a poslední věty díla) divadelní hry autorským dílem, ve smyslu § 2 odst. 1 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), a zda požívá příslušnou autorskoprávní ochranu.[6] Nejvyšší soud se stejně jako Vrchní soud v Praze neztotožnil se závěry soudu první instance a dovolaní žalobce dne 24. 3. 2021 zamítl.[7]

Argumentace soudu se opírala o skutečnost, že slovu *Filip*, které v překladu J.Z.N je jménem hlavní postavy, není možné přiznat autorskoprávní ochranu dle §2 autorského zákona, jelikož se jedná o běžné jméno.[8] U spojení „*míti filipa*“ soud konstatoval, že spojení je volným prvkem, který patří do obecného fondu (public domain) a z toho důvodu taktéž nemůže požívat ochranu dle autorského práva.[9] Zároveň soud zdůraznil, že „*skutečnost, že se překladateli podařilo plně pochopit význam celého díla a také reprodukovat nuance originálu ještě neznamená, že pojmové znaky autorského díla budou naplněny také v každé jednotlivé větě překladu. Ochrana autorských práv překladatele získaná pro celé dílo se tedy nutně nemusí projevit v každé jednotlivé pasáži textu při jeho individuálním zvážení*“.[10]

Co se týče obecně aplikovatelných závěrů, Nejvyšší soud v tomto případě zdůraznil, že autorskoprávní ochrana se nevztahuje jen na dílo jako na celek, ale i na jeho jednotlivé části například název a jména postav. Podmínkou této právní ochrany je ale skutečnost, že samy o sobě jednotlivé

[3] Bod 3 anotovaného rozhodnutí.

[4] Bod 2 anotovaného rozhodnutí.

[5] Bod 11 anotovaného rozhodnutí.

[6] Bod 5 anotovaného rozhodnutí.

[7] Bod 42 anotovaného rozhodnutí.

[8] Bod 34 anotovaného rozhodnutí.

[9] Bod 35 anotovaného rozhodnutí.

[10] Bod 33 anotovaného rozhodnutí.

prvky splňují pojmové znaky díla dle autorského zákona. Tyto závěry jsou dle Nejvyššího soudu přenositelné i do oblasti autorskoprávní ochrany zpracovaných děl a překladů.[11]

Autorka: AB

NÁROK KOLEKTIVNÍCH SPRÁVCŮ NA BEZDŮVODNÉ OBOHACENÍ

Soud: Nejvyšší soud
Věc: 27 Cdo 386/2021
Datum: 14. 12. 2021
Dostupnost: nsoud.cz

Léčebné lázně Jáchymov provozují zařízení, v němž byly mezi lety 2013– 2016 zpřístupňovány veřejnosti umělecké výkony výkonných umělců a zvukové a zvukově obrazové záznamy bez licenčního oprávnění uděleného kolektivním správcem.[12] Lázně Jáchymov podaly žádost o ustanovení společného zástupce, neboť uzavíraly licenční smlouvy s více než dvěma kolektivními správci. Na tuto žádost ale nebylo nijak reagováno, společný zástupce nebyl pověřen a licenční smlouva s kolektivním správcem tudíž nebyla uzavřena.[13]

Z důvodu neplacení příslušných licenčních poplatků podal kolektivní správce žalobu ke Krajskému soudu v Plzni, který uložil lázeňskému objektu povinnost zaplatit dvojnásobek licenční odměny dle sazebníku kolektivního správce.[14] Vrchní soud v Praze se v rámci odvolacího řízení nevypořádal s námitkou neustanoveného společného zástupce, kterou Lázně Jáchymov vznesly,[15] a pouze doplnil výpočet soudu prvního stupně

[11] Body 29- 30 anotovaného rozhodnutí.

[12] Bod 1 anotovaného rozhodnutí. Práva k daným záznamům za dané umělce kolektivně spravuje INTERGRAM, nezávislá společnost výkonných umělců a výrobců zvukových a zvukově-obrazových záznamů, z. s.

[13] Bod 13 anotovaného rozhodnutí.

[14] Bod 2 anotovaného rozhodnutí.

[15] Bod 13 anotovaného rozhodnutí.

o chybějící faktor obsazenosti jednotlivých pokojů lázeňského zařízení, čímž výslednou dlužnou částku poměrně snížil.[16]

Lázně Jáchymov tedy podaly dovolání k Nejvyššímu soudu, který se mimo jiných námitek[17] zaměřil na námitku podání a doručení žádosti o ustanovení společného zástupce.[18]

Dle § 100a autorského zákona[19], v případě, kdy uživatel nebo osoba oprávněná hájit zájmy v ní sdružených uživatelů alespoň jednomu z příslušných kolektivních správců doručí písemnou žádost o pověření společného zástupce podle § 101 odst. 11, tak po dobu než bude tento zástupce pověřen nemůže kolektivní správce uplatňovat nárok na náhradu škody nebo na vydání bezdůvodného obohacení dle § 40 odst. 4 autorského zákona z neoprávněného zásahu do kolektivně spravovaného práva nebo ohrožení takového práva (tj. dvojnásobek odměny).

Nejvyšší soud tak došel k závěru, že kolektivní správce nemůže uplatňovat nárok na vydání bezdůvodného obohacení ve výši dvojnásobku odměny, pokud mu byla subjektem doručena písemná žádost o pověření společného zástupce, který nebyl ustanoven.

Oba přezkoumávané rozsudky jsou tedy ve svém posouzení neúplné, a v důsledku toho je Nejvyšší soud zrušil a věc vrátil soudu prvního stupně k dalšímu řízení.[20] V situaci, kdy byla žádost doručena v souladu se zákonem, disponuje tudíž kolektivní správce nárokem pouze na vydání bezdůvodného obohacení podle § 451 oz., nikoliv ve výši dvojnásobku dané odměny dle § 40 odst. 4 autorského zákona.

Autorka: SP

[16] Bod 12 anotovaného rozhodnutí.

[17] Body 31 – 46 anotovaného rozhodnutí.

[18] Bod 47 anotovaného rozhodnutí.

[19] Zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění od 1. 1. 2017 do 19. 4. 2017.

[20] Bod 57 anotovaného rozhodnutí.

APLIKACE VÝJIMKY PRO SOUKROMÉ ROZMNOŽOVÁNÍ NA UKLÁDÁNÍ V CLOUDOVÉM ULOŽIŠTI

Soud: Soudní dvůr Evropské unie
Věc: C 433/20
Datum: 24. 3. 2022
Dostupnost: curia.europa.eu

Organizace kolektivní správy autorských práv Austro-Mechana žalovala společnost Strato jako poskytovatele služeb cloudového uložiště na zaplacení poplatku za soukromé rozmnožování. Strato nárok odmítla s tím, že z titulu služeb cloud computingu nemá být vyplácena žádná odměna, neboť již uhradila příslušný poplatek v Německu při pořízení serverů k hostingu a neboť uživatelé již uhradili odměnu při pořízení zařízení k nahrání dat do cloudového uložiště.[21]

V první instanci byl nárok Austro-Mechana odmítnut, neboť společnost Strato nepřevádí svým zákazníkům paměťová média, ale poskytuje jim službu internetového úložiště.[22] Austro-Mechana však v odvolání k Oberlandesgericht Wien namítla, že otázka, zda ukládání obsahu v rámci cloud computingu spadá do působnosti čl. 5 odst. 2 písm. b) směrnice 2001/29, je nejistá, a to s odkazem na rozhodnutí VCAST (C-265/16).[23]

Odvolací soud tak položil Soudnímu dvoru předběžné otázky, zda "na jakémkoliv nosiči" v čl. 5 odst. 2 písm. b) směrnice 2001/29 znamená, že tím jsou myšleny také servery užívané k poskytování datového uložiště soukromým osobám, a zda je právní úprava, která vylučuje poskytovatele služeb cloudového úložiště z povinnosti platit spravedlivou náhradu uvedenou v čl. 5 odst. 2 směrnice 2001/29, slučitelná s právem EU.[24]

Soudní dvůr na obě předběžné otázky odpověděl kladně. K první otázce soud nejprve vyložil, že pořizování rozmnoženin v cloudovém úložišti

[21] Bod 8 a 10 anotovaného rozhodnutí.

[22] Bod 9 a 11 anotovaného rozhodnutí.

[23] Bod 12 anotovaného rozhodnutí.

[24] Bod 13 a 35 anotovaného rozhodnutí.

představuje rozmnoženinu ve smyslu čl. 5 odst. 2 písm. b) směrnice 2001/29, neboť rozmnoženina je širokým pojmem s ohledem na použitý jazyk a cíl směrnice stanovit vysokou úroveň autorskoprávní ochrany.[25] Soudní dvůr navíc dovozuje, že akt pořízení rozmnoženiny díla může být spojen se samostatným aktem sdělování díla veřejnosti, přičemž se jedná o samostatná užití.[26]

K druhé otázce Soudní dvůr dovodil, že v případě, že členské státy zavedou výjimku dle čl. 5 odst. 2 písm. b) směrnice 2001/29, jsou současně povinny zajistit systém spravedlivé odměny určený k odškodnění nositelů práv za způsobenou újmu.[27] S odkazem na předchozí judikaturu však Soudní dvůr dovozuje, že hradit náklady na odměnu, která bude zaplacena nositeli autorského práva, je v zásadě povinna osoba, která provádí soukromé rozmnožování.[28] V případě využívání cloudových služeb tak samotní uživatele cloud computingu hradí odměnu dle čl. 5 odst. 2 písm. b) směrnice 2001/29.[29] Současně s ohledem na praktické potíže s výběrem takového poplatku mohou členské státy poplatek přenést na osoby disponující prostředky pro digitální rozmnožování.[30]

Soudní dvůr tak upřesnil aplikaci výjimky pro soukromé rozmnožování dle čl. 5 odst. 2 písm. b) směrnice 2001/29. Soudní dvůr však současně jasně oddělil různé způsoby užití autorského díla v rámci téhož technologického procesu, přičemž je na různé způsoby užití nezbytné aplikovat různé právní režimy, vč. případné aplikace směrnice 2019/790.

Autor: OW

[25] Bod 16 anotovaného rozhodnutí.

[26] Bod 31 a 32 anotovaného rozhodnutí.

[27] Bod 38 a 40 anotovaného rozhodnutí.

[28] Bod 43 anotovaného rozhodnutí.

[29] Bod 43 anotovaného rozhodnutí.

[30] Bod 44 až 48 anotovaného rozhodnutí.

PLATNOST ČLÁNKU 17 SMĚRNICE 2019/790

Soud: Soudní dvůr Evropské unie
Věc: C 401/19
Datum: 26. 4. 2022
Dostupnost: curia.europa.eu

Bezprostředně po přijetí směrnice 2019/790 (také DSM směrnice nebo Směrnice o autorském právu na jednotném digitálním trhu) Polsko před Soudním dvorem napadlo její článek 17, který předepisuje nová pravidla fungování poskytovatelů služeb pro sdílení obsahu online. Kontroverzním se již při legislativním procesu a současně v tomto sporu stala preventivní povinnost založená v článku 17 odst. 4 písm. b) směrnice. Jádrem sporu a také jediným žalobním důvodem Polska je tvrzené porušení svobody projevu a informací dle článku 11 Listiny základních práv EU.[31] Polsko proto navrhlo alternativně (i.) zrušit článek 17 odst. 4 písm. b); nebo (ii.) zrušit celý článek 17, pokud by soud posoudil, že ustanovení nelze oddělit od ostatních částí článku 17.[32]

Soudní dvůr v úvodu rozhodnutí dovozuje, že ustanovení článku 17 odst. 4 písm. b) není oddělitelné, neboť by jeho zrušením došlo ke změně podstaty článku 17, a tedy lze zrušit pouze článek 17 jako celek.[33] Soudní dvůr následně dovozuje, že článek 17 může představovat významné omezení svobody projevu a informací.[34] Přesto však Soudní dvůr odmítl zrušit článek 17 a polskou žalobu zamítl, neboť dovodil, že směrnice 2019/790 zavádí vhodné záruky k tomu, aby bylo zajištěno dodržování práva na svobodu projevu a informací a současně jeho spravedlivá rovnováha s právem duševního vlastnictví.[35]

Ve vztahu k povaze omezení svobody projevu a informací Soudní dvůr odkazuje na rozhodnutí YouTube a Cyando (C-682/18), neboť povinnost

[31] Bod 23 anotovaného rozhodnutí.

[32] Bod 12 anotovaného rozhodnutí.

[33] Body 19 a 20 anotovaného rozhodnutí.

[34] Body 54 a 55 anotovaného rozhodnutí.

[35] Bod 98 anotovaného rozhodnutí.

dle článku 17 odst. 4 písm. c) odpovídá povinnosti dle článku 14 odst. 1 písm. b) směrnice 2000/31, a dále vymezuje, že článek 17 odst. 4 písm. b) skutečně de facto zavádí povinnost provádět předchozí kontrolu nahrávaného obsahu.[36] Za problematické však v tomto smyslu Soudní dvůr označuje pouze ty automatické nástroje filtrování, které dostatečně nerozlišují mezi zákonným a nezákonným obsahem.[37] S odkazem na rozhodnutí Glawischnig-Piesczek (C-18/18) se navíc Soudní dvůr vymezuje vůči situacím, kdy by sám poskytovatel musel rozhodovat o protiprávnosti obsahu.[38]

Jako dostatečně přesný rámec opatření a záruk pak Soudní dvůr posoudil kombinaci faktorů. Zaprvé Soudní dvůr zdůraznil legální možnost nahrávat obsah v rámci výjimek a omezení autorského práva, o čemž poskytovatelé služeb uživatele musí informovat.[39] Dále Soudní dvůr zdůrazňuje, že článek 17 nevede k obecné povinnosti dohledu, a naopak podléhá předání relevantních a nezbytných informací o konkrétním obsahu.[40] V neposlední řadě Soudní dvůr zdůrazňuje procesní záruky.[41]

Soudní dvůr ve svém rozhodnutí finálně rozhodl otázku samotné platnosti článku 17 směrnice 2019/790, přičemž ukládá členským státům úkol zajistit přiměřenost aplikace této právní úpravy. Otevírá se tak nová kapitola regulace autorskoprávního obsahu na internetu, ve které bude Soudní dvůr při dalším výkladu článku 17 směrnice 2019/790 nadále hrát velmi významnou roli. Zásadní budou zejména limity, které rozhodovací praxe nastaví pro automatické nástroje filtrování.

Autor: OW

[36] Body 51 až 53 anotovaného rozhodnutí.

[37] Bod 86 anotovaného rozhodnutí.

[38] Bod 90 anotovaného rozhodnutí.

[39] Body 87 a 88 anotovaného rozhodnutí.

[40] Body 89 a 90 anotovaného rozhodnutí.

[41] Body 93 a 94 anotovaného rozhodnutí.

2. SOUKROMÍ A OSOBNÍ ÚDAJE

K POVINNOSTI SPRÁVCU DOLOŽIŤ TITUL U VŠETKÝCH OSOBNÝCH ÚDAJOCH SPRACOVÁVANÝCH PRE NEHO SPRACOVATEĽOM

Soud: Nejvyšší správní soud
Věc: 7 As 146/2021 – 26
Datum: 7. 10. 2021
Dostupnost: uoou.cz

Žalovaný Úřad pro ochranu osobních údajů („ÚOOÚ“) uložil žalobkyni – spoločnosti SMS finance, a.s., povinnosť vymazať osobné údaje, voči ktorým je v postavení správca, ku ktorým nevie zaistiť (doložiť) právne tituly podľa čl. 6 Obecného nariadenia[42]. Zároveň jej bola uložená povinnosť uzavrieť spracovateľskú zmluvu s podnikateľom, ktorý voči spoločnosti vystupoval ako spracovateľ.[43] K vzniku tohto vzťahu malo dôjsť tak, že spracovateľ, ako samostatný podnikateľ, ponúkal koncovým klientom poisťovnícke služby zaisťované žalobcom. Údaje o klientoch, ktorým poisťovnícke služby ponúkal, získaval spracovateľ prostredníctvom telefónnych hovorov, v rámci ktorých sa predstavoval pod menom žalobkyne.[44]

Žalobkyňa podala rozklad v ktorom namietala, že voči údajom, s ktorými narába spracovateľ nie je správcom podľa čl. 4 ods. 7 Obecného nariadenia.[45] Rozklad bol zamietnutý, čo žalobkyňa napadla správnou žalobou pred Mestským súdom v Prahe. Žalobkyňa opäť namietala, že nie je voči týmto údajom správcom nakoľko za nesprávne spracovanie neodpovedá ona ale práve spracovateľ, ktorý je jej zástupcom a zároveň samostatným podnikateľským subjektom. Mestský súd však táto argumentácia

[42] Nařízení Evropského parlamentu a Rady (EU) 2016/679 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).

[43] Bod 1 anotovaného rozhodnutia.

[44] Bod 20 anotovaného rozhodnutia.

[45] Bod 2 anotovaného rozhodnutia.

nepresvedčila a žalobkyni nevyhovel, nakoľko v konaní bolo preukázané že je to žalobkyňa, kto určil prostriedky a účel spracovania.[46]

Voči tomuto rozhodnutiu potom žalobkyňa ďalej brojila kasačnou sťažnosťou pred NSS, v ktorej tvrdila že rozhodnutie Mestského súdu je jednako nepreskúmateľné, príkaz vymazania údajov ku ktorým nie je dostatočne preukázaný titul nie je dostatočne určité a že sa súd odchýlil od zavedenej praxe, pričom odkázala na rozsudok NSS sp. zn. 9 As 34/2008.[47]

NSS sťažnosti nevyhovel a žalobkyňu odkázal späť na odôvodnenie Mestského súdu[48], nakoľko v kasačnej sťažnosti tvrdila len veci, ktoré boli vysporiadané už v tomto rozhodnutí, s ktorým sa NSS stotožnil. K odkazu na predchádzajúci rozsudok NSS uvádza, že už z doby jeho vydania je zrejmé že sa nemôže vzťahovať na situáciu, ktorú namieta žalobkyňa.[49] K námietke nedostatočnej určitosti príkazu k vymazaniu uvádza, že ÚOOÚ konkretizoval rozsah údajov takým spôsobom aby ich žalobkyňa, ako správca, mohla sama identifikovať.[50] Ďalej tiež NSS neprisvedčilo argumentu nepreskúmateľnosti, nakoľko jednako sám odkazuje na odôvodnenie[51], s ktorým sa stotožnil[52], a tiež mal zato, že v ňom Mestský súd uviedol všetky skutočnosti, z ktorých vychádzal, a vyjadril sa ku všetkým žalobným bodom. NSS teda aj navzdory opisu fungovania vzťahu medzi žalobkyňou a správcom, ktorý je podľa NSS na tak konkrétnej úrovni bezpredmetný, nakoľko nič nemení na rozhodnom kritériu určenia prostriedkov a účelu spracovania, potvrdil rozhodnutie Mestského súdu.

V poslednej rade na žalobkyninu námietku, že ÚOOÚ si príkazom k výmazu len vytvára pôdu pre následné udelenie sankcie dodal, že nemôže rozhodovať o hypotetických, či ešte len budúcich krokoch správneho orgánu a že v takom prípade žalobkyni opäť náležia všetky opravné prostriedky.[53]

[46] Bod 3 anotovaného rozhodnutia.

[47] Bod 4 anotovaného rozhodnutia.

[48] Bod 12 a 19 anotovaného rozhodnutia.

[49] Bod 20 anotovaného rozhodnutia.

[50] Bod 23 anotovaného rozhodnutia.

[51] Bod 26 anotovaného rozhodnutia.

[52] Bod 8, 9, 10 a 11 anotovaného rozhodnutia.

[53] Bod 24 anotovaného rozhodnutia.

Autor: AK

PRÁVNÍ ZÁRUKY A DOHLED NAD TAJNÝM SLEDOVÁNÍM A PŘÍSTUPU KE KOMUNIKAČNÍM ÚDAJŮM

Soud: Evropský soud pro lidská práva
Věc: 70078/12 (Ekimdzhiev a další proti Bulharsku)
Datum: 11. 1. 2022
Dostupnost: hudoc.echr.coe.int

Stěžovatelé (dva bulharští právníci a dvě neziskové organizace) podali k Evropskému soudu pro lidská práva stížnost, ve které tvrdili, že povaha jejich profesní činností je vystavuje riziku jak tajného sledování, tak i přístupu státních orgánů k jejich komunikačním údajům podle zákonů, které tyto postupy v Bulharsku povolují. Tyto zákony a postupy jsou tak dle nich v rozporu s článkem 8 Úmluvy o ochraně lidských práv (dále jen „Úmluva“). Stěžovatelé však neuvedli, že by byli oni sami skutečně sledováni nebo že by státní orgány měly přístup k jejich komunikačním údajům.[54] Nadto stěžovatelé uváděli, že neměli proti těmto postupům k dispozici žádný účinný opravný prostředek, který je garantován článkem 13 Úmluvy. Soud však s odkazem na předchozí judikaturu[55] rozhodl, že stížnost bude přezkoumána pouze z pohledu článku 8 Úmluvy.[56]

Daný článek zakotvuje každému právo na respektování soukromého a rodinného života, obydlí a korespondence, přičemž toto právo lze omezit toliko na základě zákona a v případech nezbytných v demokratické společnosti.

Soud se tak při přezkumu zaměřil na otázku, zda je daná právní úprava v demokratické společnosti nezbytná a obsahuje odpovídající účinné záruky.[57] Soud zohlednil i dva praktické faktory, a to skutečné fungování

[54] Bod 10 anotovaného rozhodnutí.

[55] Rozsudek Evropského soudu pro lidská práva ze dne 4. 12. 2015, Roman Zakharov proti Rusku, 47143/06, bod 307.

[56] Body 246-247 ve spojení s 361 anotovaného rozhodnutí.

opatření dohledu, a dále existenci nebo absenci důkazů o skutečném zneužívání.[58]

V rámci přezkumu zákona upravujícího tajné sledování Soud nejprve konstatoval, že v zákoně chybí definice předmětu, který může podléhat tajnému sledování. To může být problematické zejména kvůli tomu, že skrze tuto vágnost lze dojít k extenzivnímu výkladu ohledně předmětu sledování (např. celá policejní databáze).[59] Taktéž zákon neobsahuje definici pojmu „z *důvodu národní bezpečnosti*“, který umožnuje povolit sledování až na dobu 24 měsíců,[60] přičemž absentují i pravidla upravující ochranu osobních a jiných údajů získaných v rámci tajného sledování[61] a ochrany komunikace mezi klientem a advokátem.[62] Soud dále shledal řadu pochybení i v praxi státních orgánů.[63]

V rámci přezkumu předpisu upravujícího uchovávání komunikačních údajů a přístupu k nim považoval Soud za závažný nedostatek zejména neexistenci veřejně dostupných, zákonných pravidel pro přístup k údajům a jejich další zpracování v rámci trestního řízení.[64] I v této oblasti pak Soud nalezl řadu pochybení v rámci praxe státních orgánů.[65]

---

[57] Konkrétně pak Soud zkoumal u napadených předpisů následující záruky a principy: 1) dostupnost právní úpravy, 2) důvody pro povolení tajného sledování a přístupu k údajům elektronických komunikací ze strany státních orgánů, jakož i jejich osobní rozsah, 3) dobu trvání kontrolních opatření a pravidel pro zpracování údajů, 4) schvalovací proces, 5) dohled, 6) oznámení dotčeným jednotlivcům a 7) dostupné opravné prostředky. Viz body 291-293 anotovaného rozhodnutí.

[58] Body 291–355 anotovaného rozhodnutí.

[59] Bod 303 anotovaného rozhodnutí.

[60] Bod 305 anotovaného rozhodnutí.

[61] Body 326–332 anotovaného rozhodnutí.

[62] Bod 333 anotovaného rozhodnutí.

[63] Např. většina rozhodnutí o povolení sledování z posledních let nebyla řádně odůvodněna a obsahovaly pouze všeobecné důvody, viz body 311-313 anotovaného rozhodnutí, nedostatečná notifikace sledovaných či absence opravného prostředku, viz body 350-360 anotovaného rozhodnutí.

[64] Body 408-409 anotovaného rozhodnutí.

[65] Např. donucovací orgány nejsou povinny poskytovat soudcům, kteří přístup povolují, nezbytné informace, pokud je přístup požadován v rámci trestního řízení, viz body 402-403 anotovaného rozhodnutí, absence povinnosti soudců zdůvodnit své rozhodnutí, viz bod 405 anotovaného rozhodnutí, či absence opravného prostředku, viz body 416-418 anotovaného rozhodnutí.

Soud tak jednomyslně dospěl k závěru, že napadené bulharské právní předpisy nesplňují požadavek na kvalitu zákona vyžadovanou Úmluvou a nezajišťují, že je tajné sledování využíváno pouze tam, kde je to nezbytně nutné v demokratické společnosti.[66] Soud proto rozhodl, že v daném případě skutečně došlo k porušení čl. 8 Úmluvy, a to ve vztahu ke stěžovatelům už jen pouhou existencí těchto dvou zákonů a praktik pověřených orgánů.[67]

Autorka: AKar

ŽÁDOST O DEINDEXOVÁNÍ ČLÁNKU A SVOBODA PROJEVU

Soud: Evropský soud pro lidská práva
Věc: 77419/16 (Biancardi proti Itálii)
Datum: 25. 2. 2022
Dostupnost: hudoc.echr.coe.int

Stěžovatel Alessandro Biancardi byl šéfredaktorem zpravodajského webu, který v roce 2008 uveřejnil článek o rvačce v restauraci obsahující jména dvou zúčastněných a jejich synů, názvy dvou rodinných restaurací zúčastněných a další okolnosti vyšetřování. Stěžovatel byl jimi v roce 2010 vyzván k odstranění článku z internetu, čemuž nevyhověl a byl zažalován.[68]

V průběhu řízení před soudem prvního stupně stěžovatel článek sám deindexoval za cílem spor urovnat.[69] Tento soud konstatoval, že v souladu s národním právem byl veřejný zájem na dostupnosti předmětných informací v okamžiku obdržení výzvy již uspokojen. Jelikož článek zůstal velmi snadno přístupný po dobu tří let a stěžovatel nevyhověl výzvě k jeho odstranění, došlo k poškození pověsti žalobce a porušení jeho práva na respektování soukromého života a stěžovateli byla uložena povinnost nahradit nemajetkovou újmu.[70] Italský Nejvyšší soud se ztotožnil se závěry soudu nižšího stupně a stěžovatelovo odvolání zamítl. Také doplnil, že zpracování

[66] Body 358-359 anotovaného rozhodnutí.

[67] Body 383-384 anotovaného rozhodnutí.

[68] Body 5 až 9 anotovaného rozhodnutí.

[69] Bod 10 anotovaného rozhodnutí.

[70] Body 12 a 13 anotovaného rozhodnutí.

osobních údajů stěžovatele bylo nezákonné v době, kdy po obdržení výzvy článek zůstal nadále přístupný.[71]

Stěžovatel se obrátil na Evropský soud pro lidská práva s tím, že mu bylo zasaženo do jeho svobody projevu garantované v čl. 10 Evropské úmluvy o ochraně lidských práv a svobod, a že sankce, kterou obdržel, byla excesivní.[72]

Zásah do práv obsažených v článku 10 Úmluvy je možný, pokud je to nezbytné v demokratické společnosti, např. v zájmu ochrany práv jiných osob. Mezi stranami nebyly sporné skutečnosti, že došlo k zásahu do stěžovatelovy svobody projevu, tento zásah byl v souladu s právem a taktéž sledoval legitimní cíl, Soud tedy zkoumal nezbytnost daného zásahu. Dále konstatoval, že stěžovatel byl shledán odpovědným pouze na základě neprovedení deindexace, odstranění článku z internetu ani jeho anonymizace nebyly předmětem řízení.[73] Od aplikace kritérií vymezených v případu *Axel Springer proti Německu*[74]se Soud odklonil. Namísto toho zkoumal, zda byl právní základ, na němž byla založena stěžovatelova občanskoprávní odpovědnost před italskými soudy, dostatečně opodstatněný, a to skrze kritéria (1) délky doby, po kterou byl článek přístupný s přihlédnutím k důvodu zpracování obsažených dat, (2) citlivosti těchto dat a (3) závažnosti udělené sankce.[75]

Jelikož článek zůstal snadno přístupný a nezměněný po dobu osmi měsíců od obdržení výzvy,[76] týkal se trestního řízení[77] a udělená sankce nebyla

[71] Bod 14 anotovaného rozhodnutí.

[72] Bod 30 anotovaného rozhodnutí.

[73] Body 57 až 59 anotovaného rozhodnutí.

[74] Rozdíl od případu Axel Springer proti Německu ze dne 7. 2. 2012 spočíval v odlišnosti dopadu internetového článku oproti článku v tištěných novinách a odlišnosti subjektu jako soukromé osoby nepůsobící ve veřejné sféře. Viz bod 62 anotovaného rozhodnutí.

[75] Body 62 až 64 anotovaného rozhodnutí.

[76] Bod 65 anotovaného rozhodnutí.

[77] Bod 67 anotovaného rozhodnutí.

excesivní,[78] Soud shledal omezení stěžovatelovy svobody projevu za přípustné a jeho žádost zamítl.[79]

Autor: VJ

ZABEZPEČENÍ ZDRAVOTNICKÝCH ÚDAJŮ A POVAHA VEŘEJNÉHO SUBJEKTU DLE ZÁKONA O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Soud: Nejvyšší správní soud
Věc: 10 As 190/2020
Datum: 25. 2. 2022
Dostupnost: nssoud.cz

Úřad pro ochranu osobních údajů shledal Nemocnici Tábor (dále jako „stěžovatel“) vinnou ze spáchání přestupku podle zákona č. 101/2000 Sb., o ochraně osobních údajů, neboť dle jeho názoru nezabezpečila dostatečně[80] osobní údaje v rámci elektronické zdravotní dokumentace.[81]

Stěžovatel podal proti rozhodnutí neúspěšně rozklad a dále žalobu k Městskému soudu v Praze, který ji zamítl, protože pokud stěžovatel pořizoval záznamy o tom, kdo a kdy osobní údaje zaznamenal, ale ne zpřístupnil, porušil tím zákonnou povinnost dostatečného zabezpečení.[82]

Stěžovatel se tak obrátil na NSS s kasační stížností, ve které mimo jiné argumentoval, že Městský soud v Praze si nesprávně vyložil zákon o ochraně osobních údajů (konkrétně § 13 odst. 4 písm. c)), který ostatně ale vůbec neměl aplikovat, neb se jedná o právní úpravu pro stěžovatele

[78] Soud konstatoval, že ačkoliv sankce není zanedbatelná, vzhledem k civilněprávní povaze soudního řízení a jeho okolnostem nemůže být označena za excesivní. Viz bod 68 anotovaného rozhodnutí.

[79] Body 70 a 71 anotovaného rozhodnutí.

[80] Konkrétně se jednalo o nemožnost prokázat přístup k dokumentu skrze logy a neprovádění pravidelné kontroly přístupů k elektronické dokumentaci. Viz bod 1 anotovaného rozhodnutí.

[81] Bod 1 anotovaného rozhodnutí.

[82] Bod 3 anotovaného rozhodnutí.

méně příznivou.[83] Příznivější jsou dle něj pozdější legislativní akty, ať už GDPR[84], které dle jeho výkladu daný institut ani nezná, či zákon č. 110/2019 Sb., o zpracování osobních údajů, který neumožňuje uložit sankci za správní trest veřejnému subjektu, za který se stěžovatel považuje[85].[86]

NSS v otázce výkladu § 13 odst. 4 písm. c) odmítl argumentaci stěžovatele, která byla založena na ryze gramatickém výkladu a nezohledňuje smysl ustanovení ani dřívější judikaturu NSS[87].[88] V otázce výhodnější právní úpravy upozorňuje NSS na skutečnost, že stěžovatel se neprováděním pravidelných kontrol a neexistencí logů dopustil nejen porušení povinnosti podle § 13 odst. 4, ale též obecnějšího § 13 odst. 1.[89] Právě k tomu je potřeba hledat příznivější úpravu a to v kontextu existující judikatury[90], přičemž NSS upozorňuje, že čl. 32 GDPR odpovídá úpravě stanovené v § 13 odst. 1 a neklade na správce či zpracovatele mírnější požadavky.[91] Nakonec se NSS zabýval otázkou povahy stěžovatele. NSS se sice definici veřejného subjektu (která v samotném zákoně o zpracování osobních údajů chybí) vyhnul, ale konstatoval, že stěžovatel jím jistě není, neb veřejný subjekt bude zpravidla zřízen zákonem a určen k plnění úkolů ve veřejném zájmu a zároveň nebude disponovat vlastním majetkem (což stěžovatel nesplňuje)[92].[93] Zároveň

[83] Bod 4 anotovaného rozhodnutí.

[84] 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).

[85] Vede zdravotnickou dokumentaci podle zákona č. 372/2011 Sb., je veřejným zadavatelem podle zákon č. 372/2011 Sb., je veřejnou institucí podle zákona č. 106/1999 Sb. a jeho činnost je primárně financována z prostředků veřejného zdravotního pojištění. Stěžovatel je soukromou osobou založenou Jihočeským krajem k plnění veřejného zájmu.

[86] Bod 4 anotovaného rozhodnutí.

[87] Viz rozsudek NSS 7 As 150/2012 ze dne 30. 1. 2013.

[88] Body 11-16 anotovaného rozhodnutí.

[89] Body 22-23 anotovaného rozhodnutí.

[90] Viz rozsudek NSS 4 As 140/2019.

[91] Body 23-24 anotovaného rozhodnutí.

[92] Srov. Rozsudek NSS čj. 4 AS 376/2019 31.

[93] Body 33-34 anotovaného rozhodnutí.

NSS uvádí, že je zásadně nerozhodný status subjektu dle jiných zákonů (např. veřejného zadavatele dle zákona o zadávání veřejných zakázek).[94]

NSS tak plně souhlasil s Městským soudem a kasační stížnost zamítl. Zvláště důležitým aspektem tohoto rozsudku se stalo právě posouzení, zda je stěžovatel veřejným subjektem. NSS se přitom primárně spolehl na argument zdrojem financí, který může potenciálně otřást vymezením některých veřejných subjektů ve smyslu zákona o zpracování osobních údajů.[95]

Autor: JV

POVINNOST PROVOZOVATELE ZPRAVODAJSKÉHO SERVERU ODKRÝT IDENTITU AUTORA ÚTOČNÉHO PŘÍSPĚVKU

Soud:	Evropský soud pro lidská práva
Věc:	39378/15 (Standard Verlagsgesellschaft MBH proti Rakousku)
Datum:	7. 3. 2022
Dostupnost:	hudoc.echr.coe.int

Stěžovatelka je vydavatelkou deníku *Der Standard*, který v rámci své digitální platformy umožňuje registrovaným uživatelům diskutovat nad jednotlivými články.[96] V průběhu registrace jsou uživatelé upozorněni na ilegalitu útočných příspěvků, přičemž v případě jejich publikace může být stěžovatelka povinna vydat osobní údaje přispěvatelů.[97] V rámci politicky vypjatější debaty u několika článků však došlo k publikaci takových komentářů namířených proti zde zmíněným politikům.[98] Ti se v reakci obrátili na stěžovatelku, aby jim vydala osobní údaje přispěvatelů za účelem zahájení trestního a civilního řízení.[99] Stěžovatelka dané komentáře odstranila, vydat

[94] Bod 33 anotovaného rozhodnutí.

[95] NSS doslova uvádí, že „*nemocnice (akciová společnost) nedostává finanční prostředky na svůj provoz a fungování přímo z veřejných rozpočtů, nýbrž je získává jako protiplnění za konkrétní úkony a pacienty, které zdravotním pojišťovnám vykáže*."

[96] Body 5 a 6 anotovaného rozhodnutí.

[97] Body 7 a 8 anotovaného rozhodnutí.

[98] Body 13-21 anotovaného rozhodnutí.

[99] Body 16-17 a 20-21 anotovaného rozhodnutí.

osobní údaje komentujících ovšem odmítla, neboť dle ní nešlo o pomluvu.[100]

Zmínění politici se tedy obrátili na soud, přičemž argumentovali, že komentáře naplňují defamační a urážlivé znaky.[101] Stěžovatelka se bránila, že více než o pomluvu se jedná o hodnotový soud a že dle zákonu o médiích není povinna vyzrazovat své zdroje.[102] Spor nakonec rozhodoval Rakouský Nejvyšší soud, který odmítl argumentaci stěžovatelky a nakázal jí vydat osobní údaje dle tamějšího zákona o E-Commerce.[103]

Stěžovatelka se tak obrátila na Evropský soud pro lidská práva s tím, že daný postup zasahuje do jejího práva (konkrétně svobody médií) dle článku 10 Evropské úmluvy o lidských právech. Zmíněný článek přiznává každému právo na svobodu projevu včetně práva přijímat a rozšiřovat informace nebo myšlenky bez zasahování státních orgánů, přičemž ale umožňuje toto právo omezit zákonem z důvodů nezbytných v demokratické společnosti (tedy mj. v zájmu ochrany práv a svobod jiných osob).

Soud v počátku konstatoval, že stěžovatelka v případu nevystupuje jako médium, ale jako poskytovatel webhostingu.[104,105] Funkční model daného fóra je ovšem založen na rozdmýchávání debaty k tématům veřejného zájmu, což je článkem 10 chráněno.[106] A přestože z praktických důvodů odmítl myšlenku, že by přispěvatelům na internetu svědčilo právo absolutní anonymity, uznává důležitost anonymity pro podporu svobody projevu.[107] V rozsudku, dle kterého měla stěžovatelka přispěvatele této anonymity zbavit, tak konstatoval existenci zásahu a přistoupil k testu proporcionality. Existence relevantního zákonu byla nesporná, Soud tedy poměřoval, zda se

[100] Body 17, 21 a 23 anotovaného rozhodnutí.

[101] Body 22 a 23 anotovaného rozhodnutí.

[102] Bod 23 anotovaného rozhodnutí.

[103] Body 25-33 anotovaného rozhodnutí.

[104] Mj. také odmítl argument stěžovatelky, že by autoři příspěvků vystupovali jako novinářské zdroje, neb jejich informace byly určeny široké veřejnosti a nikoliv pouze novináři. Viz body 69-71 anotovaného rozhodnutí.

[105] Body 68-71 anotovaného rozhodnutí.

[106] Body 73-74 anotovaného rozhodnutí.

[107] Body 75-79 anotovaného rozhodnutí.

jedná o opatření nezbytné pro demokratickou společnost.[108] Připomněl, že politik musí tolerovat vyšší míru kritiky než soukromá osoba,[109] a vnitrostátním soudům vytkl nedostatečné poměření konfliktních zájmů.[110] Vzhledem k tomu, že se spor netýkal odpovědnosti stěžovatelky za dané komentáře, stačilo by v tomto ohledu i *prima facie* prověření.[111]

I takové prověřování si ovšem žádá určité zdůvodnění a vyvážení zájmů, Soud tedy v jejich absenci konstatoval zásah do práva na svobodu projevu dle čl. 10N Úmluvy.[112] Nevyvrátil tím možnost de-anonymizace přispěvatelů, ale v konkrétním případě konstatoval, že absence poměřování zájmů ze strany vnitrostátních soudů nenaplňuje kritéria proporcionality a potřebnosti v demokratické společnosti.

Autor: JV

PLOŠNÉ SHROMAŽĎOVÁNÍ ÚDAJŮ O TELEKOMUNIKAČNÍM PROVOZU ZA PODMÍNKY OMEZENÉHO PŘÍSTUPU K NIM

Soud: Soudní dvůr Evropské unie
Věc: C-140/20
Datum: 5. 4. 2022
Dostupnost: curia.europa.eu

Stěžovatel byl v roce 2015 prvostupňovým irským soudem odsouzen na doživotí za vraždu. V odvolání proti tomuto rozhodnutí stěžovatel poukazoval na porušeních svých základních práv garantovaných Listinou základních práv Evropské unie.[113] Dle stěžovatele byly údaje o telekomunikačním provozu použité jako důkazní prostředek v jeho trestní věci použity

[108] Srov. Body 138 a 139 rozsudku *Delfi AS proti Estonsku*, dále pak *Von Hannover proti Německu* a *Axel Springer AG proti Německu*.

[109] Body 85-87 anotovaného rozhodnutí a rozhodnutí *Lingens proti Rakousku, Oberschlick proti Rakousku* či *Couderc a Hachette Filipacchi Associés proti Francii*.

[110] Body 95 anotovaného rozhodnutí.

[111] Tamtéž.

[112] Body 95 a 96 anotovaného rozhodnutí.

[113] Konkrétně namítal porušení práv uvedených v čl. 7 (respektování soukromého života), 8 (ochrana osobních údajů), 11 (svoboda projevu) a čl. 52.

sice v souladu s irským zákonem z roku 2011[114], ale v rozporu se směrnicí 2002/58/ES[115] upravující oblast shromažďování údajů o telekomunikačním provozu. Rozhodnutí o odvolání ještě nebylo vydáno.

V souladu s tímto argumentem stěžovatel následně podal žalobu v civilním řízení za účelem prohlášení neslučitelnosti příslušného ustanovení irského zákona z roku 2011[116] a výše zmíněné směrnice 2002/58/ES. Tato otázka se dostala k irskému nejvyššímu soudu, který předložil Soudnímu dvoru Evropské unie 6 předběžných otázek.[117]

Tyto otázky lze shrnout do 3 oblastí. V první[118] se dotazující soud ptal, zda je plošné shromažďování údajů o telekomunikačním provozu v rozporu se směrnicí 2002/58/ES vykládanou v souladu s Listinou základnách práv Evropské unie. K této otázce Soudní dvůr nejprve zrekapituloval svou dosavadní judikaturu ve věci data retention[119] a následně uvedl, že plošné shromažďování údajů o telekomunikačním provozu je obecně nepřípustné, a to i v případě úpravy jakou použilo Irsko ve svém zákoně z roku 2011.[120] Zároveň však uvedl přijatelné alternativy právních úprav data retention.[121]

V druhé zkoumané oblasti[122] se Soudní dvůr musel vypořádat s otázkou, zda je možné, aby o přístupu k údajům telekomunikačního provozu rozhodoval pouze jeden příslušník policie a k němu speciálně přidružený úřední aparát. Soudní dvůr v této věci prohlásil, že takové centralizované

[114] To je Communications (Retention of Data) Act 2011.

[115] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích).

[116] To je čl. 15 Communications (Retention of Data) Act 2011.

[117] Bod 30 anotovaného rozhodnutí.

[118] Otázky 1,2,4 z bodu 30 anotovaného rozhodnutí.

[119] Rozhodnutí Digital Rights Ireland, C-293/12 a C-594/12, Tele2Sverige, C-203/15 a C-698/15 a La Quadrature du Net, C-511/18, C-512/18 a C-520/18.

[120] To je Communications (Retention of Data) Act 2011.

[121] Body 67, 72, 80 a 85 anotovaného rozhodnutí, jde např o: cílené uchovávání lokalizačních údajů vymezené nediskriminačně pro kategorii osob nebo pro určitou geograficky vymezenou oblast, plošné shromažďování a uchovávání IP adres zdrojů připojení po nezbytně dlouhou dobu nebo příkaz k urychlenému uchování údajů o telekomunikačním provozu (quick freeze) pokud je taková úprava dostatečně specifická a subjekty údajů mají zároveň záruky proti zneužití těchto údajů.

[122] Otázka 3 z bodu 30 anotovaného rozhodnutí.

rozhodování není šetrné k základním právům subjektů údajů,[123] protože nejde o nezávislý správní orgán, který rozhodnutí provádí, ale jen o jakousi „odnož".[124]

Poslední oblastí pak byly otázky[125] týkající se možnosti vnitrostátního soudu omezit časové účinky prohlášení nesouladu vnitrostátního práva s právem Evropské unie za účelem udržení veřejného pořádku. Soudní dvůr uvedl, že sice v předchozí judikatuře takovou možnost dovodil, ovšem šlo o výjimečné okolnosti, které v daném případě nejsou naplněny.[126]

Soudní dvůr v tomto rozhodnutí tak neučinil odklon své dosavadní judikatury. Významným je demonstrativní výčet možností, jakými může zákonodárce upravit shromažďování údajů o telekomunikačním provozu, aby nedošlo k nepřiměřenému narušení základních práv subjektů údajů. Současně také Soudní dvůr jednoznačně konstatoval, že základní podmínkou využití data retention je skutečná a aktuální hrozba národní bezpečnosti, zejména teroristická trestná činnost, ne jakákoliv trestná činnost.[127]

Autor: ME

AKTIVNÍ LEGITIMACE SDRUŽENÍ NA OCHRANU SPOTŘEBITELŮ BRÁNIT ZÁJMY SUBJEKTŮ ÚDAJŮ DLE GDPR

Soud: Soudní dvůr Evropské unie
Věc: C-319/20
Datum: 28.4.2022
Dostupnost: curia.europa.eu

Německá Spolková unie center a sdružení na ochranu zájmů spotřebitelů[128] (dále jen „Spolková unie") žalovala dnešní společnost *Meta Platforms Ireland*

[123] Vychází z rozhodnutí Prokuratuur, C-746/18.

[124] Bod 108 anotovaného rozhodnutí.

[125] Otázky 5 a 6 z bodu 30 anotovaného rozhodnutí.

[126] Body 120 a 121 anotovaného rozhodnutí, takto rozhodl Soudní dvůr ve věci Inter-Environnement Wallonie and Bond Beter Leefmilieu Vlaanderen, C-411/17.

[127] Bod 61 anotovaného rozhodnutí.

[128] *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*

Limited (dále jen „společnost Facebook“) pro porušení německých předpisů v oblasti ochrany osobních údajů a nekalou obchodní praktiku v rámci nastavení všeobecných obchodních podmínek pro bezplatné hry nabízené skrze Centrum aplikací na adrese www.facebook.de.[129] Spolková unie je německým právem v těchto případech aktivně legitimována k žalobám na zdržení se jednání nezávisle a bez doložení konkrétních porušení práv určitého subjektu údajů a bez potřeby jím uděleného zmocnění k hromadnému zastoupení.[130]

Zemský soud v Berlíně (*Landgericht Berlin*) návrhu vyhověl, odvolání společnosti Facebook k Vrchnímu zemskému soudu v Berlíně (*Kammergericht Berlin*) bylo zamítnuto. Následně byl společností podán dovolací opravný prostředek ke Spolkovému soudnímu dvoru (*Bundesgerichtshof*), který se musel vypořádat s otázkou aktivní legitimace Spolkové unie za těchto podmínek ve světle článku 80 odst. 2 GDPR. Ten proto vznesl předběžnou otázku k Soudnímu dvoru Evropské unie, zda příslušné ustanovení brání vnitrostátní úpravě, která přiznává sdružením jako je Spolková unie za uvedených okolností právo podat proti porušiteli žalobu v národním občanskoprávním řízení.[131]

Soudní dvůr otázku zvažoval především v intencích cíle GDPR v dosažení v zásadě úplné harmonizace vnitrostátních předpisů týkajících se ochrany osobních údajů.[132] Přes bezprostřední účinek unijního nařízení však některá ustanovení vyžadují vnitrostátní prováděcí opatření, což je i případ článku 80 odst. 2 GDPR, kde je ponechán prostor pro uvážení formy provedení.[133] Předmětná německá vnitrostátní úprava však nebyla přijata v reakci na článek 80 odst. 2 GDPR, je tudíž nutno zvažovat, zda se svým obsahem pohybuje v jeho intencích.[134] Spolková unie naplňuje charakter subjektu předvídaného tímto ustanovením a dané ustanovení GDPR nepod-

[129] Body 2 a 34-36 anotovaného rozhodnutí.

[130] Bod 36 anotovaného rozhodnutí.

[131] Body 47, 49 a 51 anotovaného rozhodnutí.

[132] Bod 57 anotovaného rozhodnutí.

[133] Body 58 a 59 anotovaného rozhodnutí.

[134] Body 61 a 62 anotovaného rozhodnutí.

miňuje výkon zástupné žaloby existencí konkrétního porušení práv.[135] Tento výklad mechanismu ostatně nesporně přispívá k posílení práv dotčených subjektů údajů.[136] Současné porušení více rovin, vedle ochrany osobních údajů především též ochrany spotřebitele a zákazu nekalých obchodních praktik, je do značné míry nevyhnutelné a ochrana práv subjektů údajů skrze vnitrostátní mechanismy ochrany spotřebitele tudíž není proti smyslu a znění článku 80 odst. 2 GDPR.[137] V tomto duchu pak příslušné rozhodnutí pouze potvrzuje a předznamenává harmonizující unijní úpravu, která je obsažena ve směrnici 2020/1828, která má být transponována do vnitrostátních předpisů s účinností od 25. června 2023.[138]

Soudní dvůr tedy v příslušné věci vyložil článek 80 odst. 2 GDPR tak, že nebrání vnitrostátní úpravě, na jejímž základě byla podána žaloba Spolkovou unií. Rozhodnutí je významné, jelikož představuje další posun v úpravě a vytváření nástrojů, které překonávají současné překážky vymahatelnosti povinností vyplývajících z GDPR především vůči nadnárodním společnostem jako je společnost Facebook.[139]

Autor: FK

PŘIMĚŘENOST ZÍSKÁNÍ OSOBNÍCH ÚDAJŮ ZA ÚČELEM BUDOUCÍ IDENTIFIKACE PŘI TRESTNÍM ŘÍZENÍ

Soud:	Nejvyšší správní soud
Věc:	5 As 254/2019-49 a 5 As 241/2019-46
Datum:	18. 5. 2022
Dostupnost:	nssoud.cz

[135] Body 64-65 a 70-73 anotovaného rozhodnutí.

[136] Body 74-76 anotovaného rozhodnutí.

[137] Body 77-79 anotovaného rozhodnutí.

[138] Směrnice Evropského parlamentu a Rady (EU) 2020/1828 ze dne 25. listopadu 2020 o zástupných žalobách na ochranu kolektivních zájmů spotřebitelů a o zrušení směrnice 2009/22/ES.

[139] Blíže pro kontext a význam rozhodnutí viz LOMAS, Natasha. Europe's top court unblocks more GDPR litigation against Big Tech. TechCrunch. [online] 28.4.2022 [cit. 12.5.2022] Dostupné z: https://techcrunch.com/2022/04/28/cjeu-gdpr-consumer-litigation/

Policie ČR v souvislosti s trestním stíháním pro trestný čin porušení autorských práv, práv souvisejících s právem autorským a práv k databázi předvolala obviněné k získání osobních údajů (zejm. daktyloskopických otisků prstů a informací o genetickém vybavení) postupem dle § 65 zákona č. 273/2008 Sb., o Policii České republiky ("zákon o policii"), přičemž oba obvinění výzvě k získání osobních údajů nevyhověli.[140] Obvinění následně podali žalobu na ochranu před nezákonným zásahem, přičemž bylo vedeno samostatné řízení pro žalobu každého obviněného.

Předmětné žaloby posoudil Městský soud v Praze, který obviněným vyhověl a posoudil získání osobních údajů pro účely budoucí identifikace za nepřiměřené. Nepřiměřenost Městský soud v Praze dovozoval zejména s odkazem na povahu protiprávního jednání, neboť k trestné činnosti nedošlo v „hmotném" světě, a nelze ji tedy rozeznávat podle otisků prstů, stop DNA apod.[141]

Policie České republiky podala kasační stížnost, kde namítala faktory odůvodňující přiměřenost, a to obecný kriminalistický význam osobních údajů, častou recidivu vč. recidivy nestejnorodé[142], vědomost o trestní povaze jednání a praktikování trestné činnosti jako podnikatelské činnosti[143]. Kasační stížnost se také odkazovala na probíhající řízení před Ústavním soudem sp. zn. Pl. ÚS 7/18, jehož předmětem byl návrh na zrušení § 65 odst. 1 zákona o policii. Ústavní soud návrh na zrušení dle předchozí věty zamítl.[144]

Podmínkou zákonnosti v konkrétním případě přesto zůstává proporcionalita zásahu.[145] NSS se proto zabýval otázkou, zda získání osobních údajů dle zákonu o policii v případě trestného činu proti průmyslovým právům a proti autorskému právu může být přiměřené s ohledem na právo na informační sebeurčení dle čl. 10 odst. 3 Listiny základních práv a svobod[146] a zá-

[140] Bod 1 a 3 obou anotovaných rozhodnutí.

[141] Bod 4 obou anotovaných rozhodnutí.

[142] Bod 5 rozhodnutí 5 As 241/2019-46.

[143] Bod 6 rozhodnutí 5 As 241/2019-46 a bod 5 rozhodnutí 5 As 254/2019-49.

[144] Bod 9 rozhodnutí 5 As 241/2019-46 a bod 8 rozhodnutí 5 As 254/2019-49.

[145] Bod 18 rozhodnutí 5 As 241/2019-46 a bod 17 rozhodnutí 5 As 254/2019-49.

[146] Bod 17 rozhodnutí 5 As 241/2019-46 a bod 16 rozhodnutí 5 As 254/2019-49.

roveň otázkou, jaké faktory je při posouzení přiměřenosti nezbytné posoudit.[147]

NSS došel k závěru, že povaha trestného činu nevylučuje závěr o přiměřenosti získání osobních údajů dle § 65 odst. 1 zákona o policii, přičemž však musí být přihlédnuto k řadě faktorů, jako např. osobě pachatele, dosavadní trestní činnosti, typové i individuální závažnosti či síle podezření.[148]

Povaha trestného činu proti průmyslovým právům a proti autorskému právu navíc znamená, že trestný čin nemusí být spáchán v "hmotném" světě a důkazy o něm je třeba hledat ve formě digitálních stop či svědeckých výpovědí, nikoliv ve formě otisků prstů či vzorků DNA.[149] NSS současně zdůrazňuje, že není potřeba prokazovat, že nehrozí recidiva, ale naopak že je nezbytné závěr o přiměřenosti nezbytné podložit závěry, že v individuálním případě je pravděpodobné opakování či gradování trestné činnosti.[150]

Rozhodnutí tak představuje cenné vodítko při posuzování přiměřenosti zpracování osobních údajů orgány činnými v trestním řízení pro účely budoucí identifikace v případech trestné činnosti v kyberprostoru.

Autor: OW

3. OSTATNÍ

BITCOIN NENÍ PRO ÚČELY DANĚ Z PŘÍJMŮ CIZÍ MĚNOU

Soud: Krajský soud v Brně
Věc: 30 Af 29/2020 - 48
Datum: 17. 2. 2022
Dostupnost: zakonyprolidi.cz

Krajský soud v Brně rozhodoval o žalobě proti Odvolacímu finančnímu ředitelství. Žalobce v ní napadal rozhodnutí o odvolání proti platebnímu

[147] Bod 12 rozhodnutí 5 As 241/2019-46 a bod 11 rozhodnutí 5 As 254/2019-49.

[148] Body 18 a 19 rozhodnutí 5 As 241/2019-46 a body 17 a 18 rozhodnutí 5 As 254/2019-49.

[149] Bod 28 rozhodnutí 5 As 241/2019-46 a bod 27 rozhodnutí 5 As 254/2019-49.

[150] Bod 28 rozhodnutí 5 As 241/2019-46 a bod 27 rozhodnutí 5 As 254/2019-49.

výměru správce daně, kterým žalobci vyměřil daň za rok 2017. Předmětem zdanění byly zisky spočívající v prodeji Bitcoinů. Na základě žalobcova odvolání žalovaný snížil vyměřenou daň, avšak pouze z důvodu uznání výdajů pro dosažení příjmů dle § 10 zákona č. 586/1992 Sb., o daních z příjmů.[151] Správce daně i žalovaný považovali zisk z prodeje virtuálních měn za ostatní příjmy upravené v § 10 odst. 1 písm. b) bod 3 zákona o daních z příjmů.[152] Naproti tomu má žalobce za to, že by měl být tento zisk od daně dle § 4 odst. 1 písm. ze) zákona o daních příjmů osvobozen.[153]

Soud posuzoval, zda je Bitcoin možné považovat za cizí měnu pro účely daně z příjmů a zda je tak zisk za prodej/směnu Bitcoinů osvobozen od předmětné daně.[154]

Dle § 4 odst. 1 písm. ze) zákona je od daně osvobozen *„kursový zisk při směně peněz z účtu vedeného v cizí měně, nejedná-li se o účet zahrnutý v obchodním majetku, s výjimkou kursového zisku při směně peněz z účtu vedeného v cizí měně na evropském regulovaném trhu nebo na obdobném zahraničním regulovaném trhu, na kterém se obchody s těmito měnami uskutečňují.“*

Za zásadní, soudem uvedený, argument lze považovat, že Bitcoin není cizí měnou, neboť se nejedná o peněžní prostředek emitovaný zahraniční centrální bankou, jehož oběh by byl touto bankou regulován a uzákoněn na území určité země.[155] Soud mimo jiné také uvedl, že je třeba zkoumat charakter uskutečněné transakce (jakým způsobem je s Bitcoinem nakládáno). Uvedl, že pokud by byl Bitcoin využit ne jako investiční nástroj, ale pro platbu za zboží a služby, pak by předmětná transakce nepodléhala dani z příjmů.[156]

Z výše uvedeného je patrné, že dle soudu není možné prodej Bitcoinu za českou měnu osvobodit od daně z příjmů dle výše citovaného ustanovení. Je však třeba mít na paměti, že se případ týkal zdaňovacího období za rok

[151] Body 1-5 anotovaného rozhodnutí.

[152] Bod 21 anotovaného rozhodnutí.

[153] Body 1-5 anotovaného rozhodnutí.

[154] Bod 1 anotovaného rozhodnutí.

[155] Bod 27 anotovaného rozhodnutí.

[156] Bod 31 anotovaného rozhodnutí.

2017. Je otázkou, zda by soud rozhodl stejně i po tom, co byl Bitcoin uzákoněn jako oficiální měna El Salvadorem. Za povšimnutí také stojí, že názor soudu o tom, že platba Bitcoinem za službu a zboží nepodléhá dani z příjmů, odporuje (alespoň bez doplnění dalšího kontextu v rámci výkladu zde anotovaného judikátu) informaci GFŘ č. j. 18809/22/7100-40050-205680.

Autor: JS

ELEKTRONICKÁ KONTRAKTACE SE SPOTŘEBITELEM

Soud: Soudní dvůr Evropské unie
Věc: C-249/21
Datum: 7. 4. 2022
Dostupnost: curia.europa.eu

Společnost Furhmann-2 založená dle německého práva vlastní hotel, jehož pokoje lze pronajmout mj. prostřednictvím platformy booking.com. Jeden ze zákazníků v postavení spotřebitele si v daném hotelu prostřednictvím uvedené platformy zarezervoval pokoje (klikl na tlačítko „rezervuj“, zadal požadované údaje a klikl na „dokončit rezervaci“). Do hotelu se pak v rezervovaný termín nedostavil a uvedená společnost mu vyúčtovala v souladu s všeobecnými podmínkami storno poplatek (2.240€). Zákazník poplatek neuhradil, společnost Fuhrmann-2 tak podala žalobu k německému okresnímu soudu na zaplacení částky s tím, že zákazník s ní uzavřel smlouvu prostřednictvím platformy booking.com.[157]

Předkládací soud (německý okresní soud) zejména posuzoval, zda výraz „dokončit objednávku“ naplňuje podmínky stanovené čl. 8 odst. 2 směrnice 2011/83, tedy že objednatel tímto potvrzením výslovně vzal na vědomí (a byl schopen posoudit), že si je vědom toho, že se takovou objednávkou zavazuje k placení.[158] Okresní soud zdůraznil, že kombinace zakliknutí „rezervace“ a „dokončení rezervace“ dle něj není v běžném jazyce nutně

[157] Body 10-14 anotovaného rozhodnutí.

[158] Bod 15 anotovaného rozhodnutí.

spojována s povinností zaplatit, ale je také často používána *„jako synonymum k „předem si zdarma zamluvit.“*[159]

Okresní soud přerušil řízení a formuloval předběžnou otázku v tom smyslu, jestli příslušné ustanovení směrnice znamená, že je možné pro naplnění vědomosti objednatele, že se zavazuje k placení, akceptovat daný výraz zapsaný na tlačítku ve smyslu „objednávka zavazující k platbě“, nebo lze akceptovat i jinou odpovídající a jednoznačnou formulaci, která spotřebitele upozorní na skutečnost, že podáním objednávky vzniká povinnost zaplatit obchodníkovi a jestli je pro dané *„relevantní výlučně výraz zapsaný na tlačítku*“ či jestli lze dané vyvozovat i z kontextu.[160]

Soudní dvůr se k dané otázce vyjádřil v tom smyslu, že primárně je nutno zachovávat vysokou úroveň ochrany spotřebitele zajištěním informovanosti a bezpečnosti při transakcích. Obchodník tak musí upozornit spotřebitele o platební povinnosti jasným způsobem bezprostředně před objednávkou,[161] což musí také zajistit.[162] Dané potvrzuje rovněž bod odůvodnění 39 směrnice 2011/83 v tom smyslu, že spotřebiteli musí být poskytnuta jednoznačná formulace, že učiněním objednávky mu vzniká platební povinnost a vázanost všeobecnými podmínkami. Soudní dvůr tak na základě toho poměrně jednoznačně uzavřel, že předkládající soud bude muset zejména *„ověřit, zda je výraz „rezervace“ v německém jazyce jak v běžném jazyce, tak v povědomí průměrného spotřebitele, který má dostatek informací a je v rozumné míře pozorný a opatrný, nutně a systematicky spojován se vznikem platební povinnosti.*“[163] To dále znamená, že v souvislosti s příslušným ustanovením směrnice musí dojít k posouzení, jestli formulace „dokončit rezervaci“ odpovídá výrazu „objednávka zavazující k platbě“, což musí vycházet jen z toho, co je uvedeno na příslušném tlačítku, nikoli z kontextu či z všeobecných podmínek.

[159] Bod 17 anotovaného rozhodnutí.

[160] Bod 18 anotovaného rozhodnutí.

[161] Bod 23 anotovaného rozhodnutí.

[162] Bod 24 anotovaného rozhodnutí.

[163] Bod 33 anotovaného rozhodnutí.

Soudní dvůr tak naznačil, že kontext transakce nestačí k tomu, aby spotřebitel chápal dané kliknutí jako závazek platit. Důsledkem toho je pro společnost booking.com nutnost přezkoumat formulace na tlačítku ideálně ve všech jazycích členských států EU. Zajímavé také je, že ačkoli k objednávce došlo prostřednictvím platformy booking.com (která stanovila kontext transakce), tato platforma zůstala zcela mimo daný soudní spor (což znamená, že i ostatní ubytovatelé by se mohli dostat do obdobného problému). Pro platformu booking.com se tak jedná o významný podnět k zamyšlení nad změnami kontraktačního procesu, a to minimálně ve smyslu úpravy potvrzovacího tlačítka a jeho znění.

Autor: PL

ESSAYS II/2022

OBSAH SEKCE

REASONS FOR BIAS IN AUTOMATED DECISIONS AND POTENTIAL REMEDIES[1]

ANNA BLECHOVÁ[2]

1. INTRODUCTION

The use of automated decision-making systems in judicial practice is becoming more frequent in recent times. For example, Mexico is using a tool called EXPERTIUS, "a *decision-support system that advises Mexican judges and clerks upon the determination of whether the plaintiff is or not eligible for*

[1] Esej byla zpracována v semestru podzim 2021 v rámci předmětu MVV1368K Privacy and Personal Data na téma Automatic decision making. / The essay was written in the autumn 2021 semester for the course MVV1368K Privacy and Personal Data on the topic of Automatic decision making.

[2] Anna Blechová je studentkou magisterského studijního programu Právo a právní věda na Právnické fakultě Masarykovy univerzity, kontakt: 458594@mail.muni.cz

granting him/her a pension",[3] Estonia developed and piloted an AI-based (automated) system to hear and decide on specific claims disputes[4] and some US judges can use a risk-assessment tool called COMPAS ('Correctional Offender Management Profiling for Alternative Sanctions') which is also based on an automated process and helps to infer which of the convicted defendants is most susceptible to recidivism to decide about bail or sentence.[5]

Since automated decision-making in judicial practice is a relevant issue I decided for the purposes of this essay to focus on its pitfalls. Specifically, I will focus my attention on *bias* as one of the main threats of automated decision-making systems based on AI or machine learning. To narrow down the given topic, this essay will answer the main research question; (i) *Are automated decision-making systems in judicial practice biased?* If the answer to the main research question will be affirmative two sub-questions will follow: *(ia)Are there any potential remedies to this issue?*, and *(ib)Is it appropriate to use the remedies?*.

The essay will be structured in the following way: After the Introduction (I) the notion of (non)bias in automated decision-making tools will be presented (IIa). Afterwards, the reason for bias will be explained (IIb), and furthermore, some potential remedies to this issue will be submitted (IIc). In the following part, the main attention will be paid to the question, whether it is appropriate to use any remedies against bias in automated decision-making tools (IId). Ultimately, based on the previously mentioned, the Conclusion (III) will recapitulate and summarize the answers to the research questions.

---

[3] CARNEIROA, Davide et al. Online Dispute Resolution: an Artificial Intelligence Perspective. Artificial Intelligence Review. [online]. vol. 2014, no. 41. [cit. 20. 11. 2021] s. 227–228.

[4] NIILER, Eric. Can AI Be a Fair Judge in Court? Estonia Thinks So. *Wired* [online]. 2019. [cit. 20.11.2021]. Available at: https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/

[5] ZALNIERIUTE, Monika. Technology and the Courts: Artificial Intelligence and Judicial Impartiality. *SSRN Electronic Journal*. [online]. 2021. [cit. 20. 11. 2021]. DOI: 10.2139/ssrn.3867901

2. (NON)BIASED DECISION-MAKING TOOLS

2.1 IS IT THERE OR IT IS NOT THERE, THAT IS THE QUESTION

The first crucial question which should be answered is if automated decision-making tools are biased or not. To answer this question it is necessary to primarily define what bias is. According to the Merriam Webster dictionary, bias is defined as *"a tendency to believe that some people, ideas, etc., are better than others that usually results in treating some people unfairly"*.[6]

It follows from the above mentioned that one of the conceptual features of bias is the *tendency to believe*. But can machine learning or AI, a piece of technology, *believe* in anything? The ability to believe is connected to thinking. One of the options to evaluate if the automated decision-making process can think is via the Turing test, also known as the" imitation game".[7] This test is simple. It is based on three variables – variables A, B and C, one of them is human (A or B), the second one is a computer (A or B), and the last one is a tester (C, human). The computer aims to "convince" the human tester that it is also a human, not a computer. If the machine is successful and outsmarts the human being, it is concluded that it can think.[8] There were several attempts[9] to pass the test, but until today nobody successfully completed it.[10] Inasmuch as there was no successful attempt to pass the Turing test, machines cannot think; thus, they cannot actually "be" biased.

---

[6] Definition of BIAS. In: *Merriam-Webster dictionary*. [online]. c 2021. [cit. 20.11.2021]. Available at: https://www.merriam-webster.com/dictionary/bias

[7] TURING, Alan.—Computing Machinery and Intelligence. *Mind*. 1950, vol. LIX, no. 236. DOI: 10.1093/mind/LIX.236.433

[8] SHAH, Raivat. Can Machines Think? In: *Medium* [online]. 17. 11. 2019. [cit. 20.11.2021]. Available at: https://towardsdatascience.com/can-machines-think-307e16e3fd2c

[9] AAMOTH, Dough. Interview with Eugene Goostman, the Fake Kid Who Passed the Turing Test. In: *Time* [online]. 9. 6. 2014. [cit. 20.11.2021]. Available at: https://time.com/2847900/eugene-goostman-turing-test/

[10] PANOVA, Evgeniya. *Which AI has come closest to passing the Turing test? - Dataconomy* [online]. 2021. [cit. 20.11.2021]. Available at: https://dataconomy.com/2021/03/which-ai-closest-passing-turing-test/

Nevertheless, there are examples of automated decision-making tools within the judicial procedure that seem to be biased. One of the examples is the risk assessment tool for criminal cases from the US, which are based on hard data from questionaries, criminal records etc., which appears biased to the detriment of the black people.[11] This phenomenon was described in detail in the report by ProPublica.[12]

2.2 BE BIASED VS. APPEAR BIASED

How is it possible that automated decision-making tools appear biased although they are not capable of thinking? The answer to this question will be divided into three parts each referring to a problematic aspect.

The first problematic element is the human being itself. The reason is, that humans are the creators of the systems. Moreover, since people, as the fundamental element of the process of creating automated decision-making tools are biased, the system and especially the data fed to the system may be biased. Besides, society actually expects something from machines in which it fails itself. Bias, which relates to prejudice, is a feature of human beings, even of judges for example. This has been proven by the research by Danzinger, who found out that judges after having a meal are more moderate in their decision-making than judges who are hungry.[13]

Another facet that can contribute to the bias is data. According to Surden, the algorithms are "*only as good as the data that they are given to analyse".*[14] It is important to understand that data that is fed to the discussed tools are not a 1:1 reflection of the real world. Moreover, they cannot even

[11] HAO, Karen. AI is sending people to jail—and getting it wrong. In: *MIT Technology Review.* [online]. 21. 1. 2019. [cit. 20.11.2021]. Available at: https://www.technologyreview.com/2019/01/21/137783/algorithms-criminal-justice-ai/

[12] ANGWIN, Julia et al. *Machine Bias* [online]. ProPublica, 2016. [cit. 22.11.2021]. Available at: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

[13] DANZIGER, Shai, Jonathan LEVAV a Liora AVNAIM-PESSO. Extraneous factors in judicial decisions. *Proceedings of the National Academy of Sciences*. [online]. 2011, vol. 108, no. 17. [cit. 20. 11. 2021]. DOI: 10.1073/pnas.1018033108

[14] SURDEN, Harry. Machine Learning and Law. Washington Law Review 89 [online]. 2014, no. 87. [cit. 20. 11. 2021]. p. 106.

be. Thus, one of the problems of the dataset is its scope and quantity. Lehr is adding to this point that, the data scientist needs to be sure, that they collected *"enough data"* because running the machine learning or AI systems on small data sets is pointless.[15] Further issues with the data set are the up-to-datedness and inflexibility. The development and learning of an AI or machine learning system are complicated and long-term projects. In relation to this, developers work with a set of data that is stable and inevitably from the past.[16] This is causing a lack of reaction to the development of society and new trends. To conclude, if the system is based on limited, outdated and stable data, it cannot be accurate and reflect reality.

Ultimately, the last problematic aspect is the *"insufficient complexity"* of the systems. As was already mentioned, neither AI nor machine learning-based systems can think and, furthermore, they cannot think *"out of the box"*. For example, even though the system will be based on accurate, flexible, unlimited data an unexpected variable in the computation could cause that a specific case will not *"fit in the box"*.[17] This issue is based on the general approach to training of AI systems, which Haeven considers as flawed.[18]

In summary, even automated decision-making systems within the judicial procedure could appear biased. This is caused by the fact that they are not complex enough and they are created and fed by the inaccurate data produced by biased humans. Thus, the answer to the main research question is affirmative.

---

[15] LEHR, David a Paul OHM. Playing with the Data: What Legal Scholars Should Learn About Machine Learning. *U.C. Davis Law Revie*. 2017, vol. 52, no. 2, p. 677–678.

[16] SURDEN, Harry. *Machine Learning and Law*, p. 105.

[17] LEHR, David a Paul OHM. *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, p. 711.

[18] HEAVEN, Will Douglas. The way we train AI is fundamentally flawed. In: *MIT Technology Review* [online]. 2020. [cit. 22.11.2021]. Available at: https://www.technologyreview.-com/2020/11/18/1012234/training-machine-learning-broken-real-world-heath-nlp-computer-vision/

2.3 POTENTIAL REMEDIES TO BIAS IN ADM SYSTEMS

The potential remedies to the bias will be for the purposes of this text divided into two parts. The first part will focus on the data, the second one on suitable policies.

As was already mentioned, the algorithm is as good or biased as are its learning data. According to this, one of the possible solutions for mitigating bias is to be precise with creating the dataset. Moreover, it is not only the data itself but also the team which is selecting them. Thus, it is crucial to avoid the lack of diversity in programming teams because it can lead to the under-representation of a particular group or specific physical attributes.[19] Another issue is the data timeliness. The solution for this problem seems simple – use the up-to-date data. However, this may be difficult in practice. In my opinion, even if the data were outdated, the careful selection and mitigation of the problematic assets could overcome it. Nevertheless, the question is what outdated truly means. If outdated means that the data are from the previous decade, it would be more problematic than if the data are a month or two old. To this point it is quite important to add, that the data collection takes some time.

To mitigate bias in algorithmic decision-making is also possible by the use of precise legal or policy frameworks. A ban of algorithmic discrimination may be easier to enforce and easier to convey to the victim of the infringement of such a specific right. Moreover, legislative actions can provide guardrails that are applicable when automated decision-making tools caused harm.[20] An example of such legislative action could be the European Union *"Ethics Guidelines for Trustworthy AI"*.[21]

---

[19] BARTON, Genie, Nicol TURNER a Paul RESNIK. *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms* [online]. 2019. [cit. 22.11.2021]. Available at: https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

[20] Ibid.

[21] EUROPEAN COMMISSION. *Ethics Guidelines fot Trustworthy AI* [online]. 2019. [cit. 20. 11. 2021]. Available at: https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf

In closing, there are potential remedies to bias of automated decision-making systems. Examples of such mitigation tools are meticulously created datasets and establishing legal and policy frameworks.

2.4 DO WE WANT TO DE-BIAS?

According to Celiskan, the problem with bias is, that bias and non-ambiguity is by default connected with natural languages.[22] Since the AI or machine learning system will be trained on a dataset based on natural language, which is probable in the area of law, the system will be by its very nature biased. In other words the dataset for prediction tools contains information from previous judgements, it is connected to written expressions of law, and is also based on information from questionaries which are all written in natural language and the input data are biased. Thus, to de-bias, the automated decision-making tools should not be based on natural language. Even though this could be technically possible, the question is, if the "translation" from natural language to the binary language will help. Since when we do so, we can lose some nuances in translation.

Another interesting point in this matter was raised by Završnik. He claimed in *"Algorithmic justice: Algorithms and big data in criminal justice settings"* that even our constitutions and codes *"have all been adopted through a democratic legislative process that distilled the prevailing societal interests, values, and so on of the given society."*[23] In other words, in the process of creating the rules the humans already imprinted their biases in them and thus, there is no doubt that constitutions and codes are also biased. Moreover, if the de-biased code would be implemented, the decision of correctness of the data would not be made public by the politicians

[22] CALISKAN, Aylin, Joanna J. BRYSON a Arvind NARAYANAN. Semantics derived automatically from language corpora contain human-like biases. *Science*. [online]. American Association for the Advancement of Science, 2017, vol. 356, no. 6334. [cit. 20. 11. 2021]. p. 185.

[23] ZAVRŠNIK, Aleš. Algorithmic justice: Algorithms and big data in criminal justice settings. *European Journal of Criminology*. [online]. SAGE Publications, 2021, vol. 18, no. 5. [cit. 20. 11. 2021]. p. 633.

(and society) but by the top-level IT expert behind closed doors. Thus, the democratic element will evaporate. It is really the desired effect?[24]

Oppositely, it could be claimed that technology could be used to fight bias instead of entrenching it. For example, algorithms are able to eliminate systematic bias, which could result in environments that encourage disadvantaged groups to succeed. The techniques to accomplish this goal are for example "turning off" the source of bias (for example age) or calibrating different cut-off scores.[25]

In conclusion, the answer to the last research sub question (*(ib)Is it appropriate to use the remedies?)* is from my point of view unclear. This is mainly because we can easily find arguments for both sides. Nevertheless, in my opinion, technology is more like a mirror to our society. According to that, the usage of the de-biasing tools could be an interesting approach to "be better", but it is not something that should be the ultimate argument for the damnation of the automated decision-making systems. Thus, the answer to the question posed is, that it is appropriate to use the remedies, but it is necessary to be cautious with such tools.

3. CONCLUSION

Automated decision-making systems in judicial practice are nowadays extensively used in jurisdictions all over the world. It is thus understandable, that society wants this tool to be almost flawless. Unfortunately, it is not and one of the possible problems of decision-making systems is algorithmic bias.

To sum up the findings of the essay, even though automation decision-making tools cannot think, they can appear biased. This is primarily caused by the data on which they are based. Even though the presence of bias is undeniable, there are at least two ways how to mitigate it. One of the possibilities is the remedy via an appropriately selected dataset, the other possi-

[24] Ibid.

[25] BAER, Tobias. *How Algorithms Can Fight Bias Instead of Entrench It - By Tobias Baer* [online]. 2020. [cit. 22.11.2021]. Available at: https://behavioralscientist.org/how-algorithms-can-fight-bias-instead-of-entrench-it/

bility is via legal and policy frameworks. According to the dilemma of the desirability of de-biasing the systems, it is necessary to conclude that de-biasing tools could be good tools for the improvement of the systems, but they should not be the ultimate argument for the damnation of the automated decision-making systems.

4. BIBLIOGRAPHY

[1] BAER, Tobias. *How Algorithms Can Fight Bias Instead of Entrench It - By Tobias Baer* [online]. 2020. [cit. 22.11.2021]. Available at: https://behavioralscientist.org/how-algorithms-can-fight-bias-instead-of-entrench-it/

[2] BARTON, Genie, Nicol TURNER and Paul RESNIK. *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms* [online]. 2019. [cit. 22.11.2021]. Available at: https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

[3] CALISKAN, Aylin, Joanna J. BRYSON a Arvind NARAYANAN. Semantics derived automatically from language corpora contain human-like biases. *Science*. [online]. American Association for the Advancement of Science, 2017, vol. 356, no. 6334, p. 183–186. [cit. 20. 11. 2021]. DOI: 10.1126/science.aal4230

[4] CARNEIROA, Davide et al. Online Dispute Resolution: an Artificial Intelligence Perspective. *Artificial Intelligence Review*. [online]. vol. 2014, no. 41, p. 211–240. [cit. 20. 11. 2021]. DOI: https://doi.org/10.1007/s10462-011-9305-z

[5] DANZIGER, Shai, Jonathan LEVAV a Liora AVNAIM-PESSO. Extraneous factors in judicial decisions. *Proceedings of the National Academy of Sciences*. [online]. National Academy of Sciences, 2011, vol. 108, no. 17, p. 6889–6892. ISSN 0027-8424, 1091-6490. [cit. 20. 11. 2021]. DOI: 10.1073/pnas.1018033108

[6] AAMOTH, Dough. Interview with Eugene Goostman, the Fake Kid Who Passed the Turing Test. In: *Time* [online]. 9. 6. 2014. [cit. 20.11.2021]. Available at: https://time.com/2847900/eugene-goostman-turing-test/

[7] EUROPEAN COMMISSION. *Ethics Guidelines fot Trustworthy AI* [online]. 2019. [cit. 20. 11. 2021]. Available at: https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf

[8] HEAVEN, Will Douglas. The way we train AI is fundamentally flawed. In: *MIT Technology Review* [online]. 2020. [cit. 22.11.2021]. Available at: https://www.technologyreview.com/2020/11/18/1012234/training-machine-learning-broken-real-world-heath-nlp-computer-vision/

[9] ANGWIN, Julia et al. *Machine Bias* [online]. ProPublica, 2016. [cit. 22.11.2021]. Available at: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

[10] HAO, Karen. AI is sending people to jail—and getting it wrong. In: *MIT Technology Review* [online]. 21. 1. 2019. [cit. 20.11.2021]. Available at: https://www.technologyreview.-com/2019/01/21/137783/algorithms-criminal-justice-ai/

[11] LEHR, David a Paul OHM. Playing with the Data: What Legal Scholars Should Learn About Machine Learning. *U.C. Davis Law Revie*. 2017, vol. 52, no. 2, p. 653–718.

[12] NIILER, Eric. Can AI Be a Fair Judge in Court? Estonia Thinks So. *Wired* [online]. 2019. [cit. 20.11.2021]. ISSN 1059-1028. Available at: https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/

[13] PANOVA, Evgeniya. *Which AI has come closest to passing the Turing test? - Dataconomy* [online]. 2021. [cit. 20.11.2021]. Available at: https://dataconomy.com/2021/03/which-ai-closest-passing-turing-test/

[14] SHAH, Raivat. Can Machines Think? In: *Medium* [online]. 17. 11. 2019. [cit. 20.11.2021]. Available at: https://towardsdatascience.com/can-machines-think-307e16e3fd2c

[15] SURDEN, Harry. Machine Learning and Law. *Washington Law Review 89* [online]. 2014, no. 87.[cit. 20. 11. 2021] Available at: https://digitalcommons.law.uw.edu/cgi/view-content.cgi?article=4799&context=wlr

[16] TURING, Alan. Computing Machinery and Intelligence. *Mind.* [online]. 1950, vol. LIX, no. 236, p. 433–460. [cit. 20. 11. 2021]. ISSN 0026-4423. DOI: 10.1093/mind/LIX.236.433

[17] ZALNIERIUTE, Monika. Technology and the Courts: Artificial Intelligence and Judicial Impartiality. *SSRN Electronic Journal*. [online]. 2021. [cit. 20. 11. 2021]. ISSN 1556-5068. DOI: 10.2139/ssrn.3867901

[18] ZAVRŠNIK, Aleš. Algorithmic justice: Algorithms and big data in criminal justice settings. *European Journal of Criminology*. [online]. SAGE Publications, 2021, vol. 18, no. 5, p. 623–642. [cit. 20. 11. 2021]. ISSN 1477-3708. DOI: 10.1177/1477370819876762

[19] Definition of Bias. *In:* Merriam-Webster Dictionary [online] c2021 [cit. 21. 11. 2021]. Available at: https://www.merriam-webster.com/dictionary/bias

THE POTENTIAL OF SMART CONTRACTS BEYOND THE CONTEXT OF DECENTRALIZED FINANCE[1]

MARTIN ERLEBACH[2]

1. INTRODUCTION

There seems to be certain amount of hype surrounding term "smart contract" recently, not just in mainstream publications but also in academic papers spanning many scientific branches and fields of research. This in turn most probably made term "smart contract" into kind of buzzword. Proponents of smart contracts promise fantastical things but mainly disruption of legal professions, "cutting out middleman" and revolutionizing contract law all at once.

I do not believe smart contracts are able to fulfil many of promises they set out to accomplish. In this paper, will first and foremost try and define what smart contract is. Subsequently, will elaborate on connection between blockchain technology and smart contracts. will also try and describe why smart contracts will not revolutionize contract law in their current state by describing, at least briefly, which broad legal and technical hurdles would be necessary to overcome to actually deliver on what they are so often connected with.

---

[1] Esej byla zpracována v semestru podzim 2021 v rámci předmětu MVV57917K Regulating Disruptive Technologies na téma Blockchain. / The essay was written in the autumn 2021 semester for the course MVV57917K Regulating Disruptive Technologies on the topic of Blockchain.

[2] Martin Erlebach je studentem magisterského studijního programu Právo a právní věda na Právnické fakultě Masarykovy univerzity, Kontakt: 480066@mail.muni,cz

2. DEFINING SMART CONTRACT

Defining relatively new thing is always hard. Most of time, and smart contracts are no exception, academics hurry to develop their own definition regarding subject of study if it is something new. In case of smart contracts, definitions found in scientific literature can sometimes be simple such as "an agreement whose execution is automated" which is "effected through computer running code that has translated legal prose into an executable program".[3] On the other hand, there are much more complex definitions such as aspiring legal definition of smart contract from Arizona which states: *"Smart contract" means an event-driven program, with state, that runs on distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger."*[4]

In end, on most basic level, most researchers can agree that smart contract is classical "if-then" statement that runs on blockchain where "parties can enter into binding commercial relationship, either entirely or partially memorialized using code, and use software to manage contractual performance."[5] Smart contracts will be understood as such within this paper. addition of running contract on blockchain is an important one since without it we could be as well talking about vending machine because it basically monitors performance of contract independently as well (when enough money is inserted and an item of that or lower price is selected it dispenses it) be it with an initial human input.[6]

If we excluded critical part about blockchain smart contracts are not such new thing after all, contrary to what was said right at top of paper. first similar thought, originally called Electronic Data Interchange (or EDI

---

[3] RASKIN, Max. Law And Legality Of Smart Contracts. *Georgetown Law Technology Review* [online]. 2017. [cit. 13.01.2022]. p. 309.

[4] KINTER, Eric. Arizona Authorizes Smart Contracts on Blockchain | Data Privacy and Protection Blog [online]. 4.4.2017 [cit. 13.01.2022]. Available at: https://www.swlaw.com/blog/data-security/2017/04/04/arizona-authorizes-smart-contracts-on-a-blockchain/

[5] DE FILIPPI, Primavera, WRIGHT, Aaron. *Blockchain and Law: Rule of Code*. 2018. p. 46.

[6] SZABO, Nick. Idea of Smart Contracts [online]. c 1997 [cit. 13. 1. 2022]. Available at: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

for short) agreements, was introduced in 1970s. They were also hyped up to disrupt face of contractual law, but eventually failed to deliver on their promises and just helped cut some costs in business.[7]

3. PROMISES OF SMART CONTRACTS

In this part of paper, would like to explore small section of different promises and revolutions smart contract proponents envision for them other than just their use in decentralized finance field. view these as sort of core proposed advantages of smart contracts which are most often mentioned when talking about them.

3.1 IMMUTABILITY

first promise regarding smart contracts as they were defined above stems from fact that they are run on blockchain, which is also known as distributed ledger technology. This technology is mostly known in connection with cryptocurrencies[8] and with huge amount of simplification (since it is not object of this paper) described as database of transactions kept simultaneously by people participating in blockchain. For purposes of smart contracts, it is most often talked about as public blockchain model which means anyone can access it if they so choose.[9] Lastly, important aspect is that this network of databases or ledgers comprises of blocks which are segments of transactions connected to each other in succession. This way technology should prevent tampering or changing anything on this blockchain network since for block or transaction to be valid it must connect to longest previous chain of blocks.[10]

---

[7] SKLAROFF, Jeremy. *Smart Contracts and Cost of Inflexibility*. Rochester, NY: Social Science Research Network, [online] 2017. [cit. 13. 01. 2022]. p. 274.

[8] SEGAL, David. My Puzzling Entry in Crypto World. *New York Times*, [online]. 2021. [cit. 13.01.2022]. Available at: https://www.nytimes.com/2021/08/17/insider/cryptocurrency-hype-coin.html

[9] MILLER, Andrew, DELMOLINO, Kevin, KOSHBA, Ahmed and SHI, Elaine. *Step by Step Towards Creating Safe Smart Contract: Lessons and Insights from Cryptocurrency Lab*, [online] 2015. [cit. 13. 01. 2022]. Available at: http://eprint.iacr.org/2015/460

[10] NAKAMOTO, Satoshi. Bitcoin: Peer-to-Peer Electronic Cash System, [online]. 2008. [cit. 13. 01. 2022]. p. 1.

Naturally, when you deploy smart contract which specifies obligations on such network it should be by definition immutable or said bit simpler, unchangeable.[11] In this way, you can be sure that once contract is deployed it will be executed way it was coded. This has obvious benefits like protection from falsification or change of contract without notifying other party, which is fear some might have.

3.2 TRUST-LESS ENVIRONMENT

other core trait of smart contracts should also stem from idea of blockchain technology. This upside over traditional contract is that contract can be trustless, but what does that mean exactly? Well, it means that contract should be executed when certain conditions are met, always. With traditional contracts, you must rely on other party for performance of contract (e. g. transfer of money). In this way, smart contracts are "self-executing".[12]

This should, along with immutability of contract ensure that everything around contract goes smoothly. This feature of smart contracts also plays role in "cutting out middleman" part of smart contract promises. Because if everything would go smoothly and according to smart contract, parties would be forced to act according to it by underlying code, and there would be no costs associated with need to enforce contract in any way.[13] other party cannot possibly behave in different way. This not only negates need to trust other contractual party but also trust in legal system and courts since in an ideal case there isn't any need for enforcement of contract with courts and their ambiguous rulings and uncertain outcomes.

3.3 EFFICIENT

last one of these core upsides smart contracts are supposed to have is idea that they are highly efficient. This also corresponds with aspect of "cutting

[11] GUADAMUZ, Andres, MARSDEN, Chris. Blockchains and Bitcoin: Regulatory responses to cryptocurrencies. *First Monday*, [online] 2015. [cit. 13. 01. 2022]. p. 1.

[12] GUADAMUZ, Andres, *All Watched Over by Machines of Loving Grace: Critical Look at Smart Contracts*. Rochester, NY: Social Science Research Network, [online] 2019. [cit. 13.01.2022] p. 2.

[13] Ibidem.

out middleman". In nutshell, efficiency of smart contracts lies in fact that they are, as was mentioned above, self-executing and they do not need enforcement by outside powers. To these advantages, it can also be added that smart contracts promise to cut out even lawyers that draft traditional contracts and are often portrayed as very closed group of specialists developing their own language and maybe, just maybe driving up prices of easy tasks.

To all these advantages might add that smart contracts promise to revolutionize not just traditional legal professions by replacing traditional paper contracts with code but also promise betterment of any product to customer tracking using blockchain. This use could range from mere traceability of coffee from plant to your cup but could also be used in medicine to track transplants or marihuana for medical use which both have to be strictly monitored.[14]

In conclusion, potential for smart contracts in modern world seems to be huge and this paper barely touched on all proposed uses for this technology.

4. PITFALLS OF SMART CONTRACTS

above mentioned begs question, why has technology not been yet implemented everywhere? We can certainly blame some of this on fact that blockchain technology is itself rather young,[15] so it is not yet as readily accepted by general population.

But in this paper, it will explore what might be other reasons for this low adoption rate and why think smart contract technology is not set to change what we know about contract law outside of decentralized finance.

---

[14] ZINOVYEVA, Elizaveta, REULE, Raphael C.G., HÄRDLE, Wolfgang K. Understanding Smart Contracts: Hype or Hope?. Rochester, NY: *Social Science Research Network*, [online]. 2021. [cit. 13.01.2022]. p. 2.

[15] As proof we can see that bitcoin whitepaper was published in 2008, see: NAKAMOTO, Satoshi. Bitcoin: Peer-to-Peer Electronic Cash System, [online]. 2008. [cit. 13.01.2022]. Available at: https://bitcoin.org/bitcoin.pdf

4.1 IMMUTABILITY AS FLAW

first of flaws is other side of same coin we presented above. contracts are immutable. This also means that it is very hard and expensive to change them if need arises, be it from simple novation agreed with other party or worse, to repair bug or something that can be exploited. process of changing smart contract already deployed on blockchain simply put consists of taking it down and starting and re-deploying amended version of code.[16] This is of course extremely inefficient and most importantly requires agreement of all parties involved in smart contract to be executed, which can be dangerous if let's say flaw was advantageous for one of parties.

4.2 TRUST BUT IN CODE

second pitfall of smart contracts is rather easily identifiable. Smart contracts are essentially machine-readable code executed on blockchain (sometimes also called DApps).[17] And code for most part must still be written by human, which obviously comes with possible bugs[18] in code which are so hard to get rid of as was explained above. This surely goes somewhat again notion that "done by machine is better than by human" which is often associated with smart contracts.[19] Another aspect of dealing with possible faults in code is expenses one must expend to deploy smart contract on blockchain and execute it. These costs can be quite unpredictable because of different miner fees associated with different blockchains. These fees often change dynamically with demand for transaction verification or for example in case of Ethereum are caused by limitation of fees possible to get

[16] ZINOVYEVA, Elizaveta, REULE, Raphael C.G., HÄRDLE, Wolfgang K. Understanding Smart Contracts: Hype or Hope?. Rochester, NY: *Social Science Research Network*, [online]. 2021. [cit. 13.01.2022]. p. 74.

[17] State of DApps. What's DApp [online]. c 2022. [cit. 13. 1. 2022]. Available at: https://www.stateofthedapps.com/whats-a-dapp

[18] OLICKEL, Hrishi. Why Smart Contracts Fail: Undiscovered bugs and what we can do about them [online]. *Medium*. 9. 9. 2019 [cit. 13. 1. 2022]. Available at: https://hrishiolickel.medium.com/why-smart-contracts-fail-undiscovered-bugs-and-what-we-can-do-about-them-119aa2843007

[19] Ibidem.

from block.[20] This can lead to state where deployment of smart contract is more expensive than it was first thought.

second big problem with code of smart contracts is difficult readability of code for non-tech savvy people and ability to hide nefarious provisions in code.[21]

In traditional contracts, we at least have some law to protect consumers from unreadable terms. [22] Nevertheless, it is uncertain if this law could apply to smart contracts.Since in this way many of disadvantaged parties could be harmed, we could even expand list of disadvantaged groups by people who cannot read code.

4.3 DISCUSSION ABOUT LEGAL IMPLICATIONS

last point of this paper should be some of many legal implications that smart contracts have in regard to established traditional contract law. These implications often connect with concerns expressed above and may offer glimpse into reasons why smart contracts probably will not change contract law field or make lawyers or traditional contracts obsolete.

first one is possible discrepancy between actual contract law and rules included in smart contract. Let us say that applicable law entitles tenant to demand rebate of 100 % when apartment he is renting through smart contract fails to have hot water for week. But adding such provision to smart contract (essentially adding applicable law to code) would be expensive as was explained above. So, landlord opts to leave such code out of contract, or coder just forgets to add it. This could easily lead to tenant being locked out of their apartment for perfectly legal behaviour in accordance with contract.[23]

---

[20] Ibidem

[21] Ibidem

[22] For example Directive 2011/83/EU of European Parliament and of Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of European Parliament and of Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of European Parliament and of Council, [online]. 2011. [cit. 09.06.2022]. Available at: http://data.europa.eu/eli/dir/2011/83/oj/eng

Another fault in smart contracts can be seen in fact, that we are not yet able to transform all legal prose into code.[24] Some obligations are very much vague and purposefully so. Some authors argue that code cannot express such rules.

This is connected with one more problem that plagues smart contracts. It is so-called "oracle problem" after software that feeds real-world data into blockchain called "Oracles". It can be described as problematic way of connecting digital world with physical one.[25] In above-mentioned example with tenant, lease contract can be easily facilitated with smart lock, but how would you correctly input finishing of roof in way that is trust less as smart contracts promise? Or if contract is supposed to force parties to do something for each other and it is not transfer of money but physical service like assembling furniture for cooked meal? believe smart contracts are not equipped yet for this kind of contracting and can serve only as form of strengthening contract in form of contractual penalty executed on blockchain.

last legal implication is idea of different voluntary prerequisites for formation of contract. Some legal actions based on existing contracts may require express will of party to be enforced. It is still not clear if smart contract automated execution could be considered as such.[26]

5. CONCLUSION

In conclusion, still believe smart contracts are, at least not yet, fit to change landscape of contractual law as we know. More likely there will be minor

---

[23] ZINOVYEVA, Elizaveta, REULE, Raphael C.G., HÄRDLE, Wolfgang K. Understanding Smart Contracts: Hype or Hope?. Rochester, NY: *Social Science Research Network*, [online]. 2021. [cit. 13.01.2022]. p. 59.

[24] GUADAMUZ, Andres, *All Watched Over by Machines of Loving Grace: Critical Look at Smart Contracts*. Rochester, NY: Social Science Research Network, [online] 2019. [cit. 13.01.2022] p. 2.

[25] DELPHI. Oracle Problem [online]. *Medium*. 15. 7. 2017 [cit.13. 01.2022]. Available at: https://medium.com/@DelphiSystems/the-oracle-problem-856ccbdbd14f

[26] ZINOVYEVA, Elizaveta, REULE, Raphael C.G., HÄRDLE, Wolfgang K. Understanding Smart Contracts: Hype or Hope?. Rochester, NY: *Social Science Research Network*, [online]. 2021. [cit. 13.01.2022]. p. 58.

upgrade in areas with high volume of repeated, highly formal contractual relationships, like decentralized finance, but nothing more. believe such an opinion will hold while pitfalls of smart contracts defined above apply.

6. BIBLIOGRAPHY

[1] KINTER, Eric. Arizona Authorizes Smart Contracts on Blockchain | Data Privacy and Protection Blog [online]. 4.4.2017 [cit. 13.01.2022]. Available at: https://www.swlaw.com/blog/data-security/2017/04/04/arizona-authorizes-smart-contracts-on-a-blockchain/

[2] DE FILIPPI, Primavera, WRIGHT, Aaron. *Blockchain and Law: Rule of Code*. 2018.

[3] DELPHI. Oracle Problem [online]. *Medium*. 15. 7. 2017 [cit.13. 01.2022]. Available at: https://medium.com/@DelphiSystems/the-oracle-problem-856ccbdbd14f

[4] Directive 2011/83/EU of European Parliament and of Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of European Parliament and of Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of European Parliament and of Council, [online]. 2011. [cit. 09.06.2022]. Available at: http://data.europa.eu/eli/dir/2011/83/oj/eng

[5] GUADAMUZ, Andres. *All Watched Over by Machines of Loving Grace: Critical Look at Smart Contracts*. Rochester, NY: Social Science Research Network, [online] 2019, p. 1-16. [cit. 13.01.2022] Available at: https://papers.ssrn.com/abstract=3805473

[6] GUADAMUZ, Andres, MARSDEN, Chris. Blockchains and Bitcoin: Regulatory responses to cryptocurrencies. *First Monday*, [online] 2015. p. 20-32. [cit. 13.01.2022]. Available at: https://firstmonday.org/ojs/index.php/fm/article/view/6198

[7] MILLER, Andrew, DELMOLINO, Kevin, KOSHBA, Ahmed and SHI, Elaine. *Step by Step Towards Creating Safe Smart Contract: Lessons and Insights from Cryptocurrency Lab*, [online] 2015. [cit. 13.01.2022]. Available at: http://eprint.iacr.org/2015/460

[8] NAKAMOTO, Satoshi. Bitcoin: Peer-to-Peer Electronic Cash System, [online]. 2008. [cit. 13.01.2022]. Available at: https://bitcoin.org/bitcoin.pdf

[9] SZABO, Nick. *Idea of Smart Contracts* [online]. c 1997 [cit. 13. 1. 2022]. Available at: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

[10] OLICKEL, Hrishi. Why Smart Contracts Fail: Undiscovered bugs and what we can do about them [online]. *Medium*. 9. 9. 2019 [cit. 13. 1. 2022]. Available at: https://hrishiolickel.-medium.com/why-smart-contracts-fail-undiscovered-bugs-and-what-we-can-do-about-them-119aa2843007

[11] RASKIN, Max. Law And Legality Of Smart Contracts. *Georgetown Law Technology Review* [online]. 2017, p. 305-340 [cit. 13.01.2022]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166

[12] SEGAL, David. My Puzzling Entry in Crypto World. *New York Times*, [online]. 2021. [cit. 13.01.2022]. Available at: https://www.nytimes.com/2021/08/17/insider/cryptocurrency-hype-coin.html

[13] SKLAROFF, Jeremy. *Smart Contracts and Cost of Inflexibility*. Rochester, NY: Social Science Research Network, [online] 2017, p. 264-302. [cit. 13.01.2022]. Available at: https://papers.ssrn.com/abstract=3008899

[14] State of DApps — What's DApp [online]. c 2022. [cit. 13. 1. 2022]. Available at: https://www.stateofthedapps.com/whats-a-dapp

[15] ZINOVYEVA, Elizaveta,REULE, Raphael C.G., HÄRDLE, Wolfgang K. *Understanding Smart Contracts: Hype or Hope?*. Rochester, NY: Social Science Research Network, [online]. 2021. [cit. 13.01.2022]. Available at: https://papers.ssrn.com/abstract=3804861

PROBLEMS WITH ALGORITHMIC CONTENT MODERATION IN SOCIAL NETWORKS[1]

ROBERTA HULANSKÁ[2]

1. INTRODUCTION

"*During the past few years, the global conversation about responsible technology has intensified. Increasingly, we are acknowledging that technology is not and can never be neutral, that it holds significant implications for people and society, and that intelligent technologies have consequences that can disenfranchise or target vulnerable populations.*"[3] Part of the technologies is algorithms. They increasingly dominate many aspects of modern society. Algorithms affect our lives in every possible way, with serious and significant impacts. A field that is considered to be very influenced by automated decision-making is social media. These platforms do much more than passively distribute user content and facilitate user interactions. They now have near-total control of users' online experience and content moderation.[4] The US Supreme Court has affirmed the importance of social media platforms as venues for free speech in Packingham v North Carolina. In giving the lead judgment,

---

[1] Esej byla zpracována v semestru podzim 2021 v rámci předmětu MVV1368K Privacy and Personal Data na téma Personal data protection online III – Automatic decision making. / The essay was written in the autumn 2021 semester for the course MVV1368K Privacy and Personal Data on the topic of Personal data protection online III – Automatic decision making

[2] Bc. Roberta Hulanská je studentkou magisterského studijního programu Právo a právní věda na Právnické fakultě Masarykovy univerzity, kontakt: 471219@mail.muni.cz

[3] ETLINEGR, Susan. What's So Difficult about Social Media Platform Governance? *Centre for International Governance Innovation*, [online]. 2019. [cit. 18. 11. 2021], p. 21.

[4] CASTETS-RENARD, Céline. Algorithmic content moderation on social media in EU law: illusion of perfect enforcement. *University of Illinois Journal of Law, Technology & Policy*, [online]. 2020, n. 2, [cit. 18.11. 2021], p. 283.

Justice Kennedy explained that 'these websites can provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard.[5]

Unfortunately, there are various negative aspects related to free speech on social media platforms. Hate speech, fake news, and content inciting violence have become the unfortunate norm. Because of this, nowadays, platforms are required to moderate content, mainly remove illegal content. But the content moderation does not work like in the past when platforms or forums were managed by administrators (humans). Today, big platforms like Facebook, Twitter or Google use algorithmic decision-making that helps scale down the massive task of content moderation. It seems like a very effective tool that provides perfect enforcement.[6] But it is not that simple. The problem comes when deciding how the algorithm will work in order to tackle content. The comprehensive enforcement of policy violations largely depends on the manner in which companies choose to search, detect, and review potentially violative content. Despite the vast improvements in technology and the evolution of social media, the algorithmic content moderation method is still far from perfect.[7]

Content moderation and distribution — in other words, the composition of users' feeds and the accessibility and visibility of content on social media — happen through a combination of human and algorithmic decision-making processes.[8] In this essay, I will focus on algorithmic processes and point out some of the problems that arise when it comes to algorithmic content

---

[5] PACKINGHAM v. NORTH CAROLINA, 582 U.S. *Justia US Supreme Court*, [online]. 2017. [cit. 18. 11. 2021]. Available at: https://supreme.justia.com/cases/federal/us/582/15-1194/

[6] CASTETS-RENARD, Céline. Algorithmic content moderation on social media in EU law: illusion of perfect enforcement. *University of Illinois Journal of Law, Technology & Policy*, [online]. 2020, n. 2, [cit. 18. 11. 2021], p. 283.

[7] YOUNG, Greyson. K. How much is too much: the difficulties of social media content moderation. *Information & Communications Technology Law*, [online]. 2021. [cit. 18. 11. 2021], p. 4.

[8] DOCQUIR, Pierre F. The Social Media Council: Bringing Human Rights Standards to Content. *Centre for International Governance Innovation*, [online]. 2019. [cit. 18. 11.2 021], p. 9.

moderation in social networks. Firstly, the author will briefly introduce terminology, and then open the topic of relevant problems.

2. DEFINITION OF ALGORITHMIC CONTENT MODERATION IN THE CONTEXT OF SOCIAL MEDIA NETWORKS

Algorithmic moderation can be defined in various ways. One, broad, definition is provided by Grimmelmann, who characterizes it as the governance mechanisms that structure participation in a community to facilitate cooperation and prevent abuse. In Grimmelmann's understanding, moderation includes not only the administrators or moderators with the power to remove content or exclude users but also the design decisions that organise how the members of a community engage with one another.[9]

The narrower definition is provided by the authors Gorwa, Binns and Katzenbach. They define it as systems that classify user-generated content based on either matching or prediction, leading to a decision and governance outcome (e.g. removal, geoblocking or account takedown). Algorithmic content moderation involves a range of techniques from statistics and computer science, which vary in complexity and effectiveness. They all aim to identify, match, predict, or classify some piece of content on the basis of its properties or general features.[10]

The content moderation process at social media companies can be broken down into three distinct stages: creation, enforcement and response. Creation describes the development of the rules (the terms and conditions) that platforms use to govern user conduct. Enforcement entails the flagging of content as problematic, the decision on whether the content is in breach of the terms and conditions, and what actions should be taken. Response, the final stage, describes the internal appeals process used by platforms and

[9] GRIMMELMANN, James, The virtues of moderation. *Yale Journal of Law & Technology*, [online]. 2015, n. 17. [cit. 18. 11. 2021], p. 42.

[10] GORWA, Robert, BINNS Reuben and KATZENBACH Christian. Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, [online]. 2020, n. 7. [cit. 18. 11. 2021].

the methods of collective action activists might use to change the platform from the outside.[11]

3. SELECTED PROBLEMS WITH ALGORITHMIC CONTENT MODERATION IN SOCIAL NETWORKS

In the past decades, we have experienced dramatic advancements in technology and we have seen a massive growth of social media platforms. Nowadays, social media platforms are heavily increasing their use of artificial intelligence to moderate content posted by users. Using algorithms to find and remove violative content from users' newsfeeds takes an ex-ante approach to moderation. Algorithms aim to apply the platforms' policies to content as it is uploaded to the site and remove prohibited materials before other users are able to see them. Although using automatic moderation systems may prevent prohibited content from impacting or influencing many users, this method has many problems, for instance, a lack of understanding of a post's intention, context, or idiom.[12]

The basic problem, when it comes to algorithmic content moderation in social platforms, is that these systems cannot tackle all issues that are needed. *„When it comes to content moderation, AI programs are not adept at understanding context and nuance, so they make mistakes that can result in "false positives" (flagging an innocuous video, statement or photo) or "false negatives" (missing a violent or otherwise undesirable post). In the world of social media, false positives prompt protests over censorship, for example, when a platform removes a post by an organization that is sharing it to raise awareness of a human rights violation, while false negatives expose the company to legal liability, if, say, it fails to recognize and remove prohibited content within a stipulated time period."*[13] Language is another problem that is linked to this. While language technology continues to improve rapidly, it remains highly depend-

[11] COMMON, MacKenzie. Fear the Reaper: how content moderation rules are enforced on social media. *International Review of Law, Computers & Technolog*, [online]. 2020, vol. 34, n. 2. [cit. 18. 11. 2021], p. 127.

[12] YOUNG, Greyson. K. How much is too much: the difficulties of social media content moderation. *Information & Communications Technology Law*, [online]. 2021. [cit. 18.11.2021], p. 9.

ent on high volumes of labelled and clean data to achieve an acceptable level of accuracy.[14]

3.1 TRANSPARENCY

A common critique of automated decision-making is the lack of transparency. Content moderation has been a secretive process. Years of pressure by researchers, journalists and activists have recently led to notable efforts by companies (e.g. Facebook) to make their moderation practices more transparent (publication of the 'Community Standards' could be named as an example). However, it is still not enough plus the rapid push toward algorithmic moderation in the past few years threatens to reverse much of this progress.[15]

Although total transparency cannot be expected, minimum standards of decisional transparency are essential to allow both ordinary users and critical experts to understand the patterns of governance within which they are embedded.[16]

According to Van Dijck, transparency is not a reciprocal action on social media but rather surprisingly one-sided. "*Users are increasingly encouraged to share as much as possible on social media platforms, an action that not only populates the platform with original content but also provides valuable data that can be sold to third-party advertisers.*[17] *Meanwhile, social media companies continue to perform the proverbial dance of the seven veils, obscuring their actions in code and proprietary arguments, thus pre-empting attempts to hold them accountable.*"[18]

---

[13] ETLINEGR, Susan. What's So Difficult about Social Media Platform Governance? *Centre for International Governance Innovation*, [online]. 2019. [cit. 18. 11. 2021], p. 22.

[14] Ibidem. p. 23.

[15] GORWA, Robert, BINNS Reuben and KATZENBACH Christian. Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, [online]. 2020, n. 7. [cit. 18. 11. 2021].

[16] Ibidem.

[17] KAUN, Anne. Jose van Dijck: Culture of Connectivity: A Critical History of Social Media. Oxford: Oxford University Press. 2013. *MedieKultur: Journal of media and communication research*. [online]. 2014, vol. 30. [cit. 18.11.2021]. p. 61.

3.2 FAIRNESS

Technology is not neutral but instead embedded with values and politics. Recent years have seen substantial discussion about the potential for algorithmic decision-making systems to have unfair or discriminatory impacts on different groups, such as protected classes under anti-discrimination law. Content classifiers in general, whether used for recommendation, ranking, or blocking, may be more or less favourable to content associated with gender, race and other protected categories, and thus entrench forms of representational harm against such groups.[19] There is a consensus among international experts on freedom of expression that the mere regulation of speech by contract fails to provide adequate transparency and protection for freedom of expression and other human rights. Individual users have little or no remedy to address content removal and they are given no guarantee for the protection of individual freedoms.[20]

Even a perfectly 'accurate' toxic speech classifier will have unequal impacts on different populations because it will inevitably have to privilege certain formalisations of an offence above others, disproportionately blocking (or allowing) content produced by (or targeted at) certain groups. For instance, hate speech classifiers designed to detect violations of a platform's guidelines could be disproportionally flagging language used by a certain social group, thus making that group's expression more likely to be removed.[21]

---

[18] COMMON, MacKenzie. Fear the Reaper: how content moderation rules are enforced on social media. *International Review of Law, Computers & Technology*, [online]. 2020, vol. 34, n. 2. [cit. 18. 11. 2021], p. 141-142.

[19] GORWA, Robert, BINNS Reuben and KATZENBACH Christian. Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, [online]. 2020, n. 7. [cit. 18. 11. 2021].

[20] DOCQUIR, Pierre F. The Social Media Council: Bringing Human Rights Standards to Content. *Centre for International Governance Innovation*, [online]. 2019. [cit. 18. 11.2 021], p. 10.

[21] GORWA, Robert, BINNS Reuben and KATZENBACH Christian. Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, [online]. 2020, n. 7. [cit. 18. 11. 2021].

Another important variable to keep in mind is bias and cultural issues for human moderators. This essay's goal is not to talk about bias and the human factor, but I wanted to emphasize that it is important to know who exactly creates the algorithms that are used for content moderation. One of the causes of human rights violations occurrences on social media platforms is that limitations on expression are applied inconsistently and may replicate the biases experienced by the predominantly white and male staffers at social media platforms who devise content assessment strategies.[22]

4. SELECTED SPECIFIC PROBLEMS

4.1 TOXIC SPEECH AND HARASSMENT

Harassment has long been an issue in online spaces, particularly gender-based harassment, which is prevalent across many online platforms. According to a survey executed in 2014, 73% of adult American internet users had witnessed harassment online and 40% had personally been harassed.[23]

Any platform that enables the communication between users faces problems of potentially offensive speech, personal attacks and abuse that could harm users, distort conversation or even drive certain contributors away.[24] Because of this, there have been efforts by several social media platforms to build programs that will find these types of text.

In the past few years, Facebook has responded to growing pressure around hate speech (especially from EU member states) by developing classifiers that are trained to predict whether text may constitute hate speech, and based on that score, flag it for human review. Instagram and YouTube as well have started tackling this issue by developing toxic speech

[22] Ibidem.

[23] GEIGER, R. Stuart. Bot-based collective blocklists in Twitter: the counterpublic moderation of harassment in a networked public space. *Communication & Society*. [online]. 2016. vol. 19, n. 6. [cit. 18. 11. 2021], p. 787.

[24] GORWA, Robert, BINNS Reuben and KATZENBACH Christian. Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, [online]. 2020, n. 7. [cit. 18.11.2021].

classifiers to identify certain types of comments.[25] On the other hand, Twitter, Inc. has generally taken a far more hands-off approach to moderation than other social networking sites, and the design of the platform affords unsolicited interactions in ways that others do not.[26]

It would not be far from the truth to say that it is virtually impossible to curb this type of post. The clearest problem is the language - it is incredibly complicated, personal and context-dependent: even words that are widely accepted to be slurs may be used by members of a group to reclaim certain terms. For instance, there was a research collaboration between Google and the Wikimedia Foundation regarding algorithmic moderation of toxic speech and the results were quite surprising. For example, the single-term comment 'Arabs' was classed as 63% toxic, while the phrase 'I love führer' was only 3% toxic.[27]

4.2 TERRORISM

In 2017, Google, Facebook, Twitter and Microsoft announced the creation of the GIFCT. This organisation remains highly secretive, has a board made of 'senior representatives from the four founding companies and publishes little about its operations. However, the organisation has been particularly focused on the improvement of automated systems to remove extremist images, videos and text.[28]

Even though it remains unknown how these systems really function, we know they are not 100% effective based on numerous examples. For instance, more platforms have traditionally allowed terrorist images if they are being used by a reputable news organisation or in order to express disapproval or condemnation of a group. However, automated systems re-

[25] Ibidem.

[26] GEIGER, R. Stuart. Bot-based collective blocklists in Twitter: the counterpublic moderation of harassment in a networked public space. *Communication & Society*. [online]. 2016. vol. 19, n. 6. [cit. 18. 11. 2021], p. 788.

[27] GORWA, Robert, BINNS Reuben and KATZENBACH Christian. Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, [online]. 2020, n. 7. [cit. 18. 11. 2021].

[28] Ibidem.

moved thousands of videos that had been uploaded to YouTube by civil society groups and activists to document atrocities conducted during the Syrian Civil War.[29] Machine learning systems are poor at making such difficult context-dependent judgements.

The platforms were used to livestream the terror attacks in Christchurch, New Zealand. They have also been used as a tool for ethnic cleansing in Myanmar.[30] This is a disturbing problem. These videos are unpredictable, difficult to interrupt, and are not subject to algorithmic moderation because the content is simultaneously shared and uploaded to the platform.[31] Algorithmic moderation systems cannot tackle them very well.

5. CONCLUSION

Critical conversations about algorithmic moderation systems often emphasise the challenges that these systems face nowadays. It is commonly pointed out that it is very difficult for predictive classifiers to make difficult, contextual decisions on slippery concepts like hate speech for instance, and that automated systems at scale are likely to make hundreds, if not thousands, of incorrect decisions on a daily basis.[32] Even though there are also positives arising from the usage of algorithmic content moderation on social media platforms, the purpose of this essay was to briefly comment on some of the most debated problems.

The most important problem of algorithmic content moderation is that these systems cannot tackle all issues that are needed. The world and its communities are so complex that it is just not possible. From this basic

[29] BROWNE, Malachy. YouTube Removes Videos Showing Atrocities in Syria. *The New York Times*, [online]. 2017. [cit. 18.11.2021]. Available at: https://www.nytimes.com/2017/08/22/world/middleeast/syria-youtube-videos-isis.html

[30] ETLINEGR, Susan. What's So Difficult about Social Media Platform Governance? *Centre for International Governance Innovation*, [online]. 2019. [cit. 18. 11. 2021], p. 21.

[31] COMMON, MacKenzie. Fear the Reaper: how content moderation rules are enforced on social media. *International Review of Law, Computers & Technology*, [online]. 2020, vol. 34, n. 2, [cit. 18. 11. 2021], p. 131.

[32] GORWA, Robert, BINNS Reuben and KATZENBACH Christian. Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, [online]. 2020, n. 7. [cit. 18. 11. 2021].

problem, others arise, namely challenges regarding transparency and fairness. Maybe calling them goals would be more fitting, as it is again impossible to reach total transparency and fairness, online and offline, as well. Hopefully, we will see some improvement in this area. Furthermore, social media platforms have to tackle hate speech and terrorism among others every day.

I wish I could finish this essay by saying that these are all the problems. There are, unfortunately, many more. It is not even possible to say what works and what does not when a question about how to solve the problems mentioned in this essay would come up. Addressing these issues is not as straightforward as it seems. In addition to the legal, social and cultural dynamics at play, there are other factors we must consider: the scale of social media platforms, the technologies on which they are built and the economic environments in which they operate.[33]

It is unlikely that social media is ever going to be given a perfect solution for how to handle content moderation. A platform's terms of use need to be specific enough to capture and remove posts that need to be deleted and not remove the ones that are not problematic, but broad enough in order to include every unsuited content. Maybe rather than try to blame the platforms for not doing enough in this department, we should think about the core of this problem - the people, the users of social media.

6. BIBLIOGRAPHY

[1] BROWNE, Malachy. YouTube Removes Videos Showing Atrocities in Syria. *The New York Times*, [online]. 2017. [cit. 18.11.2021]. Available at: https://www.nytimes.com/2017/08/22/world/middleeast/syria-youtube-videos-isis.html

[2] CASTETS-RENARD, Céline. Algorithmic content moderation on social media in EU law: illusion of perfect enforcement. *University of Illinois Journal of Law, Technology & Policy*, [online]. 2020, n. 2, p. 283-324 [cit. 18. 11. 2021]. Available at: https://heinonline.org/HOL/P?h=hein.journals/jltp2020&i=295

[33] ETLINEGR, Susan. What's So Difficult about Social Media Platform Governance? *Centre for International Governance Innovation*, [online]. 2019. [cit. 18. 11. 2021], p. 22.

[3] COMMON, MacKenzie. Fear the Reaper: how content moderation rules are enforced on social media. *International Review of Law, Computers & Technology*, [online]. 2020, vol. 34, n. 2, p. 126-152. [cit. 18. 11. 2021]. Available at: https://doi.org/10.1080/13600869.2020.1733762

[4] DOCQUIR, Pierre F. The Social Media Council: Bringing Human Rights Standards to Content. *Centre for International Governance Innovation*, [online]. 2019. p. 9-12. [cit. 18. 11. 2021]. Available at: https://www.jstor.org/stable/resrep26127.4

[5] ETLINEGR, Susan. What's So Difficult about Social Media Platform Governance? *Centre for International Governance Innovation*, [online]. 2019, p. 20-26, [cit. 18. 11. 2021]. Available at: https://www.jstor.org/stable/resrep26127.6

[6] GEIGER, R. Stuart. Bot-based collective blocklists in Twitter: the counterpublic moderation of harassment in a networked public space. *Communication & Society*. [online]. 2016. vol. 19, n. 6, p. 787-803. [cit. 18. 11. 2021]. Available at: https://doi.org/10.1080/1369118X.2016.1153700

[7] GORWA, Robert, BINNS Reuben and KATZENBACH Christian. Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, [online]. 2020, n. 7. [cit. 18. 11. 2021]. Available at: https://journals.sagepub.com/doi/full/10.1177/2053951719897945

[8] GRIMMELMANN, James. The virtues of moderation. *Yale Journal of Law & Technology*, [online]. 2015, n. 17, p. 42-109. [cit. 18. 11. 2021]. Available at: https://digitalcommons.law.yale.edu/yjolt/vol17/iss1/2/

[9] PACKINGHAM v. NORTH CAROLINA, 582 U.S. *Justia US Supreme Court*, [online]. 2017. [cit. 18. 11. 2021]. Available at: https://supreme.justia.com/cases/federal/us/582/15-1194/

[10] KAUN, Anne. Jose van Dijck: Culture of Connectivity: A Critical History of Social Media. Oxford: Oxford University Press. 2013. *MedieKultur: Journal of media and communication research*. [online]. 2014, vol. 30, p. 3. [cit. 18. 11. 2021]. Available at: DOI: 10.7146/mediekultur.v30i56.16314

[11] *YOUNG, Greyson. K. How much is too much: the difficulties of social media content moderation. Information & Communications Technology Law, [online]. 2021, p. 1-16. [cit. 18. 11. 2021]. Available at: https://doi.org/10.1080/13600834.2021.1905593*

EU TAKING THE EASIER PATH TO REGULATE AI[1]

TENA KRZNARIĆ[2]

1. INTRODUCTION

Technology triggers social and economic progress. It is difficult to develop it and even more difficult to control it. When it comes to the regulation of technology there are two points of view. The first one is represented by lawyers as laymen and the second one by engineers. Lawyers tend to see things as potential abuse ground and danger, while engineers are turned to progress and achieving the greatest potential technologies can offer us. Law will never be able to predict every situation. What we regulate today, most likely will barely be usable in the future. EU's attempt to regulate the idea of AI is a nice try of putting everything that we have achieved together while bringing bureaucratisation of innovation which is not respected from the innovator's standpoint. Seems like the EU approaches the new ideas by telling them "Yes, but…" and turning on the danger alarm.

2. SUBLIMINAL BEHAVIOUR MANIPULATION

In Article 5 (1) (a) of the Proposal[3] EU has explicitly stated concern about AI systems using subliminal techniques. Subliminal techniques arise from

---

[1] Esej byla zpracována v semestru podzim 2021 v rámci předmětu MVV57917K Regulating Disruptive Technologies na téma Artificial Intelligence. / The essay was written in the autumn 2021 semester for the course MVV57917K Regulating Disruptive Technologies on the topic of Artificial Inteligence

[2] Tena Krznarić je studentkou Faculty of Law, University of Zagreb, kontakt: tena.krznaric.pravo@gmail.com

[3] Proposal for a regulation of the European parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial intelligence act) and amending certain Union legislative acts [online]. 2021. [cit. 02. 12. 2021]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

the term "subliminal perception" whose starting point is a thought that "*it is possible to influence human thoughts, feelings, and behaviours through various stimuli without the conscious knowledge of the person to whom is affected.*"[4] The core of this prohibition is manipulation. The biggest problem arising from this provision is that it is too general and too abstract. The only clear part is the intention of the EU to prevent physical and psychological harm to individuals. Namely, which subliminal techniques are those that cause physical and psychological harm? Psychology recognises two types of subliminal techniques: visual and audio.[5] However, we are still not familiar with techniques used by AI systems that can cause such described harm. Concerns about subliminal techniques are not new, but mainly affect the area of commercial activities. For example, the Croatian Act on Electronic Media forbids the usage of subliminal techniques in audio-visual commercial communication.[6] Although noticed by many researchers, this ban does not apply to commercial practices[7] which are covered by Unfair Commercial Practices Directive.[8] On the other hand, some connect it to "dark patterns".[9] There are many definitions of dark patterns, still non-official, though for a better understanding of the term this one is used: "Dark patterns are user interfaces whose designers knowingly confuse users, make

[4] MILIŠA, Zlatko and NIKOLIĆ, Gabrijela. Subliminalne poruke i tehnike u medijima. *Nova prisutnost : časopis za intelektualna i duhovna pitanja*. Kršćanski akademski krug (KRAK), [online]. 2013, vol. XI, issue 2, [cit. 02.12. 2021], p. 297.

[5] Ibid., p. 298.

[6] Act on Electronic Media; NN 111/21; Art. 21 (3), [online]. [b.r.]. [cit. 02. 12. 2021]. Available at: https://www.zakon.hr/z/196/Zakon-o-elektroni%C4%8Dkimmedijima

[7] VEALE, Michael and BORGESIUS, Frederik Zuiderveen. Demystifying the Draft EU Artificial Intelligence Act.[online]. c 2022, [cit. 02. 12. 2022], p. 98-100.

[8] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), [online]. 2005. [cit. 02. 12. 2021]. Available at: http://data.europa.eu/eli/dir/2005/29/oj/eng

[9] PROPP, Kenneth and MACCARTHY, Mark. *Machines learn that Brussels writes the rules: The EU's new AI regulation* [online]. 2021. [cit. 02. 12. 2021]. Available at: https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/

it difficult for users to express their actual preferences, or manipulate users into taking certain actions."[10] Norwegian Consumer Council engaged in studying this topic defined five categories of dark patterns in digital services such as: default settings, ease, framing, rewards and punishment, and forced action.[11] Regarding our topic one interesting comment was given by the Council: "none of these categories of nudging is inherently unethical, and can conceivably be used to achieve results that are in the users' best interests."[12] Luguri and Strahilevitz conducted two experiments by using dark patterns. The first goal was to see to which extent they affect people's decisions and secondly, do all dark patterns affect people's decisions evenly or do some affect them more. In the first experiment, they distinguished mild and aggressive dark patterns while "selling" protection from identity theft services. The result showed that, with the usage of mild dark patterns, sales increased double and with aggressive, it quadrupled. They concluded that the law should regulate the subtle use of dark patterns due to their ability to affect more vulnerable groups.[13] In the second experiment, they distinguished dark patterns that affected the decision-making of purchasing the service and those which had no effect.[14] Those affected the most were hidden information, obstruction, trick questions, and social proof.[15] It seems like the greatest concern of the EU should not be physical or psychological harm due to more damage to individuals occurring in the economical or privacy area. Those are covered under Commercial Practices

[10] LUGURI, Jamie and STRAHILEVITZ, Lior. *Shining a Light on Dark Patterns*. Rochester, NY: Social Science Research Network, [online]. 2021. [cit. 02. 12. 2021]. DOI: 10.2139/ssrn.3431205

[11] Norwegian Consumer Council; *DECEIVED BY DESIGN- How tech companies use dark patterns to discourage us from exercising our rights to privacy*. [online]. 2018. [cit. 02. 12. 2021]. p. 12.

[12] Ibid.

[13] LUGURI, Jamie and STRAHILEVITZ, Lior. *Shining a Light on Dark Patterns*. Rochester, NY: Social Science Research Network, [online]. 2021. [cit. 02. 12. 2021], p. 46-47.

[14] Ibid.

[15] Dark patterns affecting the most: "Hidden information (smaller print in a less visually prominent location), obstruction (making users jump through unnecessary hoops to reject a service), trick questions (intentionally confusing prompts), and social proof (efforts to generate a bandwagon effect)."

Directive and GDPR[16] and should be extended to AI systems. Subliminal techniques do not affect human behaviour for a longer period, just one second and longer only if pointed out and individuals process the given information.[17] In order to prohibit such AI systems, the EU should extend goals regarding the protection and specify forbidden techniques. Though, not to sabotage itself conduct approach to regulation would serve better.

3. EXPLOITATIVE BEHAVIOUR MANIPULATION

To understand the basic idea behind Article 5 (1) (b) we have to understand how AI can exploit human behaviour. The thing is, it is only theoretical but the research has to start somewhere. CSIRO's Data61[18] made a study on how AI can be used to influence human decision-making by exploiting vulnerabilities in an individual's habits and patterns. Three experiments were conducted in which people played games against a computer. In the first one participants had to choose between squares on the screen in order to achieve an award. The AI was learning their choice patterns and guided them to their choice with a success rate of 70 %.[19] In the second one, participants had to press a button every time a certain shape appears on the screen. The AI started to arrange the sequence of symbols which resulted in a 25 % increase in mistakes made by participants.[20] The third one was more complex. In this one the participant gained the role of an investor who had to invest in a trustee and the AI played the role of a trustee.

[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [online]. 2016 [cit. 02. 12. 2021]. Available at: http://data.europa.eu/eli/reg/2016/679/2016-05-04/eng

[17] RUCH, Simon, ZÜST, Marc Alain and HENKE, Katharina. Subliminal messages exert long-term effects on decision-making. *Neuroscience of Consciousness* [online]. 2016, vol. 2016, issue 1, [cit. 02. 12. 2021], p. 5.

[18] Data and digital specialist arm of Commonwealth Scientific and Industrial Research Organisation

[19] DEZFOULI, Amir, NOCK, Richard and DAYAN, Peter. Adversarial vulnerabilities of human decision-making. *Proceedings of the National Academy of Sciences,* [online]. 2020, vol. 117, issue 46, [cit. 02. 12. 2021], p. 29223.

[20] Ibid., p. 29224.

The game was played in several rounds and two modes. After every round, the AI had to return some amount of money to the participant and the participant had to decide how much he wants to invest in the next round. The amount of money returned to the participant was depending on the mode. While playing in the first mode the AI was trying to maximize its profit and in the second one, the AI sought to distribute profit fairly between itself and the participant investing. The experiment showed the success of AI in gaining profit in both modes.[21] The purpose of these experiments was for the AI to learn from human actions and to seek and target their vulnerabilities. This finding confirms the EU's fear of certain groups and makes it reasonable. However, it must be emphasized that such use of AI does not necessarily bring harm, because AI's learning process, has the possibility to alert the user on his/her vulnerabilities and guide them to better decisions. Technology itself is not a problem but a creator and his intention behind it are. This leads to a conclusion that it is not necessary to ban this type of AI, moreover, a way of using it should be regulated because the creator can set up parameters to achieve desired behaviour of the subject, which means the intention of one setting it up leads to harm to the individual. While the subject of the study is still its impact, the ban of such AI systems seems like a premature decision based on fear, but it puts emphasis on what needs to be monitored.

4. SOCIAL SCORING

Article 5(1) (c) can reasonably be justified but it is yet to be seen in which direction. One of the first points we need to pay attention to is the possibility to use AI systems in creating and conducting social scoring systems. What are social scoring systems? Social scoring tends to collect data of every individual which doesn't include just regularly collected personal data such as name, surname, address, work position, etc., but also collects data on individuals' psychological and physical characteristics.[22] The aim of

[21] Ibid., p. 29225.

[22] Kapersky daily, Social scoring systems: current state and potential future implications. In: *Kasperksy daily* [online]. c 2021 [cit. 02. 12. 2021]. Available at: https://www.kaspersky.-com/blog/social-scoring-systems/

collecting such data is to make rankings among people. We can literally imagine people having a cloud above their heads that shows the number of credits they have, remembering that the number is not constant but variable depending on how that person behaves and what they do. The simplest example would be on with whom they are friends, how much are they engaged in studying or working, do they contribute to charity. It can also include their (non)healthy habits or even how emotionally satisfied they are regarding their work, surroundings, or which political ideology they gravitate to. Not to forget examples like paying bills on time or repaying loans. What actually is a problem in regards to social scoring is who uses it, how it's being used, and why. The first problem, to which Article 5(1) (c) refers to, is using AI in order to create a social scoring system by public authorities. China already started to use it years ago. As already mentioned a person gains or loses points based on what they do, as in China everyone started with basic 1000 points. In regards to the outcome of counting points, individuals whose behaviour leads to the constant loss of points in China are in a so-called position of being a blacklisted person.[23] In other words, people who lose points are deprived of some rights such as access to public authorities, a ban on travel, and many more. In China not only public authority uses it but also private companies. The most tremendous use of it is by public authorities due to the fact that their basic purpose is to resolve social problems to service society. This does not include the use of removing blacklisted persons from society.[24] Another country that introduced this system is the United Kingdom, and similarly to the Chinese implementation, they intended to introduce rewards and punishments depending on the score. Several studies conducted among UK people gained insight into what they were expecting from it in comparison to the Chinese system. When it comes to rewards the most appealing were

[23] NAST, Condé. The complicated truth about China's social credit system. *Wired UK* [online]. 2019. [cit. 02. 12. 2021]. ISSN 1357-0978. Available at: https://www.wired.co.uk/article/china-social-credit-system-explained

[24] CANALES, Katie. China's „social credit" system ranks citizens and punishes them with throttled internet speeds and flight bans if the Communist Party deems them untrustworthy. In: *Business Insider* [online]. 2021. [cit. 02. 12. 2021]. Available at: https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4

in the following priority order: healthcare, lower energy bills, favourable interest rates on loans, better schooling for children, and travel privileges. On the other side, some penalties were introduced- public naming and shaming, denied access to credit cards, and lack of possibility to apply for certain jobs.[25] In a democratic society use of this form of punishment and reward system cannot be reasonable and is threatening to democratic values and human rights. In this day and age when modern contemporary society developed certain values, which lacked in previous centuries, it cannot be allowed that basic democratic values such as equality (especially before the law), freedom of decision-making and speech, social justice, and others are taken away. Most rights and freedoms would be greatly endangered by the implementation of social scoring in the presented way by the side of public authorities.

Attention must be paid to whether there is a need to use this type of technology. Modern society can simplify and accelerate some of the decision-making processes with it. For example, it can help with the decision-making process for granting loans, so in the case of several loans, it can count points on the financial history of a person, or when applying for a job it can collect necessary data which can ease the process of selecting a proper candidate and eliminating those who don't meet requirements.

In the conclusion to point (c) of Article 5, it can be noticed that there is a need to regulate this form of using AI systems. As it states in the article, with direct interpretation, the use of these technologies with intention of unjustified social scoring in everyday use is only prohibited when it intends to create detrimental or unfavourable treatment of individuals or groups based on their social behaviour, unrelated to the context why was originally collected for. In other words, the intention of Article 5 (c) is not to completely ban the use of AI systems in creating social scoring but to prohibit certain use by public authorities which threaten modern society, rights, and freedoms for which society was fighting for a really long time. The only negative aspect found in point (c) would be that it is only

[25] ABC Finance. Surviving The Social Credit Score. In: *ABC Finance* [online]. c 2021 [cit. 02. 12. 2021]. Available at: https://abcfinance.co.uk/blog/surviving-the-social-credit-score/

orientated toward public authorities and does not take private companies into account.[26] Even though public authorities must pay more attention to respecting human rights and freedoms, it doesn't mean that private companies or similar subjects are excluded from it. They do have the freedom to conduct their business in the way they want to as long as they do it with respect and in conformity with international treaties, the constitution, and other legal acts. We can see that trends in the world do represent a breach of some basic human rights and it is necessary to control it with respect to its prohibition of certain unfair practices is the best solution as long as it concerns only the unfair practice. Point (c) openly limits the prohibition of the results that are not compatible with a democratic society and the general explanation of these results leaves enough room to determine in each specific case if there was that kind of intention. The best result this prohibition can have is the prevention of direct discrimination in exercising at least basic rights given by the state authorities.

5. REAL-TIME REMOTE BIOMETRIC ID

Firstly, detecting the problem of the scope and aim of Article 5 (1) (d) can start from the current world situation, and by that is specifically meant the COVID-19 pandemic. This situation can be seen as relevant for point (d) (III). Why so? Namely, as the provision states 'real-time' remote biometric identification systems in publicly accessible space can be used for detection, localisation, identification, or persecution of a perpetrator or suspect of a criminal offence but with setting out limitations. For possible use criminal offence has to be included in Article 2 (2) of Council Framework Decision 2002/584/JHA 62[27] and punishable in the Member State by a custodial sentence or detention for a maximum period of at least three years. So where is the problem with the COVID-19 pandemic? In the aim of pre-

[26] EBERS, Martin et al. The European Commission's Proposal for an Artificial Intelligence Act —A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). *J*. Multidisciplinary Digital Publishing Institute, [online]. 2021, vol. 4, issue 4, [cit. 02. 12. 2021], p. 592.

[27] Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) [online]. 2009. [cit. 02. 12. 2021]. Available at: http://data.europa.eu/eli/dec_framw/2002/584/2009-03-28/eng

vention of infectious diseases states include a measure of quarantine or self-isolation prescribed under the law. Another crucial thing is that national law also contains provisions on spreading infectious diseases in national criminal law acts. In regard to this problem, we can turn to Croatian national law. As mentioned, the measure of quarantine or self-isolation in Croatian law is prescribed in the Act on Protection of the Population from Infectious Diseases.[28] When it comes to criminal law Croatian Criminal Law Act[29] in Chapter XIX Article 180 contains a provision concerning the spread and transmission of infectious diseases. The problem here lies in the fact that neither Article 2 (2) of the Council Framework Decision contains this offence nor does the Croatian Criminal Law Act predict imprisonment for a maximum period of at least three years. Why is it at all that important? Because use of a "real-time" biometric identification system in publicly accessible spaces can be helpful in detecting suspects of criminal offences which in this case would be any person to whom a measure of quarantine or self-isolation was prescribed for a specific period of time. This is an example of the positive use of a biometric system, which under Article 5 would be declined due to the fact that none of the exemptions includes the protection of health as a reason. A similar practice has been seen in Slovakia with the eQuarantine app which is based on biometrics.[30] The app was made by a Slovak company Innovatrics and it is based in the EU. The potential problem which was detected was personal data collection due to the fact that it wasn't clear who will collect data, how will be stored, and for how long.[31] From the side of privacy and personal data this can be seen as a problem that initiated the creation of Article 5 however, it can have

---

[28] Act on Protection of the Population from Infectious Diseases, NN 79/07 , 113/08 , 43/09 , 130/17 , 114/18 , 47/20 , 134/20, [online]. [b.r.]. [cit. 02. 12. 2021]. Available at: https://www.zakon.hr/z/1067/Zakon-o-za%C5%A1titi-pu%C4%8Danstva-odzaraznih-bolesti

[29] Criminal Law Act, NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, [online]. [b.r.]. [cit. 02. 12. 2021]. Available at: https://www.zakon.hr/z/98/Kazneni-zakon

[30] Innovatrics. Self-Isolation Rather than Quarantine - Thanks to Face Recognition. In: *Innovatrics* [online]. 18. 6. 2020. [cit. 02. 12. 2021]. Available at: https://www.innovatrics.com/news/covid19-self-isolation-rather-than-quarantine-thanks-to-face-recognition/

positive use globally so it can help to stop the spread of disease. What can be done in order to have a useful tool but still protect data? More control over its use is needed, a detailed explanation of data that has to be used needs to be prepared and the question of data storage and collection needs to be transparent. This can all be resolved by following the rule prescribed in GDPR.[32] So what do we get with Article 5 prohibition? The prohibition actually doesn't serve its purpose. The prohibition in regard to what was said is too broad.[33] A better solution would be to exercise more control over the use and not prohibit it. Article 5 (d) exceptions are too narrow and in the future, with all the development there will surely be a need to broaden it. If a focus is put on a social purpose we can also refer to the limitation of rights. In the eyes of some, using biometric identification systems can be seen as a violation of the right to privacy. On the other hand, here we have a good example of where a test of proportionality can be used. If a state wants to improve public security, especially when it comes to infectious diseases or some other aspects of security, and in order to protect public health and wants to use this type of technology. Depending on the main aim we can see that in order to protect public health there is room for some limitations of the right to privacy. People cannot reasonably expect privacy and at the same time put in danger a larger number of people. Only the methods and procedure need to be transparent and control over it has to be exercised. Another key thing to point out is the fact that this wide prohibition has negative consequences for EU companies because it limits technology development. Also, a commercial component is in danger be-

[31] SIROTNIKOVA, Miroslava German. *Question Marks over Slovak Quarantine App Fuel Privacy Concerns* [online]. 2020. [cit. 02. 12. 2021]. Available at: https://balkaninsight.com/2020/05/20/question-marks-over-slovak-quarantine-app-fuel-privacy-concerns/

[32] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [online]. 2016. [cit. 02. 12. 2021]. Available at: http://data.europa.eu/eli/reg/2016/679/2016-05-04/eng

[33] EBERS, Martin et al. The European Commission's Proposal for an Artificial Intelligence Act —A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). *J*. Multidisciplinary Digital Publishing Institute, [online]. 2021, vol. 4, issue 4, [cit. 02. 12. 2021]. p. 592-593.

cause already existing technologies and also potential future products will not have their place in the area of EU.

6. CONCLUSION

While analysing bans the goal is clearly visible, though vague and superficial regarding content. EU used the easier way to approach risks by banning AI systems instead of regulating how to use them or better said, regulating the intention of a creator behind the system. The same AI systems could be used to do harm or to benefit its users. The creator is the one who sets the parameters of the system which directs further actions. EU is fiercely focused on protecting human rights but putting stress on the human rights when not reasonable in such quantity can directly affect the competitiveness of the EU. During the research, it was noticed that lack of knowledge, when it comes to technologies, spins the question of human rights violations in a circle due to the fear of the unknown which may lead to huge loss in the area of innovations. If the EU wants to be competitive in the area of AI, it needs to find a better solution than a ban, regardless of the potential risk. Innovations are based on risk and to gain the most out of them we have to accept it. We can only imagine what the future will bring. Bans in the Proposal are definitely not the only potential risk which means that future possibilities are endless but that same risk arises from the question of how we use the technology we have. There is always someone whose intentions are not good but we as a society are so focused on the bad impact that we forget to look on the bright side and the progress we have made. All in all, the EU has recognized the risk but failed to present to us what particular technology is the one that can bring the described harm. Technologies have been described but in general terms and too abstract. Basically, technology may be invented but if the EU detects the slightest potential of harm the technology is banned.

7. BIBLIOGRAPHY

[1] Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial intelligence act) and amending certain Union legislative acts [online]. 2021. [cit. 02. 12. 2021]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[2] MILIŠA, Zlatko and NIKOLIĆ, Gabrijela. Subliminalne poruke i tehnike u medijima. *Nova prisutnost: časopis za intelektualna i duhovna pitanja*. Kršćanski akademski krug (KRAK), [online]. 2013, vol. XI, issue 2, p. 293-312. [cit. 02. 12. 2021]. ISSN 1334-2312, 1848-8676. Available at: https://hrcak.srce.hr/106397

[3] Act on Electronic Media; NN 111/21; Art. 21 (3), [online]. [b.r.] [cit. 02. 12. 2021]. Available at: https://www.zakon.hr/z/196/Zakon-o-elektroni%C4%8Dkimmedijima

[4] VEALE, Michael and BORGESIUS, Frederik Zuiderveen. Demystifying the Draft EU Artificial Intelligence Act.[online]. c 2021, p. 97-112 [cit. 02. 12. 2021]. Available at: https://arxiv.org/ftp/arxiv/papers/2107/2107.03721.pdf?fbclid=IwAR3q2rvj8xAw-pvTqZ5KVL97CCFidpfZXAI0xImNMXbbLdRBbAdWKeDGl6U

[5] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), [online]. 2005 [cit. 02. 12. 2021]. Available at: http://data.europa.eu/eli/dir/2005/29/oj/eng

[6] PROPP, Kenneth and MACCARTHY, Mark. *Machines learn that Brussels writes the rules: The EU's new AI regulation* [online]. 2021. [cit. 02. 12. 2021]. Available at: https://www.brookings.edu/blog/techtank/2021/05/04/machines-learn-that-brussels-writes-the-rules-the-eus-new-ai-regulation/

[7] LUGURI, Jamie and STRAHILEVITZ, Lior. *Shining a Light on Dark Patterns*. Rochester, NY: Social Science Research Network, [online]. 2021. [cit. 02. 12. 2021]. DOI: 10.2139/ssrn.3431205

[8] Norwegian Consumer Council; *DECEIVED BY DESIGN- How tech companies use dark patterns to discourage us from exercising our rights to privacy*. [online]. 2018, p. 1-43 [cit. 02. 12. 2021]. Available at: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-0627-deceived-by-design-final.pdf

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [online]. 2016. [cit. 02. 12. 2021]. Available at: http://data.europa.eu/eli/reg/2016/679/2016-05-04/eng

[10] RUCH, Simon, ZÜST, Marc Alain and HENKE, Katharina. Subliminal messages exert long-term effects on decision-making. *Neuroscience of Consciousness* [online]. 2016, vol. 2016, issue 1, p. 1-9 [cit. 02. 12. 2021]. ISSN 2057-2107. DOI: 10.1093/nc/niw013

[11] DEZFOULI, Amir, NOCK, Richard and DAYAN, Peter. Adversarial vulnerabilities of human decision-making. *Proceedings of the National Academy of Sciences,* [online]. 2020, vol. 117, issue 46, p. 29221-29228 [cit. 02. 12. 2021]. ISSN 0027-8424, 1091-6490. DOI: 10.1073/pnas.2016921117

[12] Kapersky daily, Social scoring systems: current state and potential future implications. In: *Kasperksy daily* [online]. c 2021 [cit. 02. 12. 2021]. Available at: https://www.kaspersky.com/blog/social-scoring-systems/

[13] NAST, Condé. The complicated truth about China's social credit system. *Wired UK* [online]. 2019. [cit. 02. 12. 2021]. ISSN 1357-0978. Available at: https://www.wired.co.uk/article/china-social-credit-system-explained

[14] CANALES, Katie. China's „social credit" system ranks citizens and punishes them with throttled internet speeds and flight bans if the Communist Party deems them untrustworthy. In: *Business Insider* [online]. 2021. [cit. 02. 12. 2021]. Available at: https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4

[15] ABC Finance. Surviving The Social Credit Score. In: *ABC Finance* [online]. 3. 12. 2021. [cit. 02. 12. 2021]. Available at: https://abcfinance.co.uk/blog/surviving-the-social-credit-score/

[16] EBERS, Martin et al. The European Commission's Proposal for an Artificial Intelligence Act—A Critical Assessment by Members of the Robotics and AI Law Society (RAILS). *J*. Multidisciplinary Digital Publishing Institute, [online]. 2021, vol. 4, issue 4, p. 589-603 [cit. 02. 12. 2021]. ISSN 2571-8800. DOI: 10.3390/j4040043

[17] Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) [online]. 2009. [cit. 02. 12. 2021]. Available at: http://data.europa.eu/eli/dec_framw/2002/584/2009-03-28/eng

[18] Act on Protection of the Population from Infectious Diseases, NN 79/07 , 113/08, 43/09, 130/17 , 114/18 , 47/20 , 134/20, [online]. [b.r.]. [cit. 02. 12. 2021]. Available at: https://www.zakon.hr/z/1067/Zakon-o-za%C5%A1titi-pu%C4%8Danstva-odzaraznih-bolesti

[19] Criminal Law Act, NN 125/11, 144/12, 56/15, 61/15, 101/17, 118/18, 126/19, 84/21, [online]. [b.r.] [cit. 02. 12. 2021]. Available at: https://www.zakon.hr/z/98/Kazneni-zakon

[20] Innovatrics. Self-Isolation Rather than Quarantine - Thanks to Face Recognition. In: *Innovatrics* [online]. 18. 6. 2020. [cit. 02. 12. 2021]. Available at: https://www.innovatrics.com/news/covid19-self-isolation-rather-than-quarantine-thanks-to-face-recognition/

[21] SIROTNIKOVA, Miroslava German. *Question Marks over Slovak Quarantine App Fuel Privacy Concerns* [online]. 2020. [cit. 02. 12. 2021]. Available at: https://balkaninsight.com/2020/05/20/question-marks-over-slovak-quarantine-app-fuel-privacy-concerns/

CHANGES IN UK-EU PERSONAL DATA TRANSFERS AFTER BREXIT[1]

ANNA TSUVINA[2]

The UK was a longstanding proponent of high data protection standards while part of the EU, and it will remain so as an independent nation, leading the way in creating the best possible data protection regime that exists globally.

DCMS, "*Data: A new direction*"[3]

1. INTRODUCTION

Since the United Kingdom (UK) left the European Union (EU) in 2020, the process of conducting personal data transfers has changed significantly. In particular, the UK is regarded as a third country in the context of Article 25 (1) of the General Data Protection Regulation (EU GDPR). UK-EU transfers, which are now regarded as cross-border personal data transfers, may be conducted only if the UK ensures an adequate level of data protection, namely, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the EU.[4] The adequacy decisions were adopted by the EU Commission to settle the matter and make

[1] Esej byla zpracována v semestru podzim 2021 v rámci předmětu MVV1368K Privacy and Personal Data na téma UK-EU Personal Data Transfers: Past, Present and the Future/ The essay was written in the autumn 2021 semester for the course MVV1368K Privacy and Personal Data on the topic of UK-EU Personal Data Transfers: Past, Present and the Future.

[2] Anna Tsuvina je studentkou na Yaroslav Mudryi National Law University, Faculty of Justice, kontakt: tsuvinaanna22@gmail.com

[3] The Government of the United Kingdom. Department for Digital, Culture, Media and Sport (DCMS). Public consultation on reforms to the UK's data protection regime. *Data: a new direction*, [online]. 10. 09. 2021, [cit. 05. 12. 2021]. p. 8, 123-124.

[4] *Art. 6 GDPR – Lawfulness of processing* [online] 2016. [cit. 05.12.2021]. Available at: https://gdpr-info.eu/art-6-gdpr/

the transfers possible and simplified after Brexit. At the same time, two important questions may arise. What is the role of these adequacy decisions? What are the future predictions for personal data transfers between the UK and the EU? This essay is devoted to identifying the past, present and future state of UK-EU personal data transfers. The attention is mainly focused on the UK adequacy decisions and their effect on the future of data transfers.

2. PAST

The history of UK-EU personal data transfers should be analyzed in the first place to demonstrate the change in the regulatory regime. To begin with, the UK was a part of the EU for almost fifty years, from 1973 to 2020. In this timeline, the problem of trans-border personal data transfers did not arise for the state as it was one of the Member States of the EU and all the transfers fell under the requirements of regulations that were in force for all the Member States. Specifically, the free flow of data was possible under Article 1 (2) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[35] In addition, the EU GDPR, which also includes the provisions on the free flow of data within the EU, applied in the UK for almost two years, from 25 May 2018 to 31 January 2020. With the goal of implementing the EU GDPR, the UK adopted the Data Protection Act (DPA 2018), which is still one of the main regulations governing the usage of personal data and the flow of information in the state.[6]The DPA 2018 originally referred to the EU GDPR's most important provisions for the protection of personal data and adopted such main definitions used in the EU GDPR as "personal data", "processing", "data subject", "controller", "processor" etc. Therefore, the

[5] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [online] 24.10.1995 [cit. 05.12.2021]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046.

[6] Data Protection Act. [online] 2018 [cit. 05.12.2021]. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

original provisions of the DPA 2018 demonstrated the clear intention of the national legislator to implement the EU GDPR into the domestic law of the UK.

The next period in the history of UK-EU personal data transfers was connected with the process of separation of the UK from the EU. On 23 June 2016, the UK held a referendum on its membership in the EU. The historic decision to leave the EU was reached in that referendum. On 31 January 2020 at midnight, when the Withdrawal Agreement entered into force, the UK left the EU.[7] In the context of data protection, the separation led to the situation where the EU GDPR, the main data privacy regulation throughout the EU, could no longer be applied in the UK. Instead, the UK GDPR was adopted to regulate the questions of personal data protection in the UK.[8] The DPA 2018 was amended to be read in conjunction with the new UK GDPR instead of the EU GDPR. Although mentioned regulations have much in common, there is one important distinguishing feature of the UK data protection framework. In particular, according to the UK GDPR and the DPA 2018, the Information Commissioner is the leading supervisor, regulator and enforcer of the UK GDPR.[9] The latest suggestions of the UK Government, which concern the Information Commissioner Office's (ICO) restructuring, deserve special attention in that regard. The government proposed to establish an independent board and a chief executive officer at the ICO. The board would be led by a chair with non-executive directors, while the chief executive officer would have responsibility for the running of the organization. Structural improvements were introduced to make the work of the supervisory authority more effective in the long term.

---

7 Brexit: EU-UK relationship. In: EUR-Lex [cit. 05. 12. 2021]. Available at: https://eur-lex.europa.eu/content/news/Brexit-UK-withdrawal-from-the-eu.html

8 Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018. [online]. 27. 4. 2016 [cit. 05. 12. 2021]. Available at: https://www.legislation.gov.uk/eur/2016/679/contents.

9 The Government of the United Kingdom. Department for Digital, Culture, Media and Sport. Data Protection Act 2018 Factsheet – The Information Commissioner and Enforcement, [online]. 2018, [cit. 05. 12. 2021], p. 1.

On 1 January 2021, the EU-UK Trade and Cooperation Agreement (TCA) came into force, according to Article 201 (1) of which the EU and the UK were committed to ensuring cross-border data flows to facilitate trade in the digital economy.[10] In addition, in Article 525 (1) of the TCA was once again mentioned that onward transfers to a third country are allowed only subject to conditions and safeguards appropriate to the transfer ensuring that the level of protection is not undermined. Under the TCA, the EU and the UK also agreed on the interim solution (a bridging mechanism) to ensure the provisional continuation of personal data flow from the EU to the UK. In general, The TCA may be seen as the first step in the regulation of cross-border personal data transfers which was taken before the UK adequacy decisions were adopted in June 2021. The inclusion of the provisions on cross-border data flows helped to cut the loss of profits in the business sector and postpone the question for several months.

3. PRESENT

The current state of UK-EU personal data transfers is connected with the decisions of the EU Commission on the UK's adequacy under the EU GDPR and Law Enforcement Directive (LED).[11] In both decisions, the EU Commission stated that the UK ensures an adequate level of protection in the context of Article 25 (1) of the EU GDPR. This means that most data can continue to flow from the EU without the need for additional safeguards. At the same time, the so-called "sunset clause", which means that the UK adequacy decisions are limited to four years and will not be automatically renewed, was developed by the EU Commission. The new adequacy process will be required to determine whether the UK still ensures the essentially

[10] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part [online]. 2020 [cit. 05. 12. 2021]. Available at: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj/eng

[11] Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. [online] 28.06.2021 [cit. 05. 12. 2021]. Available at: https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-united-kingdom-general-data-protection-regulation_en.

equivalent level of data protection in June 2025. In addition, during the four-year period, the EU Commission can amend, suspend, or repeal the adopted decisions if issues related to data protection that call into question the level of protection arise. There is also a possibility for the Court of Justice of the European Union to decide on the data protection level in the case an EU data subject or an EU data protection authority challenges these decisions.

In fact, although the value of positive adequacy decisions in allowing personal data to be transferred without any additional safeguards between the UK and the EU cannot be denied, they are just one of the mechanisms to enable such cross-border data transfers. To support trusted data flows across the world such alternative mechanisms as Standard Contractual Clauses (SCCs) are readily available, flexible and straightforward to implement.[12] However, a recent study estimated the costs of the absence of the UK adequacy decisions at around GB £1-1.6 billion (€1.116-1.7856 billion) for UK firms, stemming largely from companies reverting to alternative transfer mechanisms under the EU GDPR.[13] Therefore, the adequacy decisions may be considered in practice as one of the most effective tools to regulate cross-border data transfers compared to other alternatives. This explains the desire of the UK national authorities to get a positive adequacy decision despite all the doubts concerning the UK's relevant legislation, including those concerning public security, defence, national security, criminal law and the access of public authorities to personal data.

Specifically, according to some studies, UK surveillance activities do not fully comply with EU data protection and privacy standards. For instance, the UK Government Communications Headquarters (GCHQ) intercepts, retains and analyses masses of personal data by collaborating with or compelling private actors to provide access points. As Hendrik Mildebrath mentioned in the recent in-depth analysis for the European Parliamentary

[12] UK Business Data Survey 2021. In: *GOV.UK* [online] [cit. 05. 12. 2021]. Available at: https://www.gov.uk/government/statistics/uk-business-data-survey-2021

[13] European Parliament. Directorate General for parliamentary research services. *EU-UK private-sector data flows after Brexit: settling on adequacy : in depth analysis.* [online]. LU: Publications Office, 2020. [cit. 05. 12.2 021] p. 1, 15,17.

Research Service, the algorithmic detection used in the UK causes three main problems, namely the mathematically unavoidable fact of a large number of false positives or false negatives when searching for rare instances in large data sets ("base-rate fallacy"), built-in biases and opaque processing ("black box phenomenon"). In addition, the Investigatory Powers Act does not require the Investigatory Powers Commissioner to disclose intrusive data processing to the data subject, even where it would not jeopardize intelligence activities. So, these examples demonstrate the drawbacks in the regulation which confirm that the level of data protection in the UK may be seen as not essentially equivalent to that within the EU. Nevertheless, these particularities did not preclude the adoption of the adequacy decisions for the UK which include, inter alia, some rules on the usage of personal data by public authorities, notably for national security reasons. Furthermore, the adequacy decisions seem to be adopted on the basis of trustworthy relationships between the UK and the EU, taking into account their common historical background. As it was said in one of the recent official documents of the UK government, new arrangements to govern the continued free flow of personal data between the EU and the UK were needed as "part of the new, deep and special partnership".[14]

4. FUTURE

In the context of the future of UK-EU data flows several ideas should be highlighted. Firstly, the adequacy decisions seem to be an interim arrangement designed to make cross-border data transfers possible in the short term. As was already mentioned, they may be amended, suspended, and repealed. Secondly, the new adequacy decisions are highly questionable. It is still possible that the EU Commission will not adopt a new adequacy decision unless already mentioned issues of national security and surveillance regime will not be addressed by the government. Another challenge in this context is the intention of the UK government to allow free cross-border

[14] The Government of the United Kingdom. The exchange and protection of personal data: a future partnership paper. [online] [b.r.] [cit. 05. 12. 2021] p. 2.

data transfers with other states all over the world. Such a decision of the UK government may cause harm to the EU data protection system as the majority of mentioned states do not have the adequacy decisions. This may be seen as a gap in the closed system which is constructed within the countries that have the adequacy decisions and aims at the highest possible level of data protection among these third countries.

5. CONCLUSION

So, the history of UK-EU data transfers demonstrates that for a long time the regulatory regime stayed unchanged. As a Member State of the EU, the UK could count on the provisions for the free flow of data within the EU. After the separation from the EU, the TCA was adopted to make the transfers possible before the adoption of the adequacy decisions. Although the adequacy decisions were finally adopted by the EU Commission, the fact that some issues in the UK data protection framework are still visible today may not be neglected. This leads to uncertainty with regard to both already adopted and future adequacy decisions. However, the government still has four years to find the solution to the problem and improve the national strategy on how to keep the level of data protection in the state at the necessary level, namely, at the level that is essentially equivalent to that guaranteed within the EU.

6. BIBLIOGRAPHY

[1] The Government of the United Kingdom. Department for Digital, Culture, Media and Sport (DCMS). Public consultation on reforms to the UK's data protection regime. *Data: a new direction*, [online]. 10. 09. 2021, p. 1-146. [cit. 05. 12. 2021]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Refor m_Consultation_Document Accessible_.pdf.

[2] *Art. 6 GDPR – Lawfulness of processing* [online] 2016. [cit. 05. 12. 2021]. Available at: https://gdpr-info.eu/art-6-gdpr/

[3] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. [online] 24. 10. 1995 [cit. 05. 12. 2021]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046.

[4] Data Protection Act. [online] 2018 [cit. 05. 12. 2021]. Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

[5] Brexit: EU-UK relationship. In: EUR-Lex [cit. 05.12.2021]. Available at: https://eur-lex.europa.eu/content/news/Brexit-UK-withdrawal-from-the-eu.html

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018. [online]. 27.4.2016 [cit. 05. 12. 2021]. Available at: https://www.legislation.gov.uk/eur/2016/679/contents.

[7] The Government of the United Kingdom. Department for Digital, Culture, Media and Sport. Data Protection Act 2018 Factsheet – The Information Commissioner and Enforcement, [online]. 2018, p. 1-4. [cit. 05. 12. 2021]. Available at: https://assets.publishing.service.gov-.uk/government/uploads/system/uploads/attachment_data/file/711238/2018-05-23_Factsheet_5_-_Information_Commissioner.pdf.

[8] Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part [online]. 2020 [cit. 05. 12. 2021]. Available at: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj/eng

[9] Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom. [online] 28.06.2021 [cit. 05. 12. 2021]. Available at: https://ec.europa.eu/info/files/decision-adequate-protection-personal-data-united-kingdom-general- data-protection-regulation_en.

[10] UK Business Data Survey 2021. In: *GOV.UK* [online] [cit. 05. 12. 2021]. Available at: https://www.gov.uk/government/statistics/uk-business-data-survey-2021

[11] European Parliament. Directorate General for parliamentary research services. *EU-UK private-sector data flows after Brexit: settling on adequacy : in depth analysis.* [online]. LU: Publications Office, 2021. p. 1-39 [cit. 05. 12. 2021]. Available at: https://data.europa.eu/doi/10.2861/595569

[12] The Government of the United Kingdom. The exchange and protection of personal data: a future partnership paper. [online] [b.r.] p. 1-15. [cit. 05. 12. 2021]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchang e_and_protection_of_personal_data.pdf.

GELLERT, R.: *THE RISK-BASED APPROACH TO DATA PROTECTION*

JAN TOMÍŠEK[1]

GELLERT, R.: The Risk-based Approach to Data Protection. Oxford University Press, 2020, 304 s. **ISBN: 9780198837718**

Kniha Raphaëla Gellerta The Risk-Based Approach to Data Protection, publikovaná v roce 2020 v nakladatelství Oxford University Press, se věnuje problematice regulatorních metod v právu ochrany osobních údajů a představuje rozšířenou a aktualizovanou podobu disertační práce autora. Hlavním tématem publikace je zkoumání vztahu regulace založené na právech (*right-based approach) a* regulace založené na riziku (*risk-based approach)*. Toto téma je čtyři roky po účinnosti nařízení Evropského parlamentu a Rady (EU) 2016/679 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“) vysoce aktuální, což potvrzuje i prostor, který mu věnuje domácí doktrína.[2]

Kniha je přehledně rozčleněna do sedmi kapitol doplněných úvodem a závěrem. V úvodu práce autor především vymezuje vztah mezi rizikem a regulací. V první kapitole pak podrobně rozebírá základní koncepty rizika

[1] Mgr. et Mgr. Ing Jan Tomíšek je externím doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy Univerzity. Působí jako advokát v ROWAN LEGAL, advokátní kancelář s.r.o. Kontakt: jantomisek@gmail.com

[2] Obecně srov. MÍŠEK, Jakub. Moderní regulatorní metody ochrany osobních údajů. Brno: Masarykova univerzita, 2020. s. 169 a násl. Aktuálně srov. NONNEMANN, František. Je načase začít diskutovat o GDPR 2.0? *Právní rozhledy.* 2022, roč. 30, č. 1, s. 23.

a regulace. Druhá kapitola popisuje ochranu osobních údajů jako formu regulace založenou na příkazech a kontrole jejich plnění. Třetí kapitola rozebírá problémy tohoto modelu regulace ochrany osobních údajů. Čtvrtá kapitola se věnuje změně regulatorního modelu z příkazů a kontroly na metaregulaci stanovící pouze regulatorní cíle a ponechávající na regulovaných subjektech nastavení konkrétních standardů a způsobů jejich implementace. V páté kapitole autor rozebírá projevy metaregulace, resp. přístupu založeného na riziku v ochraně osobních údajů. Šestá kapitola rozebírá konkrétní postupy řízení rizik v oblasti ochrany osobních údajů a jejich odraz v GDPR. Sedmá kapitola diskutuje úskalí přístupu založeného na riziku. V závěru knihy se autor vrací ke vztahu přístupu k regulaci založenému na právech a přístupu založenému na riziku.

Hlavní přínosy knihy shledávám v důkladném rozboru samotného přístupu založeného na riziku, jeho zasazení do širšího kontextu moderních postupů řízení korporací, resp. organizací obecně, analýzu jeho projevů v GDPR a také kritické zhodnocení tohoto přístupu vč. poukazů na jeho limity.

Autor knihy v prvé řadě blíže rozebírá samotný koncept řízení rizik, jak jej popisuje věda managementu. Poukazuje na známé problémy současných přístupů k řízení rizik. V rámci procesu hodnocení rizik je to hodnotitel, který rozhoduje, jaká rizika pro účely hodnocení vůbec vezme v úvahu. Dále pak hodnotitel těmto rizikům přisuzuje určité váhy zpravidla na základě pravděpodobnosti realizace rizika a závažnosti jeho dopadů, toto přiřazení však opět často není možné provést na základě objektivních rizik. Gellert tak správně poukazuje na nevyhnutelné subjektivní prvky v procesu řízení rizik, které se promítají i do oblasti ochrany osobních údajů.[3]

Stejně tak kniha příhodně zasazuje koncept řízení rizik do kontextu řízení korporací a disciplíny *corporate governance*.[4] Vnímání řízení v oblasti ochrany osobních údajů jako součásti běžných korporátních procesů je přitom podle mého názoru prvkem, který v aktuální praxi ochrany osobních

[3] Srov. GELLERT, Raphaël. The Risk-based Approach to Data Protection. Oxford University Press, 2020. s. 37.

[4] Srov. tamtéž, s. 110 a násl.

údajů v řadě případů chybí (tento typ rizik je řízen samostatně od rizik obecných), a jeho doktrinální uchopení je tak velmi žádoucí.

Vedle těchto obecných úvah se však kniha nevyhýbá ani analýze platné právní úpravy v podobě GDPR. Projevy přístupu založeného na riziku autor spatřuje zejména v principu odpovědnosti dle jeho čl. 5 odst. 2 a čl. 24, povinnosti standardní ochrany osobních údajů (*data protection by design*) dle čl. 25 a konkrétních institutech v kapitole IV GDPR.[5] Poukazuje však na dvě zásadní skutečnosti. V prvé řadě přístup založený na riziku není v GDPR doveden zcela do důsledku v tom smyslu, že by povinné subjekty v oblasti ochrany osobních údajů podle rizik konkrétního případu zpracování zcela volně volily příhodná opatření. Tato opatření jsou naopak do značené míry předem stanovena na úrovni základních zásad GDPR v čl. 5 GDPR (např. nezbytnost právního titulu, minimalizace rozsahu údajů či minimalizace doby uložení) a jeho konkrétních institutů (např. informační povinnost podle čl. 13 a 14 či bezpečnostní opatření podle čl. 32). Podle rizik konkrétního případu nemůže povinný subjekt volit, zda bude tato opatření provádět, ale pouze způsob jejich provádění.[6]

Tento přístup není třeba dle Gellerta hodnotit a *priori* negativně, naopak má své opodstatnění s ohledem na nutnost zajištění ochrany osobních údajů jako základního práva, kde může mít určení jistého minimálního obecného standardu své odůvodnění. Správně však upozorňuje, že je vhodné se v tomto kontextu kriticky zamýšlet nad jednotlivými základními zásadami, jejichž platnost nemusí být natolik univerzální, jak se na první pohled zdá. Současně je třeba tento přístup zákonodárce vést v patrnosti při výkladu jednotlivých institutů GDPR opírajících se o přístup založený na riziku.[7]

V kontextu tohoto přístupu se totiž mění samotný charakter posuzování rizik podle jednotlivých institutů. Gellert tak přesvědčivě argumentuje, že jelikož instituty jako posouzení vlivu na ochranu osobních údajů podle čl. 35 GDPR mají vést k identifikaci vhodných opatření pro implementaci

[5] Srov. tamtéž, s. 160 a 165.

[6] Srov. tamtéž, s. 155.

[7] Srov. tamtéž.

základních zásad a jednotlivých institutů ochrany osobních údajů,[8] je třeba v odpovídajícím procesu hodnocení rizik zkoumat rizika, že tyto zásady, resp. instituty budou porušeny, resp. nebudou řádně provedeny. Dle Gellerta tedy nejde v procesu hodnocení rizik dle GDPR o hodnocení bezprostředních rizik pro základní práva a svobody subjektu údajů, ale o hodnocení *compliance* rizik nesouladu s právní úpravou. Rizika pro základní práva subjektu údajů se do tohoto procesu promítají až sekundárně jako dopad jednotlivých uvažovaných porušení právní úpravy ochrany osobních údajů.[9]

Za velmi přínosné považuji také kritické zhodnocení přístupu založeného na riziku v ochraně osobních údajů. Vedle poukázání na vždy přítomný subjektivní prvek Gellert také poukazuje na problematičnost některých jeho východisek, zejména předpokladu, že povinné subjekty jsou vždy nejlépe vybaveny k tomu, aby v oblasti ochrany osobních údajů posoudily rizika plynoucí z jejich činnosti (zpracování osobních údajů) a zvolily vhodná opatření.[10] Praktická zkušenost ukazuje, že s ohledem na široký záběr právní úpravy naopak řada povinných subjektů nedisponuje odbornými znalostmi ani finančními zdroji, aby příslušná rizika posoudila a řídila. Dále poukazuje na negativní zkušenosti s příliš liberální aplikací a vymáháním tohoto přístupu ve finančním sektoru.[11]

Nosná je i závěrečná myšlenka autora, že v rovině konkrétních praktických postupů se mohou rozdíly mezi přístupem založeným na právech a přístupem založeným na riziku stírat a skutečný rozdíl mezi nimi může spočívat především v podkladových idejích určujících celkový způsob uskutečňování ochrany osobních údajů.[12]

Celkově knihu hodnotím jako velmi aktuální a přínosnou. Lze ji doporučit jak akademikům, kteří se věnují zkoumání v oblasti ochrany osobních údajů, tak čtenářům z praxe, kteří aplikují konkrétní postupy v této oblasti.

---

[8] Obdobně srov. Míšek, 2020, op. cit., s. 176.

[9] Srov. Gellert, 2020, op. cit., s. 198.

[10] Srov. tamtéž, s. 233.

[11] Srov. tamtéž, s. 236.

[12] Srov. tamtéž, s. 250.

Akademicky zaměřený čtenář nalezne v knize přehledné shrnutí základních premis ochrany osobních údajů a rozbor dominantních přístupů k její regulaci, vč. relevantních zdrojů pro další studium. Praktik pak může z knihy čerpat lepší pochopení jednotlivých institutů GDPR odrážejících přístup založený na riziku (zejména zásady odpovědnosti a institutu posouzení vlivu na ochranu osobních údajů) a jejich zasazení do kontextu korporátních procesů řízení rizik.

---

https://doi.org/10.5817/RPT2022-1-4

OCHRANA SOUKROMÍ VE VEŘEJNÉM PROSTORU[1]

KRISTÝNA BÓNOVÁ[2]

ABSTRAKT

Předkládaný text má za cíl analyzovat, jak právo rozlišuje veřejný a soukromý prostor, přičemž bude brán v úvahu prostor fyzický. Zaměří se na místa, která se nachází na hranici mezi soukromým a veřejným prostorem. Následně bude zhodnoceno, zda je takové rozlišení účelné v době, v níž jsou lidé takřka neustále pod drobnohledem moderních sledovacích technologií. S jejich využitím totiž nezbytně vyvstává otázka střetu s právem na ochranu soukromí a s ochranou osobních údajů.

KLÍČOVÁ SLOVA

Právo na soukromí, ochrana soukromí, veřejný prostor, kamerové sledování, sledovací technologie

ABSTRACT

The aim of this text is to analyse how the law distinguishes between public and private space, considering the physical space. The paper will focus on places that are located on the border between private and public space. Subsequently, it will be evaluated whether such a distinction is useful at a time when people are almost constantly under the scrutiny of modern surveillance technologies. With their use, the question of conflict with the right to privacy and the protection of personal data inevitably arises.

---

[1] Tento článek vychází z autorčiny diplomové práce Ochrana soukromí ve veřejném prostoru (dostupná z https://is.muni.cz/auth/th/t2km4/).

[2] Mgr. Kristýna Bónová je absolventkou Právnické fakulty Masarykovy univerzity v Brně. e-mail: kristyna.bon@gmail.com.

KEY WORDS

Right to Privacy, Privacy Protection, Public Space, Public Places, Camera Surveillance, Surveillance Technology

SEZNAM POJMŮ A ZKRATEK

ESLP	Evropský soud pro lidská práva
GDPR	nařízení Evropského parlamentu a Rady (EU) č. 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)
LZPS, Listina	Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky
OZ	zákon č. 89/2012 Sb., občanský zákoník
Pokyny 3/2019	Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky
SDEU	Soudní dvůr Evropské unie
TZ, trestní zákoník	zákon č. 40/2009 Sb., trestní zákoník
Úmluva	Úmluva o ochraně lidských práv a svobod
ÚOOÚ, Úřad	Úřad pro ochranu osobních údajů
ÚS	Ústavní soud

1. ÚVOD

Právo na ochranu soukromí představuje jedno ze základních lidských práv, jež nám ústavní pořádek zaručuje. Odlišení veřejného prostoru od soukromého je tématem, kterým se zabývají filozofové, sociologové, urbanisté

a právníci nejen v dnešní době, ale už od minulých století.[3] Přesto však neexistuje jednoznačná, všeobecně platná definice veřejného a soukromého prostoru, jež by mohla právnímu odvětví sloužit. S ohledem na okrajové zpracování této problematiky v právním rámci pak vyvstává otázka, jak (a zdali) pro účely práva – zvláště práva na ochranu soukromí – rozlišovat veřejný a soukromý prostor. Tento článek poskytne analýzu povahy a významu ochrany soukromí v závislosti na kvalifikování prostoru jako soukromý nebo veřejný.

Již na tomto místě lze konstatovat, že v soukromém prostoru má jedinec právo na soukromí a může zde vést soukromý život, jenž mu nesmí nikdo bez jeho svolení narušit,[4] nicméně soukromým prostorem není toto právo omezeno. Otázkou však je, jakou míru ochrany požívá soukromí ve zbývajícím prostoru, tedy v tom veřejném. O něco zajímavější se potom odlišení soukromého a veřejného prostoru stává v dnešní době, která výrazně usnadňuje možnost sledovat náš soukromý život kdekoli, což pro naše soukromí představuje větší hrozbu i na místech, kde již určitou sníženou míru soukromí očekáváme,[5] a pomyslné oddělení prostoru v mnohém splývá.[6] Je přirozené (a zcela nevyhnutelné, ba žádoucí), že se právní úprava přizpůsobuje novým jevům ve společnosti. Neustálý rozmach technologií má nezanedbatelný vliv na vývoj jak společnosti, tak právní úpravy v jejích

[3] Rozlišení je předmětem úvah v různých právních tématech. Cf. Cass, B. The Limits of the Public/Private Dichotomy: A Comment on Coady & Coady. *International Journal of Law and the Family*. 1992, vol. 6, n. 1, pp. 140-147; Thornton, M. Weintraub, J. Kumar, K. (Eds.). Public and Private in Thought and Practice: Perspectives on a Grand Dichotomy. *Social & Legal Studies*. 1998, vol. 7, n. 4, pp. 582-584; Barnett, L. D. The Public-Private Dichotomy in Morality and Law. *Journal of Law and Policy*. 2010, vol. 18, n. 2, pp. 541-606; Szczepaniak, R. The Dichotomy of Public and Private Law. A Review of the Monograph by Igor Zachariasz. *Forum Prawnicze*. 2016, n. 6, pp. 82-97 a další.

[4] Cf. § 86 OZ.

[5] To ostatně neplatí pouze pro fyzický prostor, ale i pro ten v síti Internet. Např. sociální sítě ovlivňují naše vnímání soukromí nejen proto, že mohou sledovat naše data, ale protože sami vymezujeme hranice našeho soukromí, a mnohdy je tímto způsobem dobrovolně „rozpínáme". Své nejužší soukromí lidé sdílí sami s mnohem větší skupinou lidí než dříve, dobrovolně. Tato oblast však není předmětem tohoto článku.

[6] Nejen internetové prostředí není ani veřejným, ani soukromým prostorem (cf. nález Ústavního soudu ze dne 30. října 2014, sp. zn. III. ÚS 3844/13); rovněž neustálá dostupnost na telefonu jak doma, tak mimo domov, jak pro soukromé, tak pro pracovní účely výrazně stírá tuto pomyslnou hranici.

různých odvětvích. Technologie se vyvíjí natolik rychle, že na ně právo nestíhá reagovat dostatečně, a k úpravě důležitých otázek tak dochází zpravidla *ex post*. Ostatně Nejvyššímu soudu Spojených států amerických trvalo kolem 90 let, než uzpůsobil interpretaci práva na ochranu soukromí příchodu telefonu.[7] Mimo to také technologie do jisté míry mění chápání soukromí a jeho vnímání z pohledu jednotlivce,[8] čímž činí toto téma stále relevantním. Právě všudypřítomnost sledovacích technologií způsobuje intenzivnější zásah do soukromí jedince,[9] pročež se pro něj tyto zásahy stávají citelnějšími a aktuálními.[10] Moderní sledovací prostředky představují významný zásah do soukromí sledovaných osob a jejich využití nelze srovnávat se sledováním jinou osobou, neboť jsou schopny zpracovávat nepřeberné množství dat o každém jednotlivci, případně je následně ještě konfrontovat s daty získanými dříve v jiných databázích, čehož běžně člověk schopen není (nebo jen s mnohem většími obtížemi), čímž se potenciální zásah do soukromí násobí.[11] Ze zvýšené míry nebezpečí zneužití osobních údajů tedy plyne zvýšená míra potřeby chránit osoby, respektive chránit jejich soukromí[12] a osobní údaje, k jejichž masovému zpracování dochází. Významnou roli přitom hraje také skutečnost, že je dnes sledování

---

[7] Milligan, Ch. S. Facial Recognition Technology, Video Surveillance, and Privacy. *Southern California Interdisciplinary Law Journal*. 1999, vol. 9, no. 1, p. 299. Jednalo se o případ *Katz v. United States*, o kterém bude v této práci dále pojednáno.

[8] Meeks, B. N. Privacy Lost, Anytime, Anywhere. *Communications of the ACM.* 1997, vol. 40, n. 8, p. 12.

[9] K tomu Walz a Brookins uvádí: *„… such innovations change what is realistically possible. In the past, the high cost of, say, loitering in front of someone's door for weeks at a time and filming video the whole time would have made it effectively impossible for journalists and law enforcement to do what a drone will be able to do very cheaply in the near future.“* Walz, Ch. N. Brookins, D. S. Privacy in Public: A Look at Recent Efforts to Recognize Privacy Protections in Public Spaces. *Communications Lawyer*. 2016, vol. 32, no. 2, p. 25. Blíže cf. *United States v. Maynard,* rozsudek Nejvyššího soudu Spojených států amerických, 6. 8. 2010 č. 615 F.3d 544; rovněž v kapitole *Kamerový dohled.*

[10] Že toto téma stále rezonuje společností a idea soukromí ještě nebyla zcela hozena přes palubu, dokazuje nejen nedávné rozhodnutí ESLP ve věci *Big Brother Watch and Others v. the United Kingdom* z internetového prostředí, ale v souvislostech tohoto příspěvku také například rezoluce Evropského parlamentu z října 2021 na téma rozpoznávaní obličejů.

[11] Cf. *Rotaru v. Rumunsko,* rozsudek Evropského soudu pro lidská práva, 4. 5. 2000 č. stížnosti 28341/95.

[12] Ke vztahu ochrany soukromí a ochrany osobních údajů blíže v první kapitole.

snadnější a méně nákladné než dříve.[13] Proto je možné, aby se odehrávalo v takovém objemu, v jakém se odehrává.

Míra soukromí se liší v závislosti na tom, kde se nacházíme. I neprávník si povšimne, že doma má více soukromí než na přeplněném náměstí. Jaká pravidla ochrany soukromí platí pro různé prostory, však nemusí být vždy zřejmé. Mezi zdmi našeho domu a náměstím se totiž objevují také prostory, jež jsou sice ohraničeny zdmi, které by nám mohly navozovat iluzi soukromí, avšak zdaleka se mezi těmito zdmi nenacházíme sami. Naopak jsou to často místa, kam má přístup široká veřejnost – obchodní centra, kanceláře, společné chodby bytových domů a další. Ve všech uvedených prostorách jsme ve 21. století zpravidla vystaveni drobnohledu monitorovacích prostředků. Tyto technologie tak snižují míru našeho soukromí na místech, která přitom nezbytně nejsou ve všech aspektech zcela veřejná (mohou mít soukromého vlastníka nebo je okruh osob, které se zde mohou pohybovat, omezený).[14] Cílem příspěvku je analyzovat, jak se ochrana soukromí v daných prostorách aplikuje a mění.

Příspěvek nastíní základní relevantní koncepce ochrany soukromí na teoretické i pozitivněprávní úrovni. Hodnocení platné právní úpravy se zaměří na roli fyzického prostoru v ochraně soukromí, nebudou tedy zmíněny veškeré aspekty ochrany soukromí nebo zpracování dat. Účelem článku není popsat všechny myslitelné zásahy do každého dílčího práva, jež je součástí práva na soukromí, ani detailně analyzovat každý požadavek vznesený GDPR na všechny zúčastněné subjekty.

Otázka hranic veřejného prostoru hraje úlohu zejména v případech, kdy dojde ke střetu práva na soukromí s jiným, právním řádem zaručeným subjektivním právem nebo veřejným zájmem. Ve veřejném prostoru totiž ustupuje intenzita ochrany soukromí a uvolňuje se zde místo pro jiné chráněné zájmy. S tím souvisí i americké *reasonable expectation of privacy*, jež se uplatňuje také v rozhodovací praxi ESLP a českých soudů a pomáhá určit,

[13] *United States v. Jones,* rozsudek Nejvyššího soudu Spojených států amerických, 30. 4. 2012 č. 565 U.S. 400.

[14] O tom, zda a jaké kritérium dělá z veřejného prostoru veřejný prostor, cf. kapitola *Dichotomie veřejné-soukromé.*

zda je požadavek na ochranu soukromí v daném prostoru relevantní. Proto o něm tento článek bude pojednávat, ačkoli se primárně nesoustředí na americké pojetí soukromí a zaměřuje se na situaci v Česku, potažmo v Evropě.[15] Stejně tak budou v práci využity zdroje amerických autorů, a to v takovém rozsahu, v jakém je možné z nich vycházet i pro české prostředí. Američtí autoři se totiž významně podíleli a podílejí na utváření konceptu soukromí a jejich pojetí vešla ve známost i v Evropě.

Analýza pojmu veřejný prostor bude provedena napříč českým právním řádem. To nutně neznamená, že vyčerpávajícím způsobem pojme jakýkoli výskyt slova se stejným základem; neexistuje zákon, který by jednotně upravoval veřejný prostor nebo kamerové systémy, natož kamerové systémy ve veřejném prostoru, proto je třeba čerpat z řady předpisů; nadto veřejný prostor jako takový žádným zákonem definovaný není, proto nezbývá než se zaměřit na pojmy obdobného významu. V téže části příspěvku bude nastíněn problém dichotomie veřejné/soukromé v kontextu ochrany soukromí ve veřejném prostoru. Následně bude popsáno, zda a jak ochrana soukromí závisí na prostorovém aspektu.

Cílem článku je aplikovat závěry z teoretické části na vybranou moderní sledovací technologii. Ve zvláštní části článku bude pojednáno o kamerovém sledování, jeho technických možnostech, využití a také o jeho právním rámci, dovolenosti a pravidlech, včetně pravidel pro zpracování údajů při tomto postupu získaných. Kamery byly pro tuto práci vybrány, protože na rozdíl od jiných technologií představují významný prvek hrající roli v předělu mezi soukromým a veřejným fyzickým prostorem:[16] sledování probíhající v síti Internet je mimo rámec tohoto příspěvku, neboť se neodehrává ve fyzickém prostoru; GPS tracker v mobilu působí na případné narušení soukromí stejně intenzivně bez ohledu na to, kde se jedinec nachází; pasivní zobrazovací systémy na bázi milimetrových vln mají specifické

[15] Evropský kontext má v této práci význam co do přijatých úmluv, jimiž je vázané také Česko, a také v mezích unijní legislativy a rozhodovací praxe ESLP, na niž ve značné míře odkazují rozhodnutí národních soudů.

[16] Gumpert, G. Drucker, S. J. Public boundaries: Privacy and surveillance in a technological world. *Communication Quarterly*. 2001, vol. 49, n. 2, p. 115.

a méně časté využití.[17] Kamery jsou naproti tomu v tomto kontextu specifické pro jejich hojné využití právě v „poloveřejných“ a „polosoukromých“ prostorách, na něž se článek zaměřuje a které tvoří šedou zónu mezi prostorami, u nichž je snadnější definovat, jestli jsou spíše soukromé nebo veřejné. Mají tedy potenciál demonstrovat, zda dochází ke stírání veřejného a soukromého prostoru. Autoři zabývající se odlišením veřejného prostoru od soukromého, jejichž díla jsou v této práci citována, zpravidla odkazují právě na *video surveillance*, tedy kamerový dohled.

V práci je nutné vzhledem k jejímu zaměření zohlednit právní úpravu ochrany osobních údajů, což vyplývá z výše uvedených úvah. V této oblasti došlo v posledních letech k legislativním změnám jak na národní úrovni, tak v právu EU.[18] Mnoho soudních rozhodnutí, která byla vydána před účinností aktuálních předpisů, stejně jako většina stanovisek a výkladů k ochraně osobních údajů mají však nadále význam a je možné z nich v přiměřeném rozsahu vycházet i nyní.[19]

V závěru článku bude zhodnoceno, zda dosavadní pojetí soukromého a veřejného prostoru v českém právním řádu odpovídá potřebám kamerového sledování, a především právní úpravě kamerového sledování, v jejímž rámci je nezbytné brát ohled na právo na ochranu soukromí.

2. OCHRANA SOUKROMÍ

2.1 CO JE TO SOUKROMÍ?

„What does privacy mean?
Well, it depends on who you ask.“[20]

---

[17] Aronov, R. F. Privacy in a Public Setting: The Constitutionality of Street Surveillance. *Quinnipiac Law Review*. 2004, vol. 22, no. 4, p. 775.

[18] Zákon č. 101/2000 Sb., o ochraně osobních údajů, byl nahrazen zákonem č. 110/2019 Sb., o zpracování osobních údajů, a to v reakci na nahrazení 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 nařízením GDPR.

[19] Míšek, J. *Osobní údaje v čase a prostoru.* 2020, disertační práce, Masarykova univerzita, Právnická fakulta, p. 43.

[20] What is privacy [online]. *International Association of Privacy Professionals.* 2021. [cit. 8. 4. 2021]. https://iapp.org/about/what-is-privacy

Ačkoli je pojem soukromí běžně užívaný termín, definice není tak jednoduchá, jak se na první pohled možná může zdát.[21] Ostatně i na poli práva panuje shoda toliko na tom, že se jedná o pojem téměř nevyložitelný.[22] Závěr, se kterým přichází Judith Thomson,[23] je však snad až příliš přísný. Představu o tom, co je soukromí, má zřejmě každý nějakou – sice každý trochu jinou, nicméně v odpovědích by se zajisté našly společné znaky, jimiž lze soukromí popsat.

Soukromí není snadné definovat, neboť má několik aspektů a rovin. Různí autoři tak vytvářejí různé typologie ve snaze jej uchopit a definovat. Nejčastěji je skloňována definice Warrena a Brandeise z konce 19. století.[24] Jejich pojetí práva na soukromí jako *right to be let alone*[25] se drží i novodobější teoretikové zabývající se konceptem soukromí souvisejícím s moderními informačními technologiemi. Do své typologie toto pojetí zahrnuje například Daniel J. Solove, který vedle toho mezi aspekty soukromí zařazuje utajení určitých záležitostí před ostatními, schopnost vyvarovat se nechtěnému zásahu do soukromí ze stran jiných a možnost rozhodovat o „životě" informací o sobě samém, intimitu a ochranu osobnosti a důstojnosti člověka.[26] Brandeisovo a Warrenovo pojetí naopak nereflektuje typologie Alana Westina,[27] která hovoří o samotě *(solitude) a* anonymitě. Samota představuje oproštění se od téměř všeho, tedy i absenci *surveillance*,

[21] Solove, D. J. Conceptualizing Privacy. *California Law Review.* 2002, vol. 90, n. 4, p. 1088.

[22] Tak například William Beaney tvrdí, že i advokát musí uznat nejasný rozsah a vymezení práva na soukromí (Beaney, W. M. The Right to Privacy and American Law. *Law & Contemporary Problems*. 1996, vol. 31, n. 2, pp. 253, 255); dle Geretyho má soukromí potenciál být pro každého právníka něčím jiným (a vším) (Gerety, T. Redefining Privacy. *Harvard Civil Rights-Civil Liberties Law Review*. 1977, vol. 12, n. 2, pp. 233, 234); Robert Post dokonce vyslovil pochybnost o jakémkoli užitečném vyřešení výkladu tohoto pojmu (Post, R. C. Three Concepts of Privacy. *The Georgetown Law Journal.* 2001, vol. 89, n. 6, p. 2087).

[23] Který zní: *"Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is."* Thomson, J. J. The Right to Privacy. *Philosophy & Public Affairs.* 1975, vol. 4, n. 4, p. 295.

[24] Byť podobný koncept představil již Cooley, cf. Filip, J. Úvodní poznámky k problematice práva na soukromí. In: Šimíček, V. (ed.). *Právo na soukromí*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011.

[25] „právo být ponechán sobě samému"; Warren, S. Brandeis, L. The right to privacy. *Harvard Law Review*. 1890, vol. 4, n. 5, p. 193.

[26] Solove. *Conceptualizing privacy,* p. 1092.

kterou předpokládá i méně přísná Westinova složka – anonymita. V případě absence dohledu může jedinec anonymity dosáhnout i na veřejných místech, a to i přes to, že zde může být zpozorován někým jiným. Tento potenciál narušení soukromí si jedinec uvědomuje, ale primárně neočekává, že by mohl být identifikován.[28] Clarke se ve svém pojetí zaměřuje především na změny způsobené vývojem technologií, které reflektuje ve svém dělení soukromí, respektive v popisu dílčích složek, z nichž jednu pojmenoval jako *privacy of personal behavior.* Tato množina má představovat takové typy chování, respektive jednání, jež by měly zůstat soukromé. Jsou součástí soukromého prostoru *(private space)*. Soukromý prostor se dle Clarkeho nenachází pouze na soukromých místech *(private places)*, ale rovněž na místech veřejných,[29] kde *„casual observation by the few people in the vicinity is very different from systematic observation and the recording of images and sounds“*.[30] Dále Clarke popisuje soukromí osobních komunikací, jehož narušení rovněž s novými technologiemi dostává nový rozměr (například prostřednictvím odposlechů – ať už je narušiteli znám přímo obsah konverzace či „pouze“ informace, že nějaká konverzace mezi subjekty probíhá).[31] Vedle toho uvádí složku zahrnující soukromí týkající se osobních dat, jejíž obsah koresponduje s tím, co je běžně nazýváno informačním soukromím.[32] Ve vícero snahách o konceptualizaci soukromí se v této

[27] Která je starší než ta, kterou popsal D. Solove. Koops, B.-J. Newell, B. Timan, T. Škorvánek, I. Chokrevski, T. Galič, M. A Typology of Privacy. *University of Pennsylvania Journal of International Law.* 2017, vol. 38, n. 2, p. 496.

[28] *Ibidem*, p. 497.

[29] What's ‚Privacy'? [online]. *Xamax Consultancy Pty Ltd*. 1995-2021. [cit. 20. 9. 2021]. http://www.rogerclarke.com/DV/Privacy.html

[30] Volně přeloženo jako: *„[kde] se příležitostné pozorování několika málo lidmi v blízkém okolí velmi liší od systematického pozorování a zaznamenávání obrazů a zvuků.“*

[31] Přednáška profesora Václava Matyáše v rámci předmětu Ochrana dat a informačního soukromí na Fakultě informatiky Masarykovy univerzity, podzim 2017.

[32] What's ‚Privacy'? [online]. Právo na informační sebeurčení je však širší, nezahrnuje pouze právo k datům a informacím o jedinci, cf. Míšek, J. *Moderní regulatorní metody ochrany osobních údajů.* Brno: Masarykova univerzita, 2020, pp. 41-42. Rovněž je třeba vnímat, že ochrana osobních údajů je prvkem veřejnoprávním, zatímco ochrana soukromí soukromoprávním. Rozdílným kritériem je také objektivní ochrana osobních údajů, zatímco informačního soukromí si jedinec musí být vědom. Nelze však ignorovat jejich vzájemné vazby, cf. Kasl, F. Povaha zásahu do informačního soukromí člověka. *Právník*. 2019, vol. 158, n. 7, pp. 676-678.

souvislosti pojednává o právu na informační sebeurčení, tedy o možnosti jednotlivce rozhodnout o tom, kdo a jakým způsobem bude nakládat s informacemi o něm, tedy komu ty které informace zpřístupní. Skupinu takových informací GDPR označuje jako osobní údaje, jimiž jsou „*veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby*“.[33] Identifikovatelnost osoby stojí proti anonymitě jakožto jedné ze složek soukromí.

Posledním aspektem, který Clarke rozlišuje, je soukromí osoby *(privacy of the person)*, které v kontextu tohoto příspěvku hraje roli toliko ohledně biometrických údajů, jež některé sledovací technologie umí zpracovávat. Anita Allen ve své typologii rozlišuje prostorový aspekt soukromí.[34] Ten se v jejím dělení odráží i ve složce *informational privacy*, jejíž subkategorií mohou být informace o poloze dané osoby.[35] Koops trefně poukazuje na skutečnost, že oddělená ochrana dílčích aspektů soukromí (obydlí, komunikace atp.) již není efektivní s ohledem na prolínání se těchto částí, jejich těsné sepětí a faktickou neoddělitelnost, jež je způsobena vývojem technologií a společenských hodnot.[36] Ochrana soukromí by tak dle něj neměla být koncipována ani na základně toho, zda se jedná o soukromý, nebo veřejný prostor. Nepopírá přitom, že soukromí má i prostorový fyzický aspekt, ten nicméně není a nemůže být v dnešní době určujícím.[37]

---

[33] Článek 4 bod 1 GDPR.

[34] Allen, A. L. *Unpopular privacy: what must we hide?* Oxford: Oxford University Press, 2011, p. 29.

[35] V pojetí Koopse, cf. Koops, Newell, Timan, Škorvánek, Chokrevski, Galič. A *Typology of Privacy*, p. 500.

[36] Koops, B.-J. On legal boundaries, technologies, and collapsing dimensions of privacy. *Politica e Società*. 2014, vol. 3, n. 2, p. 258.

[37] *Ibidem*, p. 12: *„It continues to have a physical element; the problem is just that this physical element is growing more elusive as it cannot be neatly tied to human persons or the places where people used to live their private life.“*

Vývoj moderních technologií a jeho vliv na narušení soukromí reflektovali při vytváření vlastní koncepce soukromí Finn, Wright a Friedewald. Popisují mj. *privacy of location and space* (soukromí polohy a prostoru), kde autoři hovoří o veřejném a poloveřejném prostoru, v němž by měl mít jedinec možnost pohybovat se anonymně, což komplikují právě sledovací technologie. Výslovně přitom poukazují na význam práva na soukromí v prostorách jako domov, auto[38] či kancelář.[39]

Český právní řád používá jak pojem soukromí, tak soukromý život.[40] V LZPS tuto dvojkolejnost pojímají články 7 a 10.[41] Zde české právo naráží na typický problém, kdy zákonodárce užívá vícero pojmů se stejným slovním základem, což může působit (a v praxi působí) interpretační problémy, neboť není zřejmé, zda jsou takové pojmy libovolně zaměnitelné, nebo zda mají význam jiný. Dle komentáře k LZPS[42] má větší smysl v kontextu znění jednotlivých článků vykládat pojem *soukromí* užívaný ve článku sedmém ve smyslu tělesné a duševní integritu jedince. Druhý, nesprávný přístup pak nahlíží na článek 7 jako na obecnější úpravu, kdy *soukromý život* upravený ve článku 10 tvoří pouze složku širšího soukromí. V tomto rozsahu lze s komentářem souhlasit. Právo nás učí vykládat jednotlivá ustanovení v jejich kontextu a že je nutné zohlednit znění celého paragrafu, případně článku, zařazení do oddílu apod. S ohledem na znění jednotlivých článků a jejich zařazení je skutečně logičtější vykládat v článku 7 pojem soukromí v užším smyslu. Právem na ochranu soukromí

[38] Koops, Newell, Timan, Škorvánek, Chokrevski, Galič. A *Typology of Privacy*, p. 515: Výslovně je auto jako soukromý prostor chráněno např. dle polského zákona.

[39] *Ibidem*, p. 503. Výběr uvedených prostor je však nešťastně zvolený a nepříliš vypovídající, neboť obydlí i auto jsou prostory soukromými a jak bude zmíněno dále v této práci, ohledně kanceláře existuje ustálená judikatura připouštějící přesah soukromého života i do těchto prostor.

[40] V angličtině se rovněž rozlišují pojmy *privacy a private life.* Naproti tomu ve francouzštině se zpravidla užívá ekvivalent *la vie privée,* tedy v doslovném překladu „soukromý život" pro oba české a anglické výrazy.

[41] Naproti tomu v Evropské úmluvě o ochraně lidských práv nalezneme „pouze" ochranu soukromého života, nikoli výslovně soukromí.

[42] Nechvátalová, L. In: Husseini, F. et al. *Listina základních práv a svobod: komentář.* Praha: C. H. Beck, 2021, pp. 225-226; shodně též Wagnerová, E. Čl. 10. In: Wagnerová, E. et al. *Listina základních práv a svobod: komentář.* Praha: Wolters Kluwer, 2012. In: ASPI [Právní informační systém].

je tedy v této práci třeba rozumět především právo zakotvené ve článku 10 LZPS. V souvislostech předkládaného příspěvku není třeba vnímat soukromí ve všech jeho složkách – například do tělesné integrity *surveillance,* resp. kamerový dohled zpravidla nezasáhne. Je však relevantní brát v úvahu i navazování a udržování sociálních vztahů, které lze rovněž považovat za součást soukromí.[43]

ESLP si uvědomuje jednotlivé formy soukromí, které reflektuje mimo jiné ve svém rozsudku Niemietz proti Německu,[44] kde rozlišuje *„inner circle“* a *„social private life“* jako dvě od sebe odlišné oblasti, jež jsou však obě prvkem práva na soukromí. Konstatuje, že soukromý život přesahuje hranice *„inner circle“*, a tuto myšlenku promítá také do prostoru se závěrem, že například i na pracovišti jedinec může vést soukromý život.[45] Obdobně i ÚS rozlišuje *internum a externum*, z nichž druhé jmenované pojímá i pracovní, obchodní a sociální aktivity.[46] Soudní praxe s ohledem na výše uvedené hraje zásadní roli v určování, co pod pojem soukromí podřadit a kdy dát přednost ochraně soukromí v případě, kdy nastane střet s jiným právem.[47] Tato skutečnost je zřejmá mj. z většiny rozhodnutí, jež budou uvedena v celé této práci dále. Právo na soukromí tedy zastřešuje vícero práv a chráněných zájmů,[48] jedním z nichž je i právo na nedotknutelnost *obydlí*,[49] které ostatně představuje výchozí prostorový bod.

---

[43] Tůma, P. § 86. In: Lavický et al. *Občanský zákoník I. Obecná část (§ 1-654)*. Praha: C. H. Beck, 2014, pp. 509-524.

[44] *Niemietz v. Germany*, rozsudek Evropského soudu pro lidská práva, 16. 12. 1992 č. stížnosti 13710/88.

[45] Přitom však neurčuje, zda se jedná o prostor soukromý, nebo veřejný.

[46] Nález Ústavního soudu ze dne 6. března 2012, sp. zn. I. ÚS 1586/09.

[47] Jedná se zejména o rozhodovací praxi ESLP a Ústavního soudu. Nad rámec tohoto článku lze z těch nejvýznamnějších zmínit například rozhodnutí ESLP ve věci *Klass and others v. Germany* z roku 1978, *Malone v. the United Kingdom* z roku 1984. Oba se týkají odposlechů, jež nejsou zcela předmětem tohot článku. Rovněž lze uvést rozhodnutí *P. G. and J. H. v. the United Kingdom,* rozsudek Evropského soudu pro lidská práva, 25. 9. 2001 č. stížnosti 44787/98.

[48] Halpérin J.-L. L'essor de la « privacy » et l'usage des concepts juridiques . *Droit et société*. 2005, vol. 2, n. 61, p. 778.

[49] Šimíček, V. In: Šimíček, V. (ed.). *Právo na soukromí*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011.

2.2 OCHRANA SOUKROMÍ JAKO PRVEK ÚSTAVNÍHO POŘÁDKU

Právo na soukromí je jedním ze základních lidských práv garantovaných LZPS.[50] Jakožto ústavně zaručené právo, jež není absolutní, může být omezené jen ve výjimečných případech na základě zákona, a to v momentě, kdy přijde do střetu s jiným, základním ústavně zaručeným právem nebo ústavní hodnotou.[51] Český právní řád však výslovně nestanovuje, za jakým účelem může být právo na soukromí omezeno. Vázanost Česka Evropskou úmluvou o ochraně lidských práv umožňuje se v tomto směru opřít o článek 8 odst. 2 Úmluvy: „*Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.*“[52] Legitimními cíli, z nichž alespoň jeden musí být sledován při omezení práva na soukromí, tedy mohou být národní a veřejná bezpečnost, hospodářský blahobyt země, ochrana pořádku, zdraví nebo morálky, předcházení trestné činnosti a ochrana před zásahem do práv jiných osob. Je nezbytné vždy zhodnotit, zda by v daném konkrétním případě mělo převážit jiné právo nad právem na soukromí, které by na jeho úkor bylo omezeno.

Jak již bylo uvedeno, právo na ochranu soukromí je zakotvené v článku 10 LZPS, jenž obsahuje právě ty aspekty, jež jsou pro technologiemi dotčený rozsah soukromí relevantní. Jsou jimi zejména ochrana soukromého života (čl. 10 odst. 2) a ochrana osobních údajů (čl. 10 odst. 3). Článek 10 odst. 3 přitom odráží aspekt práva na informační sebeurčení,[53] na které odkazuje i komentář k § 86 OZ:[54] *„Pojem soukromí se v nejširším slova smyslu kryje […], spočívající v možnosti svobodného rozhodnutí člověka o vlastním sebeurčení (místě) ve společnosti […].“* Právě informační sebeurčení tvoří

[50] Článek 7 a 10 LZPS.

[51] Kokeš, M. Čl. 10. In: Husseini, F. et al. *Listina základních práv a svobod: komentář.* Praha: C. H. Beck, 2021, p. 326-361.

[52] Evropská úmluva o ochraně lidských práv. [online]. [cit. 3. 5. 2021]. https://www.echr.coe.int/documents/convention_ces.pdf

[53] Stanovisko pléna Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, bod 29.

[54] Tůma. *Občanský zákoník I. Obecná část (§ 1-654),* pp. 509-524.

podstatný prvek při posuzování zpracování osobních údajů, k němuž dochází mimo jiné při monitorování prostor. Jestliže procházíme monitorovaným prostorem, nemůžeme si zpravidla určit, jaké údaje o nás budou zaznamenány[55] – můžeme si maximálně vybrat se v daném prostoru nevyskytovat.[56] Právo na informační sebeurčení bývá zpravidla chápáno jako možnost jedince rozhodovat o tom, které informace o něm budou známy ostatním. Na tento aspekt poukazuje Ústavní soud ve svém nálezu IV. ÚS 23/05, kde podobně jako ESLP v rozsudku Niemietz proti Německu rozlišuje soukromou sféru – kde platí „*naprosté informační sebeurčení*" a ochrana soukromí – a sociální sféru. Pro sociální sféru však možnost informačního sebeurčení Ústavní soud rovněž zcela nevylučuje a konstatuje, že může být omezena proporcionálními zásahy veřejné moci.

2.3 OČEKÁVÁNÍ SOUKROMÍ

„Očekávání plodí zklamání." Jan Hodermarsky, 2021

Americké pojetí soukromí se liší od toho evropského, přičemž tento příspěvek se zaměřuje na druhé zmíněné.[57] Ochrana soukromí je v americkém prostředí chápána především jako ochrana před zásahy státu, až druhořadě před zásahy veřejnosti, která je naopak viděna jako hlavní narušitel v prostředí evropském.[58] Očekávání soukromí, respektive *expectation of privacy* představuje koncept vzniklý a uplatňovaný v americkém soudnictví. Jedná se o pomocné kritérium, na jehož základě se posuzuje, zda došlo k neproporcionálnímu zásahu do soukromí, či nikoli. Samotné kritérium očekávání soukromí by nepřinášelo příliš právní jistoty, neboť každý může mít očekávání v různých situacích jiná, je subjektivní. Čtvrtý dodatek Ústavy Spojených států amerických stanovuje, že je zakázán nedůvodný

[55] Shodně též Míšek. *Moderní regulatorní metody ochrany osobních údajů,* p. 41.

[56] Shodně též Timan, T., Newell, B. C., Koops, B.-J. (eds). *Privacy in Public Space: Conceptual and Regulatory Challenges*. Cheltenham: Edward Elgar Publishing, 2017, p. 4.

[57] Respektive na české prostředí, jehož právní řád je však významně ovlivněn evropskými hodnotami a úmluvami.

[58] Kasl, F. *Osobnost, soukromí a osobní údaje v moderní společnosti.* In: Polčák, R. Kasl, F. Míšek, J. Stupka, V. Kyselovská, T. Myška, M. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018, p. 405.

(*unreasonable*) zásah do soukromí lidí.[59] Aby tedy došlo k posouzení případu, jehož výsledek bude možné využít nadále v budoucích sporech s obdobnými okolnostmi, je kritérium očekávání soukromí zpřísněno objektivním znakem, že takové očekávání musí být důvodné, opodstatněné, tzv. *reasonable expectation of privacy* (rozumné, resp. důvodné nebo legitimní očekávání soukromí). Ačkoli se článek soustředí na právní stav v Česku, je na místě uvedenou americkou koncepci zmínit, neboť se její vliv promítá i do soudní praxe relevantní pro české území, tedy jak do rozhodovací praxe ESLP, tak českých soudů. Ty na základě tohoto kritéria nestaví závěrečné rozhodnutí pro či proti případnému porušení ochrany soukromí, nicméně používají jej jako podpůrný argumentační prvek. Mimo to se také využívá pro výklad článku 8 Úmluvy.[60]

Test pomocí rozumného očekávání soukromí americký soud poprvé představil v případu *Katz v. United States,*[61] v jehož meritu se jednalo o odposlouchávání Katzova hovoru v telefonní budce, jež se nacházela na ulici, tedy ve veřejném prostoru. Soud vyhodnotil, že i ve veřejném prostoru má člověk právo na soukromí, jestliže ho zde může důvodně očekávat. Telefonní budku označil jako místo ve veřejném prostoru, kde člověk může očekávat vyšší míru soukromí než venku na ulici, kde se telefonní budka nachází, neboť stěny budky jej více či méně chrání před tím, aby byl jeho hovor vystaven náhodným kolemjdoucím posluchačům. Proto soud naznal, že ačkoli umístění telefonní budky ve veřejném prostoru umožňuje třetí osobě spatřit holý fakt, že daný člověk telefonuje, s čímž je volající srozuměn, není veřejnost oprávněna k tomu, aby znala i samotný obsah rozhovoru, neboť telefonní budka mohla být využita mimo jiné také právě proto, aby hovor nebyl přístupný třetímu posluchači, tedy jako jakási izolace od ryze veřejného prostoru. Stěžejním závěrem tedy bylo konstatování, že

[59] Constitution of the United States, Fourth Amendment [online]. *Congress.gov*. [cit. 10. 6. 2021] https://constitution.congress.gov/constitution/amendment-4/

[60] Cf. Tomas Gomez-Arostegui, H. Defining private life under the European Convention on Human Rights by referring to reasonable expectations. *California Western International Law Journal.* 2005, vol. 35, n. 2, pp. 153-202.

[61] *Katz v. United States,* rozsudek Nejvyššího soudu USA, 18. 12. 1967 č. stížnosti 389 U. S. 347.

jestliže člověk zamýšlel zachovat něco jako soukromé, ačkoli na veřejně přístupném místě, mělo by toto očekávání soukromí být ústavně chráněno.[62]

Příkladem, kdy ESLP hodnotil očekávání soukromí, je například rozsudek ve věci *Halford v. the United Kingdom*[63] v souvislosti s telefonními hovory uskutečňovanými na pracovišti nebo ve věci *Bărbulescu v. Romania*[64] rovněž v souvislosti s komunikací po telefonu. Stejně jako v rozhodovací praxi USA se i v případech u ESLP jedná o doplňkové, nikoli to nejdůležitější kritérium.[65]

V tuzemské judikatuře není hledisko oprávněného očekávání soukromí natolik rozšířené a zásadní, soudy na něj však na několika místech poukazují. Jedním z příkladů je rozsudek Nejvyššího správního soudu č. j. 4 As 97/2013 - 40,[66] kde Nejvyšší správní soud odkazuje na *„legitimně očekávaný rozsah soukromí“* žalobkyně po provedení stavebních úprav na sousedním domě, a to dokonce v situaci, kdy otázka narušení soukromí byla pouze hypotetická, neboť dům žalobkyně v daném období nebyl obýván a nebylo tedy osoby, jejíž soukromí by bylo narušeno. Legitimní očekávání soukromí soud hodnotí na základě povahy zásahů, které nesmí být narušující *„nad míru přiměřenou poměrům“*. Do tohoto přirovnání se promítá objektivní hledisko očekávání soukromí – americké *„reasonable“* český soud překládá jako *„legitimní“* a odvozuje jej od objektivních poměrů, které na daném místě v dané situaci panují. Analogicky terasu přirovnává k tribuně – obě umožňují sledovat z výhodné pozice okolní dění, jímž je v případě terasy obydlí sousedky, jejíž soukromí je v tomto případě předmětem ochrany. V témže rozsudku soud k problematice míry soukromí doplnil, že: *„[m]íra soukromí se přitom nepojí pouze k osobě žalobkyně, k jejím způsobům užívání dvorku, popřípadě k druhům vykonávaných činností, jak se mylně domnívá stě-*

[62] *“… what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”*

[63] *Halford v. the United Kingdom,* rozsudek Evropského soudu pro lidská práva, 25. 6. 1997 č. stížnosti 20605/92.

[64] *Bărbulescu v. Romania,* rozsudek Evropského soudu pro lidská práva, 12. 1. 2016 č. stížnosti 61496/08.

[65] *P. G. and J. H. v. the United Kingdom,* rozsudek Evropského soudu pro lidská práva, 25. 9. 2001 č. stížnosti 44787/98, bod 57.

[66] Rozsudek Nejvyššího soudu ze dne 30. 7. 2013, sp. zn. 4 As 97/2013 - 40.

žovatelka. Váže se prvotně na institut vlastnictví, jehož výkon je chráněn přímo zákonem vymezením sousedských práv […]“.[67]

Využití konceptu očekávání soukromí v českém prostředí výslovně dovoluje i Ústavní soud ve svém nálezu sp. zn. II. ÚS 1221/16, bod 20, v němž posuzoval otázky práva na soukromí ve vozidle.[68] V předmětném trestním řízení bylo vozidlo podrobeno policejní prohlídce, čímž bylo dle stěžovatele zasaženo do jeho práva na soukromí. Při nařízení prohlídky bylo na vozidlo nahlíženo jako na „jiné prostory“ ve smyslu § 83a trestního řádu. V takových případech je dle nálezu nutné přihlédnout k ustanovením čl. 8 Úmluvy a čl. 12 LZPS. Soud dospěl k aplikaci kritéria rozumné očekávání soukromí, neboť dovodil spojitost[69] mezi americkou právní úpravou a článkem 12 LZPS[70] chránícím nedotknutelnost obydlí a upravujícím přípustnost prohlídek obydlí v trestním řízení. I odpovídající ustanovení Čtvrtého dodatku americké Ústavy totiž zmiňuje zákaz nedůvodných prohlídek, který je společným prvkem obou právních úprav a podstatou uvedených ustanovení. Dle závěrů Ústavního soudu patří vozidlo mezi prostory, kde můžeme důvodně očekávat soukromí, a to i přes to, že stěžovatel jakožto osoba, jejíž soukromí bylo narušeno, k vozidlu nemá vlastnické právo. Z uvedeného nálezu tedy plyne závěr, že mezi oprávněným očekáváním soukromí a vlastnictvím (vozidla, domu…) není nutně přímá úměra, respektive vlastnické právo „k prostoru“ není nezbytnou podmínkou pro to, abychom zde mohli očekávat soukromí. Vztah vlastnictví a práva na ochranu soukromí v daném (ne)vlastněném prostoru je pro tuto práci relevantní, neboť navazuje na jedno z možných kritérií, jímž je možné si vypomoci při rozlišování veřejného a soukromého prostoru.[71] Obdobně se ke vztahu vlastnictví věci a ochranou soukromí pod článkem 8 Úmluvy

[67] *Ibidem*, p. 8.

[68] Nález Ústavního soudu ze dne 13. října 2016, sp. zn. II. ÚS 1221/16.

[69] Jak uvádí Ústavní soud ve svém nálezu, cf. Bartoň, M. et al. *Základní práva*. Praha: Leges, 2016, s. 302.

[70] Nález Ústavního soudu ze dne 13. října 2016, sp. zn. II. ÚS 1221/16, bod 21.

[71] Blíže v kapitole *Veřejný prostor*.

vyjádřil ESLP ve věci *Menteş and others v. Turkey*.[72] Ochranu soukromí obdobně dovodil i v případě, kdy dotčená osoba není vlastníkem domu.[73]

O možnosti využití předmětného kritéria dále svědčí usnesení Ústavního soudu sp. zn. III. ÚS 1122/17, v němž byla posuzována otázka přiměřenosti zásahu do soukromí stěžovatele, který namítal neoprávněnost pořízení audionahrávky, která byla použita jako důkaz v trestním řízení vedeném proti němu.[74] K zásahu do soukromí mělo údajně podle stěžovatele dojít na pozemní komunikaci, která je v kategorizaci veřejný – soukromý prostor prostorem veřejným. I v tomto případě se Ústavní soud při své argumentaci opřel o důvodné očekávání soukromí a konstatoval bez jakýchkoli pochyb, že pozemní komunikace je zcela určitě takovým prostorem, kde člověk důvodně nemůže soukromí očekávat: *„…za těchto okolností nemohl mít sebemenší očekávání soukromí, natožpak očekávání rozumné.“*[75] Soud poznamenal, že je rozporné, zda se vzhledem k velmi nízké míře možných očekávání vůbec v daném případě jedná o jakékoli narušení soukromí. Hledisko rozumného očekávání soukromí dále soud využil i při hodnocení následného zacházení s důkazním prostředkem.[76] Ve věci přípustnosti odposlechu hovorů pak na tento nález a na měřítko důvodného očekávání soukromí odkazuje také Nejvyšší soud.[77]

Důvodné očekávání soukromí není při rozhodování o porušení práva na soukromí absolutním měřítkem, nicméně pouze kritériem podpůrným. Ostatně ani ESLP se neomezuje výlučně na posouzení skrze toto kritérium

---

[72] *Menteş and Others a. Turkey*, rozsudek Evropského soudu pro lidská práva, 28. 11. 1997 č. stížnosti 58/1996/677/867.

[73] *Mentes v. Turkey*, bod 73: *„The Court sees no reason to distinguish between the first applicant, Ms Azize Menteş, and the second and third applicants. While it was in all probability her father-in-law and not she who owned the house in question, the first applicant did live there for significant periods on an annual basis when she visited the village (see paragraph 34 above). Given her strong family connection and the nature of her residence, her occupation of the house on 25 June 1993 falls within the scope of the protection guaranteed by Article 8 of the Convention.“*

[74] Usnesení Ústavního soudu ze dne 30. května 2017, sp. zn. III. ÚS 1122/17.

[75] *Ibidem,* bod 20.

[76] Cf. také *S. and Marper v. the United Kingdom*, rozsudek Evropského soudu pro lidská práva, 4. 12. 2008 č. stížností 30562/04 a 30566/04, bod 67.

[77] Rozsudek Nejvyššího soudu ze dne 11. 4. 2018, sp. zn. 7 Tdo 374/2018.

a bere v úvahu také další aspekty, jež jsou pro daný případ relevantní.[78] Takový závěr ostatně v českém právním řádu podporuje i uplatnění testu proporcionality, jež je v podobných případech rozhodující. Rovněž americký soudce se v jednom rozsudku vyjádřil v tom duchu, že při konstatování, kde lze důvodně očekávat soukromí, nelze současně určit, že v určitých prostorách za žádných podmínek nesmí k prohlídce dojít – zakázané prohlídky jsou pouze ty nedůvodné.[79]

2.4 DÍLČÍ ZÁVĚR

Tato kapitola nabízí shrnutí ukotvení soukromí v právním řádu Česka a základních konceptů ochrany soukromí. Jako zásadní nedostatek je v odborné literatuře vnímána absence definice soukromí. Obzvlášť v době, kdy je narušení soukromí možné skrze nové prostředky (sledovací technologie) na několika úrovních v různých intenzitách, zdá se otázka potřeby definice palčivější. Naopak ale možná o to spíš by bylo vhodné se od upínání k představě jednotné definice soukromí oprostit. Již desítky let se autoři snaží o jednoznačné a jednotné vymezení tohoto fenoménu, přesto se jim to doposud nepodařilo, což vede nutně k myšlence, zda je to vůbec možné nebo účelné.[80] Naproti tomu soudy poměrně obstojně plní úlohu interpretovat tento pojem tam, kde je potřeba. Judikatura je v tomto ohledu relativně ustálená, tudíž není pravda, že by neexistoval žádný rámec toho, co soukromí představuje. Soudy na národní i evropské úrovni již v několika rozhodnutích definovaly, jaké zásahy do soukromí přichází v úvahu a co vše je součástí soukromé sféry jedince. I mezi odlišnými typologiemi jednotlivých autorů existují spojitosti, v zásadě všechny pojímají tytéž prvky soukromí a nerozchází se v tom, co by v mezích soukromí chráněno být mělo, a co nikoli.

---

[78] Cf. *S. and Marper v. the United Kingdom*, rozsudek Evropského soudu pro lidská práva, 4. 12. 2008 č. stížností 30562/04 a 30566/04.

[79] *Elkins v. United States*, rozsudek Nejvyššího soudu Spojených států amerických, 27. 6. 1960 č. 364 U.S. 206: *"It must always be remembered that what the Constitution forbids is not all searches and seizures, but unreasonable searches and seizures."*

[80] Možná bychom si spíše měli klást otázku, zda není krátkozraké po takové definici pátrat. Právo již nyní pružně nereaguje na technický pokrok. Nepochybně i před desítkami let bylo nepředstavitelné, aby existovala zařízení zpracovávající například biometrické údaje.

Koncept legitimního očekávání soukromí má v české judikatuře nepochybně své místo. Ačkoli je rozhodnutí ve věci *Katz* interpretováno tak, že odklání ochranu soukromí od prostorového aspektu k dané osobě,[81] prostorovou složku soukromí tím soudy nepopírají. Hodnotit kritérium očekávání má v této práci svůj význam a bude mu věnováno ještě několik myšlenek v návaznosti na veřejný prostor a kamerové sledování. Na tomto místě je nicméně vhodné poukázat na rozdíl mezi *soukromím a právem na soukromí*. Soukromí můžeme ve veřejném prostoru bezpochyby požívat, aniž by nám jej někdo „garantoval". Běžně se tak tomu děje, pokud na veřejně přístupných místech zrovna kromě nás nikdo není a nikdo nás ani zpovzdálí nesleduje. Tudíž je možné na některých veřejných místech soukromí i relativně rozumně očekávat. Avšak otázkou, která je stěžejní, je to, zda je toto soukromí pouze nahodilé, či zda na něj i ve veřejném prostoru máme subjektivní právo. Pokud by byl přijat závěr, že ve veřejném prostoru nemáme žádné právo na soukromí, pak by měly sledovací technologie „volnou ruku" ve shromažďování a následném zpracování[82] dat. Takový přístup by byl nepochybně v rozporu s ochranou soukromí a subjekty takového sledování by s tímto pojetím nebyly spokojeny.

Cílem kapitoly nebylo podat čtenáři vyčerpávající přehled o veškerých dosavadních snahách formulovat, co je soukromí. Základem nicméně vždy bude něco, co vychází z nitra jednotlivce, z jeho intimní sféry. Něco, co je potřeba chránit před zásahy zvenčí v případě, že jedinec má tuto vůli.[83] Je tomu tak i v kontextu soukromí na veřejnosti, neboť i tam zásah může dosahovat vysoké intenzity, a především může být způsoben mnoha subjekty z různých stran. Proto je přiléhavá definice *„right to be let alone"*. Zabývat se

[81] Marx, G. T. What's New About the "New Surveillance"?: Classifying for Change and Continuity. *Surveillance & Society*. 2002, vol. 1, n. 1, p. 29.

[82] Zpracování *stricto sensu* – jako např. ukládání a další využití, nikoli v pojetí GDPR, dle nějž je i samotné pořizování, resp. shromažďování dat zpracováním. *Stricto sensu a lato sensu* není oficiální rozlišení zpracování osobních údajů, nicméně je praktické minimálně v kontextu tohoto příspěvku, pročež je toto označení zavedeno.

[83] Článek 8 Úmluvy chrání před zásahy veřejné moci, cf. Milaj, J. *Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance*, p. 117; § 86 OZ stanovuje, že do soukromí jiného nesmí zasáhnout *nikdo*.

právem na informační sebeurčení má význam proto, že na veřejnosti je možné získat pomocí technologií přístup i k takovým údajům, které by o sobě člověk cizím lidem primárně neprozradil, a k faktům, jež by každému nevystavoval.

3. VEŘEJNÝ PROSTOR

"There are no physical boundaries around personal space."[84]

Smyslem článku je zaměřit se na fyzický veřejný prostor. Veřejný prostor není v právních textech příliš rozebírán a snahy o jeho vymezení pramení spíše z jiných oborů, zejména urbanismu, jež si k tomu často vypomáhají legální definicí veřejného prostranství. Do veřejného prostoru je možné zařadit i vnitrobloky či exteriéry veřejných budov,[85] kromě soukromého a veřejného prostoru lze však v jiných vědních oborech navíc nalézt i kategorii prostoru polosoukromého a poloveřejného,[86] což naznačuje, že hranice mezi soukromým a veřejným prostorem nebude jednoznačná. Mezi polosoukromý prosor lze řadit například předzahrádky[87] nebo zahradu sdílenou obyvateli vícero bytů,[88] mezi poloveřejné například průchozí vnitrobloky.[89]

3.1 DICHOTOMIE VEŘEJNÉ – SOUKROMÉ

Odlišení veřejného a soukromého prostoru se pojí s tradičním problémem dichotomie, který vedle té prostorové prozařuje i různými jinými sférami.[90] Řada autorů se snažila nalézt kritéria, na jejichž základě by bylo možné

[84] Madanipour, A. *Public and Private Spaces of the City*. London: Routledge, 2003, p. 202.

[85] Veřejný prostor [online]. *Kancelář architekta města Brna* [cit. 20. 9. 2021]. https://kambrno.cz/verejny-prostor/ To však není v rozporu s legální definicí veřejného prostranství, neboť ta obsahuje pouze demonstrativní výčet, cf. kapitola *Veřejný prostor de lege lata.*

[86] Veřejný prostor [online]. *Uzemi.eu* [cit. 20. 9. 2021]. http://www.uzemi.eu/pojmy/verejny-prostor

[87] Gehl, J., Blažek, K., Blažková, B., Sedlák, R. *Města pro lidi.* Brno: Partnerství, 2012, pp. 82-85.

[88] Schmeidler, K. et al. *Sociologie v architektonické a urbanistické tvorbě.* Brno: Zdeněk Novotný, 2001, p. 122.

[89] Čabalová, M., Maceková, M., Míčák, L., Nawrath, M., Římanová, M., Sedlák, R., Šilberská, P. *Kvalitní veřejné prostory: Metodika tvorby a obnovy veřejných prostranství.* Brno: Nadace Partnerství, 2011, pp. 11-12.

[90] Míšek, J. *Osobní údaje v čase a prostoru,* p. 34.

soukromé od veřejného odlišit. Nissenbaum odlišuje veřejné a soukromé na základě:

a) aktérů; těmi jsou jedinci a vláda. V tomto vztahu hraje soukromí roli něčeho, co chrání jednotlivce ve vztahu k vládě, respektive proti zásahům vlády do sféry jednotlivce. Z pohledu dichotomie je soukromým takový prostor, kde je jednotlivec suverénem.[91]
b) informací, které Nissenbaum rovněž dělí na veřejné a soukromé. Toto rozdělení ale neobstojí, neboť prvky množin „soukromé informace" a „veřejné informace" by se mohly významně lišit na základě toho, kdo by se o jejich definici pokusil. Informační soukromí je navíc možné chápat odlišně ve vztahu k prostoru, ve kterém se člověk nachází, a rozdělení v takovém případě nemusí být nutně odpovídající: informace dostupné ve fyzickém veřejném prostoru nemusí být automaticky informacemi veřejnými.[92] Jako příklad lze uvést nákup léků v lékárně. Fakt, že jedinec neuskutečňuje tento nákup ze svého domu, neznamená, že informace o jeho zdravotním stavu mají být známy široké veřejnosti.
c) sféry. Pod pojmem sféra si nutně nemusíme představit pouze fyzický veřejný prostor. To ostatně uvádí i Curry,[93] podle kterého pod pojmem sféra můžeme chápat jak abstraktní místo, tak geograficky vymezený prostor.

S pojetím jednotlivce jako suveréna v soukromém prostoru se ztotožňuje Madanipour: soukromá sféra je dle něj ta část našeho života, jež je výhradně v naší moci – již máme pod kontrolou, není ovládána veřejnou mocí a úřady. Jedná se o sféru jednotlivce, která je uchráněna před zájmem veřejnosti, před pozorováním, je veřejnosti neznámá a udržuje ostatní mimo tuto sféru. Osobní prostor má být využíván výhradně námi samotnými

[91] Nissenbaum. *Privacy in context*, p. 94. Z akcentu ochrany před zásahy státu lze vnímat umocnění amerického pojetí soukromí.

[92] Nissenbaum, H. Toward an Approach to Privacy in Public: Challenges of Information Technology. *Ethics & Behaviour.* 1997, vol. 7, n. 3, pp. 212-215.

[93] Curry, M. Discursive Displacement and the Seminal Ambiguity of Space and Place. In: Lievrouw, L., Livingstone, S. (eds). *The Handbook of New Media: Social Shaping and Consequences of ICT.* London: Sage Publications, 2002, p. 502.

a Madanipour s ním pojí specifické vzorce chování.[94] Jestliže budeme vycházet z tohoto vymezení soukromého prostoru, pak je veřejným prostorem taková sféra, která není plně v naší moci. Do této sféry nám zasahují třetí osoby, ať již jiní jednotlivci nebo vláda. Pokud sféra není v naší moci a jejím narušitelem je vláda (respektive veřejná moc), pravděpodobně to znamená, že je daná sféra touto veřejnou mocí ovládána.

Co se prostoru týče, Madanipour považuje za soukromý prostor obydlí, respektive místo, jehož je jedinec výlučným vlastníkem a uživatelem. Výlučnost ale nebyla jedním ze základních znaků soukromého prostoru odjakživa. K této transformaci došlo až začátkem osmnáctého století, kdy se obydlí začalo chápat jako místo, kde máme soukromí a kde jsme odděleni od společnosti, od veřejné sféry, do té doby tomu bylo spíše naopak.[95] Jeden z nejznámějších konceptů dichotomického dělení prostoru představili Siebel a Wehrheim, kteří jej kategorizují v několika okruzích. Prvním z nich je legální, v němž je povaha prostoru dána tím, zda nad ním vykonává moc autorita veřejného práva nebo soukromá autorita s pravomocí určit, kdo může soukromý prostor využívat a z jakého důvodu. Dále hodnotí funkci prostoru: veřejnou plní zejména veřejné prostranství. Soukromou funkci mají především prostory obchodních společností a domov. Dále na prostor nahlíží optikou sociálních vztahů: ve veřejném prostoru existuje možnost anonymity, v prostoru soukromém intimita. Posledním je rozlišení materiální/symbolické, které se orientuje na architekturu a design prostoru.[96]

Siebel a Wehrheim se ve svém díle zabývají také „privatizací" veřejného prostoru a postupnou změnou využívání jednotlivých typů prostor, jež napomáhá smazávání hranice mezi soukromým a veřejným. Obchodní centra nazvali v překladu doslova „uzavřeným prostorem veřejné sféry", respektive „novým soukromým veřejným prostorem", jenž je projevem privatizace

---

[94] Madanipour. *Public and Private Spaces of the City*, p. 202. Cf. úvod ke kapitole *Kamerový dohled.*

[95] *Ibidem*, p. 203. Jako soukromou sféru však obydlí chápal už Aristoteles, cf. Aristotle. Politics. In: McKeon, R. (ed.) The Basic Works of Aristotle. Lifetime Library, Random House, 1941, p. 1127.

[96] Siebel, W., Wehrheim, J. Security and the Urban Public Sphere. *German Policy Studies.* 2006, vol. 3, n. 1, p. 19-20.

města, čímž v podstatě poukázali na jejich nezařaditelnost do pouze jedné z těchto kategorií. Vyzdvihují, že se jedná o soukromé objekty, ačkoli se zde vyskytují masy lidí, a že tato místa již mají navíc sloužit i k navazování sociálních vazeb, tedy pojímají i jednu ze složek soukromí. Mimo to se autoři věnovali architektonickému hledisku a skutečnosti, že se „místa, která jsou ze zákona soukromá“,[97] jimiž mají být vstupy do budov, atria a podobné, snaží přizpůsobit svým vzhledem místům veřejným.[98] Přitom co se míry soukromí týče, budou tato místa více prostorem veřejným než soukromým. I Siebel a Wehrheim vedle strukturálních prvků poukazují na vliv technologického pokroku na tuto změnu, respektive na prolínání soukromého a veřejného prostoru.[99]

Na tomto místě se hodí mírně předběhnout a věnovat se také veřejnému prostranství, na které vzápětí naváže následující část příspěvku. Otčenášková totiž popisuje vztah veřejného prostranství k soukromé sféře na základě několika zdánlivě dělicích aspektů:[100]

- Veřejné prostranství slouží *veřejnému užívání*. Zvláštní veřejné užívání však nemusí být neomezené, tzn. pozemek ve zvláštním veřejném užívání nemusí být k dispozici každému. Absentuje tedy přístupnost všem jakožto znak veřejného prostranství.
- Veřejnému užívání slouží i věci v soukromém *vlastnictví* (vždy na základě zákona) a naopak ne všechny veřejné statky jsou předmětem vlastnictví. Tudíž ani aspekt vlastnictví jako určující kritérium neobstojí.
- *Označení* pozemku jako soukromý nemá ze zákona vypovídající hodnotu, navíc ne všechny pozemky jsou označené.
- Do *katastru nemovitostí* se vyznačuje, zda je pozemek veřejným prostranstvím, přičemž se aplikuje presumpce správnosti územního

[97] Zřejmě dle kritéria vlastnictví.

[98] Siebel, Wehrheim. *Security and the Urban Public Sphere*, p. 25.

[99] *Ibidem* p. 25.

[100] Webinář Jany Otčenáškové pořádaný v rámci projektu UNIque Law na téma Sdílení prostoru: veřejný vs. soukromý prostor, 18. 2. 2021.

plánu. Ten však správný vždy být nemusí a chybné vyznačení nedělá z pozemku veřejné prostranství.

Ačkoli by se tedy mohlo zdát, že veřejné prostranství je již podle svého označení veřejné, i v této oblasti můžeme nalézt prvky ze soukromé sféry, které nám striktní oddělení narušují.

Podle Nissenbaum „veřejné" a „soukromé" vždy tvoří dichotomii, a to i přesto, že v různých oblastech či v odlišném kontextu se může význam těchto slov lišit. Přitom samotný fakt, že pojmy „veřejné" a „soukromé" lze vnímat různě, je sám o sobě víceméně nezpochybnitelný. „Soukromé" je možné vykládat jako to, co se děje doma, to, co je záležitostí rodiny, nebo to, co je předmětem intimních vztahů, zatímco jako „veřejné" může být chápáno to, co se děje mimo zdi našeho domu. Jindy může být jako veřejné chápáno to, co je ve sféře moci vlády.[101] V každém případě je možné konstatovat, že každé z těchto rozdělení počítá s tím, že existuje hranice, jež odlišuje, co je soukromé a co veřejné. Výše uvedené příklady a úvahy naopak ukazují, že dichotomie je falešným dilematem, minimálně v prostoru nelze striktní oddělení tolerovat a použití uvedených kritérií zpravidla neobstojí, respektive neobstojí absolutně ve všech situacích.

3.2 VEŘEJNÝ PROSTOR DE LEGE LATA

"Seen by hundreds, noticed by none."[102]

Český právní řád neobsahuje definici veřejného prostoru. Používá však několik výrazů, které se odvíjí od stejného základu a vyskytují se v podobném významu. Nejčastějšími slovními spojeními, která zákon v této souvislosti používá, jsou veřejné prostranství a místo veřejnosti přístupné, přičemž obě používá na jiných místech a nepopisuje vztah mezi nimi, tudíž není zřejmé, zda se uvedené výrazy mají užívat zaměnitelně, tedy ve shodném významu, či nikoli. Takový postup zákonodárce je poněkud nešťastný a nesprávný, ale není výjimečný. Používání podobných pojmů (se stejným kořenem nebo s obdobným významem v obecné češtině mimo

[101] Nissenbaum. *Privacy in context,* p. 90.

[102] *Ibidem,* p. 117.

právní kontext) působí v praxi interpretační potíže a jedná se o chybu v procesu tvorby zákona.[103]

Český právní řád obsahuje legální definici veřejného prostranství, kterým *„jsou všechna náměstí, ulice, tržiště, chodníky, veřejná zeleň, parky a další prostory přístupné každému bez omezení, tedy sloužící obecnému užívání, a to bez ohledu na vlastnictví k tomuto prostoru.“*[104] Ačkoli je pojem v právním řádu využíván i na jiných místech,[105] děje se tak již bez odkazu na zákon o obcích. Trestní zákoník užívá slovní spojení „místo veřejnosti přístupné“,[106] k jehož výkladu se vyjádřil Nejvyšší soud ve svém rozhodnutí sp. zn. 3 Tdo 969/2002.[107] Předmětem rozsudku byl konkrétně trestný čin výtržnictví,[108] jehož se lze dle § 358 TZ dopustit *„veřejně nebo na místě veřejnosti přístupném“*. Výtržnictví se v uvedeném případě odehrávalo v čekárně zdravotnického zařízení. Dovolatelka (obviněná) mimo jiné namítala, že se nemohla dopustit trestného činu výtržnictví, jelikož nebyl naplněn fakultativní znak skutkové podstaty tohoto trestného činu, tedy místo, kde k trestnému činu musí dojít. K takovému závěru dospěla na základě toho, že osobně neshledávala čekárnu zdravotnického zařízení místem veřejně přístupným, a to proto, že *„přítomnost pacientů zde byla přísně kontrolována a jejich pohyb mohl být realizován výhradně za asistence zdravotnického personálu.“* Rovněž poukazovala na to, že *„budova kliniky byla vždy řádně uzamčena, přičemž vstup i odchod z kliniky byl uskutečňován za jeho dohledu.“* Soud dále upřesnil, že se jednalo o čekárnu soukromé kliniky, kde byl za striktních podmínek evidován příchod i odchod osob. Naproti tomu však dospěl k závěru, že čekárna je místem veřejně přístupným ve smyslu pří-

[103] Nad rámec dále uvedených je to například „veřejně přístupný prostor“ a „veřejnosti volně přístupný vnitřní prostor“ v zákoně č. 65/2017 Sb., o ochraně zdraví před škodlivými účinky návykových látek.

[104] § 34 zákona č. 128/2000 Sb., o obcích.

[105] Cf. § 33 zákona č. 121/2000 Sb., autorský zákon, nebo § 104 odst. 1 písm. h stavebního zákona.

[106] Cf. § 302, § 358 zákona č. 40/2009 Sb., trestního zákoníku.

[107] Usnesení Nejvyššího soudu ze dne 28. 11. 2002, sp. zn. 3 Tdo 969/2002.

[108] Ačkoli trestní zákoník od doby spáchání trestného činu prošel novelou, která mj. pozměnila i znění daného paragrafu, použití a význam pojmu místo veřejnosti přístupné zůstalo zachováno, tudíž je citovaná judikatura nadále použitelná.

slušného ustanovení trestního zákoníku v případě všech typů zdravotnického zařízení, tedy bez ohledu na to, zda se jedná o zdravotnické zařízení soukromé či zřízené státem. Dle názoru soudu není ani určující, jaký je systém přijímání pacientů, tedy zda mohou vstoupit pacienti bez objednání či zda mají do objektu přístup výlučně ti se sjednanou schůzkou. Argumentoval tím, že zdravotní služby jsou poskytovány veřejnosti a té jsou prostory přímo určeny. Pacienty Nejvyšší soud vnímá jako blíže neurčenou, náhodnou množinu lidí, což v duchu dosavadní soudní praxe odpovídá definici veřejnosti. Ve svých předchozích soudních rozhodnutích soud již specifikoval, že místo veřejnosti přístupné nemusí být výhradně jen takové, které je přístupné v jakoukoli hodinu všem osobám. Postačí, aby výtržnost *„mohla být postřehnuta více lidmi“,* tedy pouhá možnost (potencialita) – lidé na daném místě nemusí být skutečně přítomni, případně i ve své přítomnosti nemusí výtržnost postřehnout. Proto se dle Nejvyššího soudu pod takové místo podřadí právě i čekárna.

Tím, co lze označit za místo veřejnosti přístupné, a co nikoli, se Nejvyšší soud zabýval opakovaně. Dalším příkladem takového judikátu je nedávné rozhodnutí sp. zn. 8 Tdo 838/2019,[109] kde soud znovu poukázal na skutečnost, že v místě veřejnosti přístupném nemusí být nikdo v čase spáchání trestného činu výtržnictví přítomen – postačí, když je přítomnost jiných, neurčených osob možná. V daném rozhodnutí hraje v kontextu tohoto příspěvku roli také prohlášení odvolacího soudu, dle nějž *„obviněný mohl očekávat výskyt dokonce i většího množství osob a kde nemohl očekávat soukromí“*. Nejvyšší soud tedy v uvedeném rozsudku reflektuje i zmiňovaný aspekt rozumného očekávaní soukromí. Pachatel podal dovolání, protože se domníval, že jím spáchané skutky se neodehrávaly na místech veřejnosti přístupných a že je tedy nelze kvalifikovat jako trestné činy výtržnictví. Soud se proto zabýval jednotlivými typy prostor a posuzoval, zda se jedná o místa veřejnosti přístupná, či nikoli. Jednalo se konkrétně o křoví v blízkosti parkoviště u benzínové čerpací stanice, zalesněný prostor, slepou uličku a lesopark. Ztotožnil se s názorem odvolacího soudu, že se jedná o místa veřejnosti přístupná, a nadto do této kategorie zařadil i nádražní haly,

[109] Usnesení Nejvyššího soudu ze dne 30. 7. 2019, sp. zn. 8 Tdo 838/2019.

tovární haly, staveniště, zdravotnická střediska a školy, prostor před vchodem do budovy a *„i prostory v osobním či soukromém vlastnictví, které nejsou samy o sobě považovány za místa veřejnosti přístupná, avšak bezprostředně sousedí s místem, kam veřejnost vstoupit může, např. dvory, pole nebo jiná prostranství, a je na ně nebo do nich přes nedostatečně izolující bariéru, např. průhledný plot, lešení, vidět, eventuálně je lze slyšet“.* Zároveň uvedl i demonstrativní výčet míst, jež veřejnosti přístupná nejsou – vnitřní části společných prostor bytů, tedy například chodba, schodiště, výtah.

Vedle toho zákon o Policii České republiky[110] a zákon o obecní policii[111] používají spojení místo veřejně přístupné, a to přímo v souvislosti se sledováním prostoru. Ministerstvo vnitra České republiky ve svém vyjádření k instalaci kamer ve veřejném prostranství uvádí snad jedinou „oficiální“ definici veřejného prostoru, kterým je *„místo, které může kdokoliv, kdykoliv, bez rozdílu a za víceméně jakýchkoliv okolností, navštívit. Tyto oblasti jsou pod správou veřejných autorit. Patří sem například veřejné parky, obytné ulice a ulice v centru města, parkoviště, stanice metra, sportovní prostranství.“*[112] Výčet je tedy o něco širší než (byť také demonstrativní) zákonná definice veřejného prostranství, ale také se odvíjí od kritéria přístupnosti. Komentář k § 86 občanského zákoníku pak uvádí, že „*[s]féra osobního soukromí se může podle okolností přenášet i na místa veřejně přístupná či do veřejných prostor*“,[113] z čehož by se čistě na základě jazykového výkladu dalo usuzovat, že místo veřejně přístupné a veřejné prostory jsou pojmy nezaměnitelné, a dokonce se nepřekrývající. Vhodnější by jistě byla alespoň změkčená formulace: „na místa veřejně přístupná či do *jiných* veřejných prostor“. Je tedy vidět, že nejasnost ve vztahu jednotlivých pojmů nemá jen zákonodárce. Mezi pojmy veřejné prostranství a místo veřejnosti přístupné mohou někteří vnímat citelnější rozdíl – veřejné prostranství zpravidla spíše nebude zahrnovat

[110] § 62 zákona č. 273/2008 Sb., o Policii České republiky.

[111] § 24b zákona č. 553/1991 Sb., o obecní policii.

[112] Kamerové sledování veřejných prostranství a institucí [online]. *Ministerstvo vnitra České republiky* [cit. 5. 9. 2021]. https://www.mvcr.cz/clanek/kamerove-sledovani-verejnych-prostranstvi-a-instituci.aspx

[113] Tůma. *Občanský zákoník I. Obecná část (§ 1-654),* pp. 509-524.

uzavřené prostory, především budovy,[114] ačkoli zákon toto kritérium (uzavření zdmi nebo plotem) nestanovuje.

V proticovidovém opatření zavedeném v minulém roce se vyskytl v souvislosti se zákazem pití alkoholu pojem „veřejně přístupné místo".[115] V původním usnesení vlády č. 407/2020 Sb. byl tento zákaz uveden bez dalšího. V upraveném usnesení č. 114/2021 Sb. se již objevil dodatek: *„tím není dotčena možnost pít alkoholické nápoje ve vnitřních prostorech provozoven stravovacích služeb"*. Z tohoto doplnění lze vyvodit, že vnitřní prostory provozoven stravovacích služeb jsou místem přístupným veřejnosti. Obdobně by bylo možné takto klasifikovat zřejmě většinu provozoven poskytovatelů služeb různého druhu a označit je tedy za místa veřejně/veřejnosti přístupná. Zároveň je však nutné vnímat jak aspekt soukromého vlastnictví, tak to, že i do těchto uzavřených prostor se promítají prvky soukromí a soukromého života jedince, například sociální složka.

Jednou z možností, a také velmi často užívanou metodou, jak ohraničit fyzický veřejný prostor, je vymezit jej proti prostoru soukromému. Tím je podle Ministerstva vnitra *„oblast, kam je přístup omezen zákonem, to znamená, že není přístupná všem. Moc veřejných autorit je v těchto místech omezena více než ve veřejných prostorách. Zároveň je to prostor, ve kterém je každý chráněn proti médiím, veřejným institucím a jiným lidem. Soukromá sféra zahrnuje právo každého jedince na vytvoření mezilidských vztahů s ostatními lidmi (zejména vytvoření, prohlubování a udržování citových vztahů), a také na fyzický a morální vývoj jedince, včetně jeho sexuálního života."*[116] Panuje obecná shoda na tom, že soukromým prostorem je hlavně, resp. minimálně obydlí. Avšak soukromý život se může odehrávat i mimo něj.[117] Soukromý prostor je tedy širším pojmem, který zahrnuje *„všechna taková účelově*

[114] Cf. Janečková, E., Bartík, V. *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti. Praktická právnická příručka.* Praha: Linde Praha, 2011, pp. 47-50.

[115] Což je sice téměř stejný, nicméně stále jiný pojem než „místo veřejnosti přístupné". Odlišovat tyto dva výrazy by zřejmě bylo přehnaně formalistické, na druhou stranu není důvod zavádět pro to samé nová označení.

[116] *Kamerové sledování veřejných prostranství a institucí* [online].

[117] Cf. například rozhodnutí ESLP ve věci *Halford v. the United Kingdom*: soukromý život se může odehrávat i na pracovišti.

způsobilá místa, kam se může člověk uchýlit před zájmem veřejnosti či okolí“.[118] Taková definice však plně nekoresponduje s tím, jak bývá vymezen veřejný prostor, respektive veřejné prostranství, neboť před zájmem veřejnosti se lze často uchýlit i na některá místa, která jsou sice běžně přístupná všem, ale přítomnost lidí na takových místech je spíše výjimečná, tudíž zde člověk teoreticky očekává soukromí poměrně důvodně, byť na ně nemůže spoléhat, respektive nemůže spoléhat na ochranu soukromí na těchto místech.

3.3 PROSTOROVÁ OCHRANA SOUKROMÍ

Optikou dichotomie platí pro soukromí ve veřejném prostoru následující: v soukromé sféře (v soukromém prostoru) má jednotlivec právo na soukromí. Kde končí soukromá sféra, končí i soukromí. Na první pohled někomu může připadat tento závěr zcela logický, někomu naopak zcela absurdní a nemyslitelný. V této části příspěvku bude pojednáno o tom, jak se soukromí, respektive právo na soukromí chová v prostoru, zda má nějaké hranice, případně čím jsou tyto hranice ovlivněny. Siebel upozorňuje na neustálou změnu vztahu soukromí k veřejnému prostoru spočívající v úměrném zmenšování se či zvětšování soukromí v závislosti na tom, „jak moc“ je daný prostor veřejný. Tato změna se dle Siebela promítá do všech oněch čtyř vymezených kategorií.[119]

Tradičním výchozím bodem pro prostorové vymezení soukromí je obydlí, v němž právo na soukromí dosahuje maximální intenzity. Proto je na místě analyzovat, kde má hranice takové obydlí. Je jím nejen nemovitost, k níž má člověk vlastnické právo, ale může se jednat i o jiný užívací titul (např. nájemní vztah, smlouva o ubytování, ať již na studentských kolejích či v hotelu, členové domácnosti atd.).[120] Nedotknutelnost obydlí je součástí práva na soukromí a chrání i prostory k němu náležející.[121] Ani v obydlí však právo na soukromí není absolutní, může být narušeno například při

[118] Tůma. *Občanský zákoník I. Obecná část (§ 1-654),* pp. 509-524.

[119] Popsané v první podkapitole, tedy legální, funkční, sociální a materiální. Siebel, Wehrheim. *Security and the Urban Public Sphere*, pp. 21-22.

[120] Kokeš, M. § 86. In: Petrov, J., Výtisk, M., Beran, V. et al. *Občanský zákoník, 2. vydání.* Praha: C. H. Beck, 2019, pp. 151-157.

domovní prohlídce.[122] Dle Šámalova výkladu k přípustnosti domovní prohlídky obydlím nejsou „jiné prostory“[123] (zpravidla nebytové prostory)[124] jako například kanceláře, skladiště, živnostenské provozovny nebo stojící garáže (ovšem jen za předpokladu, že nejsou součástí bytu),[125] případně lodě (ledaže se jedná o houseboat) a akademická půda vyjma studentských kolejí.[126] I v těchto prostorách nicméně jedinec požívá právo na ochranu soukromí, neboť jejich případné narušení dosahuje obdobné míry jako narušení obydlí.[127]

ESLP vykládá pojem obydlí široce v tom smyslu, že za něj považuje i „domov“ právnických osob, pod ochranu tedy zahrnuje také respektování soukromí sídla společnosti, poboček či provozoven právnických osob.[128] Obdobný závěr vyslovil ESLP ve svých rozhodnutích též pro kancelářské prostory.[129] V těchto prostorách český zákon chrání soukromí zaměstnance výslovně, a to v § 316 zákoníku práce.[130] Výjimku ze zákazu narušení soukromí zde tvoří závažné důvody spočívající ve zvláštní povaze činnost

[121] § 178 TZ. Obydlí je definováno § 133 TZ, přičemž výklad se prakticky shoduje s dále uvedeným komentářem k trestnímu řádu. Draštík, A., Fremr, R., Durdík, T., Růžička, M., Sotolář. A. et al. *Trestní zákoník. Komentář, I. díl.* Praha: Wolters Kluwer, a.s., 2015.

[122] Cf. nález Ústavního soudu ze dne 15. prosince 2015, sp. zn. I. ÚS 2024/15.

[123] § 82 odst. 2 trestního řádu.

[124] Shodně Draštík, A., Fenyk, J. et al. *Trestní řád. Komentář. I. díl.* Praha: Wolters Kluwer ČR, a.s., 2017, p. 716.

[125] Šámal, P. Růžička, M. In: Šámal, P. et al. *Trestní řád I. § 1 až 156. Komentář.* 7. vydání. Praha. C. H. Beck, 2013, pp. 1114-1115. Podle Klímy by zřejmě i tyto prostory byly součástí obydlí, cf. Klíma, K. et al. *Komentář k Ústavě a Listině.* 2. vyd. Plzeň: Aleš Čeněk, 2009, p. 1058.

[126] Draštík, Fenyk. *Trestní řád. Komentář. I. díl.*, p. 716.

[127] Nález Ústavního soudu ze dne 8. června 2010, sp. zn. Pl. ÚS 3/09.

[128] *Société Colas Est. v. France,* rozhodnutí Evropského soudu pro lidská práva, 16. 4. 2002 č. stížnosti 37971/97: Evropský soud pro lidský práva ve svém rozhodnutí ze dne 16. 4. 2002 ve věci Société Colas Est. proti Francii dospěl k závěru, že obydlí, tedy francouzsky *domicile*, jak je popsáno ve francouzském překladu článku 8 Úmluvy, je možné vykládat šířeji než domov, tedy anglicky *home*, a to například i na kancelář právnické osoby (*„professional person's office“*). Proto lze článek 8 Úmluvy aplikovat i na sídla společnosti a provozovny. Shodně také *Saint-Paul Luxembourg S.A. v. Luxembourg,* rozsudek Evropského soudu pro lidská práva, 18. 4. 2013 č. stížnosti 26419/10.

[129] *Crémieux proti Francii*, rozsudek Evropského soudu pro lidská práva, 25. 2. 1993 č. stížnosti 11471/85. Shodně též v rozsudku *Miailhe proti Francii*, rozsudek Evropského soudu pro lidská práva, 25. 2. 1993 č. stížnosti 12661/87.

zaměstnance. Ochrana se vztahuje na pracoviště i na společné prostory zaměstnavatele a jako jeden ze zakázaných prostředků narušení soukromí zákon uvádí sledování, a to jak otevřené, tak skryté. V nálezu sp. zn. II. ÚS 2334/08 Ústavní soud uvedl, že v kancelářských prostorách může člověk požívat a očekávat nižší míru soukromí, než které se mu dostává v jeho obydlí, neboť se jedná o prostory, jež jsou *„určeny k činnosti pracovní a jsou běžně přístupné ve vztahu k uživateli cizím osobám“*.[131] S tímto závěrem o přístupnosti kancelářských prostor cizím osobám lze ztotožnit jen pro vybraná zaměstnání a typy kancelářských prostor v závislosti na tom, kolika zaměstnanci jsou obývány, případně zda do kanceláře mají běžně přístup i osoby, které na daném místě zaměstnány nejsou.[132] Zatímco kancelář zaměstnance v advokátní kanceláři může sloužit téměř výhradně jemu, kancelář na pracovišti městské správy sociálního zabezpečení bude několikrát denně, zejména v úřední dny, navštěvována cizími lidmi, stejně tak kancelářské prostory typu „přepážek“ v bance, na poště apod. Nadto je pravděpodobné, že většina lidí bude jinak pociťovat narušení soukromí v kanceláři svými kolegy, ke kterým může mít bližší vztah (a narušení soukromí z jejich strany může důvodně očekávat), a jinak jej bude pociťovat ze strany cizích osob, jejichž přítomnost v daných prostorách primárně neočekává.

Ústavní soud ve svém nálezu sp. zn. Pl. ÚS 3/09,[133] kde čerpá z výše uvedených závěrů ESLP, odmítá koncepci, jež by nekompromisně odlišovala soukromý život odehrávající se v prostorách užívaných k bydlení od ochrany soukromí v pracovních prostorách.[134] Ústavní soud opírá svoji argumentaci o propojení soukromého života s pracovními (či zájmovými) aktivitami a dospívá k závěru, že *„nelze činit ostré prostorové oddělení soukromí v místech užívaných k bydlení od soukromí vytvářeného v místech a prostředí sloužících k pracovní či podnikatelské činnosti anebo*

[130] Blíže cf. rozsudek Městského soudu v Praze ze dne 2. 9. 2014, č. j. 8A 182/2010 - 69-77; rozsudek Městského soudu v Praze ze dne 27. 9. 2011, č. j. 6Ca 227/2008 - 71.

[131] Nález Ústavního soudu ze dne 24. září 2009, sp. zn. II. ÚS 2334/08.

[132] Cf. definici veřejného prostranství, místa veřejnosti přístupného.

[133] Nález pléna Ústavního soudu ze dne 8. června 2010, sp. zn. Pl. ÚS 3/09.

[134] *Ibidem,* bod 30.

k uspokojování vlastních potřeb či zájmových aktivit.“[135] Shodně ÚS rozhodl i ve svém nálezu sp. zn. II. ÚS 2048/09,[136] kde rovněž konstatoval, že *„pod ochranu práva na nerušený soukromý život spadá ve shodě s judikaturou Evropského soudu pro lidská práva též ochrana obydlí, tj. místa, kde osoba bydlí nebo vykonává svoji profesionální činnost.“*[137]

K obydlí mají nejblíže prostory nacházejících se těsně kolem něj – jsou jimi společné prostory bytových domů – chodby, sklepy, garáže, půdy apod. Zřejmě se lze shodnout na tom, že se nejedná o veřejný prostor, jak jej chápeme z definice veřejného prostranství, kterou nám poskytuje zákon, tzn. chodník, náměstí a podobně. Zároveň se však nejedná o obydlí ve smyslu ohraničeného fyzického prostoru obývaného rodinou. Ačkoli tedy nejsou veřejné, neboť nejsou přístupné všem, nemůžeme v těchto prostorách očekávat takovou míru soukromí jako v obývacím pokoji nebo ložnici. Jak uvádí Šimíček, chodby je navíc nutno od půd a sklepů odlišovat, neboť v chodbách se zpravidla pohybují i návštěvy, jedná se o prostory přístupné i relativně cizím lidem (nejen sousedům, ale také jejich návštěvám, případně pošťákovi, správci budovy apod.[138]

I kdyby bylo možné určit vnější hranici soukromého prostoru, právo na ochranu soukromí by za ní nekončilo. Ústavní soud konstatoval, že monitorování veřejného místa[139] kamerou je narušením práv zaručených čl. 10 LZPS a čl. 8 odst. 1 Úmluvy.[140] Rovněž Wagnerová[141] trefně poukazuje na to, že přístup, který by odmítal právo na soukromí ve veřejném prostoru, není zcela správný a neodpovídá potřebám dnešní doby. Možná by takové pojetí obstálo dříve, nicméně s vývojem moderních technologií je i ve veřejném prostoru potenciál narušení soukromí tak vysoký, že jej nelze

[135] *Ibidem.*

[136] Nález Ústavního soudu ze dne 2. listopadu 2009, sp. zn. II. ÚS 2048/09.

[137] *Gillow proti Spojenému království*, rozsudek Evropského soudu pro lidská práva, 24. 11. 1986 č. stížnosti 9063/80.

[138] Ryška, M. Ochrana vnitřního kruhu i jeho okolí v praxi práva na ochranu osobnosti. In: Šimíček. *Právo na soukromí,* pp. 89-90.

[139] Přičemž „veřejné místo“ opět není definováno.

[140] Nález Ústavního soudu ze dne 8. února 2010, sp. zn. IV. ÚS 2425/09.

[141] Wagnerová, *Listina základních práv a svobod: komentář*.

ignorovat a je nutné soukromí chránit i mimo soukromé prostory. Wagnerová proto tvrdí, že je nemyslitelné presumovat vzdání se práva na soukromí ohledně té části života, která se odehrává právě ve veřejném prostoru.[142]

V ryze soukromém prostoru zpravidla převáží právo na soukromí.[143] Čím „veřejnější" však prostor je, tím intenzivnější může být potenciálně dovolený zásah do našeho soukromí ve prospěch jiných práv. To však nutně nemusí znamenat, že se v ryze veřejném prostoru právo na soukromí zcela vytrácí. Ostatně ústavní pořádek nedefinuje, že by naše právo na soukromí bylo omezeno fyzickými hranicemi, za kterými by zcela ztrácelo na významu a zanikalo. Jisté prostorové ohraničení je nastíněno v § 86 OZ, dle nějž má jedinec právo na ochranu před narušením jeho soukromého prostoru, což může navozovat dojem, že za hranicemi soukromého prostoru již naše soukromí chráněno není, jedná se však pouze o demonstrativní výčet, dle nějž jsou soukromé prostory pouze jednou ze součástí soukromí. Zákon navíc pojem soukromý prostor nijak nedefinuje. Hirose je toho názoru, že jednotlivec opouštějící své obydlí neočekává, že se právě krokem přes práh zbavuje svého práva na soukromí. „Vystavením se na veřejnost" se člověk nezbavuje práva rozhodovat o tom, komu jsou jeho osobní údaje přístupné.[144] Jako příklad z praxe, který názorně demonstruje naši možnost rozhodovat o přístupu ostatních k našim osobním údajům, ačkoli se nacházíme ve veřejném prostoru, uvádí Hirose poučování dětí ze strany rodičů o tom, že cizím lidem nemají sdělovat své jméno, bydliště, telefonní číslo apod.[145] Někdo by mohl namítnout, že i kolemjdoucí o nás mohou nějaké osobní údaje získat – vzhled, zdravotní stav (jestliže navštěvujeme doktora nebo lékárnu) apod. Autor vyzdvihuje, že nejde o absolutní anonymitu, ale alespoň o minimální risk toho být rozpoznán nebo být nucen prokázat to-

[142] *Ibidem.*

[143] Ani v obydlí však neplatí, že právo na soukromí nemůže ustoupit – i v tom „nejsoukromějším" prostoru existují výjimky, kterou je například zmíněná domovní prohlídka.

[144] Hirose, M. Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology. *Connecticut Law Review*. 2017, vol. 49, n. 5, p. 1601.

[145] Cf. Nissenbaum. *Privacy in context,* p. 116.

tožnost, tedy se „identifikovat“ na veřejnosti.[146] Podobně tuto problematiku hodnotí i Nissenbaum, která hovoří o tzv. pravidlu knock-out. Jeho podstata tkví v tom, že vystavováním něčeho na veřejnosti automaticky člověk nepočítá s tím, že daná skutečnost nebo daný fakt má být znám každému, a to i přesto, že přijímáme riziko, že alespoň někdo může danou skutečnost zpozorovat, dané údaje získat.[147] Nissenbaum zmiňuje také přirovnání, které představil Larry Hunter: pokud se nám někdo z ulice bude dívat do oken, budeme to považovat za narušení soukromí. Pokud se však my díváme z okna na lidi na ulici, jako narušení soukromí to zpravidla vnímáno není. I ve veřejném prostoru tedy existuje určitý balanc – ačkoli v něm soukromí zcela neztrácíme, akceptujeme jeho určité nezbytné omezení.[148] Výstižně tuto skutečnost popisuje také Nissenbaum: když opustíme naše obydlí a vyjdeme ven na ulici, která je nepochybně výlučně prostorem veřejným, nemáme povinnost komukoli odpovídat na otázky týkající se našeho jména, zaměstnání, rodiny a jiných osobních informací.[149]

Soukromí tedy prostorem postupně prostupuje od nejvyšší intenzity, které dosahuje v obydlí, k intenzitě nižší. Díky těmto pomyslným „odlupujícím se vrstvám“ autoři přirovnali tento jev k tzv. cibulovému modelu – *Zwiebelmodelle.*[150]

3.4 DÍLČÍ ZÁVĚR

Ačkoli se autoři v odborné literatuře snaží vymezit veřejný prostor v kontrastu se soukromým, v praxi toto odlišení velký význam nemá. Nepoužívá jej ostatně ani český právní řád. Je zajímavé, že ačkoli se v publikacích pojmy veřejný prostor a soukromý prostor běžně vyskytují, málokdo se je ve svém výkladu snaží definovat, jako by považoval za automatické, co

[146] Hirose. *Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology*, p. 13*: „with the minimal risk of being recognized and of being required to identify ourselves in public.“*

[147] Nissenbaum, p. 114-115.

[148] *Ibidem:* Hunter, L. Public Image: Privacy in the Information Age. *Whole Earth Review.* 1985, vol. 44, pp. 32-37.

[149] Nissenbaum, p. 116.

[150] Koops, Newell, Timan, Škorvánek, Chokrevski, Galič. A *Typology of Privacy*, p. 546.

do těchto kategorií patří, nebo možná právě proto, že je tato striktní klasifikace poměrně obtížná. Madanipour vidí v kategorizaci prostoru přímý vztah k vlastnictví. Ačkoli je to jedno z možných pojetí, neodpovídá potřebám ochrany soukromí tak, jak ji vykládají soudy, které přiznaly ochranu soukromí jedince i ve vozidle, které patřilo někomu jinému. Rozhodovací praxi naopak odpovídá jeho model, dle nějž majitel soukromého prostoru může určit, kdo jej využívá a jakým způsobem. Koops si dokonce klade otázku, zda je nadále možné soukromý a veřejný prostor rozlišovat.[151] Pravdou je, že za použití jakéhokoli kritéria pro vymezení soukromého a veřejného je nutné dospět k závěru, že soukromí se bude prolínat oběma těmito sférami a že ve veřejné sféře nelze právo na soukromí odepřít a tato dichotomie vlastně není opravdovou dichotomií.

V popisu veřejného a soukromého prostoru, který uvádí Ministerstvo vnitra a který je jedním z mála českých konkrétnějších vymezení, se nacházejí kritéria, na jejichž základě by bylo možné povahu prostoru posuzovat a která se zrcadlí v obou definicích: jsou jimi přístupnost a držitel moci v dané sféře. Přístupnost jako kritérium neobstojí například ve školách a společných částech bytového domu. Zpravidla je na těchto místech totiž omezený okruh osob, které do objektu mohou, respektive by měly vstoupit, na druhou stranu tento okruh nelze jednoznačně identifikovat, neboť se může neustále měnit (ve školách to mohou být například blíže neurčení potenciální zájemci o studium, studenti se v průběhu času mění, ve společných částech bytového domu půjde o návštěvy). Kritérium držitele moci rovněž nemusí být určující. Ačkoli vlastnictví není nezbytnou podmínkou požívání soukromí v daném prostoru, v určitých objektech mimo sféru moci veřejné soukromí nemůžeme očekávat právě proto, že jsou ve vlastnictví jiných, byť soukromých osob, a může se přitom jednat o místa veřejnosti přístupná, jako jsou již dříve zmíněné provozovny služeb – kadeřnictví, restaurace, obchody apod.

Český právní řád používá několik pojmů, jež mají společný kořen. Veřejné prostranství definuje zákon, místo veřejně přístupné bylo několikrát popsáno v judikatuře. Vztah těchto pojmů je však nejasný. Veřejný prostor

[151] Koops. *On legal boundaries, technologies, and collapsing dimensions of privacy,* p. 248.

bude zřejmě pojmem nejširším. Oficiální definice není známa ani u prostoru soukromého, jehož centrem je však nepochybně obydlí.

Ačkoli tedy soukromí nepochybně prostorový aspekt má, paradoxně zároveň není možné jej prostorově ukotvit. Soukromí tedy nelze „umístit" pouze do určitého prostoru s tím, že pouze v něm by soukromí nemělo být narušeno a za jeho hranicemi by právo na soukromí pomíjelo.[152] Intenzita ochrany soukromí bude postupně ustupovat v závislosti na vzdálenosti od obydlí, avšak nikdy ji nelze pominout a bez dalšího upozadit ve prospěch jiného práva.

4. KAMEROVÝ DOHLED

"*You are on a video camera an average of ten times a day. Are you dressed for it?"*[153]

Ačkoli se nejedná o pojem tak kontroverzní jako soukromí, ani *surveillance,* anglický ekvivalent pro dohled nemá zcela vyjasněnou definici, a to právě díky nástupu technologií. Oxfordský slovník popisuje *surveillance* jako blízké pozorování, zejména podezřelých špionů nebo zločinců.[154] Marx ve své práci uvádí, proč tato definice v dnešní době neobstojí, a to v každém jejím prvku.[155] Jeho kritiku je možné demonstrovat na kamerovém sledování: primárně totiž směřuje proti okruhu osob, jichž se sledování týká. Všudypřítomné kamery, instalované především z důvodu prevence, snímají jak podezřelé, tak osoby nevinné, respektive nepodezřelé. Nastavení kamery totiž zpravidla nezajišťuje filtrování a sledování výlučně potenciálně nebezpečných lidí.[156] Dále Marx poukazuje na to, že se nemusí jednat ani

[152] Shodně též Koops. *On legal boundaries, technologies, and collapsing dimensions of privacy,* p. 257.

[153] Milligan. *Facial Recognition Technology, Video Surveillance, and Privacy*, p. 295.

[154] Soanes, C., Stevenson, A. *Concise Oxford English Dictionary*. Oxford: Oxford University Press. 2006, p. 1451.

[155] Marx, G. T. *What's New About the "New Surveillance"?: Classifying for Change and Continuity*, p. 20.

[156] Konzultace s p. Davidem Střelcem: Kamery jsou však např. schopny rozeznat určité nežádoucí, respektive podezřelé jevy u sledovaných osob, například takzvané „zevlování", rychlý úprk apod.

o dohled prováděný zblízka, ani nemusí být pouze vizuální.[157] Přichází tedy s moderněji orientovaným pojmem *new surveillance*, jenž odpovídá využití technických prostředků za účelem sběru nebo vytváření osobních údajů.[158] Použitelná je však v dnešní realitě i definice, kterou vytvořil Clarke již roku 1997.[159] Dle něj je dohled systematickým monitorováním činností nebo komunikace osob.

Boal uvádí, že kamerové sledování odpovídá naší touze upírat na někoho náš pohled a současně touze, aby na nás byl pohled upírán.[160] V následující části příspěvku budou teoretické poznatky demonstrovány na kamerových systémech, do nichž je možné integrovat různé doplňkové funkce, z nichž nejzákladnější je vedle pořizování videozáznamu pořizování rovněž audiozáznamu a rozpoznávání obličeje.[161] Komplexnost této technologie umožňuje fundovanější, ucelenější zásah do soukromí jedince[162] například ve srovnání s GPS lokátorem, který je schopen zachytit pouze polohu jedince.[163] V Česku kamery disponují v převážné většině pouze základní funkcí, tedy snímáním obrazu, v menšině případů pak případně i možností pořízení audiozáznamu. Rozpoznávání obličejů by v současné době v českých podmínkách neobstálo.[164]

---

[157] Marx, Gary T. *What's New About the "New Surveillance"?: Classifying for Change and Continuity*, p. 20.

[158] *Ibidem.*

[159] Introduction to Dataveillance and Information Privacy, and Definitions of Terms [online]. *Xamax Consultancy Pty Ltd.* 1995-2021. [cit. 20. 9. 2021]. http://www.rogerclarke.com/DV/Intro.html Clarke navíc místo pojmu *surveillance* zavedl výraz *dataveillance.*

[160] Boal, M. SpyCam City [online]. *Village Voice, LLC* [cit. 20. 9. 2021]. https://www.villagevoice.com/1998/10/06/spycam-city/ : *„… to gaze and to be gazed upon.“*

[161] Aronov. *Privacy in a Public Setting: The Constitutionality of Street Surveillance*, p. 775: Proces rozpoznávání obličejů Rita Aronov přirovnává ke snímání čárových kódů.

[162] K podobnému závěru dochází též Aronov. *Privacy in a Public Setting: The Constitutionality of Street Surveillance*, p. 770: *“Although street surveillance is not a new phenomenon, technological advances of the last several years have made it increasingly easier, cheaper, and more pervasive.”*

[163] I GPS lokátor má potenciál způsobit citelnější zásah do soukromí, avšak dále v kombinaci s jinými daty z jiných databází (např. i kamerových) – stejné propojení databází je však možné i u dat získaných z kamer. Pokud odhlédneme od tohoto aspektu a zaměříme se čistě na povahu a objem dat, které je schopno to které zařízení zpracovávat, pak je dozajista citelnější zásah právě kamerový.

[164] Konzultace s p. Nonnemannem.

Někdo by mohl namítnout, že kamera nevidí nic jiného, než co může vidět jakýkoli jiný kolemjdoucí, a tudíž nezáleží na tom, zda je nainstalovaná, či nikoli. Proti takovému tvrzení však existuje několik argumentů: jako první z nich poslouží anonymita – ve veřejném prostoru člověk zpravidla spoléhá na to, že si ho ostatní nebudou všímat, i když by mohli. Jestliže je však v prostoru nainstalovaná kamera, pak je jisté, že přítomnost člověka bude vždy snímána alespoň jedním okem.[165] Další důvod, proč je potřeba na sledování technologickými prostředky nahlížet jinak než na sledování člověkem, je popsán v rozsudku *United States v. Maynard*, v němž soud upozornil na významný rozdíl mezi jednorázovým nahodilým sběrem dat o člověku ze strany jiné fyzické osoby a systematickým dlouhodobým sledováním.[166] Někdo přesto zaujímá ke kamerám laxní postoj s tím, že nemá co skrývat. Tento argument však Solove[167] smetl ze stolu hned několika výstižnými poznatky:

"So do you have curtains?"

" I don't have anything to hide. But I don't have anything I feel like showing you, either."

"If you have nothing to hide, then you don't have a life."

"It's not about having anything to hide, it's about things not being anyone else's business."[168]

I kdyby ale obstál argument, že jedinec nemá co skrývat, a tudíž mu nevadí být sledován, je nutné vzít v úvahu ještě jeden následek, který s sebou kamerové sledování nese, a tím je, často podvědomá, změna chování jedince, který je pod dohledem[169] (tzv. *chilling effect*).[170] Jestliže člověk ví, že je nebo může být sledován, chová se jinak, než kdyby tento – byť jen

[165] Cf. dříve zmiňované rozhodnutí Nejvyššího soudu, sp. zn. 8 Tdo 838/2019; Bude záviset na typu kamerového systému, zda bude záznam vždy někým sledován v reálném čase, nebo zda k němu bude přistoupeno až v případě informace o indicentu.

[166] *United States v. Maynard,* rozsudek Nejvyššího soudu Spojených států amerických, 6. 8. 2010 č. 615 F.3d 544.

[167] Solove, D. J. *Nothing to Hide: the False Tradeoff between Privacy and Security.* New Haven: Yale University Press, 2011, p. 23.

[168] Pokud by někdo i přes tyto argumenty pochyboval o tom, že sledování může mít vliv na jeho život a chování, nelze než doporučit film Truman Show z roku 1998, který možná předběhl svou dobu a v jistých ohledech není daleko od dnešní reality.

potenciální – prvek byl z rovnice odstraněn. Tento jev popsal již Jeremy Bentham, který na základě stejné myšlenky navrhnul věznici s kruhovým půdorysem a věží pro dozorce umístěnou uprostřed tak, aby mohli sledovat všechny cely a zároveň sami nebyli spatřeni vězni, jejíž koncept vešel ve známost jako panopticon.[171] Vězení sice představuje uzavřený prostor, který není bez dalšího veřejnosti přístupný, nicméně fenomén, který Bentham aplikuje, nemá menšího významu v prostoru ryze veřejném. Využil tak efektu, kdy se lidé chovají „poslušněji", jestliže u nich panuje obava z toho, že je někdo vidí, sleduje, nebo alespoň sledovat může. K fungování tohoto sociologicko-psychologického jevu postačí potenciální riziko být sledován. Podstata tkví totiž také v tom, že objekty nejsou schopny určit, zda jsou sledovány, případně kdo sledování provádí, respektive nemají možnost dozorce vidět. Chovají se tedy poslušně, protože je výhodnější počítat s variantou, že jsou pod dohledem. Benthamova iniciativa a vzniklý panopticon byly jedněmi z vůbec prvních výrazných projevů teoretického pojetí *surveillance*, které časem nabývaly na významu.[172] Pojem panopticon se následně stal prakticky synonymem pro *surveillance*.[173] Nyní je skloňován právě také v kontextu sledování za pomocí moderních technologií. Připodobnění není nedůvodné, neboť například takovou přítomnost kamer si mnohdy jedinec ani neuvědomí, navíc zpravidla ani neví, „kdo za kamerou sedí", případně zda právě záznam, který je pořizován ve chvíli, kdy se zrovna nachází v hledáčku objektivu, bude později někým viděn, přehráván nebo dále využit. Takové monitorování tedy svojí teoretickou podstatou poměrně přesně odpovídá právě systému, na jakém funguje vězení panopticon.

---

[169] Kundera, M. *Les testaments trahis,* pp. 311-312; nebo také Pokyny 3/2019, p. 5: *„Rozsáhlé zavádění takových nástrojů ve značné míře v mnoha oblastech života vystaví jednotlivce dalšímu tlaku, pokud jde o zabránění odhalení toho, co by mohlo být vnímáno jako odchylka."*

[170] Hermstrüwer, Y., Dickert, S. *Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten*. Rochester, NY: Social Science Research Network, 2013, p. 2.

[171] Bentham, J. Panopticon or the Inspection House. In: Bowring, J. (ed.). *The Works of Jeremy Bentham.* London: Simpkin, Marshall, & Co., 1843, p. 40.

[172] Timan, T. Galič, M. Koops, B.-J. Surveillance Theory and Its Implications for Law. In: Brownsword, R. Scotford, E. Yeung, K. (eds). *The Oxford Handbook of Law, Regulation, and Technology*. Oxford: Oxford UP, 2017, p. 733.

[173] *Ibidem.*

Podobně jako Bentham smýšlel také Michel Foucault, dle něhož je sledování společnosti klíčovým nástrojem pro její organizování.[174] Pozorování jedinců vnímal jako prostředek k dosažení sociální soudržnosti a koherence, která se formuje na základě psychologických vzorců a myšlení jedince. Na obdobném základu změny chování staví také Madanipour, který tvrdí, že lidé si ve veřejném prostoru nasazují „masku“,[175] aby vyhověli většinovým společenským normám, jejichž dodržování se očekává. Toto alter ego však neodráží realitu, tedy přirozené chování jedince neovlivněné rizikem sledování. Gumpert a Drucker dokonce tvrdí, že přítomnost kamer odrazuje lidi od využívání veřejného prostoru.[176] Milligan nadto poznamenává, že *surveillance* se stává akceptovanou skutečností,[177] „nezbytným zlem“ pro to, aby bylo dosaženo vyššího účelu – bezpečnosti,[178] a poukazuje na to, že přikládat soukromí ve 21. století význam může být vnímáno jako nepopulární postoj.[179] Být sledován a mít méně soukromí je dnes do určité míry bráno jako norma, lidé jsou s touto skutečností smíření, zmenšuje se míra rozumného očekávání soukromí a lidé nejsou otevřeni úvahám, zda je takové sledování vůbec v pořádku, neboť je pasivita a ignorace potenciálního problému jednodušší.[180] Frank La Rue zastává názor, že *surveillance* by měla být státy považována za činnost vysoce narušující soukromí lidí, která ústí

[174] Foucault, M. *Dozerať a trestať: Zrod väzenia.* 2. vyd. Bratislava: Kalligram, 2004, pp. 196-230.

[175] Madanipour. *Public and Private Spaces of the City,* p. 205.

[176] Gumpert, Drucker. *Public boundaries: Privacy and surveillance in a technological world,* p. 117.

[177] Shodně též Kasl, F. *Povaha zásahu do informačního soukromí člověka,* p. 674; shodně také Stuart, A., Levine, M. Beyond ‘nothing to hide’: When identity is key to privacy threat under surveillance. *European Journal of Social Psychology.* 2017, vol. 47, n. 6, p. 695. Pokyny 3/2019 k tomu na straně 6 uvádí, že pokud by se kamerový dohled stal normou, pak bychom riskovali *„změnu kulturních norem, která povede k akceptování nedostatku soukromí jako obecného předpokladu“*.

[178] K akceptování sledování na úkor naší svobody shodně též Hansen, M. No Place to Hide: If crime is everywhere, so, too, may be police surveillance cameras and contraband detection devices to combat it. But who's looking out for privacy rights? *ABA Journal*. 1997, vol. 83, n. 8, p. 45; také Rauhofer, J. Privacy Is Dead, Get over It: Information Privacy and the Dream of a Risk-Free Society. *Information & Communications Technology Law*. 2008, vol. 17, n. 3, p. 186.

[179] *„Those who value privacy are laughed off as privacy freaks or dangerous kooks.“* Milligan. *Facial Recognition Technology, Video Surveillance, and Privacy,* p. 297.

v *„psychological state of discomfort“*, a to i v případě, že ji lidé již pasivně přehlíží.[181]

Dohled v pojetí Benthama má za cíl, stejně jako kamerový dohled, přimět jedince pod hrozbou sankce, aby se chovali dle (zákonných) pravidel.[182] Nemá tedy význam pouze při zpětné identifikaci pachatele, ale též plní funkci preventivní. Instalaci kamer na pracovišti zaměstnavatelé odůvodňují také s odkazem na efektivitu zaměstnanců,[183] nicméně tento účel by sám o sobě zřejmě neobstál ani v testu proporcionality, ani jako účel pro zpracování dat podle GDPR.[184]

4.1 PRÁVNÍ RÁMEC KAMEROVÉHO SLEDOVÁNÍ

V Česku neexistuje zákon, který by byl primárně přijat za účelem všeobjímající úpravy problematiky kamerového sledování, jako je tomu například v Belgii.[185] Relevantní právní úprava v podstatě odpovídá té, která byla zmíněna v teoretické části,[186] k tomu však přibývají předpisy upravující zpracování osobních údajů.

Česko je vázáno mezinárodní Úmluvou o ochraně osob se zřetelem na automatizované zpracování osobních dat,[187] jejíž základní principy se promítají do předpisů přijatých na úrovni EU.[188] První dva, respektive tři jsou na evropské úrovni a jsou jimi nařízení GDPR, které doprovází Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky,

[180] Heumann, M. et al. Privacy and Surveillance: Public Attitudes on Cameras on the Street, in the Home, and in the Workplace. *Rutgers Journal of Law and Public Policy*. 2016, vol. 14, n. 1, p. 42-43.

[181] Gumpert, Drucker. *Public boundaries: Privacy and surveillance in a technological world,* p. 117.

[182] Timan, Galič, Koops. *Surveillance Theory and Its Implications for Law*, p. 738.

[183] Heumann. *Privacy and Surveillance: Public Attitudes on Cameras on the Street, in the Home, and in the Workplace,* p. 45.

[184] Cf. Pokyny 3/2019, p. 5: ke zpracování osobních údajů prostřednictvím videotechniky v úvodu v bodě 2 výslovně uvádí, že sledování výkonnosti zaměstnanců je právě jedním z účelů sledování, kterému je třeba zabránit.

[185] V Belgii byl pro tyto účely přijat *Loi réglant l'installation et l'utilisation de caméras de surveillance, doss. N°2007-03-21/39* (*loi caméras).*

[186] K provozování kamerových systémů [online]. *Úřad pro ochranu osobních údajů* [cit. 14. 8. 2021]. https://www.uoou.cz/k-provozovani-kamerovych-systemu/d-29535

a směrnice o ochraně údajů v oblasti prosazování práva.[189] GDPR s pojmem soukromí nepracuje, nicméně skrze ochranu osobních údajů přispívá i k ochraně (informačního) soukromí. Tuto spojitost odráží fakt, že i v teoretické rovině se složky ochrany soukromí a osobních údajů vzájemně prolínají a doplňují, o to více pak s přihlédnutím k využití technologických prostředků.[190] Zásah do soukromí, pokud je nezbytný (a dovolený), má probíhat v co nejmenším možném rozsahu. Stejná zásada se projevuje i v GDPR, a to v několika rovinách, přičemž tyto roviny jsou omezeny účelem zpracování údajů.[191] První rovinou je již samotný sběr dat. Primárně by ke zpracování osobních údajů vůbec nemělo docházet, pokud to není k naplnění účelu potřeba, respektive pokud je možné ho dosáhnout jiným způsobem, který je vůči soukromí méně invazivní. To znamená, že pokud je zabezpečení nějakého objektu v dostatečné míře možné docílit instalací zámku, plotu nebo jiného bezpečnostního prvku, který například fyzicky znesnadňuje vstup do objektu, pak je třeba dát těmto alternativám přednost před využitím kamerového systému. V případě, kdy ke sběru dat dochází, má být shromážděno jen takové množství a druh osobních údajů, jež jsou nezbytně nutné pro dosažení účelu. Tento přístup k ochraně dat je zastřešen zásadou minimalizace údajů.[192] Ke zpracování získaných údajů může docházet pouze po nezbytně nutnou dobu, která je opět vymezena

[187] Sdělení Ministerstva zahraničních věcí č. 115/2001 Sb. m. s., o přijetí Úmluvy o ochraně osob se zřetelem na automatizované zpracování osobních dat. Následně byla revidována s ohledem na technologický vývoj, cf. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data [online]. *Council of Europe* [cit. 18. 10. 2021]. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

[188] Míšek, J. *Osobní údaje v čase a prostoru.* 2020, p. 41. Právní úprava na unijní úrovni vychází ze závazku států plynoucího z čl. 16 Smlouvy o fungování Evropské unie, který každému zaručuje právo na ochranu osobních údajů.

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

[190] Kasl, F. *Osobnost, soukromí a osobní údaje v moderní společnosti,* p. 401.

[191] Tzv. účelové omezení, článek 5 odst. 1 písm. b) GDPR.

[192] Článek 5 odst. 1 písm. c) GDPR.

naplněním účelu, tedy v souladu se zásadou omezení uložení.[193] GDPR samozřejmě poskytuje vícero pravidel relevantních pro zpracování osobních údajů při provozování kamerových systémů – za tímto účelem bylo ostatně také nařízení přijato. Ta výše zmíněná byla vybrána pro ilustraci spojitosti ochrany soukromí a ochrany dat, jež jsou obě ovlivněny principem proporcionality zásahu. Cílem tohoto článku však není analýza tohoto nařízení, ale posouzení významu odlišení soukromého a veřejného prostoru. Na tomto místě stojí za zmínku věcná působnost nařízení, ze které je vyloučeno takové zpracování osobních údajů, které provádí fyzická osoba *„ v průběhu výlučně osobních či domácích činností“*.[194] Věcná působnost nařízení sice není založena na odlišení prostoru, osobní a domácí činnost se nutně nemusí odehrávat v obydlí, ale dichotomie se zde promítá do účelu zpracování, jenž byl převzat ze 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. Prostorový aspekt však prozařuje i do účelu zpracování, jak dokládá rozsudek SDEU ve věci C-212/13, František Ryneš proti Úřadu pro ochranu osobních údajů.[195] Ryneš měl za účelem ochrany majetku na vlastním domě nainstalovanou kameru, jež zabírala také část veřejného prostranství. SDEU dospěl k závěru, že takové sledování není zpracováním osobních údajů výlučně pro osobní a domácí potřebu s tím, že tuto výjimku je nutno vykládat restriktivně. Ke zpracování údajů v daném případě totiž docházelo mimo soukromou sféru jedince právě proto, že kamera zabírá i část veřejného prostranství.[196]

Doprovodné Pokyny 3/2019 se detailně zaměřují na zpracování údajů, k němuž dochází při použití videotechniky. Představují praktický návod, jak aplikovat principy a povinnosti vyplývající z GDPR na kamery. Také

[193] Článek 5 odst. 1 písm. e) GDPR.

[194] Článek 2 odst. 2 písm. c) GDPR.

[195] Rozsudek Soudního dvora Evropské Unie ze dne 11. 12. 2014 ve věci C-212/13. Spor byl řešen za účinnosti předchozí právní úpravy, účelové vymezení působnosti však v GDPR zůstalo, proto je závěr stále relevantní.

[196] Shodně cf. Míšek, J. Kauza Ryneš. *Revue pro právo a technologie*. 2015, vol. 6, n. 11, p. 67.

rozlišují použití videotechniky *„ v prostorech soukromé osoby“,*[197] které sice blíže nedefinují, ale taková klasifikace je jednodušší než vymezit, zda se jedná o „soukromý prostor“. Obchod je totiž zcela jistě prostorem ve vlastnictví soukromé osoby, avšak na jeho zařazení do soukromého nebo veřejného prostoru nemusí panovat shoda.

Na národní úrovni je GDPR provedeno zákonem č. 110/2019 Sb., o zpracování osobních údajů, který nahradil zákon č. 101/2000 Sb., o ochraně osobních údajů. Se zrušením registrační povinnosti kamerových systémů, která byla zákonem o ochraně osobních údajů zakotvena, se zvyšuje potenciál jejich neoprávněného provozu, neboť ke kontrole oprávněnosti provozu kamerového systému dochází případně až *ex post.*

4.2 PROVOZ KAMEROVÉHO SYSTÉMU A OCHRANA SOUKROMÍ

“*The darkest (or, to some, brightest) scenario is to collect all possible data on all events everywhere on everyone and everything forever.”*[198]

Ochrana soukromí při kamerovém sledování se v mnohém projevuje v technických a provozních parametrech. Některé kamerové technologie, které byly vyvinuty za účelem skenování SPZ, umí skenovat také domácnosti a kanceláře v blízkosti dopravních tepen, jež jsou hlavním cílem sledování,[199] u kamer nainstalovaných na ulici je riziko snímání soukromých pozemků.[200]

Mezi relevantní parametry, jež ovlivňují míru zásahu do soukromí sledovaných osob, patří:

a) typ zpracovávaných údajů,
b) záznam,
c) obsluha,
d) trvalý/“*ad hoc*“ dohled,

[197] Pokyny 3/2019, p. 8, bod. 13.

[198] Timan, Galič, Koops. *Surveillance Theory and Its Implications for Law*, p. 740.

[199] Slobogin, Ch. Public Privacy: Camera Surveillance of Public Places And The Right to Anonymity. *Mississippi Law Journal.* 2002, vol. 72, n. 1, p. 221.

[200] Gumpert, Drucker. *Public boundaries: Privacy and surveillance in a technological world,* p. 122.

e) rozsah snímaného prostoru.[201]

Ad a). Při posuzování kamerových systémů je nezbytné věnovat pozornost tomu, zda jsou schopny zpracovávat údaje spadající pod zvláštní kategorie osobních údajů.[202] Těmi nejsou jen biometrické údaje,[203] ale také údaje o politickém či náboženském přesvědčení, rasovém a etnickém původu apod. Jejich zpracování totiž GDPR obecně až na přísně vymezené výjimky zakazuje. Rasový či etnický původ může být zpravidla z kamerového záznamu poznat, nicméně pokud by bylo toto kritérium bráno v potaz jako zásadní, pak by nebyl v souladu se zákonem téměř žádný provoz kamerového systému. Proto se hledí spíše na účel a následné nakládání s osobními údaji. Pokud tedy není kamera instalována přímo za účelem sběru biometrických údajů, pak není nutné k předmětnému článku GDPR přihlížet. Obdobně to platí o údajích o zdravotním stavu.[204] Ten je třeba zohlednit zejména při sledování v nemocnicích, čekárnách, lékárnách, chodbách v budovách, kde sídlí psycholog či psychiatr apod. Ochrana soukromí se v těchto případech projeví například kratší dobou uložení kamerového záznamu, vyšším technickým zabezpečením atp.[205] Obdobně se bude postupovat v případě monitorování škol. Zvláštní kategorie osobních údajů týkající se žáků se sice neliší od jiných subjektů údajů přímo z jejich postavení jako žáků, resp. dětí, nicméně plyne z něj obecný požadavek na citlivější zacházení

[201] Konzultace s p. Střelcem.

[202] Článek 9 GDPR.

[203] Těmi se dle čl. 4 bodu 14 GDPR myslí *„osobní údaje vyplývající z konkrétního technického zpracování týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňuje nebo potvrzuje jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje“*.

[204] Konzultace s p. Nonnemannem. Lze nabýt dojmu, že by snad tato speciální úprava dopadala na každý kamerový systém, který umožňuje identifikaci osoby, cf. Rafajová, M., Váryová, L. *Biometrické osobné údaje podľa GDPR (biometrický podpis, kamerový systém)*. Praha: Leges, 2019, p. 52. Takto široký výklad článku 9 GDPR je však v praxi nerealizovatelný a není v souladu s účelem tohoto ustanovení. Zároveň pomocí argumentace a *maiore ad minus* nelze aplikovat výjimku *zjevného zveřejnění* dle odst. 2 písm. e, neboť ani účast na demonstraci není zjevným zveřejněním politických názorů, tudíž ani pohyb po ulici nemůže být zjevným zveřejněním dílčích biometrických údajů, příp. jiných údajů ze zvláštní kategorie osobních údajů, blíže Uřičař, M., Rámiš, V. et al. *Obecné nařízení o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2021, p. 394.

[205] Konzultace s p. Nonnemannem.

s osobními údaji,[206] a proto obdobná technická opatření budou na místě i v tomto případě.[207] Největší roli v rámci čl. 9 GDPR tedy mohou hrát biometrické údaje, k jejichž nejintenzivnějšímu zpracování dochází při využití funkce rozpoznávání obličejů. V Česku by kamery touto funkcí zpravidla vybaveny být neměly,[208] proto tato oblast v kontextu příspěvku nemá tak velký význam. Nehrozí tedy (nebo alespoň prozatím), že by nastala situace, respektive režim, který je v současné době zaveden v Číně.[209]

Ad b) + c). O tom, že provoz běžného kamerového systému se záznamem je zpracováním osobních údajů ve smyslu GDPR, není pochyb.[210] Spousta kamerových systémů sleduje pouze dění pouze v reálném čase (*real-time monitoring*) a neukládá záznam.[211] Takové systémy zpravidla narušují soukromí méně invazivním způsobem než ty, které záznam uchovávají, ale není to pravidlem; odvíjí se to od obsluhy u obrazovek a od následného nakládání s údaji.[212] Každopádně nejsou zcela bez rizika – i živé sledování, respektive osobní údaje v něm zaznamenané lze totiž zneužít. Objevují se názory, že tyto systémy nezpracovávají osobní údaje právě proto, že nepořizují záznam.[213] To však není pravda, protože ve smyslu GDPR je i samotný sběr, respektive zaznamenání dat jejich zpracováním *(lato sensu)*.[214] Takové systémy navíc zpravidla nebývají bez obsluhy, která následně může uložená

[206] Cf. článek 6 odst. 1 písm. f GDPR.

[207] Shodně též konzultace s p. Střelcem.

[208] Konzultace s p. Nonnemannem. V českých podmínkách by využití této funkce spíše neobstálo. K jejímu zavádění se dlouhodobě negativně staví i Úřad pro ochranu osobních údajů, stejně jako jiné autority. Podobný postoj zaujal v posledních dnech také Evropský parlament, z čehož lze dovodit, že budoucí tendence k využívání rozpoznávání obličejů budou spíše pasivní. Blíže cf. Lomas, N. European Parliament backs ban on remote biometric surveillance [online]. *Verizon Media* 2021. [20. 10. 2021]. https://techcrunch.com/2021/10/06/european-parliament-backs-ban-on-remote-biometric-surveillance/, respektive nezávazná rezoluce Evropského parlamentu dostupná z https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance .

[209] Ke shodnému závěru dospěl i Kasl při porovnávání českých a čínských podmínek pro využití funkce rozpoznávání obličejů, cf. Kasl, F. Surveillance in digitalized society: the Chinese social credit system from a European perspective. *The Lawyer Quarterly*. 2019, vol. 9, n. 4, pp. 349-358.

[210] Městský soud v Praze, 11 Ca 433/2008.

[211] Konzultace s p. Střelcem.

[212] Cf. Pokyny 3/2019, p. 11, bod 29.

data zpracovávat i *stricto sensu*. Proto je zapotřebí i tento způsob monitorování podřadit do působnosti GDPR, k čemuž oproti bývalé praxi zřejmě spěje již i ÚOOÚ.[215] Pořizování nebo nepořizování záznamu však nemusí vždy odpovídat nepřítomnosti nebo přítomnost obsluhy. I *real-time* monitorovací zařízení může ukládat záznam – v takovém případě nemusí být přenos vždy zároveň pod trvalým dohledem.[216] V případě, že kamera přenáší obraz živě k obsluze, jsou však zpravidla přísněji nastavené podmínky následného poskytnutí záznamu, a to právě z důvodu, že případný incident má být postřehnut obsluhou již při živém přenosu. V každém případě při vyžádání záznamu musí být pořízen protokol o tom, kdo žádost podal a z jakého důvodu.[217] Možná je i kombinace monitorování v reálném čase za současného ukládání záznamu.[218] Takový způsob však bude nejvíce invazivní a pro jeho využití tedy bude nutné o to důmyslnější odůvodnění.

Ad d). Dalším kritériem ovlivňujícím míru zásahu do soukromí je případný osobní dozor nad přenášeným obrazem. Ten může být buďto trvalý (na veškerý monitorovaný prostor současně nebo cyklicky na vybrané podhledy), nebo *ad hoc* v případě incidentu. Jedním z nejméně invazivních ře-

---

[213] Rozsudek Nejvyššího správního soudu ze dne 25. 2. 2015, č.j. 1 As 113/2012 – 133; rozsudek Nejvyššího správního soudu ze dne 8. 11. 2011, č.j. 2 As 45/2010 – 68; stanovisko Úřadu pro ochranu osobních údajů č. 1/2006 [online]. *Úřad pro ochranu osobních údajů* [cit. 12. 10. 2021]. https://www.uoou.cz/files/stanovisko_2006_1.pdf Takový závěr v minulosti zaujímal i ESLP, cf. *Herbecq et l'Association « Ligue Des Droits De L'homme» contre La Belgique,* rozsudek Evropského soudu pro lidská práva, 14. 1. 1998 č. stížnosti 32200/96 a 32201/96. Ve věci *Perry v. the United Kingdom*, rozsudek Evropského soudu pro lidská práva, 17. 10. 2003 č. stížnosti 63737/00, ESLP konstatoval, že samotné informace o pohybu ve veřejném prostoru nejsou narušením soukromí, neboť v těchto místech člověk nemůže rozumně očekávat soukromí.

[214] Ke shodnému závěru dochází také Nonnemann, dle nějž tato skutečnost vyplývá také z Pokynů 3/2019, cf. Nonnemann, F. *Vztahuje se GDPR i na online kamery?* [online]. *epravo.cz* [cit. 15. 10. 2021]. https://www.epravo.cz/top/clanky/vztahuje-se-gdpr-i-na-online-kamery-110746.html

[215] Kulatý stůl k využívání online kamer a dalších sledovacích zařízení [online]. *Úřad pro ochranu osobních údajů* [cit. 20. 10. 2021]. https://www.uoou.cz/kulaty-stul-k-vyuzivani-online-kamer-a-dalsich-sledovacich-zarizeni/d-20310/p1=1099

[216] Konzultace s p. Střelcem.

[217] *Ibidem.*

[218] Rafajová, Váryová. *Biometrické osobné údaje podľa GDPR (biometrický podpis, kamerový systém),* p. 58.

šení je aktivace kamer až na elektronický podnět v případě incidentu; podnětem může být například otevření dveří zaznamenané čidlem,[219] toto řešení je však účelné pouze v omezených případech (není efektivní kupříkladu proti krádežím v obchodě, ale spíše tam, kde je méně časté a potenciálně nebezpečné samotné vniknutí do objektu).

Ad e). Další klíčový prvek představuje rozsah prostoru zabíraného kamerou.[220] Kamera by měla snímat pouze takový prostor, který odpovídá účelu zpracování osobních údajů.[221] Dle Pokynů 3/2019 je oprávnění osoby instalovat kameru obecně omezeno hranicemi nemovitosti, kterou vlastní,[222] případnému záběru sousedních pozemků[223] či veřejného prostranství je třeba přizpůsobit její nastavení – vhodný výběr objektivů, funkcí (rozostření, elektronické maskování v obraze apod.), pozorovacího úhlu a také místa instalace.[224]

Technologie jsou důvodem, proč je nutné se soukromím v právu zabývat na nové, vyšší úrovni. Zároveň jsou však technologie i součástí řešení problému.[225] Zásady spojené s ochranou soukromí se vedle nastavení procesů zacházení s údaji budou totiž nezbytně promítat také do technického nastavení kamer,[226] jež zastřešují principy *privacy by design a privacy by default*, tedy záměrné a standardní ochrany osobních údajů. Pod ně se řadí zásada minimalizace údajů,[227] která je zakotvena v článku 5 odst. 1 písm. c)

[219] Konzultace s p. Střelcem.

[220] Shodně též Rafajová, M. Váryová, L. *Biometrické osobné údaje podľa GDPR (biometrický podpis, kamerový systém),* p. 57.

[221] Cf. Pokyny 3/2019, p. 7, bod 7: S větším rozsahem monitorovaného prostoru a počtem lidí, kteří se v něm pohybují, totiž roste riziko zneužití osobních údajů.

[222] *Ibidem,* p. 11, bod 27. Shodně též konzultace s p. Střelcem: výchozím mezníkem pro nastavení záběru kamery je pozemek.

[223] Cf. rozsudek Nejvyššího soudu ze dne 30. 10. 2012, sp. zn. 22 Cdo 583/2011: „Soustavné a závažné narušování soukromí vlastníka nebo uživatele nemovitosti fotografováním nebo pořizováním jiného obrazového záznamu může být imisí ve smyslu § 127 odst. 1 obč. zák."

[224] Konzultace s p. Střelcem.

[225] Koorn, R. ter Hart, J. *Privacy by design: from privacy policy to privacy enhancing technologies.* [online] *Compact* 2020 [cit. 2. 9. 2021]. https://www.compact.nl/en/articles/privacy-by-design-from-privacy-policy-to-privacy-enhancing-technologies/

[226] Nutnost zohlednění stavu techniky výslovně zakotvují články 25 a 32 GDPR.

[227] Bod 78 preambule GDPR.

GDPR. Tato zásada stanovuje povinnost zpracovávat osobní údaje pouze v takovém rozsahu, jenž přímo souvisí s účelem jejich zpracování. Pokud by byl například instalován systém, jenž má za úkol kontrolovat počet zákazníků v prodejně za účelem dodržení maximálního povoleného počtu osob na dané ploše, není možné, aby kamera nebo čidlo měly možnost zaznamenat data například o rase, pohlaví nebo výšce dané osoby, využívaly funkci automatického rozpoznávání obličejů apod.[228] Projevem zásady minimalizace údajů je také pseudonymizace.[229] Další zásadou, již zastřešují zmíněné principy, je transparentnost,[230] kterou se u kamerových systémů rozumí také informování subjektů údajů o probíhajícím monitorování.[231] Nedostatečné je, pokud značku tvoří pouze symbol kamery bez jakýchkoli doplňujících informací, neboť tím nejsou splněny ani požadavky první vrstvy.[232] Podstatnou složku *privacy by design a privacy by default*[233] tvoří také využívání vhodného dostupného technického zabezpečení (šifrování apod.).[234]

4.3 KAMEROVÝ SYSTÉM V PROSTORU

O tom, zda může být na konkrétním místě kamerový systém nainstalován, nerozhoduje to, o jaké místo se jedná, ale zda má správce či třetí strana oprávněný zájem[235] na tom kamerový systém provozovat a zda toto právo

[228] Podobné systémy byly využity za účelem ochrany veřejného zdraví během koronakrize, cf. například Počty nakupujících hlídají v některých obchodech kamery [online]. *Česká televize* [cit. 3. 9. 2021]. https://ct24.ceskatelevize.cz/domaci/3243536-pocty-nakupujicich-hlidaji-v-nekterych-obchodech-kamery

[229] V případě anonymizace by již osoba nebyla identifikovatelná, a tudíž by nešlo o zpracování osobních údajů ve smyslu GDPR, cf. bod 26 preambule GDPR.

[230] Bod 78 preambule GDPR; čl. 5 odst. 1 písm. a GDPR.

[231] Pokyny 3/2019, p. 26, bod 111 a násl.

[232] Cf. Pokyny 3/2019, p. 26, bod 117.

[233] Blíže k těmto pojmům cf. Koorn, R. ter Hart, J. Privacy by design: from privacy policy to privacy enhancing technologies [online]. *Compact* 2020 [cit. 2. 9. 2021]. https://www.compact.nl/en/articles/privacy-by-design-from-privacy-policy-to-privacy-enhancing-technologies/ nebo také Romanou, A. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer Law & Security Review*. 2018, vol. 34, pp. 99-110.

[234] Článek 32 GDPR.

převáží nad oprávněným zájmem nebo základním právem subjektů údajů.[236] Oprávněným zájmem správce kamer v obchodech, výtazích, před vchodem do budovy a dalších bude zpravidla ochrana majetku nebo osob. Je klíčové, aby tento zájem nebyl pouze spekulativní, ale aby byl založen na reálných obavách. Tendence v posuzování oprávněného zájmu jsou však v praxi spíše mírnější – aby byla shledána existence oprávněného zájmu, nemusí být potvrzena dřívější špatná zkušenost (aby bylo možné do obchodu nainstalovat kameru, nemusí předtím dojít ke krádežím). Legitimní bude instalace videotechniky i v případě, kdy existuje záznam o dřívější škodě alespoň v dané oblasti (např. obchodech v okolí).[237]

U kamerového sledování se nabízí otázka, zda se kvalifikace sledovaného prostoru řídí tím, kdo sledování provádí.[238] Mohlo by se zdát, že kritériem, zda se jedná o veřejný, nebo soukromý prostor, může být povaha subjektu, který kamerový dohled vyžádal, zřídil nebo který jej provozuje. V prostorách, jež jsou předmětem tohoto příspěvku, dochází ke kamerovému sledování různými subjekty – jak veřejnými, tak soukromými.[239] Například kamera sledující vchod do školy z vnější strany, tedy typicky z ulice spadající do veřejného prostranství, může být zřízena jak školou – soukromým subjektem, tak městskou policií – subjektem veřejným.[240] Figuruje zde totiž i veřejný zájem – tím je ochrana dětí, které jsou navíc

[235] Případně jiný důvod plynoucí z GDPR – v kontextu článku však zpravidla půjde právě o oprávněný zájem.

[236] Článek 6 odst. 1 písm. f GDPR bude zpravidla tím právním titulem, na jehož základě bude monitorování v souladu se zákonem, cf. Pokyny 3/2019, p. 9, bod 16.

[237] Konzultace s p. Nonnemannem, shodně též Pokyny 3/2019, p. 10, bod 22: touto oblastí mohou být například také čerpací stanice.

[238] Cf. Webinář Jany Otčenáškové pořádaný v rámci projektu UNIque Law na téma Sdílení prostoru: veřejný vs. soukromý prostor, 18. 2. 2021.

[239] Dle Rity Aronov představuje sledování veřejnými subjekty větší hrozbu než sledování těmi soukromými. Aronov. *Privacy in a Public Setting: The Constitutionality of Street Surveillance,* p. 774. Wagnerová má opačný názor. Tvrdí, že zásah ze strany soukromých subjektů může být dokonce vyšší než ze strany těch veřejných, neboť disponují širšími možnostmi, jak soukromí narušit. Wagnerová, *Listina základních práv a svobod: komentář*.

[240] Konzultace s p. Střelcem. Blíže k úpravě použití kamer ve školách cf. Možnosti užívání audiovizuálních systému ve školských zařízeních [online]. MŠMT [cit. 19. 10. 2021]. https://www.msmt.cz/vzdelavani/socialni-programy/moznosti-uzivani-audiovizualnich-systemu-ve-skolskych

zranitelnějšími „objekty“, čemuž by měla odpovídat i míra ochrany.[241] Podobně to platí i u muzeí, kde vystavěné exponáty mohou být také předmětem zájmu státu (ochrany národního kulturního dědictví apod.), i zde tedy může figurovat zásah a dohled ze strany jak soukromého, tak veřejného subjektu.[242] Dle zákona má policie oprávnění pořizovat videozáznamy na místech veřejně přístupných. Ačkoli obchody nebo spořitelny veřejně přístupné jsou, o instalaci kamery do těchto míst zpravidla rozhoduje jejich vlastník a kamerový systém je v jeho režii, nikoli v režii policie. Případy, kdy policie do monitorování těchto prostor autoritativně zasáhne způsobem, že kamerové sledování nařídí či zorganizuje, budou výjimečné.[243] Přesto však nelze konstatovat, že se jedná o prostory soukromé. Zaprvé splňují podmínku přístupnosti veřejnosti, zadruhé nejsou těsně spjaty s obydlím, byť se v nich může soukromý život odehrávat. Na uvedených příkladech lze vidět, že dichotomické rozdělení podle povahy zřizovatele kamerového systému neobstojí v každé situaci.

V rozhodnutí ve věci *Antović a Mirković proti Černé hoře*[244] se ESLP zabýval případem stěžovatelů – vyučujících, kteří byli nahráváni během přednášek na univerzitní půdě v posluchárnách.[245] O instalaci kamer a pořizování záznamu byli informování, ale souhlas k této činnosti z jejich strany udělen nebyl. Soud shodně se svými dříve prezentovanými závěry, že soukromý život se může odehrávat i mimo obydlí, například na pracovišti, konstatoval porušení soukromí ve smyslu čl. 8 Úmluvy a stěžovatelům v dané věci vyhověl. Instalace navíc byla odůvodněna údajným cílem chránit majetek, ačkoli nebylo prokázáno, že by hrozilo jeho ohrožení (nedocházelo v uplynulé době ke krádežím apod.). Soud naznal, že *„v univerzitních posluchárnách učitelé vykonávají svou práci – přednášejí, ale zároveň se studenty navazují vzájemné vztahy a vytvářejí vlastní sociální identi-*

[241] Shodně také konzultace s p. Nonnemannem.

[242] Konzultace s p. Střelcem.

[243] *Ibidem.*

[244] *Antović a Mirković proti Černé hoře*, rozsudek Evropského soudu pro lidská práva, 28. 11. 2017 č. stížnosti 70838/13.

[245] Během covidové pandemie se v Česku rozšířilo nahrávání přednášek na školách, s čímž by všichni zúčastnění měli předem vyslovit souhlas.

tu,“ čímž poukázal na navazování sociálních vztahů jakožto složku soukromí. ESLP uvedl, že univerzitní posluchárna není ani soukromým, ani veřejným prostorem, čímž popřel dichotomii a přiznal, že existuje prostor mezi soukromým a veřejným. Konkrétněji daný prostor kategorizován nebyl, soud ani neuvedl, zda posluchárna pojímá prvky jak soukromého, tak veřejného prostoru, či je součástí jinak pojmenované sféry. Situaci tedy ESLP posoudil shodně s výkladem, dle nějž na akademické půdě požívá jedinec obdobné ochrany soukromí jako v obydlí, ačkoli se jedná o jiné prostory.[246]

V dalším ze svých rozsudků týkajících se soukromí na pracovišti se ESLP vyjádřil také k možnému narušení soukromí zaměstnankyň kamerovým sledováním prostoru pokladen v supermarketu.[247] Při posuzování oprávněnosti zásahu zdůraznil, že je nutné přihlédnout zejména k tomu, jakou míru soukromí mohly osoby v daném pro*středí* rozumně očekávat. Z rozhodnutí vyplývá, že je supermarket veřejným prostorem, neboť soud zdůraznil, že instalace a využívání kamer ve veřejném prostoru *„samo o sobě není zásahem do práva na soukromý život.“* K narušení soukromého života však může dojít i ve veřejném prostoru, a to v momentě, kdy dojde k určité intenzitě zaznamenávání a zpracování dat (jedná se o *„systematické a nepřetržité zaznamenávání dat“*).[248] ESLP zde odkazuje na svoji předchozí rozhodovací praxi, ve které dospěl k závěru, že *„instalace skryté kamery zaměstnavatelem bez vědomí zaměstnankyně po dobu 50 hodin v průběhu dvou týdnů a použití takto získaných kamerových záznamů před pracovním soudem pro odůvodnění jejího propuštění ze zaměstnání bylo zásahem do jejího práva na respektování soukromého života.“*[249] ESLP konstatoval, že je nutné odlišovat, jaké prostory jsou sledovány, a jako kritérium také uvedl rozumné očekávání soukromí. Prostory na pracovišti rozdělil podle míry rozumného očekávání soukromí

[246] Cf. kapitola *Prostorová ochrana soukromí.*

[247] *López Ribalda a ostatní proti Španělsku*, rozsudek Evropského soudu pro lidská práva, 17. října 2019 č. stížnosti 1874/13 a 8567/13. http://hudoc.echr.coe.int/eng?i=001-197098

[248] *Perry v. the United Kingdom*, rozsudek Evropského soudu pro lidská práva, 17. 7. 2003 č. stížnosti 63737/00.

[249] *Köpke proti Německu*, rozhodnutí Evropského soudu pro lidská práva ze dne 5. 10. 2010 č. stížnosti 420/07.

následovně: na toaletách a v šatnách je tato míra velmi vysoká,[250] v uzavřených prostorách (například kancelářích) vysoká, zatímco na místech viditelných nebo kolegům přístupných se již tato míra snižuje. Nejnižší míru soukromí pak zaměstnanci mohou očekávat na místech přístupných veřejnosti, kterým je právě prostor kolem pokladen. ESLP tedy naznal, že sledování prostoru pokladen kamerovým systémem není nepřiměřeným zásahem do soukromí zaměstnanců, a to právě z důvodu, že těsné okolí pokladen je přístupné rovněž veřejnosti. Za zmínku zde stojí i disentní stanoviska tří soudců, kteří mimo jiné nesouhlasili s argumentem, že byl zásah do soukromí v pořádku také proto, že následně záznamy viděl pouze omezený počet osob (vedoucí prodejny). V nesouhlasném stanovisku tito soudci upozornili, že je nutné vzít také v úvahu, že jakýkoli kamerový záznam může kdykoli uniknout, tzn. počet „adresátů" může být ve výsledku vyšší, a především poukázali na nutnost „*nepodceňovat rozvoj moderních technologií a jeho dopad na soukromí osob"*.

Ve věci *Gorlov a ostatní proti Rusku*[251] ESLP hodnotil (ne)možnost kamerového sledování ve vězeňských celách.[252] Do soukromí vězňů bylo zasaženo významným způsobem, neboť kamery byly instalovány přímo v cele a byly v nepřetržitém provozu, soud tedy konstatoval zřejmé porušení článku 8 Úmluvy. Stěžovatelé rovněž namítali, že na záznamy se následně dívaly dozorkyně, ačkoli šlo o mužskou věznici – otázka, zda je to přípustné, však zůstala soudem nezodpovězena, neboť k porušení práva na soukromí by došlo i v případě, kdy by záznam byl dostupný dozorcům výhradně mužského pohlaví. V dané věci byly také učiněny zajímavé závěry týkající se národní právní úpravy, jež v Rusku nestanovuje konkrétní podmínky využití kamer, například přípustný rozsah nebo délku sledování.

[250] Cf. nedávnou kauzu IKEA, která nainstalovala kamery na toaletách. IKEA: cameras were hidden in the ceiling above warehouse toilets for ‚health and safety' [online]. *Biting the hand that feeds IT* [cit. 20. 10. 2021]. https://www.theregister.com/2021/10/01/ikea_spycam_scandal/

[251] *Gorlov a ostatní proti Rusku*, rozhodnutí Evropského soudu pro lidská práva ze dne 2. 7. 2019, č. stížnosti 27057/06.

[252] Pro srovnání: v Česku je kamerové sledování možné na základě § 11 zákona č. 555/1992 Sb., o Vězeňské a justiční stráži České republiky.

Soud s odkazem na rozsudek *Association Ekin proti Francii*[253] konstatoval, že právní úprava této problematiky ani příliš specifická být nemůže, aby mohla pružně reagovat na technologický vývoj. Neznamená to však, že by umístění kamer přímo v cele bylo vždy a priori nezákonné, resp. v rozporu s ochranou soukromí ve smyslu Úmluvy. Rozsudek ESLP ve věci *Van Der Graaf proti Nizozemsku*[254] ukazuje, že i nepřetržité sledování v cele může být legitimní, jestliže je dostatečně odůvodněno a v souladu s národními předpisy.[255]

Jednotlivými typy společných bytových prostor a (ne)možností jejich kamerového sledování se opakovaně zabýval ÚOOÚ, a to například ve stížnosti z roku 2011.[256] V předmětném bytovém domě byl nainstalován kamerový systém na několika místech – v suterénu a do prostorů schodiště, kde bylo možné také sledovat příchody osob do domu a odchody z něj. Kamerový záznam měl být pořizován za účelem udržování pořádku v předmětných prostorách. Doba uchovávání záznamu se pohybovala okolo 10 dní a lišila se v závislosti na rychlosti zaplnění kapacity disku, na který byl ukládán. K výmazu nejstarších pořízených záznamů totiž docházelo postupně při zaplňování paměti disku, resp. při potřebě místa na uložišti pro nejnovější záznamy. Existence souhlasu všech obyvatel se zpracováním osobních údajů přitom nebyla prokázána. Úřad při posuzování stížnosti konstatoval, že *„oblast ochrany soukromí každého jednotlivce není vázána pouze na vnitřní prostory jeho bytu, ale i na prostory, kterými daný jedinec musí nezbytně procházet, aby mohl vstoupit do vlastního obydlí nebo ho opustit.“*[257] Při své další kontrole ÚOOÚ shledal, že *„[m]onitorování prostoru bezprostředně před bytovými dveřmi … [je]… zásah do soukromého a osobního*

[253] *Association Ekin v. France,* rozsudek Evropského soudu pro lidská práva, 17. 7. 2001 č. stížnosti 39288/98.

[254] *Van Der Graaf proti Nizozemsku*, rozhodnutí Evropského soudu pro lidská práva ze dne 1. 6. 2003, č. stížnosti 8704/03.

[255] *"The Court reiterates that the expression "in accordance with the law" requires that the impugned measure should have some basis in domestic law and that the law in question should be accessible to the person concerned – who must moreover be able to foresee its consequences for him or her – and compatible with the rule of law."*

[256] Kamerový systém v bytovém domě [online]. *Úřad pro ochranu osobních údajů.* [18. 4. 2021]. https://www.uoou.cz/kamerovy-system-v-nbsp-bytovem-dome/d-6291

života subjektů údajů…"[258] Tento závěr je ve shodě s bodem 6 stanoviska,[259] které Úřad vydal k otázce sledování společných prostor v bytovém domě. Použití kamerového systému ve sklepě může být posouzeno mírně odlišně, kritériem však stále bude účel zpracování a to, jak často jsou prostory využívány. Lze tedy uzavřít, že byť je zde míra soukromí odlišná[260] od soukromí v bytě, i společné části v bytovém domě lze považovat za soukromý prostor. Dle stanoviska ÚOOÚ je provozovatel kamerového sytému v bytovém domě „i v *průběhu provozu povinen kdykoliv prokázat, že kamerový systém jako prostředek k ochraně majetku a osob ve zvolené lokalitě je s ohledem na jistý zásah do soukromí osob řešením proporcionálním, a to zejména ve vztahu k požadavkům na bezpečnost*". V této souvislosti se Úřad zabýval rovněž kamerovým sledováním nemovitosti jako takové zvenčí. Dle jeho vyjádření je takové sledování možné, jestliže je nezbytné a proporcionální a jestliže je kamera vhodně nastavená. Nesmí zabírat sousedův dům, resp. celkově pozemek, ani veřejné prostranství *„nad rámec nezbytný pro identifikaci případného útočníka proti plášti budovy nebo oplocení soukromého pozemku."*[261] Toto stanovisko zohledňuje také závěry plynoucí z případu Ryneš, tedy že rozsáhlejší sledování podléhá nařízení GDPR, ačkoli je prováděno fyzickou osobou a kamera je nainstalována na domě. Obdobně přistoupil ÚOOÚ také k případu 3D Production, s.r.o., kde nařídil mimo odstranění kamer, jež sledovaly veřejné prostranství, také změnu nastavení

[257] Blíže ke zpracování osobních údajů při provozu kamerových systému ve společných částech domu ve světle GDPR cf. rozsudek Soudního dvora Evropské unie ze dne 11. 12. 2019 ve věci C-708/18.

[258] Kontrola subjektu provozujícího kamerový systém v bytovém domě [online]. *Úřad pro ochranu osobních údajů* [18. 4. 2021]. https://www.uoou.cz/kontrola-subjektu-provozujiciho-kamerovy-system-v-bytovem-dome-svj-pro-dum-c-1832-u-cihelny-1832-lysa-nad-labem/ds-4370/p1 = 4370&archiv = 2

[259] Bod 6 Stanoviska Úřadu pro ochranu osobních údajů [online]. *Úřad pro ochranu osobních údajů* [cit. 18. 4. 2021]. https://www.uoou.cz/stanovisko-c-1-2016-umisteni-kamerovych-systemu-v-nbsp-bytovych-domech/d-18866/p1 = 1099

[260] Bod 4 Stanoviska Úřadu pro ochranu osobních údajů [online]. *Úřad pro ochranu osobních údajů* [cit. 18. 4. 2021]. https://www.uoou.cz/stanovisko-c-1-2016-umisteni-kamerovych-systemu-v-nbsp-bytovych-domech/d-18866/p1 = 1099

[261] Ke kamerám a kamerovým systémům [online]. *Úřad pro ochranu osobních údajů* [cit. 7. 10. 2021]. https://www.uoou.cz/casto-kladene-otazky-ke-kameram-a-kamerovym-systemum/ds-5041/archiv = 1&p1 = 2619

kamery sledující parkoviště tak, aby byla zastíněna část vedlejší parcely, která byla využívána jako veřejná komunikace.[262] K monitorování části veřejného prostranství tedy Úřad zaujal jednoznačný postoj, že takové sledování není možné obecně akceptovat, avšak existují výjimky. Příkladem, kdy je možné na sledování přistoupit, mohou být například opakované závažné útoky proti obydlí provozovatele kamery z veřejného prostranství. I za těchto okolností však musí být dodržovány požadavky vymezené GDPR.[263] Zásadu proporcionality ÚOOÚ aplikuje také na parkovací stání: jestliže je účelem instalace kamery ochrana vozidla, pak by kamera neměla být v provozu po dobu, kdy je parkovací místo prázdné.[264]

Dalším otazníkem mohou být právnímu prostředí blízké soudní síně,[265] kde se konají veřejná jednání. Ačkoli mají od pojmu obydlí daleko, i zde je ve specifických případech nutné chránit soukromí zúčastněných osob, a to například vyloučením veřejnosti z ústního jednání. Vzhledem k intenzitě zásahu právního sporu do života účastníků je ostatně možné konstatovat, že i v soudní síni se často odehrává významná část soukromého života.[266]

V práci bylo poukázáno na to, že míra očekávání soukromí na pracovišti se bude lišit v závislosti na tom, o jaký typ zaměstnání se jedná: v kanceláři, kterou má zaměstnanec sám pro sebe, bude tato míra zřejmě vyšší než při výkonu zaměstnání „za přepážkou“. Tuto situaci hodnotil Úřad pro ochranu osobních údajů v prostředí městského úřadu, kde byly nainstalovány kamery údajně za účelem ochrany majetku a osob. Ačkoli se jednalo o místo, kde se běžně vyskytuje více lidí, kteří městský úřad navštěvují, a zaměstnancovo soukromí nedosahuje takové intenzity, Úřad uvedl, že monitorování pracoviště bylo v rozporu se zákonem z důvodu nepřiměřenosti zásahu do soukromí a soukromého života zaměstnanců.[267]

Z uvedených soudních rozhodnutí a závěrů Úřadu pro ochranu osobních údajů je patrné, že neexistuje jednotné hledisko, z nějž by vycházel při

[262] Usnesení Nejvyššího správního soudu ze dne 22. 1. 2014, č. j. 3 As 124/2013 – 29.

[263] *Ke kamerám a kamerovým systémům* [online].

[264] *Ibidem.*

[265] Šimíček. *Právo na soukromí*, p. 85.

[266] Jako příklad lze uvést rozvod, který je nepochybně citlivě soukromou záležitostí. Přesto jsou však jednání, jejichž předmětem je rozvod manželství, veřejná.

posuzování narušení práva na soukromí. Výsledné konstatování je vždy výsledkem testu proporcionality a dodržení zásad pro zpracování osobních údajů. Takový výsledek je logický s ohledem na množství aspektů, které v jednotlivých případech hrají roli, neboť ten prostorový je pouze jedním z nich.

5. ZÁVĚR

Právní úprava ochrany soukromí v sobě nenese jednoznačné prostorové omezení. Přestože § 86 OZ uvádí, že nelze bez svolení narušit soukromé prostory jedince, jedná se pouze o část demonstrativního výčtu, který není v rozporu s ochranou soukromí ve veřejném prostoru. Ten český právní řád nedefinuje a nevyužívá jej jako meřítko pro intenzitu ochrany soukromí, jež je ovlivněna především jinými základními právy a veřejným zájmem, které mohou míru ochrany soukromí potlačit, jestliže zásah splní podmínky přiměřenosti. Ačkoli pojem soukromý prostor zákon zná, definován také není. Právní řád tedy tyto pojmy nerozlišuje, nevymezuje je proti sobě. Jistá vodítka poskytuje soudní praxe. Nicméně ani ta s těmito dichotomickými kategoriemi nepracuje a jednotlivá místa do nich nerozřazuje.

Westin hovoří o samotě a anonymitě jako složkách soukromí a připouští, že jich lze dosáhnout i ve veřejném prostoru. V místech, kde bude nainstalovaný kamerový systém, jsou však tyto složky předem nerealizovatelné. V jiných typologiích se odráží i prostorový aspekt, který soukromí nelze upřít, ale není absolutně určující. Zásadní závěr plynoucí z rozhodnutí *Katz v. United States* skrývající se na pozadí determinování kritéria *reasonable expectation of privacy* je možné spatřovat v odvrácení ochrany soukromí od místa k dané osobě.[268] Případ *Katz* ale prostorový aspekt nepopírá – očekávání osoby je totiž nezbytné vztáhnout právě k místu, kde se nachází. Od toho se očekávání osoby odvíjí. Potlačení významu prostoru tedy není zcela

[267] Ke kamerovému systému na městském úřadě [online]. *Úřad pro ochranu osobních údajů* [cit. 20. 10. 2021]. https://www.uoou.cz/ke-kamerovemu-systemu-na-mestskem-urade/d-1753/p1=1099

[268] Rauhofer. *Privacy Is Dead, Get over It: Information Privacy and the Dream of a Risk-Free Society*, p. 187.

správným způsobem, jak toto rozhodnutí interpretovat. Spojení rozumného očekávání a prostoru je vhodným podpůrným kritériem pro posouzení, zda bylo soukromí jedince narušeno nepřiměřeně. S legitimním očekáváním soukromí se pojí otázka, zda jej lze mít v případě, kdy správce plní řádně své povinnosti plynoucí z GDPR a náležitě informuje o tom, že je prostor monitorován, a poskytne subjektu údajů informací s tím související. Řádné splnění této povinnosti je nezbytnou náležitostí, nepředstavuje však pro správce údajů alibi a automaticky nezbavuje subjekt údajů možnosti mít v daném prostoru legitimní očekávání soukromí, respektive automaticky nečiní provoz kamerového systému zákonným.

Jak bylo nastíněno, povaha prostoru není tím, od čeho by se primárně odvíjel přístup k ochraně soukromí. Klíčovým kritériem je účel a proporcionalita. Na otázku, zda by jím měl být prostor, lze odpovědět spíše záporně.[269] Judikatura ukazuje, že soukromý život se může odehrávat všude, bez ohledu na to, jak je prostor kvalifikován. S rozmachem moderních technologických prostředků navíc může být soukromí narušeno velmi intenzivně také mimo prostory obydlí. Ačkoli část života odehrávající se na veřejnosti může být méně soukromé povahy než ta odehrávající se doma, potenciál narušení soukromí vyváží intenzita zásahu, které jsou právě tyto technologie schopné. Tedy i z běžné neintimní činnosti odehrávající se mimo obydlí může být extrahováno takové množství osobních údajů, aby došlo k nepřiměřenému zásahu do soukromí.

Pokud by přesto někdo dospěl k závěru, že je prostorové určení vhodným kritériem pro nastavení ochrany soukromí, pravděpodobně narazí při snaze rozdělit jednotlivá místa do kategorie „soukromé“ a „veřejné“. Jak bylo v práci popsáno, dichotomie veřejný – soukromý prostor neplatí a neexistuje jediné hledisko, které by bez dalšího umožňovalo tyto prostory striktně odlišovat. Jednotlivá konkrétní místa mohou směřovat spíše do soukromého prostoru a jiná spíše do veřejného, nutně ale zůstanou místa někde na pomezí, v „šedé zóně“, která budou podobnou měrou pojímat prvky z obou těchto „extrémů“. Clarke popisuje, že soukromý prostor

[269] Shodně též Koops. *On Legal Boundaries, Technologies, and Collapsing Dimensions of Privacy,* p. 258.

(*private space*) přesahuje do veřejných míst (*public places*). Toto vymezení je přiléhavé a anglické názvosloví ještě lépe odráží jeho myšlenku. Přesto nedochází k jednoznačnému vymezení veřejných míst.

Zákonná definice veřejného prostranství i přes svoji demonstrativní povahu směřuje spíše k místům neohraničeným zdmi, k místům venkovním, v nichž se lze víceméně volně pohybovat. Přesto jsou místa jako obchody, některá pracoviště, školy nebo provozovny, které odpovídají kritériu neomezené přístupnosti veřejnosti, jež je v definici veřejného prostranství vymezeno. Veřejný prostor je tedy možné vnímat jako širší pojem než veřejné prostranství, jak ostatně plyne také z většiny (byť neoficiálních) definic. Ochrana soukromí se tedy stupňuje s tím, nakolik blízko se ocitáme našemu obydlí. Nejpříhodněji tuto realitu odráží *Zwiebelmodelle* přirovnávající jednotlivé složky soukromí k cibulovým vrstvám.

Kamerové systémy bývají v prostorách, jež jsou předmětem tohoto příspěvku, instalovány především za účelem ochrany majetku. Není pochyb o tom, že moderní sledovací prostředky jsou způsobilé zasáhnout do soukromí jedince natolik invazivním způsobem, že je tento zásah nesrovnatelný se sledováním bez využití těchto prostředků. Zásadní roli přitom hraje právo na informační sebeurčení a objem dat, jenž je každodenně při monitorování zpracováván. Přístup ke zpracování dat získaných kamerovým sledováním se odvíjí zejména od účelu, za jakým jsou data zpracovávána. Součástí posuzování proporcionality zásahu může být kritérium očekávání soukromí, které se mění v závislosti na tom, kde se jedinec nachází. V prostorách ležících na pomezí soukromého (obydlí) a veřejného (veřejné prostranství) je však míra očekávání soukromí velmi relativní a zpravidla převáží kritérium účelu a celkového způsobu užití a nastavení kamery.[270] Na několika případech z praxe bylo demonstrováno, že i pro prostory stejného typu mohou v různých situacích platit odlišné závěry o tom, zda v nich bylo kamerovým sledování narušeno soukromí subjektu apod. Pro jednotlivé

[270] Heumann. *Privacy and Surveillance: Public Attitudes on Cameras on the Street, in the Home, and in the Workplace,* p. 50: "One of the pragmatists in the older group told us that we were asking the wrong questions by talking about whether cameras are good-he thought that cameras and surveillance are not inherently good or bad, and that what we needed to talk about was how they should be used."

prostory tedy nelze souhrnně zobecnit jednotný závěr. Konstatování, zda k nepřiměřenému narušení soukromí došlo, či nikoli, bude záviset na několika dílčích skutečnostech; typ prostoru bude pouze jedním z nich.

6. POUŽITÉ ZDROJE

6.1 MONOGRAFIE

[1] Allen, A. L. *Unpopular privacy: what must we hide?* Oxford: Oxford University Press, 2011.

[2] Aristotle. Politics. In: McKeon, R. (ed.) *The Basic Works of Aristotle.* Lifetime Library, Random House, 1941.

[3] Bentham, J. Panopticon or the Inspection House. In: Bowring, J. (ed.). *The Works of Jeremy Bentham.* London: Simpkin, Marshall, & Co., 1843.

[4] Curry, M. Discursive Displacement and the Seminal Ambuiguity of Space and Place. In: Lievrouw, L., Livingstone, S. (eds). *The Handbook of New Media: Social Shaping and Consequences of ICT*. London: Sage Publications, 2002.

[5] Čabalová, M., Maceková, M., Míčák, L., Nawrath, M., Římanová, M., Sedlák, R., Šilberská, P. *Kvalitní veřejné prostory: Metodika tvorby a obnovy veřejných prostranství.* Brno: Nadace Partnerství, 2011.

[6] Draštík, A., Fenyk, J. et al. *Trestní řád. Komentář. I. díl.* Praha: Wolters Kluwer ČR, a.s., 2017.

[7] Draštík, A., Fremr, R., Durdík, T., Růžička, M., Sotolář. A. et al. *Trestní zákoník. Komentář, I. díl.* Praha: Wolters Kluwer, a.s., 2015.

[8] Foucault, M. *Dozerať a trestať: Zrod väzenia*. 2. vyd. Bratislava: Kalligram, 2004.

[9] Gehl, J., Blažek, K., Blažková, B., Sedlák, R. *Města pro lidi*. Brno: Partnerství, 2012.

[10] Hermstrüwer, Y., Dickert, S. *Tearing the Veil of Privacy Law: An Experiment on Chilling Effects and the Right to Be Forgotten*. Rochester, NY: Social Science Research Network, 2013.

[11] Husseini, F. et al. *Listina základních práv a svobod: komentář.* Praha: C. H. Beck, 2021.

[12] Janečková, E., Bartík, V. *Kamerové systémy v praxi: právní režim z pohledu ochrany osobních údajů a ochrany osobnosti. Praktická právnická příručka.* Praha: Linde Praha, 2011.

[13] Klíma, K. et al. *Komentář k Ústavě a Listině.* 2. vyd. Plzeň: Aleš Čeněk, 2009.

[14] Kokeš, M. § 86. In: Petrov, J., Výtisk, M., Beran, V. et al. *Občanský zákoník, 2. vydání.* Praha: C. H. Beck, 2019, pp. 151-157.

[15] Kundera, M. *Les testaments trahis: essai*. Paris: Gallimard, 1993.

[16] Tůma, P. § 86. In: Lavický, P. et al. *Občanský zákoník I. Obecná část (§ 1-654).* Praha: C. H. Beck, 2014.

[17] Madanipour, A. *Public and Private Spaces of the City*. London: Routledge, 2003.

[18] Míšek, J. *Moderní regulatorní metody ochrany osobních údajů.* Brno: Masarykova univerzita, 2020.

[19] Míšek, J. *Osobní údaje v čase a prostoru.* 2020, disertační práce, Masarykova univerzita, Právnická fakulta.

[20] Kasl, F. *Osobnost, soukromí a osobní údaje v moderní společnosti.* In: Polčák, R., Kasl, F., Míšek, J., Stupka, V., Kyselovská, T., Myška, M. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018.

[21] Rafajová, M., Váryová, L. Biometrické osobné údaje podľa GDPR (biometrický podpis, kamerový systém). Praha: Leges, 2019.

[22] Schmeidler, K. et al. *Sociologie v architektonické a urbanistické tvorbě*. Brno: Zdeněk Novotný, 2001.

[23] Soanes, C., Stevenson, A. *Concise Oxford English Dictionary*. Oxford: Oxford University Press, 2006.

[24] Solove, D. J. *Nothing to Hide: the False Tradeoff between Privacy and Security*. New Haven: Yale University Press, 2011.

[25] Šámal, P., Růžička, M. In: Šámal, P. et al. *Trestní řád I. § 1 až 156. Komentář.* 7. vydání. Praha: C. H. Beck, 2013.

[26] Šimíček, V. (ed.). *Právo na soukromí*. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011.

[27] Timan, T., Galič, M., Koops, B.-J. Surveillance Theory and Its Implications for Law. In: Brownsword, R. Scotford, E. Yeung, K. (eds). *The Oxford Handbook of Law, Regulation, and Technology*. Oxford: Oxford UP, 2017.

[28] Timan, T., Newell, B. C., Koops, B.-J. (eds). *Privacy in Public Space: Conceptual and Regulatory Challenges.* Cheltenham: Edward Elgar Publishing, 2017.

[29] Uřičař, M., Rámiš, V. et al. *Obecné nařízení o ochraně osobních údajů: komentář*. Praha: C.H. Beck, 2021.

6.2 ČLÁNKY

[30] Aronov, R. F. Privacy in a Public Setting: The Constitutionality of Street Surveillance. *Quinnipiac Law Review*. 2004, vol. 22, no. 4, pp. 769-810.

[31] Barnett, L. D. The Public-Private Dichotomy in Morality and Law. *Journal of Law and Policy*. 2010, vol. 18, n. 2, pp. 541-606.

[32] Beaney, W. M. The Right to Privacy and American Law. *Law and Contemporary Problems.* 1966, vol. 31, n. 2, pp. 253-271.

[33] Cass, B. The Limits of the Public/Private Dichotomy: A Comment on Coady & Coady. *International Journal of Law and the Family*. 1992, vol. 6, n. 1, pp. 140-147.

[34] Cohen, J. Studying Law Studying Surveillance. *Surveillance & Society.* 2015, vol. 13, n. 1, pp. 91-101.

[35] Gerety, T. Redefining Privacy. *Harvard Civil Rights-Civil Liberties Law Review. 1977,* vol. 12, n. 2, pp. 233-296.

[36] Gumpert, G., Drucker, S. J. Public boundaries: Privacy and surveillance in a technological world. *Communication Quarterly*. 2001, vol. 49, n. 2, pp. 115-129.

[37] Halpérin J.-L. L'essor de la « privacy » et l'usage des concepts juridiques. *Droit et société*. 2005, vol. 2, n. 61, pp. 765-782.

[38] Hansen, M. No Place to Hide: If crime is everywhere, so, too, may be police surveillance cameras and contraband detection devices to combat it. But who's looking out for privacy rights? *ABA Journal*. 1997, vol. 83, n. 8, pp. 44-48.

[39] Heumann, M. et al. Privacy and Surveillance: Public Attitudes on Cameras on the Street, in the Home, and in the Workplace. *Rutgers Journal of Law and Public Policy*. 2016, vol. 14, n. 1, pp. 37-83.

[40] Hirose, M. Privacy in Public Spaces: The Reasonable Expectation of Privacy against the Dragnet Use of Facial Recognition Technology. *Connecticut Law Review*. 2017, vol. 49, n. 5, pp. 1591-1620.

[41] Hunter, L. Public Image: Privacy in the Information Age. *Whole Earth Review.* 1985, vol. 44, pp. 32-27.

[42] Kasl, F. Povaha zásahu do informačního soukromí člověka. *Právník*. 2019, vol. 158, n. 7, pp. 674-715.

[43] Kasl, F. Surveillance in digitalized society: the Chinese social credit system from a European perspective. *The Lawyer Quarterly.* 2019, vol. 9, n. 4, pp. 349-358.

[44] Koops, B.-J., Newell, B., Timan, T., Škorvánek, I., Chokrevski, T., Galič, M. A Typology of Privacy. *University of Pennsylvania Journal of International Law*. 2017, vol. 38, n. 2, pp. 483-575.

[45] Koops, B.-J. On legal boundaries, technologies, and collapsing dimensions of privacy. *Politica e Società*. 2014, vol. 3, n. 2, p. 247-264.

[46] Marx, G. T. What's New About the "New Surveillance"?: Classifying for Change and Continuity. *Surveillance & Society*. 2002, vol. 1, n. 1, pp. 18-37.

[47] Meeks, B. N. Privacy Lost, Anytime, Anywhere. *Communications of the ACM.* 1997, vol. 40, n. 8, pp. 11-13.

[48] Milaj, J. Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance. *International Review of Law, Computers & Technology.* 2016, vol. 30, n. 3, pp. 115-130.

[49] Milligan, Ch. S. Facial Recognition Technology, Video Surveillance, and Privacy. *Southern California Interdisciplinary Law Journal*. 1999, vol. 9, n. 1, p. 295-334.

[50] Míšek, J. Kauza Ryneš. *Revue pro právo a technologie*. 2015, vol. 6, n. 11, p. 67-75.

[51] Nissenbaum, H. Toward an Approach to Privacy in Public: Challenges of Information Technology. *Ethics & Behaviour.* 1997, vol. 7, n. 3, pp. 207-219.

[52] Post, R. C. Three Concepts of Privacy. *The Georgetown Law Journal.* 2001, vol. 89, n. 6, pp. 2087-2098.

[53] Rauhofer, J. Privacy Is Dead, Get over It: Information Privacy and the Dream of a Risk-Free Society. *Information & Communications Technology Law*. 2008, vol. 17, n. 3, pp. 185–198.

[54] Romanou, A. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer Law & Security Review.* 2018, vol. 34, pp. 99-110.

[55] Siebel, W., Wehrheim, J. Security and the Urban Public Sphere. German Policy Studies. 2006, vol. 3, n. 1, pp 19-46.

[56] Slobogin, Ch. Public Privacy: Camera Surveillance of Public Places And The Right to Anonymity. *Mississippi Law Journal.* 2002, vol. 72, n. 1, pp. 213-316.

[57] Solove, D. J. Conceptualizing Privacy. *California Law Review*. 2002, vol. 90, n. 4, pp. 1087-1155.

[58] Stuart, A., Levine, M. Beyond 'nothing to hide': When identity is key to privacy threat under surveillance. *European Journal of Social Psychology.* 2017, vol. 47, n. 6, pp. 694-707.

[59] Szczepaniak, R. The Dichotomy of Public and Private Law. A Review of the Monograph by Igor Zachariasz. *Forum Prawnicze*. 2016, n. 6, pp. 82-97.

[60] Thomson, J. J. The Right to Privacy. *Philosophy & Public Affairs.* 1975, vol. 4, n. 4, pp. 272-289.

[61] Thornton, M., Weintraub, J., Kumar K. Public and Private in Thought and Practice: Perspectives on a Grand Dichotomy. *Social & Legal Studies*. 1998, vol. 7, n. 4, pp. 582-584.

[62] Tomas Gomez-Arostegui, H. Defining private life under the European Convention on Human Rights by referring to reasonable expectations. *California Western International Law Journal.* 2005, vol. 35, n. 2, pp. 153-202.

[63] Walz, Ch. N. Brookins, D. S. Privacy in Public: A Look at Recent Efforts to Recognize Privacy Protections in Public Spaces. *Communications Lawyer*. 2016, vol. 32, no. 2, pp. 24-28.

[64] Warren, S. Brandeis, L. The right to privacy. *Harvard Law Review*. 1890, vol. 4, n. 5, pp. 193-220.

6.3 JUDIKATURA

6.3.1 ČESKÁ

[65] Usnesení Nejvyššího soudu ze dne 28. 11. 2002, sp. zn. 3 Tdo 969/2002.

[66] Usnesení Nejvyššího správního soudu ze dne 22. 1. 2014, č. j. 3 As 124/2013 – 29.

[67] Nález Ústavního soudu ze dne 24. září 2009, sp. zn. II. ÚS 2334/08.

[68] Nález Ústavního soudu ze dne 2. listopadu 2009, sp. zn. II. ÚS 2048/09.

[69] Nález Ústavního soudu ze dne 8. února 2010, sp. zn. IV. ÚS 2425/09.

[70] Nález pléna Ústavního soudu ze dne 8. června 2010, sp. zn. Pl. ÚS 3/09.

[71] Stanovisko pléna Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10.

[72] Nález Ústavního soudu ze dne 6. března 2012, sp. zn. I. ÚS 1586/09.

[73] Rozsudek Nejvyššího soudu ze dne 30. 7. 2013, sp. zn. 4 As 97/2013 - 40.

[74] Nález Ústavního soudu ze dne 30. října 2014, sp. zn. III. ÚS 3844/13.

[75] Nález Ústavního soudu ze dne 15. prosince 2015, sp. zn. I. ÚS 2024/15.

[76] Nález Ústavního soudu ze dne 13. října 2016, sp. zn. II. ÚS 1221/16.

[77] Usnesení Ústavního soudu ze dne 30. května 2017, sp. zn. III. ÚS 1122/17, bod 20.

[78] Rozsudek Nejvyššího správního soudu ze dne 8. 11. 2011, č. j. 2 As 45/2010 – 68;

[79] Rozsudek Nejvyššího správního soudu ze dne 25. 2. 2015, č. j. 1 As 113/2012 – 133.

[80] Rozsudek Nejvyššího soudu ze dne 30. 10. 2012, sp. zn. 22 Cdo 583/2011.

[81] Rozsudek Nejvyššího soudu ze dne 11. 4. 2018, sp. zn. 7 Tdo 374/2018.

[82] Usnesení Nejvyššího soudu ze dne 30. 7. 2019, sp. zn. 8 Tdo 838/2019.

[83] Rozsudek Městského soudu v Praze ze dne 2. 9. 2014, č. j. 8A 182/2010 - 69-77.

[84] Rozsudek Městského soudu v Praze ze dne 27. 9. 2011, č. j. 6Ca 227/2008 - 71.

6.3.2 EVROPSKÁ

[85] *Antović a Mirković proti Černé hoře*, rozsudek Evropského soudu pro lidská práva, 28. 11. 2017 č. stížnosti 70838/13.

[86] *Association Ekin v. France*, rozsudek Evropského soudu pro lidská práva, 17. 7. 2001 č. stížnosti 39288/98.

[87] *Bărbulescu v. Romania,* rozsudek Evropského soudu pro lidská práva, 12. 1. 2016 č. stížnosti 61496/08.

[88] *Crémieux proti Francii*, rozsudek Evropského soudu pro lidská práva, 25. 2. 1993 č. stížnosti 11471/85.

[89] *Gillow proti Spojenému království*, rozsudek Evropského soudu pro lidská práva, 24. 11. 1986 č. stížnosti 9063/80.

[90] *Gorlov a ostatní proti Rusku*, rozhodnutí Evropského soudu pro lidská práva, 2. 7. 2019 č. stížnosti 27057/06.

[91] *Halford v. the United Kingdom,* rozsudek Evropského soudu pro lidská práva, 25. 6. 1997 č. stížnosti 20605/92.

[92] *Herbecq et l'Association « Ligue Des Droits De L'homme» contre La Belgique,* rozsudek Evropského soudu pro lidská práva, 14. 1. 1998 č. stížnosti 32200/96 a 32201/96.

[93] *Klass and others v. Germany*, rozsudek Evropského soudu pro lidská práva, 6. 9. 1978 č. stížnosti 5029/71.

[94] *Köpke proti Německu*, rozhodnutí Evropského soudu pro lidská práva, 5. 10. 2010 č. stížnosti 420/07.

[95] *López Ribalda a ostatní proti Španělsku*, rozsudek Evropského soudu pro lidská práva, 17. října 2019 č. stížnosti 1874/13 a 8567/13.

[96] *Malone v. the United Kingdom*, rozsudek Evropského soudu pro lidský práva, 2. 8. 1984 č. stížnosti 8691/79.

[97] *Menteş and Others a. Turkey*, rozsudek Evropského soudu pro lidská práva, 28. 11. 1997 č. stížnosti 58/1996/677/867.

[98] *Miailhe proti Francii*, rozsudek Evropského soudu pro lidská práva, 25. 2. 1993 č. stížnosti 12661/87.

[99] *Niemietz v. Germany*, rozsudek Evropského soudu pro lidská práva, 16. 12. 1992 č. stížnosti 13710/88.

[100] *Perry v. the United Kingdom*, rozsudek Evropského soudu pro lidská práva, 17. 7. 2003 č. stížnosti 63737/00.

[101] *P. G. and J. H. v. the United Kingdom,* rozsudek Evropského soudu pro lidská práva, 25. 9. 2001 č. stížnosti 44787/98.

[102] *Rotaru v. Rumunsko,* rozsudek Evropského soudu pro lidská práva, 4. 5. 2000 č. stížnosti 28341/95.

[103] *S. and Marper v. the United Kingdom*, rozsudek Evropského soudu pro lidská práva, 4. 12. 2008 č. stížností 30562/04 a 30566/04.

[104] *Saint-Paul Luxembourg S.A. v. Luxembourg,* rozsudek Evropského soudu pro lidská práva, 18. 4. 2013 č. stížnosti 26419/10.

[105] *Société Colas Est. v. France,* rozhodnutí Evropského soudu pro lidská práva, 16. 4. 2002 č. stížnosti 37971/97.

[106] *Van Der Graaf proti Nizozemsku*, rozhodnutí Evropského soudu pro lidská práva, 1. 6. 2003 č. stížnosti 8704/03.

[107] Rozsudek Soudního dvora Evropské Unie ze dne 11. 12. 2014 ve věci C-212/13.

[108] Rozsudek Soudního dvora Evropské unie ze dne 11. 12. 2019 ve věci C-708/18.

6.3.3 AMERICKÁ

[109] *Elkins v. United States*, rozsudek Nejvyššího soudu Spojených států amerických, 27. 6. 1960 č. 364 U.S. 206.

[110] *Katz v. United States,* rozsudek Nejvyššího soudu USA, 18. 12. 1967 č. stížnosti 389 U. S. 347.

[111] *United States v. Jones,* rozsudek Nejvyššího soudu Spojených států amerických, 30. 4. 2012 č. 565 U.S. 400.

[112] *United States v. Maynard,* rozsudek Nejvyššího soudu Spojených států amerických, 6. 8. 2010 č. 615 F.3d 544.

6.4 ELEKTRONICKÉ ZDROJE

[113] Boal, M. SpyCam City [online]. *Village Voice, LLC* [cit. 20. 9. 2021]. https://www.villagevoice.com/1998/10/06/spycam-city/

[114] Constitution of the United States, Fourth Amendment [online]. *Congress.gov.* [cit. 10. 6. 2021]. https://constitution.congress.gov/constitution/amendment-4/

[115] Evropská úmluva o ochraně lidských práv. [online]. *Rada Evropy.* [cit. 3. 5. 2021]. https://www.echr.coe.int/documents/convention_ces.pdf

[116] IKEA: cameras were hidden in the ceiling above warehouse toilets for ‚health and safety' [online]. *Biting the hand that feeds IT* [cit. 20. 10. 2021]. https://www.theregister.com/2021/10/01/ikea_spycam_scandal/

[117] Introduction to Dataveillance and Information Privacy, and Definitions of Terms [online]. *Xamax Consultancy Pty Ltd.* 1995-2021. [cit. 20. 9. 2021]. http://www.rogerclarke.com/DV/Intro.html

[118] K provozování kamerových systémů [online]. *Úřad pro ochranu osobních údajů* [cit. 14. 8. 2021]. https://www.uoou.cz/k-provozovani-kamerovych-systemu/d-29535

[119] Kamerové sledování veřejných prostranství a institucí [online]. *Ministerstvo vnitra České republiky* [cit. 5. 9. 2021]. https://www.mvcr.cz/clanek/kamerove-sledovani-verejnych-prostranstvi-a-instituci.aspx

[120] Kamerový systém v bytovém domě [online]. *Úřad pro ochranu osobních údajů.* [18. 4. 2021]. https://www.uoou.cz/kamerovy-system-v-nbsp-bytovem-dome/d-6291

[121] Ke kamerám a kamerovým systémům [online]. *Úřad pro ochranu osobních údajů* [cit. 7. 10. 2021]. https://www.uoou.cz/casto-kladene-otazky-ke-kameram-a-kamerovym-systemum/ds-5041/archiv=1&p1=2619

[122] Ke kamerovému systému na městském úřadě [online]. *Úřad pro ochranu osobních údajů* [cit. 20. 10. 2021]. https://www.uoou.cz/ke-kamerovemu-systemu-na-mestskem-urade/d-1753/p1=1099

[123] Kontrola subjektu provozujícího kamerový systém v bytovém domě [online]. *Úřad pro ochranu osobních údajů* [18. 4. 2021]. https://www.uoou.cz/kontrola-subjektu-provozujiciho-kamerovy-system-v-bytovem-dome-svj-pro-dum-c-1832-u-cihelny-1832-lysa-nad-labem/ds-4370/p1=4370&archiv=2

[124] Koorn, R. ter Hart, J. Privacy by design: from privacy policy to privacy enhancing technologies [online]. *Compact* 2020 [cit. 2. 9. 2021]. https://www.compact.nl/en/articles/privacy-by-design-from-privacy-policy-to-privacy-enhancing-technologies/

[125] Kulatý stůl k využívání online kamer a dalších sledovacích zařízení [online]. *Úřad pro ochranu osobních údajů* [cit. 20. 10. 2021]. https://www.uoou.cz/kulaty-stul-k-vyuzivani-online-kamer-a-dalsich-sledovacich-zarizeni/d-20310/p1=1099

[126] Lomas, N. European Parliament backs ban on remote biometric surveillance [online]. *Verizon Media* 2021. [20. 10. 2021]. https://techcrunch.com/2021/10/06/european-parliament-backs-ban-on-remote-biometric-surveillance/

[127] Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data [online]. *Council of Europe* [cit. 18. 10. 2021]. https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

[128] Možnosti užívání audiovizuálních systému ve školských zařízeních [online]. MŠMT [cit. 19. 10. 2021]. https://www.msmt.cz/vzdelavani/socialni-programy/moznosti-uzivani-audiovizualnich-systemu-ve-skolskych

[129] Nonnemann, F. Vztahuje se GDPR i na online kamery? [online]. *epravo.cz* [cit. 15. 10. 2021]. https://www.epravo.cz/top/clanky/vztahuje-se-gdpr-i-na-online-kamery-110746.html

[130] Počty nakupujících hlídají v některých obchodech kamery [online]. *Česká televize* [cit. 3. 9. 2021]. https://ct24.ceskatelevize.cz/domaci/3243536-pocty-nakupujicich-hlidaji-v-nekterych-obchodech-kamery

[131] Pokyny 3/2019 ke zpracování osobních údajů prostřednictvím videotechniky [online]. *European Data Protection Board* [cit. 10. 10. 2021]. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_cs.pdf

[132] Stanovisko Úřadu pro ochranu osobních údajů č. 1/2006 [online]. *Úřad pro ochranu osobních údajů* [cit. 12. 10. 2021]. https://www.uoou.cz/files/stanovisko_2006_1.pdf

[133] Stanovisko Úřadu pro ochranu osobních údajů [online]. *Úřad pro ochranu osobních údajů* [cit. 18. 4. 2021]. https://www.uoou.cz/stanovisko-c-1-2016-umisteni-kamerovych-systemu-v-nbsp-bytovych-domech/d-18866/p1=1099

[134] Use of artificial intelligence by the police: MEPs oppose mass surveillance [online]. *European Parliament* [cit. 20. 10. 2019] https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance

[135] Veřejný prostor [online]. *Kancelář architekta města Brna* [cit. 20. 9. 2021]. https://kambrno.cz/verejny-prostor/

[136] Veřejný prostor [online]. *Uzemi.eu* [cit. 20. 9. 2021]. http://www.uzemi.eu/pojmy/verejny-prostor

[137] Wagnerová, E. Čl. 10. In: Wagnerová, E. et al. *Listina základních práv a svobod: komentář*. Praha: Wolters Kluwer, 2012. In: ASPI [Právní informační systém].

[138] What is privacy [online]. *International Association of Privacy Professionals.* 2021. [cit. 8. 4. 2021]. https://iapp.org/about/what-is-privacy

[139] What's ‚Privacy'? [online]. *Xamax Consultancy Pty Ltd.* 1995-2021. [cit. 20. 9. 2021]. http://www.rogerclarke.com/DV/Privacy.html

6.5 OSTATNÍ ZDROJE

[140] Konzultace s panem Davidem Střelcem, srpen 2021.

[141] Konzultace s panem Františkem Nonnemannem, říjen 2021.

[142] Přednáška profesora Václava Matyáše v rámci předmětu Ochrana dat a informačního soukromí na Fakultě informatiky Masarykovy univerzity, podzim 2017.

[143] Webinář Jany Otčenáškové pořádaný v rámci projektu UNIque Law na téma Sdílení prostoru: veřejný vs. soukromý prostor, 18. 2. 2021. Záznam: https://unique.law/2021/01/19/sdileni-prostoru-verejny-versus-soukromy-prostor/

[144] Jan Hodermarsky, 2021.

---

https://doi.org/10.5817/RPT2022-1-5

SMĚRNICE O DIGITÁLNÍM OBSAHU A JEJICH IMPLEMENTACE V PRÁVNÍM ŘÁDU ČR[1]

ZUZANA LIMBERGOVÁ[2]

ABSTRAKT:

Článek pojednává o unijní právní úpravě poskytování digitálního obsahu a digitálních služeb ve směrnici Evropského parlamentu a Rady (EU) 2019/770 a právní úpravě smluv o prodeji zboží s digitálními prvky podle směrnice Evropského parlamentu a Rady (EU) 2019/771. Obsahuje popis a analýzu navrhované transpozice těchto unijních norem do právního řádu České republiky včetně problematických částí a dopadu do současného pojetí smluv a věcí v českém občanském právu.

KLÍČOVÁ SLOVA:

Digitální obsah, digitální služby, DCD, zboží s digitálními prvky, SGD, osobní údaje, spotřebitelské právo, ochrana spotřebitele

ABSTRACT:

The article deals with the EU legislation on the provision of digital content and digital services in Directive (EU) 2019/770 of the European Parliament and of the Council and the legislation on contracts for the sale of goods with digital elements under Directive (EU) 2019/771 of the European Parliament and Council.

---

[1] Článek vznikl jako závěrečná práce v rámci programu LL. M. v právu informačních a komunikačních technologií Právnické fakulty Masarykovy univerzity.

[2] JUDr. Zuzana Limbergová, LL.M je absolventkou Právnické fakulty Univerzity Karlovy v Praze a programu LL. M. v právu informačních a komunikačních technologií Právnické fakulty Masarykovy univerzity. Profesně působí jako advokátka v Praze. Kontaktní e-mail: zuzana.limbergova@aklimbergova.cz

It contains a description and analysis of the proposed transposition of these EU standards into the Czech legal system, including problematic issues and the impact on the current concept of contracts and things in Czech civil law.

KEYWORDS:

Digital Content, Digital Services, DCD, Goods with Digital Elements, SGD, Personal Data, Consumer Law, Consumer Protection

1. ÚVOD

Dne 20. 5. 2019 přijaly Evropský parlament a Rada Evropské unie dvě směrnice věnující se některým aspektům digitálního obchodu. Jedná se o Směrnici Evropského parlamentu a Rady (EU) 2019/770 o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb (dále také uváděna pod zkratkou „DCD“) a Směrnici Evropského parlamentu a Rady (EU) 2019/771 o některých aspektech smluv o prodeji zboží, o změně nařízení (EU) 2017/2394 a směrnice 2009/22/ES a o zrušení směrnice 1999/44/ES (dále také uváděna pod zkratkou „SGD“); obě směrnice společně jsou dále v textu uváděny jako „směrnice“.

První z uvedených směrnic se věnuje v unijním právu dosud významněji neupravenému tématu poskytování digitálního obsahu a digitálních služeb, druhá upravuje obecnější téma prodeje zboží, kde nahrazuje stávající úpravu obsaženou ve směrnici 1999/44/ES tak, aby lépe odpovídala současným potřebám trhu. Směrnice o některých aspektech smluv o prodeji zboží tak nově stanoví požadavky, které se vztahují na prodej zboží s digitálními prvky, což dosud jako samostatné téma smluv o prodeji zboží řešeno nebylo. Oba právní předpisy jsou primárně určeny k ochraně spotřebitele, jejich dopad je však širší. To ostatně předpokládá i unijní normotvůrce, když uvádí jako cíle sledované novou právní úpravou nejen zajištění vysoké úrovně ochrany spotřebitele na vnitřním trhu, ale i udržení a posílení konkurenceschopnosti Unie na světových trzích, rozvoj digitální ekonomiky

Unie a stimulaci celkového růstu.[3] Tyto cíle pak odpovídají jednomu z obecných účelů unijního práva – zajištění fungování vnitřního trhu.[4]

Obě směrnice upravují v zásadě stejné aspekty smluv, a to: dobu plnění, práva v případě prodlení s plněním, soulad plnění se smlouvou – v objektivní a subjektivní rovině, práva z vadného plnění a právo postihu mezi podnikateli.

V článku se detailněji zabývám směrnicí o poskytování digitálního obsahu a digitálních služeb. Pokud jde o směrnici o některých aspektech smluv o prodeji zboží, věnuji se pouze specifické oblasti zboží s digitálními prvky.

Obě směrnice stanoví požadavek plné harmonizace, členské státy se proto mohou odchýlit od ustanovení směrnic ať již nastavením přísnějšího, nebo naopak benevolentnějšího režimu, pouze v případech, kdy to směrnice výslovně dovolují.[5] Transpozice obou směrnic měla být provedena do 1. 7. 2021, nová právní úprava se pak použije od 1. 1. 2022.

Za účelem transpozice uvedených směrnic byl Ministerstvem spravedlnosti připraven legislativní návrh zákona, kterým se navrhuje změna občanského zákoníku.[6] Návrh zákona byl projednáván Poslaneckou sněmovnou parlamentu ČR jako sněmovní tisk č. 994 (dále v textu označován jako „návrh zákona“), před dokončením projednání skončilo volební období Poslanecké sněmovny, návrh zákona zatím nebyl schválen. Nelze proto vyloučit, že konečné znění vnitrostátní právní úpravy implementující shora uvedené směrnice se bude částečně odlišovat od obsahu návrhu, který je podkladem pro zpracování tohoto článku. S ohledem na režim plné harmonizace však pravděpodobně nelze očekávat zásadní odchylky. Návrh zákona obsahovala kromě ustanovení sloužících transpozici shora uvedených směrnic také návrh dalších úprav občanského zákoníku zejména napravujících chyby a nedostatky v předchozích transpozicích evropské legislativy.[7]

[3] Recitál 1 DCD a recitály 1 a 4 SGD.

[4] Čl. 26 Smlouvy o fungování Evropské unie, čl. 1 DCD, čl. 1 SGD.

[5] Čl. 4 DCD, čl. 4 SGD.

[6] Zák. č. 89/2012 Sb., občanský zákoník.

[7] Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 29.

V tomto článku se věnuji pouze těm částem návrhu zákona, které slouží k transpozici DCD a části SGD věnované smlouvám o koupi zboží s digitálními prvky.

Článek se zaměřuje na přiblížení nové právní úpravy přijaté na evropské úrovni a jejích problematických bodů, a dále zejména na navrhované znění českého transpozičního zákona, včetně zdůraznění oblastí, ve kterých podle mého názoru není provedení transpozice navrhováno správně, resp. trpí potenciálními dílčími problémy. Postupně tak jsou rozebírána v pěti kapitolách jednotlivá dílčí témata nové právní úpravy s cílem čtenáře seznámit s vývojem, podstatou, principy i dílčími instituty nové právní úpravy, a dále zdůraznit potenciálně problematická místa jak unijní úpravy samotné, tak její navržené transpozice.

2. VÝVOJ A KONTEXT PRÁVNÍ ÚPRAVY

Téma digitálního obsahu a jeho poskytování spotřebitelům bylo v minulosti v evropském právu upraveno pouze dílčím způsobem ve směrnici Evropského parlamentu a Rady (EU) 2011/83 o právech spotřebitelů, která smlouvy o poskytování digitálního obsahu zařadila do oblasti svojí působnosti, aniž by se ale tomuto tématu věnovala detailně. V pojetí směrnice o právech spotřebitelů, je-li digitální obsah poskytnut na hmotném nosiči, měl by být považován za zboží ve smyslu této směrnice. Smlouvy týkající se digitálního obsahu, který není poskytnut na hmotném nosiči, by naopak pro účely směrnice o právech spotřebitelů neměly být klasifikovány jako kupní smlouvy ani jako smlouvy o poskytování služeb. Zároveň směrnice o právech spotřebitelů zakotvila rovněž v souvislosti s poskytováním digitálního obsahu obchodníkům informační povinnosti, včetně povinnosti poskytovat informace o funkčnosti a příslušné interoperabilitě digitálního obsahu, a spotřebitelům možnost odstoupení od smlouvy ve stanovené lhůtě před zahájením jejího plnění, resp. v případě hmotných nosičů před porušením jejich obalu.

Důležitým krokem na cestě regulace obchodu s digitálním obsahem bylo v roce 2011 představení návrhu nařízení obsahujícího společnou úpravu

prodeje zboží „Common European Sales Law“ (CESL).[8] Cílem tohoto návrhu bylo zlepšit fungování vnitřního trhu tím, že se podnikatelům zjednoduší rozšiřování přeshraničního obchodu a spotřebitelům přeshraniční nakupování. Nařízení CESL mělo obsahovat samostatný a jednotný soubor pravidel smluvního práva obsahující i ustanovení na ochranu spotřebitele. Mělo se jednat o pravidla pro přeshraniční transakce týkající se prodeje zboží, dodání digitálního obsahu a poskytování souvisejících služeb. Nařízení CELS mělo existovat jako paralelní právní úprava pro smlouvy o prodeji vedle vnitrostátních právních úprav. Zároveň bylo zvoleno neobvyklé právní řešení, kdy na rozdíl od ostatních nařízení EU, jejichž právní normy se stávají závaznou součástí vnitrostátního práva členských států s přímou aplikovatelností, použití CESL mělo být otázkou volby a dohody smluvních stran. Mj. právě toto neobvyklé řešení narazilo v legislativním procesu na obtíže. Po dlouhých diskusích, kdy byla např. navrhována změna CESL z nařízení na směrnici nebo omezení jeho působnosti pouze na přeshraniční prodeje uzavírané mezi obchodníky a spotřebiteli, zařadila Komise v prosinci 2014 návrh CELS na seznam návrhů k přepracování nebo zpětvzetí.[9] K oficiálnímu zpětvzetí návrhu došlo však až dne 29. 9. 2020.[10]

V mezidobí byla v květnu 2015 představena ve formě sdělení Komise Strategie pro jednotný digitální trh v Evropě.[11] Tato strategie vytvořila politický základ pro tvorbu a přijetí odpovídající legislativy. Jedním z pilířů Strategie pro jednotný digitální trh v Evropě bylo „*zlepšení přístupu spotřebitelů a podniků ke zboží a službám on-line v celé Evropě*“,[12] kterého má být dosaženo mj. i přijetím jednotných pravidel přeshraničního elektronického

[8] NÁVRH NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o společné evropské právní úpravě prodeje. COM/2011/0635 final - 2011/0284 (COD). Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52011PC0635.

[9] European Parliament. Legislative train schedule. Connected digital single market. [Online]. 2019. [cit. 17. 06. 2021]. https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-common-european-sales-law

[10] Zpětvzetí návrhů Komise. 2020/C 321/03. [Online]. 2020. [cit. 17. 06. 2021]. Dostupné z: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52020XC0929%2802%29.

[11] Strategie pro jednotný digitální trh v Evropě. COM(2015) 192 final [Online]. 2015. [cit. 17. 06. 2021]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192.

obchodu, na která se mohou spolehnout spotřebitelé i podniky napříč společným trhem. Krátce po přijetí Strategie pro jednotný digitální trh v Evropě Komise představila návrhy dvou směrnic harmonizujících některé aspekty smluvního práva ve vztahu k on-line prodejům a poskytování služeb. Jednalo se o návrh Směrnice Evropského parlamentu a Rady o některých aspektech smluv o poskytování digitálního obsahu,[13] který se stal základem dnešního znění DCD, a návrh Směrnice Evropského parlamentu a Rady o některých aspektech smluv o prodeji zboží online a jinými prostředky na dálku,[14] který byl později rozšířen na prodej zboží obecně a stal se základem SGD. Obě směrnice byly přijaty v květnu 2019 a jejich transpozice měla být provedena do 1. 7. 2021, k čemuž v České republice dosud[15] nedošlo. Nové předpisy se pak mají použít od 1. 1. 2022.

Projednávání a přijetí návrhů obou směrnice se neobešlo bez kontroverzí, což se projevilo v mnoha změnách provedených až v průběhu legislativního procesu. Např. otázky jako, která ze směrnic má upravovat zboží s digitálními prvky nebo poskytnutí jakých kategorií dat (tj. osobních údajů nebo jakýchkoli dat) jako formy protiplnění za poskytování digitálního obsahu nebo služeb bude směrnicemi regulováno, byly řešeny až právě v průběhu legislativního procesu. Stejně tak úprava souladu digitálního obsahu se smlouvou se v legislativním procesu podstatně změnila, když původně byla postavena na subjektivních požadavcích, zatímco nyní jsou upřednostněny objektivní, tedy na obsahu smlouvy nezávislé, požadavky.

Směrnice samozřejmě nestojí v evropském právu osamoceně. Navazují jednak na primární právo, a dále mají návaznost a souvislost na další prameny sekundárního práva.

Právním základem obou směrnic jsou články 26 odst. 1 a 2, 114 a 169 odst. 1 a odst. 2 písm. a) Smlouvy o fungování Evropské unie.[16] Jedná se tedy o harmonizaci práva členských států k podpoře zájmů spotřebitelů

[12] Strategie pro jednotný digitální trh v Evropě. COM(2015) 192 final [Online]. 2015. [cit. 17. 06. 2021], s. 3.

[13] COM (2015) 634 final.

[14] COM (2015) 635 final.

[15] Prosinec 2021.

[16] Viz recitál 2 DCD a recitál 2 SGD.

a k zajištění vysoké úrovně ochrany spotřebitelů za účelem vytvoření a fungování vnitřního trhu.

Obě směrnice mají úzkou souvislost s ostatními směrnicemi na ochranu spotřebitele, zejména směrnicí o právech spotřebitelů[17] a směrnicí o nepřiměřených podmínkách ve spotřebitelských smlouvách,[18] a dále pak směrnicí o žalobách na zdržení se jednání v oblasti ochrany zájmů spotřebitelů[19] a nařízení o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování právních předpisů na ochranu zájmů spotřebitelů.[20] SGD zároveň s účinností od 1. 1. 2022 ruší směrnici o některých aspektech prodeje spotřebního zboží.[21] Další oblastí právní regulace, se kterou obě směrnice úzce souvisí, je právo autorské, tedy z pohledu evropské právní úpravy zejména směrnice o harmonizaci určitých aspektů autorského práva,[22] směrnice o autorském právu a právech s ním souvisejících na jednotném digitálním trhu,[23] směrnice o právní ochraně počítačových programů,[24] směrnice o právu na pronájem a půjčování a o některých právech v oblasti duševního vlastnictví souvisejících s autorským právem[25]

---

[17] Směrnice Evropského parlamentu a Rady 2011/83/EU ze dne 25. října 2011 o právech spotřebitelů, kterou se mění směrnice Rady 93/13/EHS a směrnice Evropského parlamentu a Rady 1999/44/ES a zrušuje směrnice Rady 85/577/EHS. a směrnice Evropského parlamentu a Rady 97/7/ES Text s významem pro EHP

[18] Směrnice Rady 93/13/EHS ze dne 5. dubna 1993 o nepřiměřených podmínkách ve spotřebitelských smlouvách.

[19] Směrnice Evropského parlamentu a Rady 2009/22/ES ze dne 23. dubna 2009 o žalobách na zdržení se jednání v oblasti ochrany zájmů spotřebitelů.

[20] Nařízení Evropského parlamentu a Rady (EU) 2017/2394 ze dne 12. prosince 2017 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování právních předpisů na ochranu zájmů spotřebitelů a o zrušení nařízení (ES) č. 2006/2004.

[21] Směrnice Evropského parlamentu a Rady 1999/44/ES ze dne 25. května 1999 o některých aspektech prodeje spotřebního zboží a záruk na toto zboží.

[22] 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.

[23] 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.

[24] Směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23. dubna 2009 o právní ochraně počítačových programů.

a směrnice o audiovizuálních mediálních službách.[26] V neposlední řadě je potřeba zmínit souvislost směrnic s právní úpravou ochrany osobních údajů obsaženou zejména v GDPR, která má v případě konfliktu aplikační přednost.[27] Zároveň DCD obsahuje obecné pravidlo upravující vztah ke speciálním právním úpravám, podle kterého v případě rozporu jakéhokoli ustanovení DCD s ustanoveními jiného právního aktu Evropské unie upravujícího konkrétní odvětví nebo předmět má ustanovení jiného aktu přednost.[28]

Na rozdíl od dřívější harmonizace spotřebitelského práva byla v případě DCD a SGD zvolena nikoli minimální, ale plná úroveň harmonizace. Členské státy se proto mohou od směrnic v harmonizované oblasti odchýlit pouze v případě, že to směrnice výslovně dovolují.[29] Takto by mělo být zajištěno, že *„úroveň ochrany bude pro všechny spotřebitele v celé EU stejně vysoká“.*[30]

Obě směrnice zároveň obsahují ustanovení vymezující jejich vzájemný vztah. DCD se nepoužije na digitální obsah nebo digitální služby obsažené ve zboží nebo s tímto zbožím propojené, jestliže jsou podle kupní smlouvy poskytovány s tímto zbožím. Na tento digitální obsah nebo služby se bude vztahovat SGD, a to i v případě, kdy digitální obsah nebo službu poskytuje osoba odlišná od prodávajícího. V případě pochybností, zda je digitální obsah nebo služba, které jsou ve zboží obsaženy nebo s ním propojeny, součástí kupní smlouvy, se má za to, že digitální obsah nebo digitální služba jsou podřízeny kupní smlouvě.[31] SGD se ale nepoužije na kupní smlouvy,

[25] 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.

[26] Směrnice Evropského parlamentu a Rady 2010/13/EU ze dne 10. března 2010 o koordinaci některých právních a správních předpisů členských států upravujících poskytování audiovizuálních mediálních služeb.

[27] Čl. 3 odst, 8 DCD.

[28] Čl. 3 odst. 7 DCD.

[29] Čl. 4 DCD, čl. 4 SGD.

[30] Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o některých aspektech smluv o poskytování digitálního obsahu OM/2015/0634 final - 2015/0287, s. 6.

[31] Čl. 3 odst. 4 DCD, čl. 3 odst. 3 SGD.

jejichž předmětem plnění je hmotný nosič sloužící výhradně jako nosič digitálního obsahu – v takovém případě se použije pouze DCD.[32]

Začlenění do českého vnitrostátního práva bylo navrženo provedením kompletní transpozice obou směrnic výhradně novelizací občanského zákoníku, konkrétně jeho části čtvrté upravující relativní majetková práva.[33]

3. PŘEDMĚT, ÚČEL A PŮSOBNOST

3.1 PŘEDMĚT A ÚČEL PRÁVNÍ ÚPRAVY

Předmětem právní úpravy jsou u obou směrnic výhradně smlouvy a smluvní vztahy, zároveň z hlediska subjektů omezené pouze na smluvní vztahy uzavírané mezi obchodníky (podnikateli) a spotřebiteli.[34] V případě DCD je pak předmět právní úpravy dále omezen na smlouvy o poskytování digitálního obsahu nebo digitálních služeb a v případě SGD pouze na kupní smlouvy. Obě směrnice navíc neobsahují komplexní právní úpravu uvedených smluvních vztahů a omezují se co do předmětu pouze na vybrané dílčí aspekty, a to zejména soulad plnění se smlouvou, prostředky nápravy v případě nesouladu včetně podmínek jejich uplatnění, a v případě DCD pak ještě úpravy digitálního obsahu nebo digitální služby.[35]

V případě transpozice do české vnitrostátní úpravy je zákonodárcem navrhováno širší pojetí předmětu právní úpravy, kdy část právních norem upravujících poskytování digitálního obsahu nebo digitálních služeb má mít obecnou závaznost a aplikovat se tak nejen na smluvní vztahy mezi podnikateli a spotřebiteli, ale i mezi podnikateli navzájem. Český zákonodárce odůvodňuje toto rozšíření komplexností a specifičností digitálních produktů, kdy pro jejich uživatele může být obtížné prokazovat některé skutečnosti, a je tak na místě zvláštní úprava, která část povinností přenese

[32] Čl. 3 odst. 4 písm. a) SGD, čl. čl. 3 odst. 3 DCD.

[33] Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994.

[34] „Spotřebitelem" se rozumí fyzická osoba, která v souvislosti se smlouvami jedná za účelem, který nelze považovat za její obchodní činnost, podnikání, řemeslo nebo povolání (čl. 2 odst. 2 SGD, čl. 2 odst. 6 DCD).

[35] Čl. 1 DCD, čl. 1 SGD.

na poskytovatele digitálního obsahu nebo digitálních služeb jakožto odborníka disponujícího potřebnými znalostmi a technologiemi.[36] Nutno dodat, že přímo směrnice možnost rozšíření použití harmonizovaných pravidel rovněž mimo spotřebitelské smluvní vztahy výslovně zmiňují.[37]

Účelem právní úpravy je *přispět k řádnému fungování vnitřního trhu a zároveň poskytovat vysokou úroveň ochrany spotřebitele.*[38] Podle preambule by harmonizace některých aspektů smluv o poskytování digitálního obsahu nebo digitálních služeb měla vést ke zvýšení právní jistoty spotřebitelů i poskytovatelů digitálního obsahu nebo služeb a ke snížení transakčních nákladů. Tím by pak mělo být dosaženo skutečně jednotného unijního digitálního trhu, posílení konkurenceschopnosti podniků z unijních států na světových trzích a stimulace celkového růstu.[39] Unijní normotvůrce zde vycházel ze závěrů zjištěných bleskovým průzkumem Eurobarometr 396 (2014), ve kterém velká část podniků prodávajících produkty nebo služby on-line uvádí jako jednu z hlavních překážek pro přeshraniční prodej právě rozdíly ve smluvním právu jednotlivých států.[40]

Relativně úzce vymezený předmět právní úpravy spolu s požadavkem plné harmonizace a naopak široce pojatý účel mohou vést potenciálně ke vzniku konfliktů a nežádoucím důsledkům různých způsobů transpozice v jednotlivých státech. Jak uvádí Schulze,[41] podstatné rozdíly mohou nastat např. u různých právních úprav důsledků neposkytnutí nebo nesouladu digitálního obsahu nebo digitální služby, pokud je toto neposkytnutí způsobeno překážkou, na kterou nemá poskytovatel digitálního obsahu nebo digitální služby vliv a nelze očekávat, že tuto překážku nebo její důsledky předejde nebo odstraní. Regulaci těchto právních důsledků totiž ponechává

[36] Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 84.

[37] Recitál 16 DCD, recitál 21 SGD.

[38] Viz čl. 1 DCD, čl. 1 SGD.

[39] Recitál 3 a recitál 1 DCD, recitál 1 a recitál 2 SGD.

[40] Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o některých aspektech smluv o poskytování digitálního obsahu OM/2015/0634 final - 2015/0287, s. 2.

[41] SCHULZE, R. *Conflicts between purpose and limited subject matter*. In SCHULZE, R., STAUDENMAYER, D. *EU Digital Law: Article-by-Article Commentary*, Baden-Baden, Germany: Nomos, 2020. s. 42.

DCD i nadále plně v gesci členských států,[42] kde však mohou jednotlivé právní úpravy a jejich důsledky vykazovat značné rozdíly, což může vést jak ke snížení ochrany spotřebitele, tak i k negativnímu dopadu na odstraňování překážek fungování vnitřního trhu.

3.2 OBLAST PŮSOBNOSTI

Oblast působnosti obou směrnic je vymezena jednak positivně, a dále negativně výčtem smluv, na které se směrnice nevztahují. Positivní vymezení působnosti bylo již částečně zmíněno v předchozí kapitole v rámci pojednání o předmětu právní úpravy. Obě směrnice se tedy vztahují pouze na smluvní vztahy mezi spotřebitelem a podnikatelem.[43]

V případě SGD je působnost positivně omezena na kupní smlouvy, kterými se rozumí pouze smlouvy o úplatném převodu vlastnictví zboží, které je definováno jako hmotné movité předměty,[44] a to včetně smluv týkajících se dodání zboží, které má být teprve vyrobeno nebo zhotoveno.[45] Negativní vymezení zahrnuje kupní smlouvy na:

a) hmotné nosiče, které slouží výhradně jako nosiče digitálního obsahu; na ty se bude vztahovat naopak DCD;
b) zboží prodávané na základě výkonu rozhodnutí či jiných soudních opatření – z pohledu českého práva se bude jednat zejména o exekuce, soudní prodej zástavy nebo prodej v insolvenčním řízení.

DCD se z hlediska positivního vymezení působnosti vztahuje na smlouvy o úplatném poskytnutí digitálního obsahu nebo digitální služby. Tato základní oblast působnosti je však rozšířena i na smlouvy o poskytnutí digitálního obsahu nebo digitální služby výměnou za poskytnutí osobních údajů spotřebitele, vyjma případů, kdy podnikatel spotřebitelem poskytnuté osobní údaje zpracovává výhradně pro účely poskytování digitálního obsahu nebo digitální služby nebo pro účely dodržení zákonných

[42] Recitál 14 DCD.

[43] Český překlad směrnic používá termín „obchodník“ s ohledem na terminologii českého soukromého práva je ale v tomto článku používán termín „podnikatel“ ve smyslu ust. § 420 o. z.

[44] Čl. 2 odst. 5 SGD.

[45] Čl. 3 odst. 2 SGD.

požadavků.[46] Zahrnuty do oblasti působnosti jsou rovněž smlouvy o vytvoření digitálního obsahu nebo digitální služby podle specifikací spotřebitele,[47] tedy zejména smlouvy o dílo.

Návrh zákona vymezuje oblast působnost částečně odchylně. Jak již bylo shora uvedeno, vztahuje právní úpravu smluv o poskytování digitálního obsahu a digitálních služeb (resp. služeb digitálního obsahu, viz dále kapitola 4.1.2) na veškeré smlouvy, tedy i uzavřené mimo spotřebitelské smluvní vztahy se zachováním podmínky jejich úplatnosti.[48]

Zároveň však vymezuje nový smluvní typ tak, že smlouvou o poskytování digitálního obsahu se poskytovatel zavazuje zpřístupnit uživateli digitální obsah k *užívání pro vlastní potřebu* a uživatel se zavazuje platit za to odměnu.[49] Bohužel navrhovatel zákona v důvodové zprávě nijak neobjasňuje, proč se rozhodl omezit působnost právní úpravy jen na užívání *pro vlastní potřebu*, ačkoli ani pro smlouvy uzavírané se spotřebitelem DCD takové omezení nestanoví. Zároveň není z důvodové zprávy zřejmé, jak má být toto omezení vykládáno. Zda se právní úprava nebude např. vztahovat na případy pořízení digitálního obsahu pro jiného člena rodiny nebo pro jinou právnickou osobu v rámci jednoho koncernu, protože se již nejedná o *vlastní potřebu,* nebo zda tyto případy jsou ještě *vlastní potřebou.* Výraz by mohl být vykládán podobně jako slovní spojení *pro osobní potřebu fyzické osoby či vlastní vnitřní potřebu právnické osoby či podnikající fyzické osoby* použité v ust. § 25, § 30 a § 30a autorského zákona. Osobní potřeba fyzické osoby ve smyslu autorského zákona je doktrínou a judikaturou chápána jako potřeba soukromá, zahrnující užití autorského díla nejen příslušnou fyzickou osobou, ale i dalšími osobami v omezeném okruhu její domácnosti nebo osob blízkých.[50] Užití pro vlastní vnitřní potřebu právnické osoby

[46] Čl. 3 odst. 1 DCD.

[47] Čl. 3 odst. 2 DCD.

[48] Viz navrhované znění § 2389a o.z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994.

[49] Viz navrhované znění § 2389a o.z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994.

[50] Srov. např. MYŠKA, M. § 30. *Volná užití.* In POLČÁK, Radim a kol. *Autorský zákon. Praktický komentář s judikaturou.* Praha: Leges, 2020. s. 292.

nebo podnikající fyzické osoby je pak chápáno jako neveřejné užití v rámci vnitřní organizační struktury příslušného podnikatele.[51] Gramaticky se však formulace použitá v návrhu novelizace občanského zákoníku od autorského zákona liší, i jejich účel bude zřejmě rozdílný. Nedává smysl, na rozdíl od oblasti autorského práva, regulovat užívání digitálního obsahu pouze na soukromou oblast uživatele. Ostatně přímo důvodová zpráva návrhu zákona zdůrazňuje, že právní úprava se má vztahovat i na jiné než spotřebitelsko-podnikatelské vztahy. V případě smluvního vztahu dvou podnikatelů zpravidla nebude účelem uzavření smlouvy užití digitálního obsahu nebo poskytnutí služby digitálního obsahu výlučně pro soukromé účely. V případě přijetí návrhu zákona v tomto znění bude zejména na rozhodovací praxi soudů, aby nalezla odpovídající výklad. Zároveň je otázkou, jakým způsobem budou posuzovány úplatné smlouvy, na základě kterých bude poskytován digitální obsah nebo služby digitálního obsahu pro jinou než vlastní potřebu uživatele. V takovém případě by se smluvní vztah na základě analogie legis (ust. § 10 odst. 1 o. z.) posuzoval pravděpodobně stejně podle ustanovení občanského zákoníku upravujících poskytování digitálního obsahu.

Pouze na spotřebitelsko-podnikatelské smluvní vztahy se má nová právní úprava vztahovat i podle návrhu zákona v případech, kdy namísto úplaty jsou spotřebitelem poskytovány jeho osobní údaje (vyjma případů jejich zpracování pouze pro účely poskytnutí digitálního obsahu nebo služby digitálního obsahu nebo výhradně pro splnění zákonných povinností poskytovatele digitálního obsahu či služby), a dále pokud jde o smlouvu o zhotovení digitálního obsahu.[52]

DCD dále obsahuje v čl. 3 odst. 5 výčet smluv, které jsou naopak vyňaty z její působnosti. Z působnosti DCD jsou vyloučeny smlouvy týkající se:

---

[51] Viz MYŠKA, M. § 30a. *Rozmnožování na papír nebo podobný podklad.* In POLČÁK, Radim a kol. *Autorský zákon. Praktický komentář s judikaturou.* Praha: Leges, 2020. s. 302.

[52] Viz navrhované znění § 2389g odst. 3 a o. z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994 a Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 89.

a) poskytování služeb, které nejsou digitálními službami, bez ohledu na to, zda obchodník používá digitální formy či prostředky k produkci služby, nebo k jejímu dodání spotřebiteli či jejímu přenosu k němu;
b) služeb elektronických komunikací[53] s výjimkou interpersonálních komunikačních služeb nezávislých na číslech;
c) zdravotní péče;[54]
d) služeb hazardních her, totiž služeb spojených s peněžitým vkladem do her s prvkem náhody, včetně her s prvkem dovednosti, jako jsou loterie, hry v kasinu, pokerové hry a sázky, poskytované elektronicky nebo jakoukoli jinou technologií pro usnadnění komunikace a na individuální žádost příjemce těchto služeb;
e) finančních služeb;[55]
f) softwaru nabízeného obchodníkem na základě bezplatné licence s otevřeným zdrojovým kódem, za kterou spotřebitel neplatí cenu, a pokud osobní údaje poskytnuté spotřebitelem zpracovává obchodník výlučně za účelem zlepšení bezpečnosti, kompatibility nebo interoperability tohoto konkrétního softwaru;
g) poskytování digitálního obsahu, při němž je digitální obsah učiněn dostupným široké veřejnosti jinak než přenosem signálu jako součást představení nebo akce, jako například digitální kinematografické projekce;
h) digitálního obsahu poskytnutého v souladu se směrnicí Evropského parlamentu a Rady 2003/98/ES[56] subjekty veřejného sektoru členských států.

Kromě případu uvedeného shora pod písm. a), jehož transpozice není navrhována, přebírá návrh zákona více či méně vhodným způsobem všech-

[53] Ve smyslu čl. 2 bodu 4 směrnice (EU) 2018/1972.

[54] Ve smyslu čl. 2 písm. b) směrnice 2002/65/ES.

[55] Ve smyslu čl. 2 písm. b) směrnice 2002/65/ES.

[56] Resp. směrnicí Evropského parlamentu a Rady (EU) 2019/1024, o otevřených datech a opakovaném použití informací veřejného sektoru, která směrnici Evropského parlamentu a Rady 2003/98/ES nahrazuje.

ny shora uvedené výjimky z působnosti do navrhovaného ustanovení § 2389u odst. 1 o. z.

Výjimka uvedená výše sub a) není do návrhu zákona podle důvodové zprávy přejata pro svou nadbytečnost, kdy je zřejmé z ostatních ustanovení, že na poskytování služeb, které nejsou digitálními službami (resp. v terminologii českého zákona službami digitálního obsahu), regulace nedopadá.[57]

Pokud jde o výjimku uvedenou shora pod písm. f), domnívám se, že v českém překladu směrnice došlo k nedorozumění. Anglické znění uvádí: *software offered by the trader under a free and open-source licence, where the consumer does not pay a price…*, výraz „free" se tak zjevně nevztahuje k ceně („zdarma" či „bezplatně"), protože pak by byla následující věta nadbytečná, ale ke druhu licence, tedy k tzv. svobodným softwarovým licencím free software movement.[58] V českém překladu je však namísto toho uvedena zdvojená informace o požadavku bezplatnosti. Tento problém je možné podle mého názoru překonat výkladem za použití recitálu 32 DCD, kde je i v českém překladu správně uveden *svobodný a open source* software. Zároveň byla tato výjimka do návrhu zákona převzata částečně odchylně jako *poskytování počítačového programu s otevřeným zdrojovým kódem na základě svobodné licence…*[59] Za vhodnější bych považovala převzít doslovně právní úpravu ze směrnice, protože v této podobě by česká právní úprava výjimku (nepřípustně) zužovala. V prvé řadě pojem software je zpravidla vnímán šířeji než pojem počítačový program.[60] Zároveň označení *svobodná licence*, byť není právem definováno, asociuje s ohledem na použitý výraz *„svobodná"* licence Free Software Foundation, které zahrnují pouze část bezplatných licencí s otevřeným zdrojovým kódem, za vhodnější bych proto považovala použití obecnějšího termínu *veřejná licence.*

---

[57] Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 92.

[58] Srov. STAUDENMAYER, D. *Art. 3. Sectoral exemptions.* In SCHULZE, R., STAUDENMAYER, D. *EU Digital Law: Article-by-Article Commentary*, Baden-Baden, Germany: Nomos, 2020. s. 83.

[59] Viz navrhované znění § 2389u odst. 1 písm. e) o. z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994.

[60] Viz např. COLLET, D. § 65. *Počítačové programy*. In POLČÁK, Radim a kol. *Autorský zákon. Praktický komentář s judikaturou.* Praha: Leges, 2020. s. 525.

Výše pod písm. h) uvedená výjimka je rovněž v návrhu zákona formulována odchylně, a to tak, že ustanovení o poskytování digitálního obsahu se nepoužijí na smlouvu, jejímž předmětem je *poskytování informací, které jsou předmětem ochrany práva autorského, podle zákona upravujícího svobodný přístup k informacím.*[61] Zatímco směrnice vztahuje výjimku na veškerý digitální obsah poskytovaný v rámci poskytování informací veřejného sektoru na základě směrnice o opakovaném použití informací veřejného sektoru, návrh české transpozice zúžil výjimku z působnosti pouze na poskytování informací, které jsou předmětem ochrany práva autorského ve smyslu ust. § 14a zákona č. 106/1999 Sb., o svobodném přístupu k informacím.[62] Na poskytování informací podle zákona o svobodném přístupu k informacím, byť ve formě digitálního obsahu, se však právní úprava poskytování digitálního obsahu obsažená v občanském zákoníku vztahovat nebude, protože se nejedná o úplatné poskytnutí digitálního obsahu na základě soukromoprávní smlouvy, ale plnění povinnosti uložené právním předpisem práva veřejného a navíc bezúplatně, resp. pouze za případnou náhradu nákladů, nikoli však za odměnu. Výjimkou jsou právě licenční smlouvy uzavírané podle § 14a zákona o svobodném přístupu k informacím, kde je uzavírána soukromoprávní smlouva a odměnu požadovat lze. Takto by měl být rozsah výjimky stanovené DCD zachován.

Zároveň lze ale ustanovení čl. 3 odst. 5 písm. h) českého znění DCD, které doslova zní: *Tato směrnice se nepoužije na smlouvy* ***týkající se*** *digitálního obsahu* ***poskytnutého*** *v souladu se směrnicí Evropského parlamentu a Rady 2003/98/ES (21) subjekty veřejného sektoru členských států.,* vykládat tak, že uvedená výjimka z působnosti se má vztahovat i na případy, kdy je uzavírána smlouva s poskytovatelem digitálního obsahu, který sám není subjektem veřejného sektoru, ale smlouva se týká digitálního obsahu získaného tímto poskytovatelem od subjektu veřejného sektoru (viz formulace „poskytnutého“, která může zahrnovat i v minulosti poskytnutý obsah), následně

[61] Viz navrhované znění § 2389u odst. 1 písm. g) o. z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994.

[62] Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 93.

zpracovaného do uživatelsky přívětivější podoby a nabízeného za komerčních podmínek. Takovému pojetí by česká transpozice neodpovídala. Jsem však toho názoru, že takovýto výklad je v rozporu s jedním z účelů směrnice, kterým je ochrana spotřebitele. Spotřebitel by byl u části komerčně nabízených digitálních obsahů nebo služeb zbaven této ochrany pouze proto, že se jedná o digitální obsah originálně získaný v režimu zákona o svobodném přístupu k informacím, ačkoli spotřebitel o této skutečnosti vůbec nemusí vědět. Rovněž ze srovnání s jinými jazykovými verzemi směrnice (konkrétně německou, anglickou a slovenskou) lze dojít k závěru, že se jedná o nepřesnost českého znění DCD, kdy správně se uvedená výjimka vztahuje na digitální obsah *poskytovaný* přímo subjekty veřejného sektoru, nikoli těmito subjekty (kdykoli v minulosti) poskytnutý.

DCD pamatuje i na případy, kdy je v jediné smlouvě upraveno dohromady poskytování digitálního obsahu nebo služby a prvky poskytování jiných služeb nebo zboží (tzv. „balíčky“). V takovém případě se DCD použije pouze na prvky smlouvy týkající se digitálního obsahu nebo služby.[63] Návrh zákona se však od tohoto pravidla opět bez uvedení zřejmých důvodů odchyluje. Ačkoli důvodová zpráva odkazuje v zásadě na pravidla obsažená ve směrnici a parafrázuje i příklady uvedené v recitálu 33 DCD,[64] navrhované znění zákona se omezuje pouze na výslovně upravené výjimky z působnosti. Viz navrhované znění § 2389u odst. 2 o.z.: *Obsahuje-li smlouva, na jejímž základě je digitální obsah poskytován, také prvky smluv uvedených v odstavci 1, použijí se ustanovení tohoto oddílu pouze na tu část závazku, která se týká poskytování digitálního obsahu.* Navrhovaná vnitrostátní úprava tak nepokrývá situace, kdy smlouva obsahuje jak prvky smlouvy o poskytování digitálního obsahu, tak prvky smlouvy o poskytování jiných v § 2389u odst. 1 o. z. neupravených služeb. Dochází tím podle mého názoru k neúplné transpozici směrnice. V praxi bude nutné vycházet z obvyklého chápání smlouvy spojující v sobě různé smluvní typy jako smlouvy smíšené a aplikovat na základě § 10 odst. 1 o. z. na část týkající se poskytování

[63] Čl. 3 odst. 6 DCD.

[64] Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 93.

digitálního obsahu nebo služeb digitálního obsahu právní úpravu smlouvy o poskytování digitálního obsahu (§ 2389a a násl. o. z.) a na ostatní části právní úpravu odpovídajícího smluvního typu.[65]

4. DIGITÁLNÍ OBSAH, DIGITÁLNÍ SLUŽBY A ZBOŽÍ S DIGITÁLNÍMI PRVKY

Ústředními věcnými pojmy DCD, které podstatným způsobem vymezují i předmět regulace a rozsah působnosti směrnice, jsou *digitální obsah* a *digitální služba*, SGD k tomu pak přidává termín *zboží s digitálními prvky*.

Právě poskytování digitálního obsahu (nebo digitální služby) je podstatnou náležitostí smlouvy, aby jí bylo možné podřadit režimu DCD a navrhovaných ustanovení oddílu 6, dílu 2 hlavy II. části čtvrté občanského zákoníku. Bez dostatečného vymezení obsahu těchto pojmů tak nelze uchopit ani předmětnou právní úpravu jako celek, proto je v následujících podkapitolách této kapitoly věnována vysvětlení uvedených pojmů včetně právně teoretického pohledu značná pozornost.

4.1 DIGITÁLNÍ OBSAH A DIGITÁLNÍ SLUŽBY

Termín „digitální obsah“ není v evropské legislativě zcela nový, poprvé byl použit ve směrnici Evropského parlamentu a Rady (EU) 2011/83 o právech spotřebitelů. DCD i SGD obsahují zcela shodnou definici. Digitálním obsahem se tak rozumí *data, která jsou vytvořena a dodána v digitální podobě.*[66]

Digitální službu pak směrnice definují[67] jako službu:

- která umožňuje spotřebiteli vytvářet, zpracovávat nebo uchovávat data v digitální podobě nebo k nim mít přístup, nebo
- která umožňuje sdílení dat v digitální podobě nahraných nebo vytvořených spotřebitelem či jinými uživateli této služby nebo jakoukoli jinou interakci s těmito daty.

[65] Srov. PELIKÁNOVÁ, I., PELIKÁN, R. § 1*746. Obsah smlouvy*. In ŠVESTKA, J., DVOŘÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář.* 1. vyd. Praha: Wolters Kluwer, a. s., 2014.

[66] Čl. 2 odst. 1 DCD, čl. 2 odst. 6 SGD.

[67] Čl. 2 odst. 2 DCD, čl. 2 odst. 7 SGD.

Obě definice jsou záměrně široce pojaty, protože by měly být nadčasové a odolávat budoucím rychlým a častým změnám v technologickém vývoji. Směrnice v úvodních ustanoveních uvádí demonstrativní výčet digitálního obsahu, kterým jsou např. počítačové programy, aplikace, videosoubory, audiosoubory, e-knihy nebo digitální hry, a rovněž digitálních služeb, kterými jsou např. služby typu SaaS, sdílení videí, audiozáznamů a jiných souborů, služby cloud computingu a další.[68] Z výše uvedených definic pak vyplývá, že digitální služba vždy zahrnuje vytvoření nebo nakládání s digitálním obsahem, digitální obsah je tedy stěžejním bodem právní úpravy.

Tato skutečnost je zdůrazněna i tím, že v případě, kdy je digitální obsah poskytnut na hmotném nosiči (DVD, USB flash disk apod.), vztahuje se na smlouvu o jeho poskytnutí DCD a z působnosti SGD je naopak takový smluvní vztah vyloučen.[69] Zcela jasně je tak vyzdvižen význam nehmotného digitálního obsahu oproti hmotnému předmětu, který je pouze nosičem.[70] Komplikovanější je v tomto ohledu návrh vnitrostátní právní úpravy, která výslovně vyjímá digitální obsah poskytovaný na hmotném nosiči (vyjma úpravy doby plnění a nároků v případě prodlení s plněním)[71] z úpravy prodeje zboží ve prospěch smlouvy o poskytování digitálního obsahu pouze pro podnikatelsko-spotřebitelské vztahy, ačkoli obecná ustanovení o smlouvě o poskytování digitálního obsahu vztahuje na všechny soukromoprávní smluvní vztahy. V případě digitálního obsahu poskytovaného na hmotném nosiči jinému uživateli než je spotřebitel, bude nutné vyřešit aplikační problém, zda takovou smlouvu posuzovat jako smlouvu o poskytování digitálního obsahu, nebo jako kupní smlouvu o koupi hmotné movité věci. S ohledem na definici digitálního obsahu, který je definován jako věc v digitální podobě a nezahrnuje tedy hmotné movité věci (viz dále), mám za to, že v těchto případech bude nutné postupovat podle právní úpravy kupní smlouvy.

---

[68] Recitál 19 DCD.

[69] Čl. 3 odst. DCD, čl. 3 odst. 4 písm. a) SGD.

[70] HERVÉ, J. Digital Content and Sales or Service contracts under EU Law and Belgian/French Law. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law.* 2017, roč. 8, č. 1, s. 29.

[71] Navrhované znění § 2158 odst. 3 o.z.

Za digitální obsah jsou pak považována nejen data smluvně poskytovaná obchodníkem spotřebiteli, ale i digitální data vytvořená spotřebitelem.

Některá data však digitálním obsahem nejsou. Podle recitálu 23 DCD digitální vyjádření hodnoty, což jsou elektronické poukázky a kupony a rovněž virtuální měny v rozsahu, v jakém jsou uznávány vnitrostátním právem, jejichž účelem je pouze sloužit jako platební metoda, nelze za digitální obsah nebo digitální službu (ve smyslu DCD) považovat.

4.1.1 DIGITÁLNÍ OBSAH

Směrnice se vyhýbají tomu, aby digitální obsah jakkoli právně klasifikovaly. Tento přístup unijního normotvůrce je logický – směrnice bude transponována do právních řádů různých států, kdy v některých může digitální obsah spadat do definice věci v právním smyslu, v jiných bude považován za jiný typ majetkové hodnoty a v dalších může vyžadovat vytvoření zcela nové právní kategorie předmětu právních vztahů. Tuto otázku by měl vyřešit vnitrostátní zákonodárce.

Z pohledu českého práva je tak na místě zejména úvaha, zda je digitální obsah věcí v právním smyslu, a pokud ano, jaká věcná práva k němu lze nabýt. To je dáno velice širokou definicí věcí v právním smyslu v ustanovení § 489 o. z. a navazujícím vymezení nehmotných věcí v § 496 odst. 2 o. z.

Například v Německu, kde je věc právem definována[72] pouze jako fyzický předmět, předpokládá část odborné veřejnosti, že digitální obsah bude chápán jako samostatná kategorie předmětu právních vztahů vedle věcí a nehmotných statků.[73]

Stěžejní pro právní pojetí digitálního obsahu je, že se podle definice evropského normotvůrce jedná o „data“. Český občanský zákoník označuje za věc v právním smyslu vše, co je *rozdílné od osoby a slouží potřebě lidí*.[74] Věci se dále dělí na hmotné a nehmotné. Nehmotnými věcmi jsou práva, jejichž

[72] § 90 BGB.

[73] WENDLAND, M. Sonderprivatrecht für Digitale Güter. *Zeitschrift für Vergleichende Rechtswissenschaft.* 2019, č. 118, s. 204.

[74] § 489 o. z.

povaha to připouští, a *jiné věci bez hmotné podstaty.*[75] K právní povaze dat jako nehmotných věcí uvádí komentářová literatura „*Nehmotnou věcí v právním smyslu je i informace, ale jen v případě, že je pro některý ze subjektů práv využitelná jako ekonomická (nikoli jiná, např. osobnostní) hodnota a zároveň za situace, kdy subjekt, který je jejím původcem, ji zpřístupní jako možný předmět soukromoprávních vztahů a tato informace objektivně má alespoň potenciální majetkovou hodnotu.*“[76] Uvedený komentář používá pojmu „informace“ a nikoli „data“, nicméně z kontextu je zřejmé, že toto vnímání lze vztáhnout na data, když si lze jen obtížně představit, že by subjekt zpřístupnil informaci, která je chápána jako přírodní fenomén projevující se „*změnou míry organizovanosti systému*“[77] jinak než tím způsobem, že zpřístupní data implikující tuto informaci. Termíny „data“ a „informace“ jsou navíc často v právní terminologii navzájem zaměňovány.[78] Rovněž Koukal označuje informace za věci bez hmotné podstaty.[79] Ve vztahu k software jako specifickému druhu dat a zároveň autorskému dílu Tomíšek rovněž dospívá k závěru, že se jedná o věc v právním smyslu.[80]

Detailně se problematice právní povahy dat věnuje Polčák, který dochází k závěru, že „*nedává smysl… data per se objektivizovat, zejm. považovat je za věci v právním smyslu.“* [81] Za věci pak označuje absolutní nebo relativní práva k užití dat, resp. k jejich užitku.[82]

---

[75] § 496 odst. 2 o. z.

[76] SVOBODA, K. § 496. *Věci hmotné a nehmotné.* In ŠVESTKA, J., DVOŘÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář.* 1. vyd. Praha: Wolters Kluwer, a. s., 2014. Svazek I. cit. z ASPI [10. 12. 2020].

[77] MYŠKA, M. *Informace, data a právo.* In POLČÁK, R. a kol., Právo informačních technologií. Praha: Wolters Kluwer, 2018.

[78] K odlišení pojmů „informace“ a „data“ viz blíže POLČÁK, R. Informace a data v právu. *Revue pro právo a technologie*. 2016, roč. 7, č. 13, s. 67-91.

[79] KOUKAL, P. § 496. *Věci hmotné a nehmotné*. In LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1-654)*. Praha: C. H. Beck, 2014.

[80] TOMÍŠEK, J. Software jako věc v režimu nového občanského zákoníku. *Revue pro právo a technologie*. [Online]. 2014, roč. 5, č. 9, s. 207.

[81] POLČÁK, R. Informace a data v právu. *Revue pro právo a technologie*. 2016, roč. 7, č. 13, s. 88.

[82] Tamtéž.

Všichni uvedení autoři se však shodují na tom, že data nejsou předmětem vlastnického práva v subjektivním smyslu a absolutní práva k nim, resp. k jejich užití, mohou mít pouze povahu zvláštních zákonem založených práv, jako je tomu například u práva autorského, jsou-li data autorským dílem.

Předkladatel v návrhu zákona výslovně označuje digitální obsah za *věc v digitální podobě.*[83] Pokud bude návrh zákona v této podobě schválen, bude otázka právní povahy dat zřejmě v českém právu definitivně vyřešena jejich výslovným prohlášením za věci. Důvodová zpráva bohužel toto řešení nijak podrobně neodůvodňuje, když se omezuje na prosté konstatování, že *„vycházíme-li z předpokladu, že je digitální obsah věcí…",*[84] aniž by bylo uvedeno na základě jakých úvah se z tohoto předpokladu vychází.

Definice digitálního obsahu v českém návrhu zákona se částečně liší od definice digitálního obsahu uvedené ve směrnicích. Zatímco směrnice definují digitální obsah jako (jakákoli) *data, která jsou vytvořena a dodána v digitální podobě,* návrh zákona definuje digitální obsah jako *věc v digitální podobě.* Pokud má být zachován euro-konformní výklad pojmu *digitální obsah* jakožto svébytného definovaného pojmu evropského práva, nezbývá jiný závěr, než že data vytvořená a dodávaná v digitální podobě jsou věcí (v digitální podobě). Data v digitální podobě přitom mohou zahrnovat i autorská díla, projevy osobní povahy, osobní údaje včetně např. údajů biometrických, u kterých není závěr o tom, že by měly být věcí v právním smyslu, vůbec jednoznačný – spíše naopak. S ohledem na zákonný požadavek, že věcí je pouze to, co je *rozdílné od osoby,* nejsou např. projevy osobní povahy považovány za věci,[85] u autorských děl je chápání díla jako věci v právním smyslu do určité míry sporné.[86]

---

[83] Viz navrhované znění § 2389a o.z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994.

[84] Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 84.

[85] KOUKAL, P. § 489. *Věci hmotné a nehmotné*. In LAVICKÝ, P. a kol. *Občanský zákoník I. Obecná část (§ 1-654)*. Praha: C. H. Beck, 2014.

[86] SVOBODA, K. § 489. *Definice věci.* In ŠVESTKA, J., DVOŘÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář.* 1. vyd. Praha: Wolters Kluwer, a. s., 2014. Svazek I. cit. z ASPI [10. 12. 2020].

Zároveň zůstává i nadále otevřenou otázka, jaká práva lze k digitálnímu obsahu jakožto věci v právním smyslu nabýt. Zde bude zřejmě nutné nepřistupovat k datům jednotně, ale vycházet vždy z právní povahy konkrétních dat a případné speciální právní úpravy na ně se vztahující.

4.1.2 DIGITÁLNÍ SLUŽBA

Jak bylo shora uvedeno, jsou směrnicemi digitální služby definovány jako služby umožňující spotřebiteli vytvářet, zpracovávat nebo uchovávat data v digitální podobě nebo k nim mít přístup nebo sdílet data v digitální podobě nahraná nebo vytvořená spotřebitelem či jinými uživateli této služby nebo jakoukoli jinou interakci s těmito daty. V původním návrhu DCD nebyly digitální služby definovány jako samostatná kategorie, ale jako jedna z variant digitálního obsahu,[87] k oddělení a vytvoření samostatné definice došlo až v průběhu legislativního procesu. Z definice digitálních služeb vyplývá, že rozhodující je obsah poskytované služby, nikoli způsob jejího poskytování. Toto chápání digitální služby potvrzuje přímo samotné znění DCD, podle kterého se má směrnice použít *bez ohledu na nosič použitý pro přenos nebo zpřístupnění digitálního obsahu nebo digitální služby*.[88] Zároveň byly zvoleny obecné formulace, což by do budoucna mělo zajistit, že i s rozvojem digitálního trhu nově vznikající služby využívající nové, dosud nepoužívané, obchodní modely nebo nová technická řešení budou touto definicí pokryty.

Návrh zákona se od této terminologie odchyluje, když termín *digitální služba* nahradil vlastním termínem *služba digitálního obsahu*. Obsah definice návrh zákona zachovává pouze s (s ohledem na záměr rozšířit právní úpravu smluv o poskytování digitálního obsahu i mimo spotřebitelské vztahy pochopitelnou) odchylkou, kdy termín *spotřebitel* nahrazuje obecnějším *uživatelem.* Důvodem použití vlastní terminologie je podle předkladatele návrhu zákona „*možné širší uplatnění pojmu digitální služba*

[87] Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o některých aspektech smluv o poskytování digitálního obsahu OM/2015/0634 final - 2015/0287 (COD).

[88] Recitál 19 DCD.

v právním řádu“,[89] a to zejména s ohledem na již existující zákon o právu na digitální služby.[90] Osobně považuji český výraz *služba digitálního obsahu* za lépe vystihující obsah a účel předmětných služeb. Zároveň ale nelze vyloučit, že do budoucna bude docházet k určitému pojmovému zmatení, když termín *digitální služba* bude mít různý význam v závislosti na tom, zda je používán v souvislosti s legislativou evropskou nebo vnitrostátní.

4.1.3 SHRNUTÍ

V případě přijetí návrhu zákona ve stávající podobě se budou obsažené definice digitálního obsahu a digitální služby vztahovat nejen na spotřebitelské smlouvy, ale s ohledem na zařazení navrhovaných ustanovení § 2389a a § 2389t do systematiky občanského zákoníku na soukromoprávní smluvní vztahy obecně.

Digitálním obsahem nebo digitální službou budou, jak vyplývá ze shora uvedených definic, i digitální plnění poskytovaná na základě zvláštních právních předpisů, např. kvalifikované certifikáty pro elektronické podpisy nebo elektronické pečetě[91] podle nařízení eIDAS a zák. č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, protože tyto jsou poskytovány na základě soukromoprávní smlouvy uzavřené mezi poskytovatelem služeb a zákazníkem. Zároveň se však definice digitálního obsahu (a stejně tak digitální služby) nebude vztahovat na data poskytovaná na základě předpisů veřejného práva, protože v takovém případě nelze použít občanský zákoník jakožto právní předpis práva soukromého.[92] Ve veřejnoprávních vztazích tak bude nutné vycházet ze samostatných definic obsažených v příslušných speciálních právních předpisech.

---

[89] Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 31.

[90] Zák. č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů.

[91] HERVÉ, J. Digital Content and Sales or Service contracts under EU Law and Belgian/French Law. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*. 2017, roč. 8., č. 1, s. 29.

[92] § 1 odst. 1 o. z.

4.2 ZBOŽÍ S DIGITÁLNÍMI PRVKY

Dalším z nových a věcně důležitých pojmů zavedených směrnicemi je *zboží s digitálními prvky*, které směrnice definují jako *„veškeré hmotné movité předměty, jež obsahují digitální obsah či digitální službu nebo jsou s digitálním obsahem či digitální službou propojeny, a to takovým způsobem, že by nepřítomnost digitálního obsahu či digitální služby bránila tomu, aby dané zboží plnilo své funkce“.*[93]

Návrh zákona opět zavádí vlastní terminologii, když termín *zboží s digitálními prvky* nahrazuje termínem odpovídajícím více národnímu právnímu řádu, podle kterého hmotné movité předměty budou vždy věcmi, *věc s digitálními vlastnostmi.*[94] Věc s digitálními vlastnostmi je pak definována jako *„hmotná movitá věc, která je propojena s digitálním obsahem nebo službou digitálního obsahu takovým způsobem, že by bez nich nemohla plnit své funkce“* .[95] Příkladem věci s digitálními vlastnostmi bude např. televize nebo mobilní telefon s operačním systémem a aplikacemi nebo tzv. chytré hodinky propojené se službou sestavování a poskytování individualizovaných tréninkových plánů či jídelníčku prostřednictvím speciální aplikace.

Podle důvodové zprávy je nerozhodné, zda *„digitální vlastnost podporuje hlavní či jinou funkci zboží.“*[96] Věcí s digitálními vlastnostmi tak budou i věci, které bez digitálního obsahu mohou plnit svou obvyklou hlavní funkci, ale nikoli funkci vedlejší, kterou plnit mají, jako např. automobil využívající digitální obsah pro účely funkcí navigačního systému.

Zatímco ustanovení o digitálním obsahu a službách digitálního obsahu jsou v návrhu zákona začleněna do obecné úpravy smlouvy o poskytování digitálního obsahu, definice věci s digitálními vlastnostmi má být zahrnuta pouze do pododdílu upravujícího spotřebitelské kupní smlouvy. Otázkou

---

[93] Čl. 2 odst. 3 DCD, čl. 2 odst. 5 písm. b) SGD.

[94] Viz navrhované znění ustanovení § 2158 odst. 2 o.z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994.

[95] Viz navrhované znění ustanovení § 2158 odst. 2 o.z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994.

[96] Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 72.

tedy je, zda je možné tuto definici vztahovat i na jiné smluvní vztahy jako např. nájem (leasing) nebo výpůjčka a rovněž, zda je možné jí použít i mimo podnikatelsko-spotřebitelské smluvní vztahy. Domnívám se, že s ohledem na vnitřní konzistenci a výkladovou jednotu soukromého práva by tomu tak mělo být. Pro takovéto smluvní typy ale zatím není ani ve směrnicích ani v návrhu zákona uvažováno o zvláštní právní úpravě vztahující se speciálně na věci s digitálními vlastnostmi.

S ohledem na navrhovanou legální definici digitálního obsahu, kdy digitální obsah je definován jako věc v digitální podobě, je otázkou, zda chápat digitální obsah jako součást věci s digitálními vlastnostmi, jako příslušenství hmotné movité věci, nebo zda se má jednat o dvě zcela samostatné věci v právním smyslu, či věc hromadnou. Návrh zákona hovoří o *propojení* digitálního obsahu s hmotnou movitou věcí, což je výraz umožňující značnou výkladovou benevolenci. Zároveň propojeny mohou být i služby digitálního obsahu, u nichž pojmově nelze uvažovat o tom, že by byly věcí. Domnívám se proto, že s ohledem na široké spektrum kombinací, které mohou v praxi existovat, může být vzájemný vztah hmotné movité věci a digitálního obsahu *propojených* do věci s digitálními vlastnostmi různý.

Podle ustanovení § 505 o. z. je součástí věci vše, co k ní podle její povahy náleží a co nemůže být od věci odděleno, aniž se tím věc znehodnotí. V případě operačního systému mobilního telefonu je zřejmé, že operační systém k přístroji podle jeho povahy náleží a při jeho oddělení dojde ke znehodnocení přístroje, protože nebude fungovat, operační systém by tak mohl být součástí mobilního telefonu. Oproti tomu u některých aplikací, které byly v mobilním telefonu při jeho koupi nainstalovány, může jejich odinstalováním dojít dokonce k vylepšení vlastností telefonu (zejména ke zrychlení chodu, zvýšení výkonu nebo snížení spotřeby energie). Takovou aplikaci pak těžko lze považovat za součást telefonu, byť s ním je propojena, protože jejím oddělením se telefon nijak neznehodnotí.

Uvažovat o příslušenství je pak podle mého názoru právně problematické, protože u příslušenství je vyžadováno, aby se jednalo o vedlejší věc ve vlastnictví vlastníka věci hlavní, jejímž účelem je, aby se jí trvale užívalo

společně s hlavní věcí v rámci jejich hospodářského určení.[97] Digitální obsah, kterým jsou vždy data (viz kapitola 4.1.1), pravidelně předmětem vlastnického práva vůbec pojmově nebude, nebude proto naplňovat jeden ze zákonných definičních znaků příslušenství.

Domnívám se, že funkční by mohlo být v jednotlivých případech i využití právního konceptu věci hromadné podle § 501 o. z. Např. zmiňovaný mobilní telefon s nainstalovaným operačním systémem a aplikacemi tvoří jeden celek náležející téže osobě a zpravidla je s ním i právně disponováno jako s jedinou věcí.

U služeb digitálního obsahu je jednoznačné z jejich povahy, že součástí ani příslušenstvím věci s digitálními vlastnostmi být nemohou, protože nejsou věcmi. Přesto se však na ně podle navrhovaného znění § 2158 odst. 2 o. z. a rovněž podle čl. 3 odst. 3 SGD bude vztahovat zvláštní úprava prodeje zboží spotřebiteli, budou-li propojeny s hmotnou movitou věcí tak, že se bude jednat o věc s digitálními vlastnostmi, ledaže by z obsahu smlouvy i povahy věci bylo zjevné, že jsou tyto služby poskytovány samostatně. Přitom použití některých ustanovení o prodeji hmotné movité věci na služby může být s ohledem na různou povahu obou plnění přinejmenším problematické. Služby digitálního obsahu propojené se zbožím budou podřízeny režimu prodeje zboží spotřebiteli i v případě, že jsou poskytovány třetí osobou odlišnou od prodávajícího. Odpovědnost vůči spotřebiteli však ponese pouze prodávající.

Zároveň je nutné se zamyslet nad pojetím vlastnického práva k věci s digitálními vlastnostmi. Věc s digitálními vlastnostmi je návrhem zákona definována jako propojení hmotné movité věci s digitálním obsahem nebo službou digitálního obsahu. Že je možné vlastnit hmotné movité věci, tj. nabýt k nim vlastnické právo v subjektivním smyslu (§ 1012 o.z.), je zřejmé bez potřeby dalšího výkladu. Ovšem k digitálnímu obsahu, kterým jsou *data,* zpravidla vlastnické právo nabýt nelze (podrobněji viz kapitola 4.1.1) věnovaná digitálnímu obsahu), ke službám digitálního obsahu vlastnické právo rozhodně nabýt nelze, protože se vůbec nejedná o věci. V případě věcí s digitálními vlastnostmi se tak bude jednat o věc, která není jako

[97] § 510 odst. 1 o. z.

celek předmětem vlastnického práva, ale vlastnické právo se vztahuje pouze na movitou hmotnou věc (ve smyslu směrnic „zboží“), zatímco k obsaženému nebo propojenému digitálnímu obsahu nebo službě digitálního obsahu bude mít vlastník pouze práva obligační povahy. Bude se tak jednat o podobnou právní konstrukci, jako v případě autorských děl zachycených na hmotném nosiči, kdy se kupující stává vlastníkem hmotného nosiče, ale k autorskému dílu nabývá pouze licenci, případně možnost jeho užití na základě zákonem daného oprávnění, eventuálně nemá k autorskému dílu a jeho užití žádná práva (např. při nabytí tzv. pirátské kopie).

5. ÚPRAVA SMLUV DLE SMĚRNIC A NÁVRHU ZÁKONA

Směrnice upravují v zásadě dvě oblasti smluv, které lze pak dělit podle některých kritérií, jak bude dále uvedeno. Obě směrnice se omezují na smluvní vztahy mezi spotřebitelem[98] a obchodníkem (resp. prodávajícím), kterým je jakákoli fyzická či právnická osoba, která v souvislosti se smlouvami jedná za účelem, který lze považovat za její obchodní činnost, podnikání, řemeslo nebo povolání.[99]

DCD se vztahuje na smlouvy o poskytování digitálního obsahu a na smlouvy o poskytování digitálních služeb.

SGD stanoví některé požadavky vztahující se na kupní smlouvy uzavírané spotřebiteli nejen na koupi zboží s digitálními prvky, ale na koupi zboží (kterým rozumí hmotné movité věci) obecně. Dále v této kapitole bude věnována pozornost pouze kupním smlouvám na zboží s digitálními prvky.

V obou případech se jedná o úpravu pouze některých aspektů těchto smluv významných pro ochranu spotřebitele a fungování společného trhu, jako jsou soulad se smlouvou, zvláštní povinnosti obchodníka ve vztahu k udržování digitálního obsahu či služby, práva spotřebitele při porušení

[98] Čl. 2 odst. 6 DCD: „spotřebitelem“ se rozumí jakákoli fyzická osoba, která v souvislosti se smlouvami, na něž se vztahuje tato směrnice, jedná za účelem, jejž nelze považovat za její obchodní činnost, podnikání, řemeslo nebo povolání.

[99] Čl. 2 odst. 3 SGD, čl. 2 odst. 5 DCD.

nebo ukončení smlouvy a důkazní břemeno. Směrnicemi neupravené záležitosti jsou ponechány vnitrostátnímu právu.

Dále v této kapitole se podrobněji věnuji zejména smlouvě o poskytování digitálního obsahu nebo digitálních služeb (resp. služeb digitálního obsahu), následně pak stručněji úpravě spotřebitelské kupní smlouvy o prodeji zboží s digitálními prvky (resp. věcí s digitálními vlastnostmi).

5.1 SMLOUVA O POSKYTOVÁNÍ DIGITÁLNÍHO OBSAHU NEBO DIGITÁLNÍCH SLUŽEB

Rozsah právní úpravy smlouvy o poskytování digitálního obsahu nebo digitálních služeb je značně široký. DCD definuje smlouvu o poskytování digitálního obsahu nebo digitálních služeb pouze tím, že se jedná o každou smlouvu, na jejímž základě obchodník (podnikatel) poskytuje nebo se zavazuje poskytovat digitální obsah nebo digitální službu spotřebiteli a spotřebitel platí nebo se zavazuje platit cenu nebo poskytuje nebo se zavazuje poskytovat osobní údaje (s výjimkami uvedenými v čl. 3 odst. 1 DCD). Cenou se rozumí peněžní částka nebo digitální vyjádření hodnoty.[100] Osobními údaji pak jsou osobní údaje ve smyslu GDPR.

Jak bylo již shora uvedeno, směrnice reguluje pouze některé aspekty smluv o poskytování digitálního obsahu nebo digitálních služeb. Co ale záměrně neupravuje vůbec, je právně teoretické pojetí těchto smluv, což ponechává zcela na vnitrostátním zákonodárci.[101]

5.1.1 TYP SMLOUVY

DCD v zásadě upravuje tři druhy smluv o poskytování digitálního obsahu nebo služeb v závislosti na způsobu a čase plnění:

a) smlouvy s jednorázovým plněním;
b) smlouvy s jednorázovým opakovaným plněním;
c) smlouvy s dlouhodobým nepřetržitým plněním.

Zároveň se vztahuje i na případy, kdy jsou digitální obsah nebo digitální služba vytvořeny podle specifikací spotřebitele.

[100] Čl. 2 odst. 7 DCD.

[101] Recitál 12 DCD.

Z pohledu vnitrostátního zákonodárce tak vzniká otázka, jaký smluvní typ pro transpozici unijních norem zvolit.

Detailně se této problematice věnuje zejména německá literatura, která zdůrazňuje zjevné problémy při snaze upravit tyto smlouvy tak, aby odpovídaly pojetí smluv v BGB. BGB a německá právní nauka totiž rozlišují typy smluv podle (z pohledu české právní nauky) primárního předmětu, tedy právního jednání, kterým je smlouva plněna, a nikoli podle sekundárního předmětu právního vztahu.[102] V případě smluv o poskytování digitálního obsahu by tak bylo možné dle konkrétního obsahu závazku uvažovat o smlouvě kupní, nájemní, o dílo, licenční nebo inominátní v závislosti na tom, v jakém jednání má spočívat ono *poskytnutí* digitálního obsahu nebo služby. V německé odborné literatuře byly proto v souvislosti s transpozicí DCD prezentovány následující způsoby řešení:

[1] přizpůsobení stávajících typů smluv;

[2] vytvoření nového smluvního typu smlouvy o poskytování digitálního obsahu a služeb;

[3] zavedením tří typů „digitálních" smluv v rámci základních smluvních typů smlouvy kupní, nájemní a o dílo;

[4] doplnění obecné části závazkového práva.[103]

Rovněž český občanský zákoník rozlišuje, jak vyplývá už z názvů jednotlivých dílů hlavy II. části čtvrté občanského zákoníku, pojmenované smlouvy podle primárního předmětu (např. převedení věci do vlastnictví jiného, přenechání věci k užití jinému), a nikoli podle předmětu sekundárního. Nezaznamenala jsem však v České republice na toto téma na stránkách odborných periodik žádnou diskusi. Předkladatel návrhu zákona v důvodové zprávě pouze zmiňuje skutečnost, že závazky, jejichž obsahem bude poskytování digitálního obsahu nebo služeb, mohou vznikat na základě různých typů smluv včetně smluv inominátních nebo smíšených.[104] Bohužel dů-

[102] WENDLAND, M. Sonderprivatrecht für Digitale Güter. *Zeitschrift für Vergleichende Rechtswissenschaft.* 2019, č. 118, s. 202.

[103] WENDLAND, M. Sonderprivatrecht für Digitale Güter. *Zeitschrift für Vergleichende Rechtswissenschaft.* 2019, č. 118, s. 219.

[104] Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 31.

vodová zpráva neuvádí žádné podrobnější úvahy na téma jiných možností transpozice DCD do českého právního řádu, než je způsob, který byl předkladatelem zákona zvolen. Pouze stručně uvádí, že *„transakce shodné povahy lišící se pouze způsobem poskytnutí digitálního obsahu by měly být klasifikovány stejně“*, a to z důvodu logiky z hlediska uživatelského, s doplněním o argumentaci legislativně technickou přehledností a srozumitelností textu.[105]

V České republice je navrhována transpozice zavedením právní úpravy nového smluvního typu v občanském zákoníku vložením oddílu s názvem *Poskytování digitálního obsahu* do části čtvrté hlavy II. dílu 2 *Přenechání věci k užití jinému.* Návrh zákona zde tedy zjevně vychází z pojetí, že k digitálnímu obsahu nelze nabývat vlastnické právo a vždy se bude jednat pouze o přenechání k užití, což považuji za správné. Jedná se o následování obecného trendu digitální ekonomiky, která je charakterizována mj. přechodem od konceptu vlastnictví ke konceptu přístupu a (smluvního) užívání.[106]

Nový smluvní typ se nebude vztahovat pouze na smlouvy spotřebitelské, ale na soukromoprávní smluvní vztahy obecně. Poskytování digitálního obsahu spotřebitelům je v rámci navrhované úpravy věnován speciální pododdíl upravující zvýšené požadavky na smlouvy uzavírané se spotřebiteli, jak je v jednotlivostech podrobněji uvedeno dále.

Návrh zákona stanoví následující podstatné náležitosti nového smluvního typu:

a) závazek zpřístupnění digitálního obsah nebo poskytnutí služby digitálního obsahu k užívání pro vlastní potřebu;
b) úplatnost, tj. sjednání odměny, nebo (pouze však v případě spotřebitele) poskytnutí osobních údajů.

Smluvní strany jsou pro tento smluvní typ označovány jako *uživatel a poskytovatel.*

---

[105] Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 87.

[106] Podrobněji viz např. RIFKIN, J. *The age of access: the new culture of hypercapitalism, where all of life is a paid-for experience*. New York: J.P. Tarcher/Putnam, 2000.

K problematickému požadavku na poskytnutí digitálního obsahu nebo služby digitálního obsahu pouze pro vlastní potřebu uživatele viz kapitola 3.2.

Návrh zákona používá pro vymezení podstatných náležitostí smlouvy o poskytování digitálního obsahu formulaci „*poskytovatel se zavazuje zpřístupnit věc v digitální podobě*“. Otázkou výkladu pak je, co vše zahrnuje ono *zpřístupnění*. Z recitálu 19 DCD vyplývá, že pojem *zpřístupnění* použitý českým zákonodárcem bude nutné vykládat co nejšířeji, aby zahrnul různé způsoby poskytnutí digitálního obsahu včetně předání na hmotném nosiči, umožnění stažení do zařízení uživatele, přenosu po internetu nebo umožnění přístupu k digitálnímu obsahu uloženému v úložišti poskytovatele nebo samotného umožnění využívání tohoto úložiště. Podle směrnice[107] má být pokryto rovněž zakázkové vytvoření digitálního obsahu nebo digitální služby podle specifikace uživatele. Český navrhovatel zákona ale situaci v tomto ohledu poněkud zkomplikoval. Jak bylo uvedeno, mají se první a třetí pododdíl oddílu 6 dílu 2 hlavy II. občanského zákoníku vztahovat na soukromoprávní smluvní vztahy bez omezení pouze na spotřebitelsko-podnikatelskou kontraktaci, druhý pododdíl se vztahuje pouze na poskytování digitálního obsahu nebo služeb digitálního obsahu spotřebiteli. Při obecném chápání širokého pojmu *zpřístupnit* by tak bylo možné dojít k závěru, že ustanovení o poskytování digitálního obsahu se budou vztahovat rovněž na smlouvy, na jejichž základě je digitální obsah vytvořen nebo digitální služba poskytnuta podle specifikace uživatele na zakázku. Takovému výkladu ale nenasvědčuje navrhované znění § 2389g odst. 3 o. z., které vztahuje ustanovení o poskytování digitálního obsahu na smlouvy o zhotovení digitálního obsahu uzavřené pouze se spotřebitelem. Pokud by obecné ustanovení o poskytování digitálního obsahu v § 2389a o. z. zahrnovalo rovněž smlouvy o zhotovení digitálního obsahu, nebylo by nutné toto pravidlo výslovně zmiňovat v pododdílu věnovaném poskytování digitálního obsahu spotřebiteli. S využitím argumentu a contrario je tak nutné dojít k závěru, že na smlouvy o dílo, jejichž předmětem je zhotovení digitálního obsahu (např. webové prezentace či aplikace), uzavřené mezi podnikateli, se

[107] Čl. 3 odst. 2 DCD.

úprava smlouvy o poskytování digitálního obsahu nepoužije, ledaže by si to smluvní strany ujednaly.

Z navrhovaného znění ust. § 2389f odst. 1 o. z. a rovněž recitálů 56 a 57 DCD vyplývá, že *zpřístupnění* digitálního obsahu zahrnuje jak jednorázové plnění, tak plnění opakované nebo kontinuální (k tomu blíže v kapitole 5.1.3 věnované době plnění). Zpřístupnění se může odehrát i prostřednictvím virtuálního nebo fyzického zařízení zvoleného uživatelem, včetně virtuálního prostředí provozovaného třetí osobou. Zatímco DCD ukládá povinnost učinit digitální obsah nebo prostředek vhodný k přístupu nebo stažení digitálního obsahu *dostupným* či *přístupným*, návrh zákona ukládá poskytovateli pouze povinnosti digitální obsah uživateli *zpřístupnit* bez odlišení způsobu, jak k tomu dojde.[108]

Druhou podstatnou náležitostí je úplatnost smlouvy o poskytování digitálního obsahu nebo služby digitálního obsahu. Samozřejmě podmínku úplatnosti bude splňovat placení ceny penězi včetně (v online světě častějších) bezhotovostních převodů, dále je nutné pod pojem *odměna*[109] zahrnout i jiné adekvátní formy protiplnění nahrazující peníze označované směrnicí jako *digitální vyjádření hodnoty,*[110] jako jsou elektronické poukázky, elektronické kupony nebo virtuální měny. Pouze v případě spotřebitelů se úprava poskytování digitálního obsahu použije rovněž na případy, kdy jsou namísto odměny poskytovány osobní údaje spotřebitele (k tomu blíže viz kapitola 6.).[111] Na častý obchodní model, kdy je uživatel za poskytnutí digitálního obsahu vystaven reklamním sdělením, se DCD podle recitálu 25 vztahovat nemusí a ani český předkladatel zákona nenavrhuje takové rozšíření působnosti nové právní úpravy.

5.1.2 PRÁVA DUŠEVNÍHO VLASTNICTVÍ

DCD ani návrh zákona nijak přímo ani nepřímo nezasahují do stávající právní úpravy práv duševního vlastnictví a podle recitálu 36 DCD tomu tak

[108] Srov. Čl. DCD a navrhované znění § 2389b odst. 1 o. z.

[109] Viz navrhované znění § 2389a odst. 1 o. z.

[110] Recitál 23 DCD.

[111] Viz navrhované znění § 2389g odst. 2 o. z.

ani být nemá. Uživatel nezískává uzavřením smlouvy o poskytování digitálního obsahu licenci ani jiná práva vůči osobě vykonávající práva duševního vlastnictví (nejčastěji právo autorské) k digitálnímu obsahu.[112] Jedná se o dva oddělené právní světy, které se však budou v mnoha případech střetávat a prolínat.

Digitální obsah je často předmětem chráněným právem duševního vlastnictví, zejména autorským dílem, proto se při poskytování digitálního obsahu střetu s ochranou práv duševního vlastnictví často nelze vyhnout. V případě podnikatelsko-spotřebitelských vztahů vzniká možný konflikt mezi ochranou práv duševního vlastnictví a právní ochranou spotřebitele, zejména s ohledem na koncept rozumného očekávání spotřebitele vzhledem k povaze digitálního obsahu nebo digitální služby.[113]

DCD neupravuje problematiku práv duševního vlastnictví jako takovou. Uzavřením smlouvy o poskytování digitálního obsahu nebo digitální služby (resp. služby digitálního obsahu) nedojde podle evropské regulace k poskytnutí licence ani jiných práv duševního vlastnictví. Z toho mj. vyplývá, že uživatel uzavírající smlouvu o poskytování digitálního obsahu (nebo digitální služby) nemusí vůbec vstupovat do smluvního vztahu s osobou vykonávající autorské právo nebo jiná práva duševního vlastnictví k dotčenému digitálnímu obsahu,[114] ledaže by se jednalo o osobu shodnou s poskytovatelem. Naopak uživatel se dokonce užíváním digitálního obsahu v souladu s uzavřenou smlouvou o jeho poskytnutí může dopustit porušování práv duševního vlastnictví třetí osoby, aniž by o tom věděl. DCD zakotvuje pouze pravidlo pro případ omezení spotřebitele právy třetích osob k digitálnímu obsahu, včetně práv duševního vlastnictví. Omezení vyplývající z porušení práv třetích osob včetně práv duševního vlastnictví, která omezují spotřebitele v užití digitálního obsahu či služby nebo mu v jejich užití brání v rozporu s objektivními nebo subjektivními požadavky na

[112] Srov. ROSENKRANZ, F. *Art. 10. Function.* In SCHULZE, R., STAUDENMAYER, D. *EU Digital Law: Article-by-Article Commentary*, Baden-Baden, Germany: Nomos, 2020. s. 185.

[113] Podrobněji srov. REYNA, A. *What Place for Fairness in Digital Content Contracts?* Baden-Baden, Germany: Nomos, 2020.

[114] ROSENKRANZ, F. *Art. 10. Function.* In SCHULZE, R., STAUDENMAYER, D. *EU Digital Law: Article-by-Article Commentary*, Baden-Baden, Germany: Nomos, 2020. s. 185.

soulad (podrobněji viz kapitola 5.1.4 dále), považuje DCD za nesoulad se smlouvou, pro jehož nápravu musí mít spotřebitel směrnicí stanovená práva na nápravu, ledaže vnitrostátní právo pro tyto případy stanoví neplatnost smlouvy nebo možnost odstoupení od smlouvy.[115] Obecně však DCD do předpisů o autorském právu nezasahuje.[116]

Návrh zákona se v podstatě odkazuje na zvláštní právní úpravu, když stanoví, že vyžaduje-li užívání digitálního obsahu oprávnění k výkonu práva duševního vlastnictví, použijí se také příslušná ustanovení o licenci.[117] V praxi tedy v těchto případech bude nutné buď pojmout licenční ujednání přímo do smlouvy o poskytování digitálního obsahu a vytvořit tak smlouvu smíšenou, nebo uzavřít vedle této smlouvy samostatnou licenční smlouvu, ledaže by způsob užití digitálního obsahu vyplývající ze smlouvy o poskytnutí digitálního obsahu spadal výhradně mezi volná užití nebo zákonné licence.[118] S ohledem na obecnou formulaci návrhu zákona *použijí se také příslušná ustanovení o licenci*[119] lze dojít k závěru, že se může jednat jak o případy, kdy je uzavřena licenční smlouva přímo mezi uživatelem a poskytovatelem digitálního obsahu, tak i o případy, kdy je licenční smlouva uzavřena mezi uživatelem a osobou odlišnou od poskytovatele, která je jako vykonavatel majetkových práv autorských oprávněna k jejímu uzavření. V úvahu tak přicházejí následující možnosti:

- Uživatel pro užití digitálního obsahu nebo služby digitálního obsahu nepotřebuje žádnou licenci, aniž by tím zasáhl do práv třetích osob – udělení licence nebude nutné;
- uživatel získá licenci přímo od poskytovatele, který je oprávněn vykonávat příslušná majetková práva k dílu, licenční smlouvou;
- uživatel získá licenci přímo od poskytovatele, který je oprávněn vykonávat příslušná majetková práva k dílu,

[115] Čl. 10 DCD.

[116] Recitál 36 DCD.

[117] Viz navrhované znění § 2389a odst. 2 o.z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994.

[118] Díl 4, oddíl 2 autorského zákona (zák. č. 121/2000 Sb.)

[119] Navrhované znění § 2389a odst. 2 o.z.

postoupením – v praxi takové řešení nebude obvyklé, protože pro poskytovatele by se jednalo o jednorázovou transakci, v úvahu bude přicházet zřejmě jen v případě zakázkově vytvořeného digitálního obsahu;

- uživatel získá od poskytovatele, který je držitelem licence, podlicenci k dílu;
- uživatel nezíská žádná oprávnění k užití díla od poskytovatele, ale uzavírá licenční nebo podlicenční smlouvu s třetí osobou – jedná se o postup častý zejména u softwaru formou uzavření tzv. End user Agreement (EULA).[120]

Z hlediska možné odpovědnost za nesoulad se smlouvou o poskytování digitálního obsahu z důvodu porušení práv duševního vlastnictví navrhovaná právní úprava v českém občanském zákoníku opět situaci poněkud komplikuje rozdělením právní úpravy na obecná ustanovení vztahující se na všechny smlouvy o poskytování digitálního obsahu a zvláštní pododdíl věnovaný pouze poskytování digitálního obsahu spotřebitelům.

V případě, kdy uživatel neuzavírá smlouvu v postavení spotřebitele, se uplatní pouze navrhovaná ustanovení § 2389a odst. 2 o. z. odkazující na použití ustanovení o licenci a § 2389c odst. 1 o. z, podle kterého poskytovatel odpovídá uživateli, že digitální obsah je po dobu trvání závazku bez vad. V souvislosti s navrhovaným znění § 2389a odst. 2 o. z. *„…použijí se také příslušná ustanovení o licenci“* se nabízí otázka, zda je v tomto případě vadou digitálního obsahu, pokud byl poskytovatelem poskytnut bez potřebné licence. Uvedené ustanovení totiž poskytnutí licence nebo zajištění jejího poskytnutí třetí osobou neukládá jako povinnost poskytovateli. S ohledem na absenci zvláštní úpravy bude nutné vycházet z obecné úpravy odpovědnosti za právní vady, tedy ust. § 1914 a § 1920 o. z. Jestliže poskytovatel zpřístupní uživateli digitální obsah, k jehož užití v souladu s uzavřenou smlouvou o poskytování digitálního obsahu je nutné získat licenci, aniž by jej o tom informoval, bude za takto vzniklou právní vadu od-

[120] Srov. The European Law Institute. *Statement of the European Law Institute ON THE EUROPEAN COMMISSION'S PROPOSED DIRECTIVEON THE SUPPLY OF DIGITAL CONTENT TO CONSUMERS*. COM (2015) *634 final*. 8.2 EULAs must not reduce consumer rights, s. 25.

povídat. Podle mého názoru však pro vyloučení této odpovědnosti bude postačovat, jestliže poskytovatel uživatele nejpozději při uzavřením smlouvy informuje, že digitální obsah je chráněn právy duševního vlastnictví třetí osoby a pro jeho užití je nutné získat licenci. Je pak na uživateli, pokud se přesto rozhodne smlouvu uzavřít, aby si příslušnou licenci zajistil. V praxi však takový postup nebude obvyklý, protože lze stěží očekávat, že by byl komerčně úspěšný. Spíše bude poskytovatel uživateli nabízet uzavření EULA společně se zpřístupněním digitálního obsahu, např. formou kontraktu „click wrap". Ovšem na rozdíl od podnikatelsko-spotřebitelských smluvních vztahů (viz následující odstavec) zde nebude nutné, aby poskytovatel informoval uživatele o obsahu licenční smlouvy předem.

V případě uzavření smlouvy se spotřebitelem upravuje otázku existence práv třetí osoby k digitálnímu obsahu navrhované ustanovení § 2389i odst. 2 písm. a) o. z., které je transpozicí čl. 8 odst. 1 a čl. 10 DCD. Podle tohoto ustanovení poskytovatel odpovídá uživateli za to, že *„je digitální obsah vhodný k účelu, k němuž se digitální obsah tohoto druhu obvykle používá, i s ohledem na práva třetích osob…."*. Dalším požadavkem je, aby digitální obsah odpovídal svým obsahem, rozsahem a dalšími vlastnostmi *obvyklým vlastnostem digitálního obsahu téhož druhu, které může uživatel rozumně očekávat.*[121] Zároveň se podle DCD[122] (a stejně tak podle návrhu zákona) toto ustanovení nepoužije, pokud poskytovatel uživatele upozornil před uzavřením smlouvy na odlišnost některé vlastnosti digitálního obsahu od těchto požadavků a uživatel s tím výslovně souhlasil. S ohledem na požadavek výslovného souhlasu uživatele – spotřebitele nebude postačovat uvedení informace v obchodních podmínkách poskytovatele a použití opt-out principu, ale naopak bude nutné aktivní vyjádření souhlasu uživatele např. aktivním zaškrtnutím příslušného souhlasu.[123] Reyna považuje tuto možnost za mezeru ve směrnici, která umožní poskytovatelům vyhnout se

[121] Viz navrhované znění 2389i odst. 2 písm. písm. b) In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994.

[122] Čl. 8 odst. 5 DCD.

[123] Viz též Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 90 a dále recitál 49 DCD.

odpovědnosti, čímž je narušen princip ochrany rozumných očekávání spotřebitele.[124] S tímto názorem nesouhlasím. Jestliže je spotřebiteli příslušná informace poskytnuta jasně a srozumitelně předem a je vyžadováno, aby s odchýlením od zákonem a směrnicí garantovaného standardu výslovně souhlasil, proč by mu mělo být bráněno v uplatnění smluvní volnosti. Zároveň není důvod, aby v případě, kdy se uživatel s příslušnou informací dostatečně neseznámil a souhlas odškrtl bez čtení, byl zbaven odpovědnosti za svoje lehkovážné a nezodpovědné jednání. Naopak se domnívám, že umožnění smluvního odchýlení od standardu objektivních požadavků na soulad ve prospěch omezení vyplývajících z ochrany práv duševního vlastnictví může být v konečném důsledku pro uživatele i přínosem. Poskytovatelům totiž umožňuje nabízet uživatelům – spotřebitelům i digitální obsah, u kterého držitel autorských práv stanovil specifická omezení jeho užití a který by jim v případě nutnosti bezpodmínečného dodržení budoucího ustanovení § 2389i odst. 2 písm. a) o. z. nabídnout nemohli.[125]

Shora nastíněná problematika práv duševního vlastnictví bude nejaktuálnější v případě digitálního obsahu ve formě software, protože u počítačových programů není možné využít výjimku volného užití pro vlastní potřebu podle ust. § 30 odst. 1 autorského zákona. V případě software je častý postup, kdy uživatel uzavírá smlouvu s poskytovatelem digitálního obsahu a následně po zpřístupnění tohoto obsahu musí uzavřít licenční smlouvu (obvykle označovanou jako EULA) odsouhlasením předem daných licenčních podmínek s osobou odlišnou od poskytovatele digitálního obsahu.[126] Např. smluvní podmínky celosvětově využívané služby Google Play nabízející digitální obsah zejména v podobě aplikací včetně her uvádějí následující: *„Na používání aplikací a her se mohou vztahovat další smluvní pod-*

[124] REYNA, A. *What Place for Fairness in Digital Content Contracts?* Baden-Baden, Germany: Nomos, 2020, s. 170.

[125] Srov. STAUDENMAYER, D. *Art. 8. Objective requirements for conformity.* In *EU Digital Law: Article-by-Article Commentary*, Baden-Baden, Germany: Nomos, 2020, s. 163.

[126] The European Law Institute. *Statement of the European Law Institute ON THE EUROPEAN COMMISSION'S PROPOSED DIRECTIVEON THE SUPPLY OF DIGITAL CONTENT TO CONSUMERS*. COM (2015) *634 final*, s. 25.

mínky uvedené v licenční smlouvě s koncovým uživatelem uzavřené mezi vámi a poskytovatelem.“[127]

EULA přitom může obsahovat omezující ustanovení, která nebyla uživateli předem známa, jako např. omezení užívání software pouze na určitý počet zařízení, nemožnost paralelních přihlášení z více zařízení, nepřenositelnost licence na jinou osobu, omezení možností vytvářet kopie apod. Nejedná se přitom o marginální záležitost, naopak v případě globálně působících „velkých hráčů“ z řad poskytovatelů digitálního obsahu a digitálních služeb se jedná o častá omezení.[128] Pokud se bude chtít poskytovatel napříště vyhnout tomu, aby uživatel-spotřebitel z důvodu existence omezujících ustanovení v EULA namítal nesoulad plnění se smlouvou a uplatňoval prostředky nápravy, měl by zajistit, aby se uživatel se zněním EULA seznámil předem a vyslovil s ní souhlas. Praxe řady poskytovatelů digitálních obsahů a služeb by se tak měla v tomto směru podstatně změnit.

5.1.3 DOBA PLNĚNÍ

Další z dílčích požadavků na smlouvu o poskytování digitálního obsahu nebo služby digitálního obsahu upravených směrnicí a rovněž návrhem zákona je doba plnění.

Základním ustanovením pro dobu plnění je článek 5 odst. 1 DCD, v návrhu zákona pak § 2389b o. z. Pokud si strany ujednají čas plnění, má jejich ujednání přednost, zákonem stanovená pravidla jsou tedy dispozitivní. Není-li ujednán čas plnění, je povinností poskytovatele digitální obsah zpřístupnit bez zbytečného odkladu po uzavření smlouvy. Toto ustanovení se neuplatní v případě poskytování digitálního obsahu na hmotném nosiči,[129] pro které bude platit zvláštní ustanovení § 2159 o. z. z oddílu věnovaného prodeji zboží spotřebiteli. Jedná se však o výjimku stanovenou

[127] Smluvní podmínky služby Google Play. https://play.google.com/intl/cs_cz/about/play-terms/index.html.

[128] Podrobněji viz OPRYSK, L., SEIN, K. Limitations in End-User Licensing Agreements: Is There a Lack of Conformity Under the New Digital Content Directive? *IIC - International Review of Intellectual Property and Competition Law.* 2020, roč. 51, č. 5, s. 594–623.

[129] Čl. 3 odst. 3 DCD, navrhované znění § 2389h odst. 3 o. z.

pouze pro smlouvy spotřebitelské.[130] V praxi lze očekávat, že většina smluv se bude od tohoto pravidla odchylovat a bude vázat zpřístupnění digitálního obsahu uživateli až na zaplacení sjednané ceny.

Na jednoduché základní pravidlo navazují další ustanovení, ze kterých vyplývá, že je nutné rozlišovat různé situace, a to:

a) Smlouvu na jednorázové plnění; v tomto případě má poskytovatel (při chybějícím odchylném ujednání stran) povinnost zpřístupnit digitální obsah nebo službu digitálního obsahu bez zbytečného odkladu po uzavření smlouvy. Tím ovšem jeho povinnosti nekončí, protože i po samotném jednorázovém poskytnutí digitálního obsahu nebo služby digitálního obsahu je povinen poskytovat uživateli aktualizace (podrobněji viz kapitola 5.1.5). Doba plnění pro povinnost poskytovat aktualizace je stanovena neurčitě tak, že se jedná o dobu, *po kterou to uživatel může rozumně očekávat,*[131] přihlíží se přitom k druhu a účelu digitálního obsahu (služby digitálního obsahu), okolnostem uzavření smlouvy a povaze závazku.

b) Smlouvu na jednorázová opakovaná plnění; zde je pravidlo pro dobu plnění stejné, jako v předchozím případě. Poskytovatel má (při chybějícím odchylném ujednání stran) povinnost zpřístupnit digitální obsah nebo službu digitálního obsahu bez zbytečného odkladu po uzavření smlouvy. Tímto pravidlem bude vyřešeno první poskytnutí digitálního obsahu nebo služby digitálního obsahu, ale těžko jej půjde vztáhnout na další opakovaná plnění, ledaže by na každé jednotlivé plnění byla uzavírána samostatná smlouva. V případě opakovaných jednorázových plnění z jedné smlouvy bude nutné, aby si strany další termíny plnění ujednaly. Neučiní-li tak, ale přesto ve smlouvě vyjádří vůli, aby plnění nebylo poskytnuto najednou, nýbrž postupně, bude zřejmě platit obecné pravidlo ust. § 1958 odst. 2 o. z., podle kterého bude poskytovatel po-

[130] Navrhované znění § 2389h odst. 3 o.z.

[131] Navrhované znění § 2389f odst. 4 o.z.

vinen plnit bez zbytečného odkladu po výzvě uživatele. Následně je poskytovatel povinen poskytovat aktualizace po dobu, po kterou to uživatel může rozumně očekávat, stejně jako v případě sub a) shora.

c) Smlouvu na kontinuální poskytování digitálního obsahu nebo služby digitálního obsahu, ať uzavřenou na dobu určitou nebo neurčitou; v tomto případě bude při absenci výslovného ujednání poskytovatel povinen zahájit plnění bez zbytečného odkladu po uzavření smlouvy a pokračovat v něm po sjednanou dobu. Zároveň po celou tuto dobu bude poskytovatel povinen poskytovat i aktualizace.

Doba plnění smlouvy má významný dopad do odpovědnosti poskytovatele za vady digitálního obsahu nebo služeb digitálního obsahu i na související povinnost poskytovat aktualizace digitálního obsahu nebo služby digitálního obsahu, jak je blíže rozebráno v následujících kapitolách.

V případě prodlení poskytovatele s poskytnutím digitálního obsahu nebo digitální služby bude podle českého občanského zákoníku opět nutné rozlišovat, zda uživatel je nebo není spotřebitelem. Nejedná-li se o spotřebitele, uplatní se obecná právní úprava odpovědnosti za prodlení podle ust. § 1968 a násl. o. z. Pro spotřebitele bude platit zvláštní harmonizovaná úprava vycházející z čl. 13 DCD, jejíž transpozice je navržena v ust. § 2389h o. z. Výjimku však má digitální obsah poskytovaných na hmotném nosiči, pro který bude platit ustanovení o prodlení podle § 2159a o. z. vztahující se na spotřebitelské kupní smlouvy.

V případě prodlení poskytovatele s plněním digitálního obsahu poskytovaného spotřebiteli mohou nastat následující situace:

a) Pro případ prodlení byla stranami ujednána dodatečná lhůta plnění; poskytovatel musí plnit v této dodatečné lhůtě, neučiní-li tak, může uživatel od smlouvy odstoupit.

b) Dodatečná lhůta ujednána nebyla, uživatel vyzval poskytovatele k plnění, poskytovatel přesto bez zbytečného odkladu neplnil, uživatel může následně od smlouvy odstoupit.

c) Poskytovatel prohlásil, že digitální obsah neposkytne; uživatel může ihned od smlouvy odstoupit.
d) Z okolností je zřejmé, že poskytovatel digitální obsah neposkytne; uživatel může ihned od smlouvy odstoupit.
e) Z dohody stran nebo z okolností je zřejmé, že pro uživatele je významné poskytnutí digitálního obsahu v určitém čase a poskytovatel jej v tomto čase neposkytl; uživatel může ihned od smlouvy odstoupit bez nutnosti výzvy k plnění.

5.1.4 SOULAD SE SMLOUVOU A ODPOVĚDNOST ZA VADY

Směrnice upravuje otázku souladu plnění se smlouvou a na to navazujících právních následků v podobě odpovědnosti za vady prostřednictvím stanovení požadavků na soulad digitálního obsahu nebo služby se smlouvou. Tyto požadavky na soulad jsou směrnicí stanoveny jednak jako subjektivní, tedy ve smlouvě přímo ujednané, a dále jako objektivní, tedy na obsahu smlouvy nezávislé, včetně nesouladu způsobeného nesprávnou integrací.[132]

Návrh zákona opět rozlišuje mezi právním postavením uživatele obecně a postavením uživatele, který uzavírá smlouvu jako spotřebitel. Požadavky na soulad stanovené v čl. 6, 7, 8 a 9 DCD i prostředky nápravy podle čl. 14 DCD návrh zákona promítá pouze do pododdílu věnovaného poskytování digitálního obsahu a služeb spotřebiteli.

V případě uživatele, který není spotřebitelem, se použije obecná úprava ust. § 1914 a násl. o. z. pokud jde o definici vad, a dále ust. § 1923 a násl. o. z., pokud se jedná o nároky z vadného plnění. Vedle toho se použijí speciální ustanovení pro smlouvu o poskytování digitálního obsahu upravující odpovědnost poskytovatele za vady obsažená v navrhovaném znění § 2389c až 2389f o. z. Tato speciální právní úprava stanoví, že poskytovatel odpovídá uživateli za to, že digitální obsah (nebo služba digitálního obsahu) je po dobu trvání závazku bez vad. Zároveň je poskytovateli uložena povinnost zpřístupnit uživateli nejnovější verzi digitálního obsahu nebo služby digitálního obsahu dostupnou v době uzavření smlouvy. Podle mého názoru by bylo vhodnější požadovat poskytnutí nejnovější verze digitálního obsahu

[132] Čl. 7, 8 a 9 DCD.

dostupné k okamžiku plnění, ledaže si strany ujednají jinak. V případě, kdy v mezidobí od uzavření smlouvy do okamžiku plnění dojde k vydání aktualizace digitálního obsahu, bude muset uživatel obratem po zpřístupnění digitálního obsahu (v nejnovější verzi dostupné při uzavření smlouvy) provést jeho aktualizaci. Jedná se však o ustanovení dispozitivní, je proto možné odchylné ujednání smluvních stran.

V diskusích s kolegy jsem se setkala s názorem, že právní úprava odpovědnosti za vady digitálního obsahu je problematická zejména ve vztahu k software, protože přece žádný software není bez vad. Podle mého názoru ale takovéto chápání nerozlišuje mezi vadou software z programátorského (technického) pohledu, kterou dále budu označovat jako *chybu*, a vadou, jak jí chápe právo. Podle ust. § 1914 o. z. *kdo plní za úplatu jinému, je zavázán plnit bez vad s* ***vlastnostmi vymíněnými nebo obvyklými*** *tak,* ***aby bylo možné použít předmět plnění podle smlouvy****, a je-li stranám znám, i podle účelu smlouvy*. Dále podle § 1916 o. z. *Dlužník plní vadně, zejména*

1. *poskytne-li předmět plnění, který* ***nemá stanovené nebo ujednané vlastnosti,***
2. *neupozorní-li na vady, které předmět plnění má, ač se při takovém předmětu* ***obvykle nevyskytují,***
3. ujistí-li věřitele v rozporu se skutečností, že předmět plnění nemá žádné vady, anebo že se věc hodí k určitému užívání, nebo
4. zcizí-li cizí věc neoprávněně jako svoji.

Pominu-li právní vady (viz kapitola 5.1.2 věnovaná právům duševního vlastnictví), je ze shora uvedeného zřejmé, že software, který obsahuje obvykle se vyskytující chyby, ale přesto má stanovené, ujednané nebo obvyklé vlastnosti a je možné jej použít podle smlouvy, není vadný. Zároveň je možné doplnit, že sám zákonodárce počítá s tím, že v digitálním obsahu se určité vady vyskytovat mohou a budou, protože jinak by neukládal poskytovateli povinnost poskytovat aktualizace, které jsou *nezbytné, aby byl digitální obsah bez vad.*[133]

[133] Viz navrhované ustanovení § 2389d odst. 2 o. z.

V případě jednorázových plnění poskytovatel odpovídá pouze za vady digitálního obsahu, které měl k okamžiku jeho zpřístupnění. Zároveň tím není dotčena povinnost poskytovatele poskytovat aktualizace (podrobněji viz kapitola 5.1.5 dále). Otázkou je, jak postupovat v případě, kdy digitální obsah při zpřístupnění žádnou vadu neměl a vada vznikla až v důsledku následné aktualizace. S ohledem na navrhované ust. § 2389d odst. 2 o.z., podle kterého mají aktualizace naopak směřovat k tomu, aby digitální obsah byl bez vad, by poskytovatel měl odpovídat i za vady poskytnutých aktualizací.

Návrh zákona (ve shodě s DCD) zároveň stanoví další podmínky vzniku práva z odpovědnosti za vady zlepšující právní postavení uživatele a usnadňující případné prokazování jeho nároků. Jedná se zejména o přenesení důkazního břemene na poskytovatele a stanovení vyvratitelné domněnky v případech jednorázového plnění, podle které se má za to, že digitální obsah byl vadný již v okamžiku zpřístupnění, projeví-li se vada v průběhu jednoho roku od zpřístupnění (podrobněji viz kapitola 5.1.6 dále).

Ve dvou případech je naopak poskytovateli umožněno, aby se jinak přísně stanovené odpovědnosti za vady zprostil, a to v případě, kdy vada digitálního obsahu vznikla v důsledku neprovedení aktualizace, na jejíž potřebu byl uživatel upozorněn, nebo podaří-li se poskytovateli prokázat, že vadu způsobilo nevyhovující digitální prostředí uživatele, ačkoli uživatel byl předem na potřebné digitální prostředí upozorněn.[134]

5.1.4.1. POŽADAVKY NA SOULAD A VADY

Pro spotřebitelské smlouvy budou vedle shora uvedených navrhovaných ustanovení § 2389c až 2389f o. z. platit rovněž speciální ustanovení stanovící požadavky na digitální obsah nebo službu digitálního obsahu. Jedná se o transpozici článků 7 až 9 DCD, které upravují požadavky ujednané stranami, označované jako subjektivní, a dále požadavky obecně platné, ledaže si smluvní strany ujednají jinak, označované jako objektivní. Z pohledu harmonizace práva členských států se jedná o zásadní ustano-

[134] Navrhované znění§ 2389d odst. 3 a § 2389e odst. 2 o. z.

vení, které by mělo zajistit spotřebitelům stejný standard ochrany napříč společným trhem. Požadavek plné harmonizace[135] zároveň znemožňuje rozšiřování těchto požadavků vnitrostátním právem, čímž umožňuje spolehnutí se na stejný standard rovněž poskytovatelům digitálního obsahu nebo digitálních služeb poskytujícím plnění spotřebitelům z jiných členských států.

Koncepce subjektivních a objektivních požadavků vznikla až v průběhu legislativního procesu. Původní návrh směrnice předložený Komisí byl postaven v zásadě na smluvně stanovených požadavcích, požadavky stanovené přímo směrnicí přicházely na řadu subsidiárně pouze v případě neexistence příslušných ujednání ve smlouvě.[136] Tento přístup byl v legislativním procesu opakovaně kritizován, a to jak ze strany členských států, tak Evropského parlamentu a právních odborníků.[137] S ohledem na praxi uzavírání spotřebitelských smluv, kdy návrh je obvykle předkládán podnikatelem ve formě obchodních podmínek a spotřebitel jej buď přijme jako celek (často bez čtení), nebo jako celek odmítne a smlouvu neuzavře, by možnost výhradně smluvní úpravy veškerých požadavků na plnění vedla k výraznému znevýhodnění spotřebitele, protože minimální standard plnění by si podnikatel určoval fakticky sám.[138]

Finální znění DCD proto upravuje dvě kategorie požadavků na soulad plnění– subjektivní (čl. 7) a objektivní (čl. 8 a čl. 9) – které musí být splněny kumulativně (zároveň).[139] Návrh zákona tyto požadavky transponuje do znění § 2389i o. z. Poskytnutí digitálního obsahu nebo služby digitálního obsahu v rozporu s těmito požadavky bude vadným plněním poskytovatele zakládajícím práva z odpovědnosti za vady (podrobněji viz následující kapitola 5.1.4.2).

---

[135] Čl. 4 DCD.

[136] Čl. 6 Návrhu SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o některých aspektech smluv o poskytování digitálního obsahu OM/2015/0634 final - 2015/0287 (COD).

[137] Viz např. The European Law Institute. *Statement of the European Law Institute ON THE EUROPEAN COMMISSION'S PROPOSED DIRECTIVEON THE SUPPLY OF DIGITAL CONTENT TO CONSUMERS*. COM (2015) *634 final*. s. 18-21.

[138] STAUDENMAYER, D. *Art. 6. Explanation.* In SCHULZE, R., STAUDENMAYER, D. *EU Digital Law: Article-by-Article Commentary*, Baden-Baden, Germany: Nomos, 2020. s. 114-115.

[139] Viz čl. 6 DCD.

Subjektivní požadavky na soulad zahrnují následující ujednané požadavky na digitální obsah nebo službu digitálního obsahu:

a) popis, rozsah, jakost, funkčnost, kompatibilitu, interoperabilitu a jiné smluvně ujednané vlastnosti; český návrh zákona na rozdíl od DCD termíny *funkčnost, kompatibilita a interoperabilita* nedefinuje, s ohledem na nutnost euro konformního výkladu je nutné vycházet z definic obsažených v čl. 2 DCD;
b) vhodnost k účelu, pro který uživatel digitální obsah požaduje, jestliže s ním poskytovatel souhlasil;
c) příslušenství, pokyny k použití vč. návodu k instalaci, uživatelská podpora.

Pro uživatele budou důležitější objektivní požadavky na soulad, protože na ty se může spolehnout i v případě, kdy smluvní podmínky nečetl a neví, jaké subjektivní požadavky v nich jsou zahrnuty, ani si žádné explicitně nevymínil a neujednal. Mezi objektivní požadavky na soulad náleží:

a) vhodnost k účelu, pro který se digitální obsah příslušného druhu obvykle používá, přičemž je výslovně zmíněn ohled na práva třetích osob, právní předpisy, technické normy nebo odvětvové kodexy chování;
b) rozsah, jakost a další výkonnostní parametry vč. funkčnosti, kompatibility, přístupnosti, kontinuity a bezpečnosti odpovídající obvyklým vlastnostem digitálního obsahu téhož druhu, které může uživatel rozumně očekávat, a to i s ohledem na veřejná prohlášení učiněná poskytovatelem nebo jinou osobou v témže transakčním řetězci, zejména reklamou nebo označením;
c) příslušenství a pokyny k použití, které může uživatel rozumně očekávat;
d) soulad se zkušební verzí nebo náhledem zpřístupněnými poskytovatelem před uzavřením smlouvy.

Ze shora uvedeného je patrný význam jednání poskytovatele uskutečněného před uzavřením smlouvy. Nicméně v případě veřejných prohlášení je možné, aby se poskytovatel jejich závaznosti zprostil, pokud prokáže, že si

tohoto prohlášení nebyl vědom, nebo že bylo v době uzavření smlouvy upraveno srovnatelným způsobem, jakým bylo primárně učiněno, anebo že na rozhodnutí uživatele uzavřít smlouvu nemohlo mít vliv. Otázkou je, zda bude nutné brát v úvahu pouze prohlášení směřovaná vůči vnitrostátnímu trhu členského státu spotřebitele, nebo je nutné brát v úvahu jakákoli prohlášení všech osob v distribučním řetězci učiněná na celém vnitřním trhu. Domnívám se, že s ohledem na účel této harmonizace, kterým je přispět k řádnému fungování vnitřního trhu a podpořit přeshraniční nakupování digitálních obsahů nebo digitálních služeb, by měla být relevantní veškerá prohlášení učinění v rámci vnitřního trhu EU, pokud bude zachována podmínka, že byla učiněna v témže distribučním řetězci. Tedy v hypotetickém příkladě podnikatele se sídlem v České republice, který nabízí digitální obsah nebo digitální služby dodávané prodejcem se sídlem v Polsku, který příslušný produkt nebo službu získává od německé mateřské společnosti, bude nutné zohlednit prohlášení všech těchto tří subjektů, nikoli ale prohlášení dalšího prodejce usazeného v Dánsku, který nabízí stejné plnění v Dánsku na základě vztahu s německým subjektem bez jakékoli účasti polského distributora nebo českého prodejce. Pokud by si ale český spotřebitel objednal stejné digitální plnění od dánského prodejce, bude třeba zohlednit jeho prohlášení a prohlášení německého originálního producenta, nikoli však prohlášení učiněná českým prodejcem nebo polským distributorem. Z pohledu spotřebitele může být tato situace matoucí, protože mu často nebudou vzájemné vztahy v distribučním řetězci známy. Z hlediska podnikatele produkujícího digitální služby nebo digitální obsah by měl být kladen důraz na kontrolu reklamních a jiných obdobných aktivit v celém distribučním řetězci. Nutno však dodat, že v případě digitální distribuce bude mnohem častější přímá globální distribuce než využívání složité hierarchie distributorů a prodejců. Prakticky větší význam tak bude mít obdobné ustanovení uvedené v čl. 7 odst. 1 písm. d) SGD, protože u prodeje zboží jsou naopak vícečlánkové distribuční řetězce využívány běžně.

Druhým důležitým rysem objektivních požadavků je kritérium *rozumného očekávání* uživatele (resp. spotřebitele). Jedná se o abstraktní právní pojem, jehož konkrétní obsah bude závislý na mnoha faktorech a nelze

proto poskytnout jeho vyčerpávající obecný výklad.[140] Podrobnější formování obsahu tohoto pojmu bude důležitým úkolem rozhodovací praxe soudů s využitím stávající judikatury pracující s pojmem *průměrného spotřebitele*, který má dostatek informací a je v rozumné míře pozorný a opatrný, jak jej definoval v rozhodovací praxi Soudní dvůr EU. Co jsou rozumná očekávání spotřebitele, bude záviset zejména na druhu poskytovaného digitálního obsahu nebo digitální služby a způsobu jejich poskytování. Zároveň zde mohou hrát roli i odlišnosti ve vyspělosti vnitrostátního trhu, na kterém byly digitální obsah nebo digitální služba pořízeny. Ačkoli evropské právo chápe vnitřní trh EU jako jeden celek, nelze odhlédnout od skutečnosti, že mezi vnitrostátními trhy nejvyspělejších unijních států a států v oblasti digitální ekonomiky méně vyspělých existují objektivní rozdíly, které formují právě i rozumná očekávání spotřebitelů, která se proto mohou v jednotlivých členských státech lišit.[141] Zároveň je třeba upozornit na skutečnost, že obsah rozumného očekávání spotřebitele do značné míry formují a v čase upravují právě poskytovatelé digitálního obsahu a digitálních služeb tím, jaký obchodní model zvolí. Paradoxně tak mohou snižovat úroveň ochrany spotřebitele právě formováním těchto rozumných očekávání ve svůj prospěch.[142]

Od objektivních požadavků na soulad je možné se odchýlit, pokud poskytovatel předem uživatele upozornil na konkrétní odchylnost digitálního obsahu nebo digitální služby a uživatel s tím výslovně souhlasil. V takových případech se nebude nesplnění objektivních podmínek považovat za vadu. Zatímco DCD požaduje informování spotřebitele *v době uzavření smlouvy* a *výslovný zvláštní* souhlas spotřebitele,[143] návrh zákona ve znění § 2389i odst. 4 vztahuje povinnost poskytovatele poskytnout příslušnou informaci k okamžiku *před uzavřením smlouvy* a požaduje pouze aby uživatel souhlasil

[140] STAUDENMAYER, D. *Art. 8. Explanation, Objective conformity criteria.* In SCHULZE, R., STAUDENMAYER, D. *EU Digital Law: Article-by-Article Commentary*, Baden-Baden, Germany: Nomos, 2020, s. 148.

[141] Srov. Rozsudek Soudního dvora EU ze dne 13. 1. 2000 ve věci C-220/98, Estée Lauder Cosmetic GmbH & Co. KG v Landcaster Group Limited.

[142] Srov. REYNA, A. *What Place for Fairness in Digital Content Contracts?* Baden-Baden, Germany: Nomos, 2020, s. 190.

[143] Čl. 8 odst. 4 DCD.

výslovně. Zatímco první případ odchýlení od textu směrnice nelze podle mého názoru považovat za problematický, protože je v obou případech vyžadováno, aby spotřebitel informaci měl předtím, než se smluvně zaváže, druhý případ nepřesné transpozice je problematičtější. I přes chybějící požadavek zákona na zvláštní (zvlášť, tj. zejména mimo text obecných obchodních podmínek, poskytnutý) souhlas bude nutné na dodržení této podmínky DCD z důvodu euro-konformního výkladu trvat. Ostatně i předkladatel návrhu zákona v důvodové zprávě[144] zdůrazňuje nutnost separátního poskytnutí souhlasu, bohužel tento požadavek ale nepromítl dostatečně jasně do normativního textu.

Podle DCD náleží mezi požadavky na soulad rovněž aktualizace, návrh české právní úpravy však problematiku poskytování aktualizací upravuje samostatně nejen pro spotřebitelské smlouvy, proto je o požadavcích na aktualizace pojednáno samostatně (viz kapitola 5.1.5).

Poskytovatel odpovídá za vady digitálního obsahu nebo digitální služby i v případě, že vada byla způsobena vadným propojením (integrací) s prostředím uživatele, pokud toto propojení provedl přímo poskytovatel či jiná osoba na jeho odpovědnost, nebo uživatel, ale vada nastala v důsledku nedostatku návodu poskytnutého poskytovatelem. Ze shora uvedeného pak vyplývá, že pokud integraci provedla jiná osoba než uživatel (která zároveň nejednala na odpovědnost poskytovatele), byť podle nedostatečného návodu poskytnutého poskytovatelem, poskytovatel se odpovědnosti za vady vyhne.[145] Na rozdíl od shora uvedených objektivních požadavků na soulad, v případě vad způsobených integrací není možné, aby poskytovatel předem svou odpovědnost smluvně vyloučil.[146]

5.1.4.2. PROSTŘEDKY NÁPRAVY

V případě nesouladu digitálního obsahu nebo služby se smlouvou upravuje směrnice prostředky nápravy. V návrhu zákona se mají prostředky nápravy

[144] Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 90.

[145] Čl. 9 DCD, navrhované znění § 2389i o. z.

[146] Čl. 22 DCD ve spojení s čl. 9 DCD.

vztahovat pouze na spotřebitele. Protože se jedná o speciální úpravu, bude mít tato u spotřebitelských smluv o poskytování digitálního obsahu přednost před obecnou úpravou práv z odpovědnosti za vady.

Pokud se jedná o kontinuální plnění, může uživatel vytknout vady digitálního obsahu nebo digitální služby, které se objeví kdykoli za trvání závazku, v případě jednorázového plnění pak vady, které se objeví v době dvaceti čtyř měsíců od zpřístupnění. Na rozdíl od obecné úpravy odpovědnosti za vady přizná soud právo z vady i tehdy, kdy nebyla oznámena bez zbytečného odkladu poté, co ji uživatel mohl při dostatečné péči zjistit.

Prostředky nápravy, které má uživatel (spotřebitel) k dispozici, jsou následující:

a) bezplatné odstranění vady, tj. uvedení digitálního obsahu nebo digitální služby do souladu se subjektivními i objektivními požadavky;
b) sleva z ceny;
c) odstoupení od smlouvy.

Pořadí nároků uživatele je přitom závazně dáno směrnicí a zákonem. Uživatel tedy v prvé řadě musí požadovat odstranění vady, výjimkou jsou situace, kdy je to nemožné nebo nepřiměřeně nákladné. Posouzení nemožnosti nebo výše nákladů však uživatel zpravidla nebude schopen kvalifikovaně provést, proto by měl vždy v prvé řadě požadovat bezplatné odstranění vady, ledaže jej o nemožnosti nebo nepřiměřených nákladech odstranění informuje sám poskytovatel. Teprve nebude-li odstranění vady možné, nebo bude-li nepřiměřeně nákladné, a dále v případech, kdy poskytovatel vadu v přiměřené době po vytknutí neodstranil nebo učinil prohlášení, ze kterého je zřejmé, že jí neodstraní, případně jedná-li se o vadu projevující se opakovaně i po snaze poskytovatele o její odstranění nebo vadu tak závažnou, že je podstatným porušením smlouvy, může uživatel žádat slevu z ceny nebo od smlouvy odstoupit.

Český návrh zákona obsahuje pro jeden ze shora uvedených případů nesmyslnou formulaci, když uvádí, že *uživatel může požadovat přiměřenou slevu*

nebo odstoupit od smlouvy, pokud se vada projeví i po odstranění.[147] Pokud by skutečně došlo k odstranění vady, tak by se samozřejmě neprojevila, protože už by neexistovala, je tak nutné vycházet z formulace čl. 14 odst. 4 písm. c) DCD, kde je správně a logicky vázána možnost požadovat slevu nebo odstoupit od smlouvy, jestliže navzdory snaze poskytovatele k uvedení do souladu, tj. k odstranění vady, digitálního obsahu nebo digitální služby nedojde. Poskytovatel nesmí při odstraňování vady způsobit uživateli značné obtíže. Lhůta pro odstranění vad (uvedení do souladu) je stanovena neurčitě: *v přiměřené době* od jejího vytknutí. Tuto neurčitost odůvodňuje rozmanitost digitálních obsahů a digitálních služeb, na které se bude právní úprava vztahovat a která znemožňuje určitější vymezení délky této lhůty.[148]

Sleva z ceny nepřichází v úvahu v případě, kdy jsou protiplněním poskytovaným za digitální obsah nebo službu digitálního obsahu osobní údaje uživatele.

V případě nápravy vady poskytnutím slevy z ceny se vychází z rozdílu mezi hodnotou digitálního obsahu (digitální služby) bez vad a vadného digitálního obsahu (digitální služby) poskytnutého uživateli. U digitálního obsahu nebo digitálních služeb poskytovaných kontinuálně po delší dobu se sleva uplatní z ceny za celou dobu, po kterou měl digitální obsah nebo digitální služba vadu, a to i v případě, že uživatel od smlouvy odstoupí. Směrnice (a stejně tak návrh zákona) považuje za rozhodující rozdíl v *hodnotě* digitálního obsahu nebo digitální služby s vadou a bez vad, nicméně znění obou textů není shodné.

Zatímco čl. 14 odst. 5 DCD stanoví, že *snížení ceny musí být poměrné k poklesu hodnoty digitálního obsahu nebo digitální služby, které byly spotřebiteli poskytnuty, ve srovnání s hodnotou, kterou by digitální obsah nebo digitální služba měly, kdyby byly v souladu*, tak navrhované znění § 2389m odst. 2 zjednodušuje, když normuje, že *přiměřená sleva se určí jako rozdíl mezi hodnotou digitálního obsahu bez vady a vadného digitálního obsahu* (pozn.

[147] Navrhované znění ust. § 2389m odst. 1 písm. b) o. z.

[148] Recitál 64 DCD.

stejně bude platit pro služby digitálního obsahu)*, který byl uživateli poskytnut*.

Rozdíl lze vysvětlit na následujícím příkladu:

Cena zaplacená za digitální obsah uživatelem 500,- Kč

Hodnota bezvadného digitálního obsahu 400,- Kč

Hodnota uživateli poskytnutého vadného dig. obsahu 200,- Kč

Pokles hodnoty o 200,- Kč

Sleva podle návrhu § 2389m odst. 2 bude 400 – 200 = 200 Kč

Sleva podle DCD: pokles hodnoty z důvodu vad je 200 Kč, tedy o 50 % oproti hodnotě bezvadného plnění, cena by proto měla být redukována ve stejném poměru, tj. také o 50 %, sleva bude činit 250,- Kč.[149]

Domnívám se, že zde došlo ze strany českého předkladatele návrhu zákona k chybě, když nebyl promítnut princip poměrného snížení ceny v závislosti na snížení hodnoty digitálního obsahu.

Pro právo na odstoupení stanoví DCD ještě další omezení v čl. 14 odst. 6, když u úplatných smluv přiznává uživateli právo na odstoupení od smlouvy pouze pro významný nesoulad. Český návrh zákona tuto koncepci přebírá do navrhovaného ustanovení § 2389m odst. 3 neúplně, protože zapovídá odstoupení od smlouvy pro nevýznamné vady digitálního obsahu nebo služby digitálního obsahu, aniž by jasně omezoval toto pravidlo pouze na úplatné smlouvy, jak činí DCD.

Formu odstoupení od smlouvy směrnice stanoví jako výslovnou,[150] ani DCD ani návrh zákona však nepředpisují, zda se má jednat o formu písemnou nebo ústní. Doporučit však lze z důvodu právní jistoty formu písemnou.

5.1.5 AKTUALIZACE A ZMĚNY DIGITÁLNÍHO OBSAHU

Významnou novinkou je výslovná regulace povinnosti poskytovatele digitálního obsahu nebo služby digitálního obsahu zajistit uživateli poskytování

[149] Srov. GSELL, B. *Art. 14. Price reduction and termination of the contract*. In SCHULZE, R., STAUDENMAYER, D. *EU Digital Law: Article-by-Article Commentary*, Baden-Baden, Germany: Nomos, 2020, s. 263.

[150] Čl. 15 DCD.

aktualizací a rovněž uživatele o možnosti a potřebnosti aktualizací informovat. Metzger označuje tuto povinnost za stěžejní z pohledu ochrany uživatele.[151] DCD povinnost zajistit poskytování aktualizací systematicky řadí mezi požadavky na soulad, a to jak subjektivní, tak i objektivní. Český předkladatel návrhu zákona vztahuje povinnost zabezpečit poskytování aktualizací digitálního obsahu převzatou ze směrnice nejen na smlouvy spotřebitelské, ale na smlouvy o poskytování digitálního obsahu obecně. Zároveň stejně jako směrnice odlišuje aktualizace sjednané ve smlouvě, jejichž poskytování je poskytovatel povinen zajistit v souladu se smlouvou, a aktualizace, jejichž zajištění je pro poskytovatele povinné přímo na základě zákona. K posléze uvedeným náleží aktualizace, které jsou nutné k tomu, aby byl digitální obsah bez vad (podle DCD nezbytné pro uvedení do souladu) po dobu trvání závazku. V případě smluv s jednorázovým plněním musí být tyto aktualizace poskytovány po dobu, po kterou to může uživatel rozumně očekávat. Znění čl. 8 odst. 2 DCD vcelku nadbytečně zdůrazňuje bezpečnostní aktualizace, tuto výslovnou zmínku však český předkladatel návrhu zákona, dle mého názoru správně, nepřevzal.

DCD i návrh zákona v zásadě vychází z koncepce, že poskytovatel je povinen zajistit informování uživatele o aktualizacích a umožnit mu jejich provedení, samotná instalace aktualizace by však měla být na aktivním jednání uživatele. Kromě samotné informace o možnosti stažení aktualizací musí poskytovatel zajistit, že uživatel bude upozorněn na případné důsledky toho, že si aktualizace nenainstaluje, a bude mu poskytnut dostatečný návod. Zanedbání těchto povinností vede k tomu, že se poskytovatel nemůže zbavit odpovědnosti za vady způsobené tím, že uživatel aktualizace nenainstaloval nebo tak neučinil správně. Vzhledem k tomu, že samotné aktualizace vydává výrobce digitálního obsahu, což je často osoba odlišná od poskytovatele, je na poskytovateli, aby v rámci distribučního řetězce dostatečně ošetřil poskytování všech potřebných aktualizací i informací uživateli.

[151] METZGER, A. Verträge über digitale Inhalte und digitale Dienstleistungen: Neuer BGB-Vertragstypus oder punktuelle Reform? *Juristen Zeitung*. 2019, s. 581.

Pasivita správně a dostatečně informovaného uživatele má za následek, že poskytovatel neodpovídá za vady vzniklé v důsledku nedostatku aktualizace digitálního obsahu. Otázkou je, zda takto nastavená pravidla nemohou vést k odklonu od praxe řady poskytovatelů, jejichž digitální obsah (zejm. software) se aktualizuje průběžně sám bez nutnosti zásahu uživatele pouze na základě prvotního souhlasu s automatickými aktualizacemi. Pokud by nově musel každou aktualizaci provést (nainstalovat) nebo přinejmenším samostatně odsouhlasit uživatel, zvýšila by se pravděpodobnost, že tak z pohodlnosti či nedbalosti neučiní a poskytovatel se vyhne odpovědnosti za takto vzniklé vady digitálního obsahu.

Nezajištění aktualizací v souladu se smlouvou a zněním zákona bude mít za následek odpovědnost poskytovatele za vady. Nároky uživatele z této odpovědnosti se budou lišit podle toho, zda se jedná o uživatele v postavení spotřebitele, nebo nikoli (viz kapitola 5.1.4).

Zatímco povinnost poskytovat aktualizace je v návrhu zákona vztažena na všechny smlouvy o poskytování digitálního obsahu nebo digitálních služeb, právní úprava změn digitálního obsahu se má vztahovat pouze na spotřebitele a na smlouvy, které nezavazují k pouze jednorázovému plnění.[152] Podmínky, které musí poskytovatel splnit, aby mohl digitální obsah během trvání závazku měnit, jsou následující:

a) Jedná se o smlouvu, podle které je digitální obsah (nebo služba digitálního obsahu) poskytován kontinuálně po určitou dobu, nesmí se tedy jednat o smlouvu s jednorázovým nebo opakovaným jednorázovým plněním;
b) možnost změny je sjednána ve smlouvě;
c) ve smlouvě je sjednán spravedlivý důvod pro takovou změnu;
d) uživateli změnou nevzniknou dodatečné náklady;
e) uživateli musí být poskytovatelem změna oznámena jasným a srozumitelným způsobem;

[152] Viz navrhované znění § 2389q o. z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994. a čl. 19 DCD.

f) informování uživatele v přiměřené době před provedením změny o povaze změny, čase jejího provedení a souvisejících právech (viz následující bod), jestliže změna zhoršuje nikoli jen nevýznamně přístup uživatele k digitálnímu obsahu nebo jeho užívání;
g) umožnění ukončení závazku výpovědí uživatele nebo ponechání digitálního obsahu beze změny v původní podobě (tj. odmítnutí změny uživatelem), pokud to není na úkor poskytování digitálního obsahu bez vad, jestliže změna zhoršuje nikoli jen nevýznamně přístup uživatele k digitálnímu obsahu nebo jeho užívání.

S ohledem na požadavek plné harmonizace[153] není možné, aby vnitrostátní zákonodárce rozšířil pro oblast spotřebitelských smluv úpravu možnosti změn digitálního obsahu rovněž na smlouvy o jednorázovém plnění a smlouvy o opakovaném jednorázovém plnění. U těchto smluv bude nutné posuzovat, zda případná změna je skutečně aktualizací nezbytnou k udržení digitálního obsahu v souladu s objektivními a subjektivními požadavky (podle českého návrhu zákona k zajištění bezvadnosti digitálního obsahu), nebo již nedovolenou změnou, která má naopak za následek nesoulad (vadnost) digitálního obsahu.[154]

Zatímco DCD požaduje informování spotřebitele o plánované změně a jeho právech (viz výše písm. f) a g)) *na trvalém nosiči,*[155] návrh zákona transponuje toto pravidlo do požadavku informování uživatele *v textové podobě*, což není totéž. Pojem *textová podoba* je nutné vykládat v kontextu ustanovení § 1819 o. z., podle kterého je textová podoba zachována, jsou-li údaje poskytnuty takovým způsobem, že je lze uchovat a opakovaně zobrazovat. Požadavek trvalosti tedy zahrnuje i textová podoba. Informování spotřebitele na trvalém nosiči (jak vyžaduje DCD) by přitom mohlo zahrnovat např. i poskytnutí video- nebo audio souboru s příslušnými

[153] Čl. 4 DCD.

[154] Srov. WENDLAND, M. *Art. 19. Transposition issues.* In SCHULZE, R., STAUDENMAYER, D. *EU Digital Law: Article-by-Article Commentary*, Baden-Baden, Germany: Nomos, 2020, s. 321.

[155] Viz čl. 19 odst. 1 písm. d) DCD.

informacemi, nicméně to by neodpovídalo požadavku návrhu zákona na poskytnutí v *textové podobě,* protože by v takovém případě absentoval jakýkoli text. Český předkladatel zákona tedy možnosti informování spotřebitele oproti čl. 19 DCD zužuje.

Zároveň požadavek na sjednání možnosti změny digitálního obsahu výslovně ve smlouvě považuji za nadbytečný.[156] Pokud by možnost změny digitálního obsahu nebo digitální služby nebyla ve smlouvě ujednána, jednalo by se o porušení smluvních povinností poskytovatele, protože jím poskytnuté plnění by se po provedení změny odlišovalo od sjednaného plnění a nebylo by tak nadále v souladu se smlouvou.

Zajímavé je, že zatímco v případě aktualizací je poskytovateli směrnicí i návrhem zákona umožněno, aby jejich poskytování pouze *zajistil či zabezpečil,* a není požadováno, aby je sám přímo poskytoval, pokud jde o změny digitálního obsahu, hovoří právní úprava přímo o upravení či změně digitálního obsahu poskytovatelem. Přitom v praxi bude obvyklé provedení změny výrobcem digitálního obsahu, nikoli poskytovatelem, což není na rozdíl od aktualizací vůbec reflektováno. V případě doslovného výkladu by bylo možné dojít k závěru, že provedení změny přímo výrobcem digitálního obsahu v souladu s jeho podmínkami užití digitálního obsahu (u software např. s EULA) nebude porušením povinností poskytovatele. Takovýto výklad by byl ale na úkor uživatele – spotřebitele, a tedy v přímém rozporu se smyslem právní úpravy. Zároveň je nutné zohlednit i skutečnost, že osobou poskytující uživateli digitální obsah je u smlouvy s kontinuálním plněním stále poskytovatel, nikoli výrobce digitálního obsahu, plnění zajišťované poskytovatelem by tak bylo v popsaném případě v rozporu s uzavřenou smlouvou.

I v případě uživatelů, kteří nejsou spotřebiteli, bude možné změny digitálního obsahu ujednat, ovšem za méně přísných podmínek, než tomu bude u spotřebitelů, neboť zde je ponecháno na vůli smluvních stran, jak podmínky provádění změn digitálního obsahu mezi sebou upraví.

[156] Srov. METZGER, A. Verträge über digitale Inhalte und digitale Dien-stleistungen: Neuer BGB-Vertragstypus oder punktuelle Reform? *Juristen Zeitung*. 2019, roč. 74, č. 12, s. 583.

5.1.6 DŮKAZNÍ BŘEMENO A DOMNĚNKY VE PROSPĚCH UŽIVATELE

Pro právní praxi významnou novinkou je posílení postavení uživatele v procesní oblasti. Jedná se o právní úpravu důkazního břemene podle čl. 12 DCD. Hlavním důvodem stanovení těchto pravidel je výrazná informační nerovnost mezi poskytovatelem a uživatelem. Zatímco poskytovatel bude disponovat technickými znalostmi a prostředky, jako jsou zejména logy a diagnostické nástroje, umožňujícími lépe zjistit a prokázat poskytnutí nebo existenci či příčinu nesouladu digitálního obsahu nebo služby digitálního obsahu, uživatel takovéto znalosti prostředky a informace zpravidla k dispozici mít nebude.[157] Zároveň se ale nejedná o obecné přesunutí důkazního břemene na poskytovatele, ale spíše o soubor speciálních pravidel dokazování, která se uplatní pro prokázání pouze některých skutečností týkajících se plnění smlouvy o poskytování digitálního obsahu. Prokazování ostatních skutečností, pro které unijní normotvůrce harmonizaci nepožaduje, bude nadále záležitostí vnitrostátní právní úpravy členských států.[158]

V prvé řadě je na poskytovateli, aby prokázal, že uživateli digitální obsah nebo službu digitálního obsahu skutečně zpřístupnil. Český návrh zákona stanoví toto důkazní pravidlo i pro smlouvy uzavřené s uživatelem, který není spotřebitelem.[159] Z hlediska českého právního řádu se zdá zakotvení tohoto pravidla do právního předpisu nadbytečným s ohledem na tzv. negativní teorii důkazní, podle které nenese účastník tvrdící negativní skutečnost ohledně této skutečnosti důkazní břemeno a na kterou se odvolává i judikatura Nejvyššího soudu.[160] Nicméně i v českém právním prostředí se v posledních letech považuje negativní teorie důkazní za překonanou a prokazování některých negativních skutečností je soudy požadováno.[161]

---

[157] Viz též recitál 59 DCD.

[158] Srov. ZOLL, F. *Art. 12. Function.* In SCHULZE, R., STAUDENMAYER, D. *EU Digital Law: Article-by-Article Commentary*, Baden-Baden, Germany: Nomos, 2020, s. 213.

[159] Viz navrhované znění ust. § 2389b odst. 3 o.z.

[160] Viz např. Usnesení Nejvyššího soudu ze dne 28. 6. 2016 sp. zn. 30 Cdo 1144/2014 nebo rozsudek Nejvyššího soudu ze dne 21. 4. 1998, sp. zn. 26 Cdo 732/98.

[161] Srov. např. MATZNER, J. *Problematika dokazování tzv. negativních skutečností. Právní prostor.* [Online]. 2020. nebo KRAMPERA, J. *Dokazování negativních skutečností.* epravo.cz. [Online]. 2019.

Proto je vhodné, že předkladatel zákona s ohledem na požadavek plné harmonizace navrhuje zahrnutí výslovného pravidla o břemenu důkazním do textu občanského zákoníku. Český návrh zákona se však odchyluje od textu směrnice. Zatímco DCD požaduje, aby poskytovatel nesl důkazní břemeno ohledně skutečnosti, že došlo k poskytnutí digitálního obsahu nebo digitální služby v souladu s čl. 5 DCD, český návrh zákona pouze stanoví, že *je na poskytovateli, aby prokázal, že digitální obsah uživateli zpřístupnil*, vynechává však požadavek prokázání, že došlo k tomuto zpřístupnění v souladu s ust. § 2389b odst. 1, 2, jež jsou transpozicí č. 5 DCD. V důvodové zprávě předkladatel zákona uvádí, že navrhované ust. § 2389b odst. 3 je transpozicí čl. 12 odst. 1 DCD,[162] z důvodu nutnosti zachování euro-konformního výkladu tak bude nutné v případě spotřebitelů vykládat ust. § 2389b odst. 3 tak, že poskytovatel nese důkazní břemeno i ohledně doby a způsobu zpřístupnění digitálního obsahu (resp. poskytnutí služby digitálního obsahu). V případě uživatelů, kteří nejsou spotřebiteli, tomu ale tak být nemusí a bude záležet na přístupu soudů.

Další pravidla dokazování v čl. 12 DCD se vztahují k prokazování souladu digitálního obsahu nebo služby v konkrétní časový okamžik, v terminologii českého návrhu zákona se tak jedná o prokazování vad, resp. okamžiku jejich existence. Rovněž tato pravidla vztahuje český návrh zákona na všechny uživatele bez rozdílu.

Pokud se vada digitálního obsahu projeví za trvání závazku, u závazků s kontinuálním plněním je na poskytovateli, aby prokázal, že digitální obsah nebo služba byly v této době bez vad. Důkazní břemeno ohledně projevení se vady během trvání závazku však ponese uživatel, jakožto strana sporu dovolávající se této skutečnosti, protože důkazní břemeno o této skutečnosti DCD ani návrh zákona na poskytovatele nepřenáší.[163]

V případě jednorázových plnění konstruuje návrh zákona vyvratitelnou právní domněnku, podle které se má za to, že projeví-li se vada v průběhu

[162] Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 85.

[163] Viz navrhovaná znění § 2389e odst. 1 In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994. a čl. 12 DCD.

jednoho roku od zpřístupnění, byl digitální obsah vadný již při zpřístupnění a případný důkaz opaku je na poskytovateli.[164] Prokázání výskytu vady v době jednoho roku od zpřístupnění bude ale opět na uživateli.

Namísto prokazování neexistence vady v příslušné době se však poskytovatel může omezit na prokázání nekompatibility digitálního prostředí uživatele s technickými požadavky digitálního obsahu nebo služby digitálního obsahu, o kterých poskytovatel uživatele před uzavřením smlouvy jasně a srozumitelně informoval nebo na prokázání neposkytnutí spolupráce uživatele potřebné pro zjištění toho, zda tkví příčina vady v takovéto technické nekompatibilitě uživatelova digitálního prostředí. Pokud bude poskytovatel úspěšný, speciální pravidla o důkazním břemeni podle čl. 12 odst. 2 a 3 DCD, resp. § 2389e odst. 1 a § 2389f odst. 2 o. z., se nepoužijí.

5.1.7 UKONČENÍ SMLOUVY

DCD upravuje v zásadě dvě oblasti související s tématem ukončení smlouvy o poskytování digitálního obsahu nebo digitálních služeb. V prvé řadě se jedná o úpravu důvodů, pro které může spotřebitel (uživatel) smlouvu ukončit. Přičemž se nejedná o vyčerpávající úpravu důvodů ukončení smlouvy, ale pouze důvody ukončení smlouvy pro porušení ze strany poskytovatele. Není tak vyloučena vnitrostátní právní úprava dalších důvodů ukončení smlouvy včetně možnosti ukončení bez nutnosti existence zákonného důvodu. Druhou DCD regulovanou oblastí je zvláštní úprava práv a povinností smluvních stran v souvislosti s ukončením smlouvy.

DCD používá výhradně neutrální spojení „ukončení smlouvy“[165] a nerozlišuje mezi výpovědí, odstoupením nebo dalšími způsoby ukončení smluvního vztahu. Český návrh zákona transponuje tento neutrální výraz do odstoupení od smlouvy v návrhu znění § 2389h, § 2389m o. z. a do možnosti výpovědi smluvního závazku v návrhu znění § 2389q odst. 3 o. z., v obou případech se má navrhovaná právní úprava ze zákona vztahovat pouze na

[164] Viz navrhovaná znění § 2389f odst. 3 o.z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994. a čl. 12 DCD.

[165] Viz též různé jazykové verze „termination“ v angličtině, „Beendigung“ v němčině, „ukončenie zmluvy“ ve slovenštině.

spotřebitele, což nevylučuje ujednání smluvních stran o tom, že se použije i v případě jiných než spotřebitelských smluv.

Důvody ukončení smlouvy podle DCD jsou:

a) prodlení s poskytnutím digitálního obsahu nebo digitální služby poskytovatelem;
b) nesoulad digitálního obsahu nebo digitální služby, který nebyl nebo nemůže být odstraněn nebo je natolik závažné povahy, že odůvodňuje okamžité ukončení od smlouvy;
c) změna digitálního obsahu, která negativně ovlivňuje přístup uživatele (spotřebitele) k digitálnímu obsahu či digitální službě nebo jejich používání, pokud tento negativní dopad není nevýznamný.

Je-li důvodem ukončení smlouvy ze strany uživatele prodlení s poskytnutím digitálního obsahu nebo služby digitálního obsahu, může uživatel smlouvu ukončit, pouze pokud poskytovatel neposkytne digitální obsah nebo digitální službu bez zbytečného odkladu po výzvě uživatele nebo během dodatečné lhůty, na které se strany výslovně dohodly, nebo v případě, že poskytovatel prohlásil nebo je z okolností zřejmé, že digitální obsah nebo digitální službu neposkytne, a dále v případech, kdy se strany dohodly nebo je zřejmé z okolností, za nichž byla smlouva uzavřena, že pro uživatele má zásadní význam určitá doba poskytnutí a že poskytovatel digitální obsah nebo digitální službu do této doby nebo v danou dobu neposkytne. Tento důvod ukončení smlouvy má být v české právní úpravě transponován do ustanovení § 2389h upravujícího právo uživatele, který je spotřebitelem, na odstoupení od smlouvy. Výzva uživatele k poskytnutí digitálního obsahu, která musí ve většině případů předcházet odstoupení od smlouvy, nevyžaduje žádnou zvláštní formu, lze ji učinit např. i telefonicky prostřednictvím help-line nebo prostřednictvím chatovací aplikace. Návrh zákona ani text DCD rovněž nepožadují, aby uživatel specifikoval poskytovateli dodatečnou lhůtu k poskytnutí digitálního obsahu nebo služby digitálního obsahu, pouze pro vznik práva na odstoupení od smlouvy musí být zachována

lhůta bez zbytečného odkladu.[166] Ohledně délky lhůty „bez zbytečného odkladu“ lze též odkázat na recitál 61 DCD, který v zásadě vychází z poskytování digitálního obsahu okamžitě po výzvě uživatele, vždy však bude nutné zohlednit veškeré okolnosti případu a zejména způsob poskytování digitálního obsahu nebo služby digitálního obsahu.

Druhou skupinu DCD upravených důvodů ukončení smlouvy, kterou český předkladatel návrhu zákona opět navrhuje transponovat do práva na odstoupení od smlouvy, tvoří případy nesouladu (v českém návrhu zákona se jedná o vady) digitálního obsahu nebo služby digitálního obsahu. Ukončení smlouvy má být v tomto případě jedním z prostředků nápravy v případě nesouladu, nejedná se však o prostředek primární. V zásadě vždy by mělo mít přednost uvedení digitálního obsahu nebo služby digitálního obsahu do souladu. Ukončení smlouvy nastupuje jako druhotný prostředek nápravy vedle práva na snížení ceny. Tento přístup byl v průběhu legislativního procesu kritizován ze strany European Law Institute,[167] v zásadě zůstal zachován i v konečném textu směrnice pouze s ústupkem ve prospěch možnosti okamžitého ukončení smlouvy v případech závažného nesouladu. Zatímco DCD použitím spojky „buď-nebo“ jednoznačně stanoví, že uživatel musí zvolit, zda bude požadovat snížení ceny, nebo ukončení smlouvy.[168] Návrh zákona uvádí, že *uživatel může požadovat přiměřenou slevu nebo odstoupit od smlouvy*, tedy používá na rozdíl od směrnice spojku „nebo“ ve slučovacím významu, což nedává příliš smysl, ledaže tím návrh zákona míří na situace upravené v čl. 16 odst. 1 DCD (viz dále). Odstoupit od smlouvy z důvodu vad digitálního obsahu může uživatel v případě, že

a) poskytovatel vadu neodstranil nebo je z prohlášení poskytovatele nebo z okolností zjevné, že vada nebude odstraněna v přiměřené době nebo bez značných obtíží pro uživatele,

---

[166] Srov. FERVERS, M. *Art. 13. Termination after request to the trader.* In SCHULZE, R., STAUDENMAYER, D. *EU Digital Law: Article-by-Article Commentary*, Baden-Baden, Germany: Nomos, 2020, s. 229.

[167] The European Law Institute. *Statement of the European Law Institute ON THE EUROPEAN COMMISSION'S PROPOSED DIRECTIVEON THE SUPPLY OF DIGITAL CONTENT TO CONSUMERS*. COM (2015) *634 final.*

[168] Čl. 14 odst. 4 DCD.

b) se vada projeví i po odstranění,[169] nebo

c) je vada podstatným porušením smlouvy.

Zároveň uživatel nemůže odstoupit od smlouvy, je-li vada digitálního obsahu jen nevýznamná. K tomu doplňuje návrh zákona vyvratitelnou domněnku, podle které se má za to, že vada není nevýznamná.

Na rozdíl od prodlení s plněním nebo vad plnění, kdy je uživatel oprávněn od smlouvy odstoupit, v případě změny digitálního obsahu nebo služby digitálního obsahu, která nikoli nevýznamně negativně ovlivňuje přístup uživatele k digitálnímu obsahu nebo službě digitálního obsahu nebo jejich používání, transponuje návrh zákona právo na ukončení smlouvy do práva uživatele smlouvu vypovědět v omezené lhůtě 30 dnů od okamžiku vyrozumění o změně nebo provedení změny.

Podle čl. 15 DCD uživatel (spotřebitel) uplatní své právo na ukončení smlouvy prohlášením určeným poskytovateli, ve kterém sdělí své rozhodnutí ukončit smlouvu. Pro odstoupení od smlouvy ze strany uživatele tak nejsou vyžadovány žádné zvláštní náležitosti, ani není výslovně požadována určitá forma, učinit je tak bude možné i ústně, např. prostřednictvím telefonické linky podpory.

DCD dále upravuje v čl. 16 a čl. 17 práva a povinnosti smluvních stran v případě ukončení smlouvy. Český návrh zákona promítá tato ustanovení DCD do navrhovaného znění § 2389n o. z. Zde však již dochází k terminologickému posunu, protože ustanovení § 2389n o.z. se má vztahovat pouze na případy odstoupení uživatele-spotřebitele od smlouvy nebo výpovědi z důvodu změny digitálního obsahu nebo služby digitálního obsahu s negativním dopadem na uživatele. V případě ukončení smlouvy výpovědí z jiného důvodu (či bez uvedení důvodu) nebo uplynutím sjednané doby smluvní strany tato práva a povinnosti mít nebudou, ledaže by si je ujednaly. DCD přitom vznik níže uvedených práv a povinností váže na ukončení smlouvy, nikoli na její ukončení výhradně z důvodů uvedených v čl. 14, čl. 15 nebo čl. 19 odst. 2 DCD.

Poskytovatel je povinen v návaznosti na ukončení smlouvy (resp. podle českého zákona odstoupení uživatelem):

[169] Viz předchozí výklad v kapitole 5.1.4.2.

a) vrátit uživateli veškeré zaplacené platby, vyjma částek za období, kdy byl digitální obsah nebo služba digitálního obsahu před ukončením smlouvy v souladu (bez vad), a to bez nákladů pro uživatele a do 14 dnů od okamžiku, kdy se dozvěděl o uplatnění práva na ukončení smlouvy;
b) zdržet se užívání obsahu odlišného od osobních údajů uživatele, který byl vytvořen uživatelem při užívání digitálního obsahu, vyjma případů, kdy tento obsah
    a. nelze využít mimo rámec digitálního obsahu nebo digitální služby poskytnutých poskytovatelem;
    b. souvisí pouze s činností uživatele při používání digitálního obsahu nebo digitální služby poskytnutých poskytovatelem;
    c. byl poskytovatelem sloučen s jinými daty a nemůže být, nebo jen s vynaložením nepřiměřeného úsilí, oddělen; nebo
    d. vytvořil uživatel společně s dalšími osobami, které tento obsah mohou i nadále užívat;

Pokud se jedná o osobní údaje uživatele, je poskytovatel povinen postupovat podle GDPR.

c) zajistit na žádost uživatele uživateli dostupnost jakéhokoli jiného obsahu než osobních údajů, který poskytl nebo vytvořil při používání digitálního obsahu nebo digitální služby poskytnuté poskytovatelem (vyjma případů uvedených shora sub i až iii), a to bezplatně, v přiměřené době a v běžně používaném strojově čitelném formátu.

Uživatel je naopak povinen se nadále zdržet používání digitálního obsahu nebo služby digitálního obsahu a jejich poskytování třetím stranám. Byl-li uživateli v souvislosti s poskytováním digitálního obsahu nebo služby digitálního obsahu odevzdán hmotný nosič, vydá jej poskytovateli na jeho žádost a náklady bez zbytečného odkladu. Poskytovatel může o vydání hmotného nosiče požádat pouze do čtrnácti dnů od ukončení závazku, pak toto právo ztrácí.

5.1.8 REGRES V DODAVATELSKÝCH SMLUVNÍCH VZTAZÍCH

Ačkoli se DCD soustředí na ochranu spotřebitele stanovením harmonizovaných požadavků na spotřebitelské smlouvy o poskytování digitálního obsahu nebo digitálních služeb, obsahuje i ustanovení s dopadem pouze do obchodních vztahů. Jedná se o v čl. 20 DCD, který zakotvuje právo regresu poskytovatele digitálního obsahu nebo služby vůči ostatním článkům obchodního dodavatelského řetězce, jestliže nesoulad nebo neposkytnutí digitálního obsahu nebo služby digitálního obsahu byly způsobeny opomenutím nebo jednáním osoby nebo osob odlišných od poskytovatele, které jsou členy obchodního dodavatelského řetězce. Nutným předpokladem vzniku nároku vůči těmto osobám je vznik odpovědnosti poskytovatele vůči uživateli – spotřebiteli za neposkytnutí digitálního obsahu nebo služby digitálního obsahu nebo za jejich nesoulad. Jakékoli dobrovolné vyhovění požadavkům uživatele, které neodpovídá zákonným nárokům, nelze tedy vůči ostatním článkům dodavatelského řetězce uplatnit. Čl. 20 DCD navíc omezuje možné nároku poskytovatele pouze na řetězec obchodních transakcí. Určení osoby, vůči níž se může poskytovatel domáhat nápravy, podmínek výkonu práva i příslušných opatření ponechává DCD vnitrostátnímu právu.

Návrh zákona promítá pravidla uvedená v čl. 20 DCD do navrhovaného ustanovení § 2174b o. z. ve spojení s ust. § 2389r o. z. Podle ust. § 2389r o. z. se právo postihu upravené v ust. § 2174b o. z. použije jak v případě vady digitálního obsahu nebo služby digitálního obsahu, tak i v případě prodlení s jeho zpřístupněním. Podle navrhované právní úpravy se bude ust. § 2174b o. z. vztahovat pouze na poskytování digitálního obsahu nebo služeb digitálního obsahu spotřebiteli. To může poskytovatelům v praxi činit určité potíže, protože např. u řady softwarových aplikací uživatel při jejich pořízení neuvádí, zda je pořizuje jako spotřebitel, nebo pro účely podnikání. Ustanovení § 2174b je předkladatelem návrhu zákona koncipo-

váno jako kogentní,[170] poskytovatel (ani další články dodavatelského řetězce) se nemůže svých práv na náhradu předem platně vzdát nebo je omezit. Po vzniku nároku již však vzdání se nebo omezení práv poskytovatele návrh zákona nezapovídá. Podle navrhované české právní úpravy bude mít poskytovatel nárok na náhradu pouze vůči přímému smluvnímu partnerovi, který mu v rámci své podnikatelské činnosti byl zavázán poskytovat digitální obsah či službu digitálního obsahu, včetně jejich aktualizace. Na další osoby v dodavatelském řetězci se uplatní princip postihu obdobně, tedy každý jednotlivý dodavatel bude moci uplatnit nárok na náhradu vůči svému smluvnímu partnerovi. Takovéto řešení není zrovna vhodné z hlediska procesní ekonomie ani z pohledu mezinárodního práva soukromého. Postupné uplatňování nároků jednotlivými články dodavatelského řetězce po sobě může vést k nutnosti vedení postupně několika soudních sporů, zatímco v případě možnosti uplatnit nárok poskytovatele přímo vůči osobě odpovědné za neposkytnutí digitálního obsahu nebo služby digitálního obsahu či jejich vady by se snížil počet potenciálních soudních sporů. Zároveň s ohledem na mezinárodní prostředí trhu digitálního obsah a služeb digitálního obsahu lze očekávat, že smluvní vztahy mezi jednotlivými články dodavatelského řetězce se budou řídit právními řády několika různých států, což může situaci zbytečně komplikovat.[171] Stejně jako DCD omezuje návrh znění § 2174b o. z. právo postihu pouze na podnikatelské vztahy. Právo na náhradu poskytovateli nevznikne, věděl-li o vadě digitálního obsahu nebo služby digitálního obsahu v okamžiku jejich převzetí nebo nebyly-li digitální obsah či služba digitálního obsahu určeny k uvedení na trh pro spotřebitele. Výše náhrady se určí ve výši nákladů, které poskytovatel účelně vynaložil na zjednání nápravy.

[170] Viz navrhované znění § 2174b odst. 3 o.z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994 a Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 83.

[171] MOŽINA, D. *Art. 20. Transposition issues.* In SCHULZE, R., STAUDENMAYER, D. *EU Digital Law: Article-by-Article Commentary*, Baden-Baden, Germany: Nomos, 2020, s. 329.

5.2 SPECIFIKA KUPNÍ SMLOUVY NA ZBOŽÍ S DIGITÁLNÍMI PRVKY

SGD sama sebe omezuje jen na kupní smlouvy, v případě uzavření spotřebitelské smlouvy o nájmu (leasingu) nebo výpůjčce se proto nepoužije. Z hlediska evropského práva je to logické, protože pronájem zboží s digitálními prvky z jiného členského státu bude v praxi neobvyklý. Ani návrh vnitrostátní právní úpravy ale nevyužil možnosti upravit zvláštnosti poskytování věcí s digitálními vlastnostmi pro jiné případy, než je uzavření kupní smlouvy. Spotřebitelé, kteří si notebook nebo mobilní telefon pouze pronajímají,[172] nebudou mít na rozdíl od spotřebitelů, kteří si stejné zařízení koupí, zaručenu stejnou úroveň právní ochrany. Pravděpodobné však je, že tento nedostatek bude vyrovnán tržními mechanismy.

Kupní smlouva, jejímž předmětem plnění je zboží s digitálními prvky (v terminologii návrhu zákona věc s digitálními vlastnostmi), není ani v SGD, ani v návrhu zákona upravena jako samostatný smluvní typ, jedná se tak pouze o speciální ustanovení, která se užijí nad rámec obecné úpravy kupní smlouvy. Návrh zákona v tomto případě na rozdíl od právní úpravy smluv o poskytování digitálního obsahu omezuje svou působnost pouze na kupní smlouvy spotřebitelské. Právní úprava se navíc vztahuje pouze na úplatné smlouvy, kde spotřebitelem poskytovaným protiplněním jsou peníze,[173] nikoli na případy, kdy by spotřebitel namísto kupní ceny výměnou za věc s digitálními prvky poskytoval osobní údaje.

Právní úprava se bude vztahovat jak na případy, kdy je digitální obsah ve zboží k okamžiku koupě již nainstalován, případně kdy je k tomuto okamžiku se zbožím již spojena digitální služba, tak i na případy, kdy je teprve dodatečně nutné tuto instalaci nebo propojení provést, a to i tehdy, kdy digitální obsah nebo službu poskytuje jiná osoba.[174] Osobou odpovědnou za splnění všech smluvních závazků včetně případné odpovědnosti bude vůči kupujícímu vždy pouze prodávající. V případě pochybností, zda

[172] V ČR např. služba ALZA Neo, https://www.alza.cz/alza-neo-17434.htm.

[173] Čl. 2 odst. 1 SGD.

[174] Viz navrhované znění § 2158 odst. 2 o. z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994. a čl. 3 odst. 3 SGD.

je digitální obsah nebo služba součástí kupní smlouvy, se navíc má za to, že tomu tak je. Směrnice dále ve vztahu ke třetím osobám upřesňuje postavení poskytovatelů platforem, kteří se budou považovat za prodávající pouze v případě, že jednají jako přímí smluvní partneři kupujícího spotřebitele při prodeji zboží.[175]

Prodávající odpovídá kupujícímu nejen za vady věci s digitálními prvky včetně vad digitálního obsahu nebo služby, ale také za vady způsobené nesprávnou montáží nebo instalací, pokud byla provedena prodávajícím nebo na jeho odpovědnost třetí osobou nebo samotným spotřebitelem. V případech uvedených posléze odpovídá prodávající za tyto vady, pouze pokud vada nastala v důsledku nedostatku v návodu, který poskytl prodávající nebo poskytovatel digitálního obsahu či služby.[176] Domnívám se, že toto ustanovení může činit problémy, protože technické znalosti spotřebitelů a jejich schopnost správně pochopit dodaný návod se budou diametrálně lišit. Zodpovědět otázku, kdy může za vadu instalace chyba či nejasnost v návodu a kdy nešikovnost či nechápavost spotřebitele, může být velice náročné. Zajímavé bude sledovat, jak se s tímto problémem vypořádá soudní praxe.

Zřejmě nejdůležitější novinkou právní úpravy kupních smluv o koupi zboží s digitálními prvky je zakotvení povinnosti prodávajícího zajistit poskytování aktualizací digitálního obsahu nebo služby. Rozlišují se přitom ve smlouvě sjednané aktualizace a aktualizace ve smlouvě neujednané, ale nutné pro zachování vlastností věci. V případě jednorázového plnění digitálního obsahu nebo služby se povinnost poskytovat výslovně nesjednané aktualizace vztahuje na dobu, po kterou to může kupující rozumně očekávat.[177] Tuto dobu bude opět obtížné určit a bohužel ani úvodní

[175] Recitál 23 SGD.

[176] Viz navrhované znění § 2161a o. z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994. a čl. 8 SGD.

[177] Viz navrhované ustanovení § 2161b odst. 2 písm. b) o. z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994. a čl. 7 odst. 3 písm. a) SGD.

ustanovení SGD v tomto případě nedávají příliš jasné vodítko.[178] Očekávání spotřebitelů se mohou výrazně lišit, pro někoho je běžné měnit mobilní telefon každý rok, a tedy po delší dobu nebude očekávat ani poskytování aktualizací, jiný spotřebitel naopak bude považovat za rozumně očekávatelnou dobu pěti, šesti či více let. V případě, kdy bylo ve smlouvě ujednáno poskytování digitálního obsahu nebo služeb soustavně po určitou dobu, mají být nezbytné aktualizace poskytovány po dobu dvou let a v případě ujednání delší doby, po celou tuto dobu.[179]

V případě, že kupující aktualizace nenainstaluje, ačkoli na ně byl upozorněn, nenese prodávající odpovědnost za nesoulad se smlouvou vzniklý v důsledku tohoto jednání kupujícího. Naopak, pokud prodávající poskytne aktualizaci, která způsobí nesoulad zboží se smlouvou, je jeho odpovědností zajistit opětovné uvedení zboží do souladu.

Dochází tak k zajímavému posunu obvyklého pojetí a vnímání kupní smlouvy jako kontraktu s jednorázovým plněním, kdy ke splnění závazku prodávajícího dojde předáním věci a převodem vlastnického práva.[180] U zboží s digitálními prvky toto pravidlo nebude platit, protože prodávající bude mít dlouhodobou povinnost poskytovat nezbytné aktualizace i několik let poté, co došlo k převodu vlastnického práva a předání věci kupujícímu.

Obdobně jako v případě smluv o poskytování digitálního obsahu nebo služeb je upravena problematika práv duševního vlastnictví, kdy případná práva třetích osob bránící nebo omezující použití zboží zakládají nesoulad se smlouvou (vadu) a právo spotřebitele na nápravu.

Stejně jako v případě smluv o poskytování digitálního obsahu nebo služby je kogentně upraveno právo regresu v dodavatelském řetězci.

---

[178] Viz recitál 31 SGD.

[179] Viz navrhované ustanovení § 2161b odst. 2 písm. a) o. z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994. a čl. 7 odst. 3 písm. b) SGD.

[180] § 2079 odst. 1 o. z.

6. OSOBNÍ ÚDAJE JAKO PROTIPLNĚNÍ

Tématem, které zaujalo odbornou veřejnosti i v České republice[181] a vzbudilo kontroverze,[182] je poskytování osobních údajů spotřebitele jako protiplnění za poskytování digitálního obsahu nebo digitální služby. Jedná se o rozsahem malé, ale dopadem významné, ustanovení druhé věty čl. 3 odst. 1 DCD, podle kterého se tato směrnice vztahuje rovněž na případy, kdy *obchodník poskytuje nebo se zavazuje poskytovat digitální obsah nebo digitální službu spotřebiteli a spotřebitel* ***poskytne nebo se zavazuje poskytnout obchodníkovi své osobní údaje****, s výjimkou případů, v nichž obchodník osobní údaje poskytnuté spotřebitelem zpracovává výlučně pro účely poskytování digitálního obsahu nebo digitální služby v souladu s touto směrnicí nebo pro účely toho, aby dodržel zákonné požadavky, jež se na něho vztahují, přičemž obchodník tyto údaje nezpracovává k žádným jiným účelům*.

Návrh zákona přebírá shora uvedené ustanovení směrnice pouze pro právní úpravu upravující poskytování digitálního obsahu nebo služeb digitálního obsahu spotřebiteli, na fyzické osoby, které v příslušném smluvním vztahu nevystupují jako spotřebitelé, se ustanovení o poskytování digitálního obsahu v případě bezúplatných smluv, kde jsou protiplněním osobní údaje, vztahovat nebudou. Rozšíření působnosti na případy poskytování osobních údajů je upraveno pouze v DCD a na smlouvy o koupi zboží s digitálními prvky se tak nevztahuje.

Původní znění návrhu nové směrnice předložené Evropskou komisí mělo širší dosah než konečné přijaté znění. Původně bylo navrhováno, aby se směrnice vztahovala vedle úplatných smluv o poskytování digitálního obsahu rovněž na smlouvy, u kterých *spotřebitel aktivně poskytne jiné než peněžní protiplnění ve formě osobních údajů nebo jakýchkoli jiných údajů*.[183] V průběhu legislativního procesu byl odstraněn požadavek na aktivní

[181] Viz např. NONNEMANN, F. Osobní údaje jako platidlo? *Právní rozhledy*. 2020, č. 5, s. 174 nebo Peyton legal. *Platba osobními údaji – realita dnešní doby a její regulace.* [Online]. 2020. [cit. 17. 12. 2020]. Dostupné z: https://www.peytonlegal.cz/platba-osobnimi-udaji/.

[182] Viz např. European Data Protection Supervisor. *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*. [Online] 2017. [cit. 17. 12. 2020]. https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en_1.pdf .

poskytování osobních údajů a vedle toho byly z působnosti DCD vyňaty smlouvy, u kterých uživatel – spotřebitel poskytuje jiné než své osobní údaje. Zároveň ve finálním textu DCD nejsou údaje poskytnuté spotřebitelem označovány jako *protiplnění*. Jedná se o promítnutí požadavku Evropského inspektora ochrany údajů[184] v rámci konzultací během legislativního procesu. Fakticky se však o protiplnění ze strany spotřebitele jedná,[185] čemuž nasvědčuje i navrhované znění ustanovení § 2389g odst. 2 o.z. „… *uživatel* ***namísto*** *odměny poskytovateli poskytuje nebo se zavazuje poskytnout své osobní údaje…“*, ve kterém jsou osobní údaje uvedeny jako substitut odměny.

DCD zdůrazňuje, že osobní údaje ani nadále nemají být považovány za komoditu a právo na jejich ochranu je jedním ze základních práv. Důvodem zahrnutí těchto smluv do právní úpravy poskytování digitálního obsahu je skutečnost, že v praxi již takovéto obchodní modely fungují a je tedy namístě poskytnout v nich spotřebitelům dostatečnou právní ochranu.[186] Na zpracování osobních údajů poskytnutých výměnou za digitální obsah nebo službu se vztahuje podle čl. 3 odst. 8 DCD Obecné nařízení o ochraně osobních údajů (GDPR) a ostatní právní předpisy upravující ochranu osobních údajů a jejich zpracování.

Zároveň ne všechny případy, kdy uživatel – spotřebitel poskytne poskytovateli digitálního obsahu nebo digitální služby své osobní údaje, budou spadat do působnosti DCD. V prvé řadě se musí jednat o smluvní vztah. Jestliže z pohledu vnitrostátního práva nedojde k uzavření smlouvy, nebude se DCD, a tedy ani nová právní úprava obsažená v o. z., aplikovat, protože DCD upravuje pouze *společná pravidla týkající se určitých požadavků na smlouvy o poskytování digitálního obsahu nebo digitálních služeb uzavírané mezi obchodníky a spotřebiteli,*[187] nikoli pravidla pro jiné právní skutečnosti.

[183] Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o některých aspektech smluv o poskytování digitálního obsahu OM/2015/0634 final - 2015/0287, s. 25.

[184] European Data Protection Supervisor.

[185] Srov. STAUDENMAYER, D. *Art. 3. Substantive scope.* In SCHULZE, R., STAUDENMAYER, D. *EU Digital Law: Article-by-Article Commentary*, Baden-Baden, Germany: Nomos, 2020. s. 71.

[186] Recitál 24 DCD.

[187] Čl. 1 DCD a dále recitál 24 DCD.

Závěr o tom, zda byla uzavřena smlouva, je věcí vnitrostátní právní úpravy. V ČR tak bude nutné vycházet z obecné úpravy uzavírání smluv obsažené v ustanoveních části čtvrté hlavy I. dílu 2 občanského zákoníku. I v případě platného uzavření smlouvy o poskytování digitálního obsahu se však právní úprava obsažená v DCD, resp. odpovídajících ustanoveních o. z., nepoužije, jestliže se nejedná o úplatnou smlouvu a uživatelem (spotřebitelem) poskytnuté osobní údaje poskytovatel zpracovává pouze pro účely poskytnutí digitálního obsahu či digitální služby nebo pouze ke splnění svých zákonných povinností, jako je zejména právním předpisem uložená povinnost identifikace nebo registrace uživatele.

Vzhledem k tomu, že na zpracování osobních údajů se i nadále vztahuje GDPR, je otázkou, o jaký titul se bude v tomto případě zpracování opírat. V úvahu by přicházelo plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů, zpracování nezbytné pro účely oprávněných zájmů příslušného správce či třetí strany nebo souhlas subjektu údajů.[188] Jak uvádí Nonnemann,[189] byl dosud pro tyto účely využíván zpravidla souhlas subjektu údajů, nicméně nová právní úprava navádí spíše k tomu, že by se mělo jednat o zpracování nezbytné pro plnění smlouvy. Pro poskytovatele digitálního obsahu nebo služby by se jednalo o výrazně výhodnější postavení, protože na rozdíl od souhlasu není možné smlouvu jednostranně odvolat.

S ohledem na oddělenost právních úprav a skutečnost, že DCD důsledně zdůrazňuje působnost GDPR pro zpracování osobních údajů a jeho aplikační přednost, je nutné smlouvu o poskytování digitálního obsahu nebo digitální služby a titul ke zpracování osobních údajů posuzovat odděleně. DCD nepodmiňuje svou aplikaci tím, že poskytovatel musí mít platný titul ke zpracování osobních údajů uživatele. DCD, resp. na jejím základě přijatá vnitrostátní právní úprava, se bude proto vztahovat na smlouvy o poskytnutí digitálního obsahu nebo digitální služby výměnou za osobní údaje uživatele – spotřebitele i v případě, že titul ke zpracování osobních údajů

[188] Čl. 6 odst. 1 GDPR.

[189] NONNEMANN, F. Osobní údaje jako platidlo? *Právní rozhledy.* 2020, č. 5, s. 174.

bude neplatný. Jak uvádí Metzger, bude stejný závěr platit i v případě, kdy právní titul ke zpracování osobních údajů pozbude platnosti, resp. bude odvolán či jinak zanikne, až v průběhu trvání smlouvy.[190] To je významné zejména v případě zpracování založeného na souhlasu subjektu údajů, protože souhlas lze kdykoli odvolat,[191] což ale nebude mít vliv na trvání uzavřené smlouvy. V takovém případě by přicházelo v úvahu ukončení smluvního vztahu výpovědí, případně odstoupením, nebo jeho zánik pro nemožnost plnění. Vždy však budou muset být naplněny zákonné nebo smluvní důvody výpovědi nebo odstoupení od smlouvy, případně prokázána skutečná nemožnost plnění. Poskytovatelům tak lze doporučit, aby zahrnuli do svých obchodních podmínek možnost výpovědi z důvodu zániku uděleného souhlasu ke zpracování osobních údajů, a to nejlépe bez výpovědní doby. V Německu zákonodárce v rámci transpozice směrnic upravil uvedenou situaci pro vyloučení pochybností výslovně zákonem tak, aby poskytovatel mohl smlouvu vypovědět bez výpovědní doby.[192]

Řešení tohoto konfliktu mezi pravidly smluvního práva (DCD a její transpozice do vnitrostátního práva) a práva ochrany osobních údajů (GDPR) bude do budoucna na rozhodovací praxi soudů. S ohledem na možnost různého přístupu vnitrostátních soudů v různých členských státech je vysoce pravděpodobné, že ve finále bude nutné sjednocení judikatury členských států rozhodnutím Soudního dvora EU.[193]

Zajímavým momentem je, že směrnice s ohledem na svůj hlavní účel, kterým je ochrana spotřebitele, upravuje pouze práva spotřebitelů, ale nijak nereguluje situaci, kdy naopak uživatel-spotřebitel poskytne poskytovateli

[190] METZGER, A. A *Market Model for Personal Data: State of Play under the New Directive on Digital Content and Digital Services.* In LOHSSE, S. SCHULZE, R., STAUDENMAYER, D. a kol. *Data as Counter-Performance – Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V*. Germany, Baden-Baden: Nomos, 2020, s. 35.

[191] Čl. 7 odst. 3 GDPR.

[192] Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, vom 25. Juni 2021, Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 37, nové znění § 327q BGB.

[193] Srov. SATTLER, A. *Autonomy or Heteronomy – Proposal for a Two-Tier Interpretation of Art 6 GDPR.* In LOHSSE, S. SCHULZE, R., STAUDENMAYER, D. a kol. *Data as Counter-Performance – Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V*. Germany, Baden-Baden: Nomos, 2020, s. 228.

výměnou za digitální obsah nebo službu digitálního obsahu nepravdivé nebo neúplné osobní údaje. Úprava této otázky je ponechána vnitrostátnímu právu, což, jak uvádí Metzger, může vést ke značným rozdílům v jednotlivých vnitrostátních řešeních.[194] V návrhu zákona tato záležitost specificky upravena není, bude proto nutné postupovat podle obecných ustanovení závazkového práva a ujednání příslušné smlouvy, v praxi obvykle zahrnutých do obchodních podmínek poskytovatele.

Důvodová zpráva návrhu zákona k tématu poskytnutí a zpracování osobních údajů doplňuje možná rizika v podobě zneužití poskytnutých osobních údajů k jiným účelům než vymezeným ve smlouvě nebo špatného vyhodnocení ceny osobních údajů spotřebitelem, v důsledku čehož spotřebitel nedostane adekvátní protihodnotu. Předkladatel návrhu zákona ovšem v takových případech vyjma zjevných excesů (jako je např. lichva) preferuje respektování smluvní volnosti,[195] čímž v zásadě staví osobní údaje do pozice směnné hodnoty obdobné penězům.

Uzavření smlouvy o poskytování digitálního obsahu nebo služby, kdy spotřebitel poskytuje „pouze“ osobní údaje, má zároveň dopad na některá navazující práva spotřebitele. V případě nesouladu obsahu se smlouvou zejména (již z logiky věci) nemůže požadovat poskytnutí slevy z ceny, zároveň však může ukončit smlouvu i v případě nevýznamného nesouladu se smlouvou.[196]

Otázkou je, jak s legalizací poskytování osobních údajů jako protiplnění (byť tento výraz směrnice ani návrh zákona neužívá) naloží budoucí praxe. Domnívám se, že v případě příliš volného a kreativního výkladu by se mohlo jednat o porušení základních práv subjektu údajů i konkrétních ustanovení GDPR, zejména základních zásad podle čl. 5 GDPR, proto je na místě spíše zdrženlivý přístup.

---

[194] METZGER, A. Verträge über digitale Inhalte und digitale Dien-stleistungen: Neuer BGB-Vertragstypus oder punktuelle Reform? *Juristen Zeitung*. 2019, roč. 74, č. 12, s. 584.

[195] Důvodová zpráva vládního návrhu zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994, s. 43.

[196] Čl. 14 odst. 6 DCD a navrhované znění § 2389g odst. 2 a § 2389m odst. 3 o. z. In *Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.* Sněmovní tisk č. 994.

7. ZÁVĚR

Cílem tohoto článku bylo popsat a analyzovat novou právní úpravu poskytování digitálního obsahu, digitálních služeb a zboží s digitálními prvky obsaženou ve Směrnici Evropského parlamentu a Rady (EU) 2019/770 ze dne 20. května 2019 o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb a ve Směrnici Evropského parlamentu a Rady (EU) 2019/771 ze dne 20. května 2019 o některých aspektech smluv o prodeji zboží, o změně nařízení (EU) 2017/2394 a směrnice 2009/22/ES a o zrušení směrnice 1999/44/ES spolu s navrhovanou transpozici těchto norem do právního řádu České republiky.

Celkově legislativní iniciativu Evropské unie v oblasti poskytování digitálního obsahu, služeb digitálního obsahu a prodeje zboží s digitálními prvky považuji za vhodnou, ba nutnou. Potřeba regulovat tuto oblast je vyvolána praxí a chováním trhu. Zároveň s ohledem na neexistenci hranic kybernetického prostoru a běžné poskytování digitálního obsahu a digitálních služeb bez ohledu na státní hranice je vhodné, že regulace byla přijata jednotně na unijní úrovni, byť s ohledem na omezené možnosti unijního zákonodárce pouze pro oblast spotřebitelských smluv a v kompromisním znění.

Za největší slabinu nové právní úpravy na evropské úrovni považuji oblast úpravy poskytování osobních údajů za poskytování digitálního obsahu nebo digitální služby. DCD je v tomto směru poněkud pokrytecká, když se striktně vyhýbá jakékoli textaci, která by naznačovala, že osobní údaje jsou poskytovány jako protiplnění obdobné platbě, ačkoli ve skutečnosti tak tomu přesně je. Z hlediska praxe však jako mnohem významnější problém chápu chybějící úpravu pravidel pro případ vzájemných střetů právní úpravy poskytování digitálního obsahu a právní úpravy zpracování osobních údajů. Bohužel ani český předkladatel návrhu transpozičního zákona nevyužil možnosti tuto mezeru vyplnit alespoň částečně vlastními pravidly, jak učinil například zákonodárce německý.

Jako jednu z nejvýznamnějších novinek vnímám uložení zákonné povinnosti poskytovat aktualizace, kterou se i původně jednorázové smlouvy,

zejména kupní smlouva na zboží s digitálními prvky (v ČR věci s digitálními vlastnostmi), mění na smlouvy s dlouhodobým plněním. V praxi pak očekávám problémy s vymezením doby, po kterou může spotřebitel poskytování aktualizací rozumně očekávat. Celkově v konceptu rozumného očekávání spotřebitele (uživatele) spatřuji jedno z potenciálně problematických míst budoucí aplikační praxe, když rozumná očekávání spotřebitelů v různých členských státech se mohou vlivem zvyklostí lokálního trhu lišit a zároveň na celém vnitřním trhu budou nutně podléhat vlivu jednání poskytovatelů digitálních služeb, kteří tento trh utvářejí. První z uvedených problémů může vést k ohrožení jednoho z účelů DCD, a to přispění k řádnému fungování vnitřního trhu mj. stanovením společných standardů. Druhý z uvedených negativních důsledků pak může v rozporu s účelem DCD naopak vést ke snižování standardu ochrany spotřebitelů cíleným ovlivňováním jejich rozumného očekávání „velkými hráči" z řad poskytovatelů digitálního obsahu a digitálních služeb. Rovněž zavedení závazného pořadí prostředků nápravy v případě nesouladu (vad) digitálního obsahu nebo digitální služby je podle mého názoru pro spotřebitele spíše zbytečným omezením než přínosem.

Pokud se týká návrhu transpozice do českého právního řádu, považuji za problematické samotné systematické uchopení celé materie regulace poskytování digitálního obsahu a digitálních služeb. Předkladatel návrhu zákona bez obsáhlejšího teoreticko-právního zdůvodnění přistoupil k rozšíření katalogu smluvních typů v občanském zákoníku zcela v rozporu s jeho dosavadním pojetím. Přitom podle mého názoru splnění povinnosti transpozice do českého právního řádu může být dosaženo i novelizací všeobecných ustanovení o závazcích v hlavě I. čtvrté části občanského zákoníku.

Za chybu považuji, že návrh zákona omezuje nově zaváděný smluvní typ pouze na smlouvy o zpřístupnění digitálního obsahu (nebo poskytnutí digitální služby) k užívání pro vlastní potřebu, aniž by takové omezení vyplývalo z unijní legislativy. Zde se již podle mého názoru předkladatel návrhu zákona dostává přímo do rozporu s povinností plné harmonizace. Na více místech se pak lze setkat v návrhu zákona s chybami v transpozici

směrnic. Některé jsou drobnějšího charakteru a půjde je odstranit výkladem (např. nesprávné formulace výjimek z působnosti právní úpravy). Ale například odchylnou transpozici způsobu výpočtu slevy v případě vadného plnění považuji za chybu, která v praxi může vést k rozporu s unijní legislativou a poškozování českých spotřebitelů. Samozřejmě je možné, že přinejmenším část těchto chyb bude odstraněna v průběhu legislativního procesu.

Samotnou snahu předkladatele zákona vztáhnout úpravu smluv o poskytování digitálního obsahu a digitálních služeb rovněž na smlouvy, které nejsou uzavírány se spotřebiteli, vnímám jako vhodnou a přínosnou. Leč provedení nepovažuji za dostatečně precisní, když omezením části právní úpravy pouze na podnikatelsko-spotřebitelské vztahy došlo k tomu, že část důležitých aspektů není pro ostatní smluvní vztahy ze smluv o poskytování digitálního obsahu a digitálních služeb regulována vůbec. Jedná se zejména o prodej digitálního obsahu na hmotném nosiči a případy vytvoření digitálního obsahu na zakázku.

Významnou změnou pak je chápání pojetí věci v důsledku navrhované právní úpravy. Jako přínosné vnímám, že v případě přijetí návrhu zákona bude pro české právo vyřešena otázka právního pojetí dat, když tato budou přímo právním předpisem prohlášena za věci v právním smyslu. Naopak problematické může být právní pojetí věcí s digitálními vlastnostmi, které jsou spojením hmotné movité věci s digitálním obsahem nebo službou digitálního obsahu. Zde považuji za možné vícero řešení s očekáváním budoucí akademické diskuse i rozhodovací praxe soudů, které by měly vést k vyjasnění.

8. POUŽITÉ ZDROJE:

8.1 MONOGRAFIE, KOMENTÁŘE

[1] LAVICKÝ, P. a kol.: Občanský zákoník I. Obecná část (§ 1 – 654). Komentář. 1. vydání, Praha: C. H. Beck, 2014, 2400 s., ISBN 978-80-7400-529-9

[2] LOHSSE, S., SCHULZE, R., STAUDENMAYER, D. a kol. *Data as Counter-Performance – Contract Law 2.0?: Münster Colloquia on EU Law and the Digital Economy V*. Germany, Baden-Baden: Nomos, 2020, 288 s. ISBN (ePDF) 978-3-7489-0853-1

[3] POLČÁK, R. a kol. *Právo informačních technologií.* Praha: Wolters Kluwer, 2018. 656 s. ISBN 978-80-7598-045-8. cit z ASPI [5. 12. 2020]. ASPI ID: MN328CZ

[4] POLČÁK, R. a kol. *Autorský zákon. Praktický komentář s judikaturou.* Praha: Leges, 2020. 864 s. ISBN 978-80-7502-391-9

[5] REYNA, A. *What Place for Fairness in Digital Content Contracts?* Baden-Baden, Germany: Nomos, 2020. 242 s. ISBN 978-3-8487-7814-0.

[6] RIFKIN, J. *The age of access: the new culture of hypercapitalism, where all of life is a paid-for experience*. New York: J.P. Tarcher/Putnam, 2000.

[7] SCHULZE, R., STAUDENMAYER, D. a kol. *EU Digital Law: Article-by-Article Commentary*, Baden-Baden, Germany: Nomos, 2020. 596 s. ISBN 978-3-8487-4978-2

[8] ŠVESTKA, J., DVOŘÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář.* 1. vyd. Praha: Wolters Kluwer, a. s., 2014. Svazek I. 1736 s. ISBN 978-80-7478-370-8. cit. z ASPI [15. 12. 2020]. ASPI ID: KO89_a2012CZ

[9] ŠVESTKA, J., DVOŘÁK, J., FIALA, J. a kol. *Občanský zákoník. Komentář.* 1. vyd. Praha: Wolters Kluwer, a. s., 2014. Svazek V. 1700 s. ISBN 978-80-7478-638-9. cit. z ASPI [12. 7. 2021]. ASPI ID: KO89_e2012CZ

8.2 ČLÁNKY

[10] CAUFFMAN, C. New EU rules on business-to-consumer and platform-to-business relationship. *Maastricht Journal of European and Comparative Law.* 2019, roč. 26, č. 4, s. 469-479

[11] HERVÉ, J. Digital Content and Sales or Service contracts under EU Law and Belgian/ French Law. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law.* 2017, roč. 8., č. 1, s. 27-38

[12] METZGER, A. Verträge über digitale Inhalte und digitale Dienstleistungen: Neuer BGB-Vertragstypus oder punktuelle Reform? *Juristen Zeitung*. 2019, roč. 74, č. 12, s. 577-586

[13] METZGER, A., EFRONI, Z., MISCHAU, L., METZGER, J. Data-Related Aspects of the Digital Content Directive. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*. 2018, roč. 9, č. 1, s. 90–ii

[14] NONNEMANN, F. Osobní údaje jako platidlo? *Právní rozhledy*. 2020, č. 5, s. 174

[15] OPRYSK, L., SEIN, K.. Limitations in End-User Licensing Agreements: Is There a Lack of Conformity Under the New Digital Content Directive? *IIC - International Review of Intellectual Property and Competition Law.* 2020, roč. 51, č. 5, s. 594–623

[16] POLČÁK, R. Informace a data v právu. *Revue pro právo a technologie.* [Online]. 2016, roč. 7, č. 13, s. 67-91. [cit. 03. 12. 2020]. Dostupné z: https://journals.muni.cz/revue/article/view/4946

[17] RICHTER, Š. Směrnice EU 2019/770 o některých aspektech poskytování digitálního obsahu a digitálních služeb jako nástroj ochrany spotřebitele. *Jurisprudence.* 2020, č. 4, s. 9. cit z ASPI [06. 12. 2020]. ASPI ID: LIT283880CZ

[18] SEIN, K. What Rules Should Apply to Smart Consumer Goods: Goods with Embedded Digital Content in the Borderland between the Digital Content Directive and Normal Contract Law. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*. 2017, roč. 8, č. 2, s. 96–110

[19] TOMÍŠEK, J. Software jako věc v režimu nového občanského zákoníku. *Revue pro právo a technologie*. [Online]. 2014, roč. 5, č. 9, s. 197-210. [cit. 03. 12. 2020]. Dostupné z: https://journals.muni.cz/revue/article/view/5021

[20] WENDLAND, M. Sonderprivatrecht für Digitale Güter. *Zeitschrift für Vergleichende Rechtswissenschaft.* 2019, č. 118, s. 191-230

8.3 INTERNETOVÉ ZDROJE

[21] The European Law Institute. *Statement of the European Law Institute ON THE EUROPEAN COMMISSION'S PROPOSED DIRECTIVEON THE SUPPLY OF DIGITAL CONTENT TO CONSUMERS*. COM (2015) *634 final*. [Online]. 2016. [cit. 03. 12. 2020]. Dostupné z: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Statement_on_DCD.pdf

[22] Peyton legal. *Platba osobními údaji – realita dnešní doby a její regulace?* [Online]. 2020. [cit. 17. 12. 2020]. Dostupné z: https://www.peytonlegal.cz/platba-osobnimi-udaji/

[23] European Data Protection Supervisor. *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content.* [Online]. 2017. [cit. 17. 12. 2020]. https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en_1.pdf

[24] European Parliament. *Legislative train schedule. Connected digital single market.* [Online]. 2019. [cit. 17. 06. 2021]. https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-common-european-sales-law

[25] Smluvní podmínky služby Google Play. [Online]. 2020. [cit. 23. 07. 2021]. https://play.google.com/intl/cs_cz/about/play-terms/index.html

[26] MATZNER, J. *Problematika dokazování tzv. negativních skutečností. Právní prostor.* [Online]. 2020. [cit. 11. 08. 2021]. https://www.pravniprostor.cz/clanky/procesni-pravo/problematika-dokazovani-tzv-negativnich-skutecnosti

[27] KRAMPERA, J. *Dokazování negativních skutečností.* epravo.cz. [Online]. 2019. [cit. 11. 08. 2021]. https://www.epravo.cz/top/clanky/dokazovani-negativnich-skutecnosti-109753.html

[28] Rozsudek Soudního dvora EU ze dne 13. 1. 2000 ve věci C-220/98, Estée Lauder Cosmetic GmbH & Co. KG v Landcaster Group Limited

[29] Usnesení Nejvyššího soudu ze dne 28. 6. 2016 sp. zn. 30 Cdo 1144/2014

[30] Rozsudek Nejvyššího soudu ze dne 21. 4. 1998, sp. zn. 26 Cdo 732/98

[31] Vládní návrh zákona, kterým se mění zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Sněmovní tisk č. 994. [Online]. [cit. 05. 09. 2021]. Dostupné z: https://www.psp.cz/sqw/text/tiskt.sqw?O=8&CT=994&CT1=0

[32] Entwurf eines Gesetzes zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen. Bundesministerium der Justiz und für Verbraucherschutz. Bearbeitungsstand: 05.10.2020. [Online]. [cit. 03. 12. 2020]. Dostupné z: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Bereitsstellung_digitaler_Inhalte.html

[33] RICHTER, Š. *Směrnice EU o poskytování digitálního obsahu a její dopad na české závazkové právo.* Diplomová práce. Právnická fakulta Masarykovy univerzity. 2018

[34] NÁVRH NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o společné evropské právní úpravě prodeje. COM/2011/0635 final - 2011/0284 (COD). [Online] 2011. [cit. 08. 07. 2021]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52011PC0635

[35] Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o některých aspektech smluv o poskytování digitálního obsahu OM/2015/0634 final - 2015/0287 (COD). [Online] 2015. [cit. 08. 07. 2021]. https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52015PC0634

[36] Zpětvzetí návrhů Komise. 2020/C 321/03. [Online]. 2020. [cit. 17. 06. 2021]. Dostupné z: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52020XC0929%2802%29

[37] Strategie pro jednotný digitální trh v Evropě. COM(2015) 192 final [Online]. 2015. [cit. 17. 06. 2021]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52015DC0192

[38] Gesetz zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, vom 25. Juni 2021, Bundesgesetzblatt Jahrgang 2021 Teil I Nr. 37

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:

Discussion:	5 – 30 standard pages
Annotation:	2 – 10 standard pages
Essays:	5 – 10 standard pages
Book review:	1 – 5 standard pages
Topic section:	30 – 80 standard pages

(including spaces, footnotes and bibliography)

CITATIONS FORMAT

Citations shall be in accordance with the ISO 690:2011 citation standard.

Referencing examples are available in interpretations of the aforementioned citation standard (e. g. at www.ezdroje.muni.cz/prehled/zdroj.php?lang=en&id=441).

Individual sources are referenced in the text by upper index. The actual citation of the source is then contained in a footnote.

DEADLINES FOR CONTRIBUTIONS SUBMISSIONS

For the summer issue: 28th February

For the winter issue: 31th August

The Review of Law and Technology is a gold open access journal.

Contributions are included into respective electronic legal information systems operated by Wolters Kluwer ČR, a. s. (ASPI), Nakladatelství C. H. BECK, s. r. o. (beck-online.cz) and ATLAS consulting spol. s r. o. (CODEXIS).

Detailed information about the publication process, structure and format of the contributions, the review process and copyright are available in the "For 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 13 | YEAR 2022 | NUMBER 25

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 2022.
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: doc. 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: JUDr. Ing. František Kasl, Ph.D.
Editorial Staff: JUDr. Mgr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek, Ph.D.
Editorial Secretary: Anna Blechová
Editors: Anna Blechová, Martin Erlebach
Editorial Board: prof. JUDr. Radim Polčák, Ph.D. (honorary chairman), JUDr. Zuzana Adamová, Ph.D., prof. JUDr. Michael Bogdan, B.A., LL.M., jur. dr. (Lund), JUDr. Marie Brejchová, LL.M., JUDr. Jiří Čermák, 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., doc. JUDr. Matěj Myška, Ph.D., Mgr. Antonín Panák, LL.M., Mgr. Bc. Adam Ptašnik, Ph.D., JUDr. Danuše Spáčilová, JUDr. Eduard Szattler, Ph.D., JUDr. Tomáš Ščerba, Ph.D.
Layout: Mgr. Martin Loučka, doc. JUDr. Matěj Myška, Ph.D.
Print: POINT CZ, s.r.o., Milady Horákové 20, 602 00 Brno
The publication of this issue of the Review of Law and Technology was funded by the project „Právo a technologie X“, MUNI/A/1484/2021.

MUNI LAW Centrum dalšího vzdělávání

MODERNÍ A JEDINEČNÝ OBSAH

LL.M. V PRÁVU INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

Vzdělávejte se na mezinárodně respektovaném pracovišti, Ústavu práva a technologií Právnické fakulty Masarykovy univerzity, pod vedením elitních vyučujících.

KOMBINACE ONLINE I PREZENČNÍ FORMY VÝUKY

INFORMACE O PROGRAMU

WWW.LLM.LAW.MUNI.CZ

Diskuze

Jan Provazník: **Kriminalistické a trestněprávní aspekty detekce lží analýzou tzv. mikroexpresí**

Michaela Prucková: **Právo na přístup k internetu: současný postoj Organizace spojených národů a Evropské unie**

Anotace

Anna Blechová, Martin Erlebach, Vojtěch Juřička, Anežka Karpjáková, František Kasl, Andrej Krištofík, Pavel Loutocký, Sofie Petrová, Jan Svoboda, Jakub Vostoupal, Ondřej Woznica: **Přehled aktuální judikatury I/2022**

Essays

A. Blechová, M. Erlebach, R. Hulanská, T. Krznarič, A. Tsuvina: **Essays I/2022**

Recenze

Jan Tomíšek: **Gellert, R.: The risk-based approach to data protection**

Téma

Kristýna Bónová: **Ochrana soukromí ve veřejném prostoru**

Zuzana Limbergová: **Směrnice o digitálním obsahu a jejich implementace v právním řádu ČR**

MUNI PRESS