22

REVUE PRO PRÁVO A TECHNOLOGIE

Ústav práva a technologií Právnické fakulty Masarykovy univerzity

Ročník 11 / Rok 2020 / Číslo 22

Revue.law.muni.cz

MUNI LAW

Ústav práva a technologií

Masivní rozšíření nových technologií a možností šíření a zpracování osobních údajů stálo za zavedením nového regulačního rámce ochrany osobních údajů v podobě nařízení EU č. 2016/679 (Obecné nařízení o ochraně osobních údajů). Monografie Moderní regulatorní metody ochrany osobních údajů vychází z důsledné teoretické analýzy základních zásad a principů ochrany osobních údajů, které je třeba při zpracování osobních údajů brát v potaz. Publikace dále identifikuje slabé stránky předchozí právní úpravy spočívající zejména v její nízké flexibilitě. Ve své klíčové části pak publikace představuje performativní regulaci jako moderní regulatorní metodu zvolenou evropským zákonodárcem pro Obecné nařízení, která umožňuje překonání nedostatků bývalé úpravy, ale která zároveň přinesla řadu výzev v interpretační a aplikační praxi. Publikace tyto výzvy identifikuje a nabízí možnosti jejich překonání a řešení.

Tato publikace vznikla na Masarykově univerzitě v rámci řešení projektu "Právo a technologie VIII", číslo projektu MUNI/A/0989/2019 podpořeného z prostředků účelové podpory na specifický vysokoškolský výzkum, kterou poskytlo MŠMT v roce 2020.

REVUE PRO PRÁVO A TECHNOLOGIE

ROČNÍK 11 | ROK 2020 | ČÍSLO 22

DISKUZE

ANOTACE

RECENZE

TÉMA

Revue pro právo a technologie
Odborný recenzovaný časopis pro technologické obory práva a právní vědy zařazený na Seznamu recenzovaných neimpaktovaných periodik vydávaných v České republice a v databázi ERIH PLUS.
Recenzovány jsou příspěvky v sekci Diskuze a Téma.
Vychází dvakrát ročně. Toto číslo vyšlo 31. 12. 2020.
ISSN 1804-5383 (Print), ISSN 1805-2797 (Online), Ev. č. MK ČR E 19707
Vydává Masarykova univerzita, Žerotínovo nám. 9, 601 77 Brno, ČR, IČ 00216224
Šéfredaktor a kontaktní osoba: JUDr. Matěj Myška, Ph.D., Ústav práva a technologií Právnické fakulty Masarykovy univerzity, Veveří 70, 611 80 Brno, ČR, tel: +420 549 494 751, fax: +420 541 210 604, e-mail: revue@law.muni.cz | www.revue.law.muni.cz
Zástupce šéfredaktora: Ing. Mgr. František Kasl
Redakce: JUDr. Mgr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek, Ph.D.
Tajemnice redakce: Anna Blechová
Editoři: Anna Blechová, Martin Erlebach
Redakční rada: doc. JUDr. Radim Polčák, Ph.D. (čestný předseda), JUDr. Zuzana Adamová, Ph.D., prof. JUDr. Michael Bogdan, B.A., LL.M., jur. dr. (Lund), JUDr. Marie Brejchová, LL.M., JUDr. Jiří Čermák, doc. JUDr. Bc. Tomáš Gřivna, Ph.D., doc. JUDr. Josef Kotásek, Ph.D., JUDr. Bc. Zdeněk Kučera, Ph.D., Mgr. Ing. Zbyněk Loebl, LL.M., JUDr. Ján Matejka, Ph.D., prof. RNDr. Václav Matyáš, M.Sc., Ph.D., JUDr. Matěj Myška, Ph.D., Mgr. Antonín Panák, LL.M., Mgr. Bc. Adam Ptašnik, Ph.D., JUDr. Danuše Spáčilová, JUDr. Eduard Szattler, Ph.D., JUDr. Tomáš Ščerba, Ph.D.
Grafická úprava: Mgr. Martin Loučka, JUDr. Matěj Myška, Ph.D.
Tisk: POINT CZ, s.r.o., Milady Horákové 20, 602 00 Brno
Vydání tohoto čísla časopisu Revue pro právo a technologie bylo financováno z projektu „Právo a technologie VIII“, MUNI/A/0989/2019.

POKYNY PRO AUTORY

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

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

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

Příspěvky se podávají prostřednictvím redakčního systému dostupného na adrese www.revue.law.muni.cz.

DOPORUČENÝ ROZSAH PŘÍSPĚVKŮ:

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

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

CITAČNÍ STANDARD

Použité prameny je nutné citovat v souladu s citační směrnicí ČSN ISO 690:2011.

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

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

TERMÍNY PRO DODÁNÍ PŘÍSPĚVKŮ

Do letního čísla: 31. března

Do zimního čísla: 30. září

Časopis se hlásí k politice otevřeného přístupu realizovaného zlatou cestou.

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

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

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

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

ČO VIEŠ O MOJOM VOZIDLE? OCHRANA OSOBNÝCH ÚDAJOV A KYBERNETICKÁ BEZPEČNOSŤ V KONTEXTE AUTONÓMNYCH VOZIDIEL

JOZEF ANDRAŠKO[1], MATÚŠ MESARČÍK[2]

ABSTRAKT

Autori sa v článku zameriavajú na vybrané otázky toku údajov v kontexte autonómnych vozidiel. V prvých častiach príspevku sú postupne predstavené základné pojmy danej problematiky a načrtnutá právna úprava. Následne sú charakterizované prieniky s právnou úpravou kybernetickej bezpečnosti a ochrany osobných údajov. Osobitný dôraz je kladený na otázku osobnej pôsobnosti a súvisiacej zodpovednosti v oblasti ochrany osobných údajov medzi jednotlivými aktérmi spracúvania osobných údajov v autonómnom vozidle.

KĽÚČOVÉ SLOVÁ

autonómne vozidlá, autonómne systémy, automatizované systémy, kybernetická bezpečnosť, ochrana osobných údajov

ABSTRACT

The authors focus on selected issues of data flow in the context of autonomous vehicles. The first parts of the paper gradually introduce the basic concepts of

[1] JUDr. Jozef Andraško, PhD., odborný asistent, Ústav práva informačných technológií a práva duševného vlastníctva, Univerzita Komenského v Bratislave, Právnická fakulta, e-mail: jozef.andrasko@flaw.uniba.sk.

[2] JUDr. Matúš Mesarčík, PhD. LL.M, odborný asistent, Ústav práva informačných technológií a práva duševného vlastníctva, Univerzita Komenského v Bratislave, Právnická fakulta, e-mail: matus.mesarcik@flaw.uniba.sk.

the issue and outline the legislation. Subsequently, the interferences with the legal regulation of cyber security and personal data protection are highlighted. Special emphasis is placed on the issue of personal scope and related liability in the field of personal data protection among the various actors in the processing of personal data in an autonomous vehicle.

KEYWORDS

autonomous vehicles, autonomous systems, automated systems, cyber security, data protection

1. ÚVOD

Výrobcovia automobilov ako Tesla, Mercedes, Toyota, GM, Nissan, Volkswagen a ďalší už dlhšiu dobu testujú autonómne vozidlá, najmä čiastočne autonómne vozidlá. Plne autonómne vozidlo, kedy sa nevyžaduje, aby ho riadil vodič a kde je možné naplánovať trasu z bodu A do bodu B, sa zdá byť nateraz nedosiahnuteľným konceptom, ktorý by sa mal v spoločnosti uplatniť. Avšak z právneho hľadiska testovanie a najmä následné zavádzanie autonómnych vozidiel spochybňuje viaceré právne inštitúty, najmä v oblasti zodpovednosti, súkromia, ochrany údajov, typového schválenia vozidiel, právnej subjektivity autonómnych systémov, autorských práv a pod.

Tento príspevok sa venuje vybraným právnym otázkam týkajúcich sa autonómnych vozidiel, a to konkrétne otázkam kybernetickej bezpečnosti a ochrany osobných údajov. Otázka kybernetickej bezpečnosti v súvislosti s autonómnymi vozidlami má viacero aspektov. V prvom rade ide o situácie, kedy dochádza ku kybernetickým útokom voči autonómnemu alebo automatizovanému systému, kedy je automobil ovládaný na diaľku útočníkom. Zo sveta sú známe kybernetické útoky, kedy došlo ku kybernetickému bezpečnostnému incidentu, ktorý spôsobil, že útočníci ovládali riadenie, preraďovanie, brzdy, otváranie okien, klimatizáciu automobilu s určitým stupňom automatizácie. Taktiež môže ísť o situácie, kedy útočník nechce získať kontrolu nad vozidlom ale chce získať prístup k lokalizačným

údajom, resp. k iným osobným údajom, ktoré sa spracúvajú v rámci činnosti autonómneho vozidla.

V druhej kapitole tohto príspevku dôjde k objasneniu rozdielu medzi autonómnymi a automatizovanými systémami. Autori sa taktiež budú venovať pojmu autonómne vozidlo v kontexte jednotlivých úrovní automatizácie, ako aj konceptu prepojených vozidiel, kde načrtnú rôzne druhy komunikácie, v rámci ktorej dochádza k spracúvaniu osobných údajov. V ďalšej kapitole sa autori venujú vybraným legislatívnym aktom Európskej únie (ďalej len „EÚ"), ktoré upravujú problematiku autonómnych vozidiel, resp. infraštruktúry s ktorou autonómne a prepojené vozidlá komunikujú, a to z pohľadu kybernetickej bezpečnosti a ochrany osobných údajov. V piatej časti sa autori článku zamýšľajú nad správnym vymedzením postavenie rôznych aktérov spracúvania osobných údajov v autonómnom vozidle. V prvom kroku je načrtnutá osobná pôsobnosť Všeobecného nariadenia na ochranu údajov (GDPR) a súvisiace otázky zodpovednosti. Následne je kriticky vyhodnotené usmernenie Výboru na ochranu údajov (EDPB), ktoré sa týka spracúvania údajov v autonómnych vozidlách. V závere tejto časti sú načrtnuté tri modelové prípady prepojenia autonómnych vozidiel a analýza postavenia jednotlivých potenciálnych aktérov spracúvania osobných údajov.

2. AUTONÓMNE SYSTÉMY A AUTOMATIZOVANÉ SYSTÉMY

Autonómne vozidlo (*autonomous vehicle*), automatizované vozidlo (*automated vehicle*),[3] samo jazdiace vozidlo (*self-driving vehicle*) či vozidlo bez vodiča (*driverless vehicle*). Tieto pojmy sa najčastejšie v médiách, ale aj odbornej a vedeckej literatúre spájajú s konceptom vozidla, kedy niektoré alebo všetky jazdné úlohy vykonáva vozidlo, presnejšie povedané, jeho systémy, bez toho, aby ich musel vykonávať vodič.[4] Práve tieto systémy, ktoré sú podstatou vozidiel schopných vykonať všetky alebo niektoré jazdné úlohy bez intervencie vodiča, možno deliť na automatizované a autonómne.

[3] Preklad anglického pojmu *automated* možno v slovenčine preložiť ako automatizovaný alebo automatický.

[4] Pre účely tohto príspevku používame zaužívaný pojem autonómne vozidlo.

Jeden zo spôsobov ako odlíšiť autonómny systém a automatizovaný systémom je zamerať sa na ich schopnosť prispôsobenia sa, učenia sa a rozhodovania, ktoré je integrované do systému. Automatizované systémy zvyčajne fungujú na základe vopred definovaných parametrov a sú veľmi obmedzené v tom, aké úlohy môžu vykonávať. Autonómny systém sa naopak učí prispôsobiť sa meniacemu sa prostrediu a vyvíja sa so zmenou prostredia. Údaje na základe ktorých sa učí sú aj mimo toho, čo sa predpokladalo pri zavedení systému.[5]

Ak sa na to pozrieme z inej perspektívy, automatizovaný systém vykonáva konkrétne úlohy s dobre pochopenými parametrami, ktoré sú známe vopred. Je navrhnutý tak, aby vykonával špecifickú funkciu opakovane a efektívne. Autonómny systém radí a pomáha definovať, aké je správne rozhodnutie alebo úkon pri vyvíjajúcom sa prostredí, ktoré nie je vopred určené.[6]

Konkrétnym príkladom automatizovaného systému sú kontroly súladu (*compliance*) na úrovni infraštruktúry a aplikácií v prostredí spoločnosti. Tieto systémy monitorujú dodržiavanie presne stanoveného súboru noriem súladu a informujú organizáciu, keď systémy nedosiahnu súlad. Tieto systémy môžu tiež vykonať dobre definované úkony na nápravu problému, to však neznamená, že sú autonómne. Výslovne sú nakonfigurované tak, aby podnikli konkrétne úkony, čo organizácii umožňuje dôveru v to, čo sa presne deje s ich prostredím. Tieto systémy často označujú problém, aby užívateľ alebo správca mohol problém vyriešiť. Ide o podpornú technológiu, pri ktorej pomáha človeku vykonávať jeho prácu a nenahrádza ho.[7]

Príkladom autonómneho systému je detekcia narušenia siete, hľadanie anomálií v inak normálnej sieťovej prevádzke. Autonómne systémy sa taktiež využívajú na hľadanie zero-day útokov pred ich vykonaním (*zero- day exploits*).[8] Ďalším príkladom aplikácie autonómneho systému je smart vy-

[5] MATTESON S. *Autonomous versus automated: What each means and why it matters*. [on-line]. Dostupné z: https://www.techrepublic.com/article/autonomous-versus-automated-what-each-means-and-why-it-matters/ [citované 28.9.2020].

[6] Tamže.

[7] Tamže.

[8] Tamže.

sávač Roomba. Jeho funkciou je čistenie podlahy, avšak na základe spätnej väzby z okolia sa rozhoduje, kde bude čistiť. Pri narážaní na objekty sa učí, ako sa im časom vyhnúť a zostaví mapu priestoru, ktorý čistí. Musí sa neustále učiť, pretože nábytok, predmety a domáce zvieratá menia prostredie, v ktorom pôsobí.[9]

Autonómne systémy nemožno stotožňovať len s algoritmom (softvérom).[10] Autonómne systémy nie sú naprogramované len k výkonu určitých činností, ale aj k tomu, aby sa určité činnosti naučili vykonávať sami. Inými slovami, podstata autonómnych systémov nie je len schopnosť autonómne existovať a fungovať, ale aj vytváranie svojho vlastného kódu (softvéru)[11] nezávisle od svojho autora.[12]

Typickým príkladom využitia autonómnych systémov sú autonómne vozidlá, a to najmä úrovne 3 a vyššie. Ako uvádza Polčák, autonómne vozidlá nemožno z pohľadu práva prirovnávať ku klasickým automobilom, a to najmä s ohľadom na skutočnosť, že autonómne vozidlá sa riadia sami.

---

[9] Tamže.

[10] Z právneho pohľadu možno softvér (počítačový program) chápať ako súbor príkazov a inštrukcií vyjadrených v akejkoľvek forme použitých priamo alebo nepriamo v počítači alebo v podobnom technickom zariadení a zároveň musí byť výsledkom tvorivej duševnej činnosti autora. Inými slovami, softvér predstavuje súbor inštrukcií a príkazov, ktoré sú vytvorené priamo alebo sprostredkovane autorom, čiže fyzickou osobou. Naprogramovaný systém má presne stanovené funkcionality a vykonáva to, na čo ho programátor predurčil.

[11] Konkrétnou aplikáciou autonómneho systému bol autonómny robot Tay spoločnosti Microsoft pre sociálnu sieť Twitter. Hlavnou úlohou robota Tay bolo vyhodnocovať obsah komunikácie a následne vytvárať populárne príspevky. Po určitom čase začal Tay vytvárať nenávistné príspevky, najmä kvôli nenávistnému obsahu na sociálnej sieti Twitter. Tay bol naprogramovaný na to, aby sa učil komunikovať, nie na to aby komunikoval. Za týmto účelom sa Tay sám programoval. Softvér, na základe ktorého Tay posielal svoje tweety si vytváral sám, a človek nebol schopný vykonávať úpravy v neustále meniacom sa kóde, ktorý Tay používal na učenie sa. Tay bol po dvoch neúspešných pokusoch o preprogramovanie vypnutý. Bližšie pozri: POLČÁK, R. *Odpovědnost umělé inteligence a informační útvary bez právní osobnosti.* In Bulletin Advokace 11/2018, s. 24. [on-line]. Dostupné z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2018/BA_11_2018_web.pdf. [citované 28.9.2020].

[12] POLČÁK, R. *Odpovědnost umělé inteligence a informační útvary bez právní osobnosti*. In Bulletin Advokace 11/2018, s. 24. [on-line]. Dostupné z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2018/BA_11_2018_web.pdf. [citované 28.9.2020].

V prípade autonómnych vozidiel by sa nemala používať analógia s automobilom, ale so softvérom, ktorý takýto systém riadi.[13]

V štandarde SAE J3016:Sep 2016: Taxonómia a definície pojmov súvisiacich so systémami automatizovaného riadenia pre cestné motorové vozidlá (ďalej len „SAE štandard"), sa rozlišuje medzi pojmami autonómny (*autonomous*) a automatizovaný (*automation*). Automatizácia predstavuje v zmysle SAE štandardu použitie elektronických alebo mechanických zariadení ako náhrada ľudskej práce. Automatizácia v kontexte jazdy je vhodný termín pre systémy, ktoré vykonávajú časť alebo všetky dynamické jazdné úlohy.[14] [15]

Výraz „autonómny" sa už dlho používa v komunitách výskumu týkajúceho sa robotiky a umelej inteligencie na označenie systémov, ktoré majú schopnosť a oprávnenie nezávisle a sebestačne rozhodovať. Postupom času sa toto použitie náhodne rozšírilo tak, aby zahŕňalo nielen rozhodovanie, ale predstavuje funkčnosť celého systému, čím sa stalo synonymom pre automatizáciu.

V jurisprudencii sa autonómia vzťahuje aj na schopnosť samo riadenia (*self-governance*). V tomto zmysle je „autonómny" tiež nesprávny názov, ktorý sa uplatňuje na automatizovanú technológiu jazdy, pretože ani tie najpokročilejšie systémy automatizovanej jazdy nie sú „samo riadiace". Systémy automatizovanej jazdy skôr fungujú na základe algoritmov a inak sa

---

[13] Tamže, s. 23 – 30.

[14] Dynamické jazdné úlohy (*dynamic driving task,* DDT) sú v zmysle bodu 3.13 SAE štandardu *„Všetky prevádzkové a taktické funkcie v reálnom čase potrebné na prevádzku vozidla v cestnej premávke, s výnimkou strategických funkcií, ako sú plánovanie ciest a výber cieľov a trasových bodov, zahŕňajúc bez obmedzenia:*

1.1.1 bočné riadenie pohybu vozidla pomocou riadenia (funkčné);

2.1.1 pozdĺžne riadenie pohybu vozidla pomocou zrýchlenia a spomalenia (funkčné);

3.1.1 monitorovanie jazdného prostredia prostredníctvom detekcie objektov, udalostí, rozpoznávania, klasifikácie a prípravy reakcií (operatívnych a taktických);

4.1.1 vykonanie reakcie na objekt a udalosť (operatívna a taktická);

5.1.1 plánovanie manévrov (taktické); a zvyšovanie viditeľnosti pomocou osvetlenia, signalizácie a gestikulovania atď. (Taktické)."

[15] Bod 7.1 SAE štandardu.

riadia príkazmi používateľov. Z tohto dôvodu SAE štandard nepoužíva pojem „autonómny“ na opis automatizácie jazdy.[16]

V závislosti od toho aké systémy sa využívajú pri jednotlivých úrovniach automatizácie, SAE štandard rozlišuje medzi systémom automatizovaného riadenia (*Driving automation system*) a systémom automatického riadenia (*Automated driving system*). Systém automatizácie riadenia (*Driving automation system*) predstavuje *„Hardvér a softvér, ktoré sú kolektívne schopné trvalo vykonávať časť alebo všetky dynamické jazdné úlohy; tento výraz sa všeobecne používa na opis každého systému, ktorý je schopný úrovne 1-5 automatizácie jazdy.“*[17]

Na rozdiel od tohto všeobecného pojmu pre akýkoľvek systém úrovne 1-5, je systém automatického riadenia (*Automated driving system*) špecifickým pojmom pre systém úrovne 3-5. Systém automatického riadenia je definovaný ako *„Hardvér a softvér, ktoré sú kolektívne schopné trvalo vykonávať všetky dynamické jazdné úlohy, bez ohľadu na to, či je obmedzená na konkrétnu doménu prevádzkového návrhu;*[18] *tento výraz sa používa špecificky na opis systému automatizácie riadenia na úrovni 3, 4 alebo 5.“*[19]

SAE štandard taktiež popisuje pojem samo jazdenie (*Self-driving*), ktorý sa týka situácií, keď nie je prítomný žiadny vodič alebo žiadny užívateľ nevykonáva dynamické jazdné úlohy, alebo situácií, keď systém automatizácie jazdy vykonáva akúkoľvek časť dynamických jazdných úloh.[20]

3. DEFINÍCIA POJMU AUTONÓMNE VOZIDLO

Autonómne vozidlá sú často chápané ako vozidlá bez vodiča, samo jazdiace a robotické vozidlá. Vo všeobecnosti, sa autonómne vozidlá dajú opísať ako *„počítačom riadené vozidlá, ktoré jazdia samy, spoliehajúc sa na množstvo*

[16] Bod 7.1.1 SAE štandardu.

[17] Bod 3.8 SAE štandardu.

[18] Prevádzková doména v zmysle bodu 3.22 SAE štandardu predstavuje: *„Prevádzkové podmienky, za ktorých je daný systém automatizácie riadenia alebo jeho vlastnosť osobitne navrhnutá tak, aby fungovala, okrem iného vrátane environmentálnych, geografických a denných obmedzení a/alebo požadovanej prítomnosti alebo neprítomnosti určitej premávky alebo charakteristiky vozovky.“*

[19] Bod 3.2 SAE štandardu.

[20] Bod 7.1.3 SAE štandardu.

zdrojov údajov, aby získali prístup k jazdnému prostrediu a riadili prevádzku vozidla.“[21]

Pokiaľ ide o vymedzenie pojmu autonómne vozidlo, neexistuje všeobecný konsenzus. Autonómne vozidlo je definované v právnych predpisoch prijatých v niektorých štátoch USA. Každý zo štátov s podrobnou legislatívou o autonómnych vozidlách má inú definíciu. Napríklad Nevada definuje autonómne vozidlá ako *„motorové vozidlo, ktoré je vybavené systémami automatického riadenia, ktoré je navrhnuté tak, aby fungovalo na úrovni automatizácie jazdy na úrovni 3, 4 alebo 5 podľa SAE J3016. Tento pojem zahŕňa plne autonómne vozidlo.*“[22] Plne autonómne vozidlo je definované ako „*vozidlo vybavené systémom automatického riadenia, ktorý je navrhnutý tak, aby fungoval na úrovni automatizácie riadenia na úrovni 4 alebo 5 podľa SAE J3016.“*[23] Nevada bola prvým štátom, ktorý povolil testovanie autonómnych vozidiel na verejných cestách.

Na úrovni členských štátov Európskej únie bola prijatá právna úprava týkajúca sa autonómnych vozidiel v Nemeckej spolkovej republike. Od 21. júla 2017 je účinná novela nemeckého zákona o cestnej premávke (Straßenverkehrsgesetz - StVG), ktorá upravuje problematiku motorových vozidiel s vysoko alebo plne automatizovanými jazdnými funkciami (*highly or fully automated driving functions*) na nemeckých verejných cestách.[24] Vozidlá s vysoko alebo plne automatizovanými jazdnými funkciami v zmysle

---

[21] COLLINGWOOD, L. *Privacy implications and liability issues of autonomous vehicles*. In Information & Communications Technology Law, roč. 26. č. 1, 2017, s. 32-45.

[22] Autonomous Vehicles. State of Nevada Register of Administrative Regulations. § 482A. [online]. Dostupné z: https://www.leg.state.nv.us/NRS/NRS-482A.html#NRS482ASec036. [citované 28.9.2020].

[23] Tamže, § 482A.036.

[24] [On-line]. Dostupné z: https://www.bmvi.de/EN/Topics/Digital-Matters/Automated-Connected-Driving/automated-and-connected-driving.html. [citované 28.9.2020]. Taktiež pozri CZARNECKI, K. *English Translation of the German Road Traffic Act Amendment Regulating the Use of “Motor Vehicles with Highly or Fully Automated Driving Function” from July 17, 2017* [On-line]. Dostupné z: https://www.researchgate.net/profile/Krzysztof_Czarnecki3/publication/320813344_English_Translation_of_the_German_Road_Traffic_Act_Amendment_Regulating_the_Use_of_Motor_Vehicles_with_Highly_or_Fully_Automated_Driving_Function_from_July_17_2017/links/59fbbe680f7e9b9968bb5a0f/English-Translation-of-the-German-Road-Traffic-Act-Amendment-Regulating-the-Use-of-Motor-Vehicles-with-Highly-or-Fully-Automated-Driving-Function-from-July-17-2017.pdf [citované 28.9.2020].

nemeckého zákona o cestnej premávke zodpovedajú úrovni 3 a úrovni 4 autonómnych vozidiel v zmysle taxonómie autonómnych vozidiel zavedených v štandarde SAE J3016:Sep 2016.

Motorové vozidlá s vysoko alebo plne automatizovanými jazdnými funkciami v zmysle nemeckého zákona o cestnej premávke sú vozidlá, ktoré majú technické vybavenie, ktoré:

1.1.1 „je schopné po aktivácii vykonať jazdnú úlohu - vrátane pozdĺžneho a priečneho riadenia - pre príslušné motorové vozidlo (kontrola vozidla),

2.1.1 je schopné dodržať dopravné predpisy vzťahujúce sa na jazdnú úlohu vozidla počas vysoko automatizovanej alebo plne automatizovanej jazdy,

3.1.1 vodič môže kedykoľvek manuálne prejsť na ručné ovládanie alebo ho manuálne deaktivovať,

4.1.1 je schopné rozpoznať potrebu manuálneho ovládania vozidla vodičom,

5.1.1 je schopné vizuálne, akusticky, hmatovo alebo inak zrozumiteľne informovať vodiča vozidla o požiadavke odovzdať vodičovi kontrolu nad vozidlom s dostatočnou časovou rezervou pred odovzdaním kontroly a

6.1.1 upozorňuje na použitie, ktoré je v rozpore s popisom systému.“[25]

Novela nemeckého zákona o cestnej premávke taktiež zaviedla povinné vybavenie vozidla s vysoko alebo plne automatizovanými jazdnými funkciami čiernou skrinkou. V prípade nehody čierna skrinka identifikuje, či vodič alebo systém ovládal vozidlo v danom momente, a preto objasňuje, či zodpovednosť nesie vodič alebo potenciálne výrobca.[26]

[25] § 1a ods. 2 nemeckého zákona o cestnej premávke.

[26] § 63a nemeckého zákona o cestnej premávke.

3.1 ÚROVNE AUTOMATIZÁCIE

Na pochopenie autonómnych vozidiel je potrebné v prvom rade pochopiť jednotlivé úrovne automatizácie.[27] Autonómne vozidlá sú klasifikované na základe úrovne automatizácie. Podľa SAE štandardu sú autonómne vozidlá rozdelené do šiestich úrovní, ktoré sa stupňujú. Tieto úrovne sa považujú skôr za opisné ako normatívne a viac technické, než právne. Vo všeobecnosti možno povedať, že úrovne SAE štandardu určujú predovšetkým to, ako je dynamická jazdná úloha rozdelená medzi človeka - vodiča a stroj. Na úrovni 0 (bez automatizácie) je vykonávaná výlučne ľudským vodičom a na úrovni 5 (úplná automatizácia) výlučne systémom automatického riadenia.[28]

1.1.1 Úroveň 0 (bez automatizácie). Ľudský vodič vykonáva všetky úlohy spojené s vedením vozidla.

2.1.1 Úroveň 1 (podpora vodiča). Ľudský vodič riadi vozidlo, ale niektoré jazdné úlohy riadi systém. Príklad: parkovací asistent alebo tempomat.

3.1.1 Úroveň 2 (čiastočná automatizácia). Systém alebo viac systémov dokáže ovládať riadenie a rýchlosť vozidla, zatiaľ čo vodič vozidla musí neustále sledovať dynamické jazdné úlohy a prostredie. Príklady: funkcia automatického parkovania, systém udržiavania jazdného pruhu, systémy núdzového brzdenia.

4.1.1 Úroveň 3 (podmienená automatizácia). Vozidlá úrovne 3 a vyššie sa považujú za vozidlá s autonómnymi jazdnými systémami. Vozidlo monitoruje jazdné prostredie prostredníctvom systémov automatického riadenia. Ľudský vodič nemusí monitorovať dynamické jazdné úlohy, ale musí byť schopný kedykoľvek a bez predchádzajúceho upozornenia prevziať kontrolu nad vozidlom. Vozidlo sa môže samo rozhodovať. Príklady: vozidlo môže pred se-

[27] Pre účely tohto článku používame pojem úrovne automatizácie. V SAE štandarde sa hovorí o úrovniach automatizácie riadenia (*levels of driving automation*) a nie o úrovniach autonómie.

[28] International Transport Forum and Corporate Partnership Board: *Autonomous Driving: Regulatory Issues*. 2015. [on-line]. Dostupné z: https://www.itf-oecd.org/sites/default/files/docs/15cpb_autonomousdriving.pdf. [citované 28.9.2020].

bou rozpoznať pomalšie sa pohybujúce vozidlo a môže sa rozhodnúť, či spomalí alebo ho predbehne. Príklad: diaľničný pilot.

5.1.1 Úroveň 4 (vysoká automatizácia). Za určitých podmienok (špecifické režimy jazdy) môže vozidlo vykonávať všetky jazdné úlohy. Ľudský vodič môže prevziať kontrolu nad vozidlom, najmä ak podmienky menia vopred definované prípady použitia (napr. práce na ceste, odklony od cesty alebo keď si to vodič vozidla želá). Príklad: mestská automatizovaná jazda.

6.1.1 Úroveň 5 je (úplná automatizácia). Ľudský vodič sa nevyžaduje. Systémy automatického riadenia zvládajú všetky aspekty jazdných úlohy bez toho, aby človek musel zasahovať. Vozidlo nevyžaduje žiadne pedále, volant. Systémy automatického riadenia robia nezávislé rozhodnutia. Vozidlo môže zvládnuť situácie, keď nastane nepredvídateľná udalosť alebo sa zmení fyzické prostredie. Príklad: úplná cesta z bodu A do bodu B.[29]

Šesťstupňová škála SAE bola prijatá rôznymi národnými a medzinárodnými orgánmi, ako je napríklad National Highway Traffic Safety Administration v USA (NHTSA), Society of Motor Manufacturers and Traders Australia's National Transport Commission (NTC), the UK's Department for Transport (DfT) a European Road Transport Research Advisory Council (ERTRAC).[30]

3.2 PREPOJENÉ VOZIDLÁ

Aby došlo k úplnému využitiu potenciálu autonómnych vozidiel, je potrebné aby tieto vozidlá komunikovali s inými vozidlami, resp. s inými objektmi. V tomto zmysle možno autonómne vozidlá chápať ako prepojené

[29] YEEFEN LIM, H. *Autonomous Vehicles and the Law Technology, Algorithms and Ethics.* Edward Elgar Publishing, 2018, s. 4-5. SKEETE, JP. Level 5 autonomy: *The new face of disruption in road transport.* In Technological Forecasting and Social Change, Elsevier, roč. 134(C), 2018, s. 22-34.

[30] TAEIHAGH, A. and SI MIN LIM, H. *Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks.* Transport Reviews, roč. 39. č.1, 2019, s. 103-128.

vozidlá (*connected vehicles*). Takéto vozidlo integruje prepojenie s autonómiou, čo sú odlišné, ale súvisiace technológie.

Autor Jean-Pauil Skeete objasňuje, že *„plné výhody autonómie možno dosiahnuť iba vtedy, keď vozidlo dokáže rozpoznať aj iné vozidlá (V2V) a jeho fyzické prostredie (vehicle to infrastructure, V2I).“*[31]

Autor Kouroutakis okrem toho tvrdí, že vozidlo komunikuje aj s inými zariadeniami, ako sú smartfóny, tablety, inteligentné hodinky, osobné počítače (*vehicle to device*, *V2D*).[32]

Podľa Inštitútu inžinierstva a technológie možno považovať prepojené vozidlá za vozidlá cestnej premávky, ktoré sú vybavené troma druhmi komunikačných systémov. V prvom prípade ide o internetový prístup a zvyčajne vnútornú sieť, častokrát bezdrôtovú, ktorá umožňuje pripojenie na zariadenia vo vnútri vo vozidle alebo aj mimo vozidla (známe ako *vehicle to Internet*, V2I).[33]

Ďalším druhom komunikačných systémov sú technológie *vehicle to vehicle* (V2V), ktoré umožňujú vozidlám komunikovať navzájom.[34]

Autonómne vozidlá sa taktiež môžu stať súčasťou komunikácie v rámci internetu vecí (*vehicle to IoT*, V2IoT) ako pripojená entita, ktorá prijíma údaje z externého zdroja a zdieľa údaje, ktoré zaznamenáva so vzdialenou treťou stranou pre rôzne účely.[35] Nakoľko ide o výmenu informácií medzi rôznymi zariadeniami a stranami, otázky týkajúce sa kybernetickej bezpečnosti a ochrany osobných údajov sú viac ako na mieste.[36]

---

[31] SKEETE, JP: *Level 5 autonomy: The new face of disruption in road transport.* In Technological Forecasting and Social Change, Elsevier, vol. 134(C), 2018, s. 22-34.

[32] KOUROUTAKIS, A. E.: *Autonomous Vehicles; Regulatory Challenges and the Response From UK and Germany*. 46 Mitchell Hamline Law Review forthcoming. 2019.

[33] The institution of Engineering and Technology: *Automotive Cyber Security. An IET/KTN Thought Leadership Review of risk perspectives for connected vehicles*, s. 7. [on-line]. Dostupné z: https://www.theiet.org/media/2309/iet-automotive-cyber-security-tlr-lr-1.pdf. [citované 28.9.2020].

[34] Tamže.

[35] Tamže.

4. PRÁVNA ÚPRAVA[37]

V nasledujúcej časti príspevku budeme analyzovať právne predpisy na úrovni práva EÚ, ktoré upravujú problematiku autonómnych vozidiel, a to najmä z pohľadu kybernetickej bezpečnosti a ochrany osobných údajov. Konkrétne budeme skúmať, či právna úprava už v procese typového schvaľovania vozidiel kladie požiadavky na bezpečnosť automatizovaných, resp. autonómnych systémov, tak aby v rámci komunikácie s inými entitami boli dostatočne zabezpečené a aby nedochádzalo k narušeniu integrity, dôvernosti a dostupnosti informácií. Taktiež sa budeme venovať otázke či legislatíva, ktorá upravuje cestnú infraštruktúru napr. v podobe inteligentného dopravného značenia, upravuje problematiku ochrany osobných údajov a kybernetickej bezpečnosti v rámci komunikácie s vozidlami.

4.1 TYPOVÉ SCHVÁLENIE MOTOROVÝCH VOZIDIEL

Pred samotným uvedením vozidiel na trh, tak aby ich bolo možné používať na verejných komunikáciách, musí byť vozidlo typovo schválené v súlade s administratívnymi postupmi a technickými požiadavkami. Právna úprava, ktorá by explicitne upravovala typové schválenie autonómnych vozidiel neexistuje, avšak súčasné právne predpisy EÚ za určitých podmienok dovoľujú zavedenie autonómnych vozidiel na trh.

Problematika schvaľovania motorových vozidiel, ako aj systémov pre takéto vozidlá je upravená na úrovni práva EÚ nariadením Európskeho parla-

[36] Prepojené vozidlá v súčasnosti najčastejšie komunikujú na základe technologických riešení založených na senzoroch alebo založených na prepojení. V prvom prípade ide najmä o stereo kamery, RADAR (*radio detection and ranging*), LIDAR (*light detection and ranging*) a pod. V druhom prípade ide o komunikačné technológie s krátkym dosahom, ktoré pracujú vo vyhradenom frekvenčnom pásme 5,9 GHz alebo technológie s dlhším dosahom ako mobilné siete 3G, 4G či 5G.

[37] Na úrovni EÚ bolo prijatých niekoľko nezáväzných dokumentov, ktoré sa týkajú regulácie umelej inteligencie a výslovne spomínajú v rôznych kontextoch autonómne vozidlá. Príkladom je *White Paper on Artificial Intelligence: a European approach to excellence and trust*. V zmysle tohto dokumentu technológie umelej inteligencie môžu pre používateľov predstavovať nové bezpečnostné riziká, v prípade ak sú zabudované do výrobkov a služieb. Ako príklad sa uvádza autonómne vozidlo, ktoré v dôsledku chyby v technológii rozpoznávania objektov môže nesprávne identifikovať predmet na ceste a spôsobiť nehodu, ktorá má za následok zranenia a materiálne škody.

mentu a Rady (EÚ) 2018/858 z 30. mája 2018 o schvaľovaní motorových vozidiel a ich prípojných vozidiel, ako aj systémov, komponentov a samostatných technických jednotiek určených pre takéto vozidlá a o dohľade nad trhom s nimi, ktorým sa menia nariadenia (ES) č. 715/2007 a (ES) č. 595/2009 a zrušuje smernica 2007/46/ES (ďalej len „nariadenie o typovom schválení vozidiel“). Predmetné nariadenie sa uplatňuje od 1. septembra 2020.

Technológie, ktoré nie sú upravené v nariadení o typovom schválení vozidiel, ako napríklad systém automatického riadenia je možné schváliť prostredníctvom postupu výnimiek, ktoré sú upravené v predmetnom nariadení v čl. 39, ktorý upravuje výnimky pre nové technológie alebo nové koncepcie. V takýchto prípadoch sa schválenie udeľuje na základe vnútroštátneho *ad hoc* posúdenia bezpečnosti, pričom je potrebné povolenie zo strany Komisie. Komisia prijme vykonávacie akty, ktorými rozhodne o udelení povolenia. Vnútroštátny schvaľovací orgán môže do prijatia vykonávacích aktov udeliť predbežné typové schválenie EÚ pre typ vozidla, na ktorý sa vzťahuje požadovaná výnimka. Predbežné povolenie bude platné len na území členského štátu daného schvaľovacieho orgánu, avšak schvaľovacie orgány ostatných členských štátov môžu akceptovať predbežné typové schválenie EÚ na svojom území za predpokladu, že o tom písomne informujú schvaľovací orgán, ktorý predbežné typové schválenie EÚ udelil.[38]

Nariadenie o typovom schválení vozidiel špecificky neupravuje problematiku ochrany osobných údajov či kybernetickej bezpečnosti. V zmysle recitálu 62 predmetného nariadenia sa považuje za dôležité, aby výrobcovia vykonávali všetky opatrenia potrebné na zabezpečenie súladu s pravidlami týkajúcimi sa spracúvania a prenosu osobných údajov, ktoré vznikajú pri používaní vozidla. Pri používaní autonómnych a prepojených vozidiel, kde sú využívané rôzne systémy automatického riadenia či komunikačné systémy dochádza k spracúvaniu a prenosu osobných údajov.

Nakoľko existovali rôzne prístupy pri aplikovaní výnimiek pre nové technológie alebo nové koncepcie, Komisia vydala 12. februára 2019

[38] Čl. 39 nariadenia o typovom schválení vozidla.

Usmernenia týkajúce sa výnimky na schválenie automatizovaných vozidiel EÚ (ďalej len „usmernenia“).[39] Cieľom týchto usmernení je zosúladiť postup členských štátov pri vnútroštátnom *ad hoc* hodnotení automatizovaných vozidiel a zjednodušiť vzájomné uznávanie tohto hodnotenia, ako aj zabezpečiť spravodlivú hospodársku súťaž a transparentnosť. Pokyny sa zameriavajú na automatizované vozidlá, ktoré môžu riadiť samy seba v obmedzenom počte jazdných situácií na úrovni automatizácie 3 a 4 podľa SAE štandardu.[40]

Usmernenie sa oblasti ochrany osobných údajov a kybernetickej bezpečnosti venuje najmä v dvoch častiach. Prvou časťou sú usmernenia o inštalácii nahrávacích zariadení (*event data recorders*). V zmysle usmernení č. 23-27 by automatizované vozidlá mali byť vybavené palubným zariadením, ktoré zaznamenáva prevádzkový stav systému automatického riadenia a stav vodiča s cieľom určiť, kto šoféroval počas nehody. Tieto zhromaždené údaje umožňujú určiť zodpovednosť v prípade nehody a umožňujú posúdiť, či vodič alebo vozidlo správne zareagovali na situáciu. Medzi tieto údaje možno považovať napr. prevádzkový stav systému automatického riadenia, stav vodiča, informácie o okolí, kontrolné informácie o vozidle. Palubné zariadenie musí byť schopné uchovávať údaje zabezpečeným spôsobom, dodržiavať právne predpisy EÚ o ochrane údajov a byť chránené pred manipuláciou, pričom by mal byť umožnený prístup k takým to údajom vnútroštátnym orgánom. Na základe získaných skúseností môžu byť vyvinuté konkrétnejšie požiadavky na zariadenia na záznam údajov (čas záznamu, čas uchovávania, na aké účely sa údaje používajú, štandardizovaný prístup, spôsob zaobchádzania s osobnými údajmi atď.).[41]

Výrobca vozidla je v zmysle usmernení povinný poskytnúť nasledovné informácie:

1 typ uložených údajov,
2 miesto uloženia,
3 trvanie uloženia,

[39] V názve a texte usmernenia sa používa pojem automatizované vozidlo (*automated vehicle*).

[40] Usmernenie, s. 1.

[41] Usmernenie, s. 5.

4 prostriedky na zabezpečenie bezpečnosti a ochrany údajov,

5 prístup k údajom.[42]

V časti o kybernetickej bezpečnosti je v usmerneniach vyjadrená požiadavka, aby vozidlo bolo skonštruované tak, aby chránilo vozidlo pred automatizovaným hacknutím pomocou najmodernejších techník a bolo v súlade s právnymi predpismi EÚ o ochrane údajov. Patrí sem napr. hodnotenie rizika výrobcom, návrhové opatrenia a primerané procesy na zabránenie, zmiernenie a reakciu na kybernetické útoky.

Výrobcovia vozidiel taktiež majú prijať opatrenia, ako napríklad tie, ktoré súvisia s aktualizáciou softvéru atď. nainštalovaného v automatizovaných vozidlách, ktoré sú potrebné na zabezpečenie prevádzkovej kybernetickej bezpečnosti počas celej jej životnosti.[43]

4.2 INTELIGENTNÉ DOPRAVNÉ SYSTÉMY

Jedným z praktických príkladov, kedy vozidlo môže komunikovať s IoT, resp. infraštruktúrou sú inteligentné dopravné systémy. Príklady aplikácie inteligentných dopravných systémov v cestnej doprave zahŕňajú riadenie a kontrolné systémy mestskej a diaľničnej premávky, elektronický výber mýta, navigáciu trasy a pod. Problematiku zavádzania inteligentných dopravných systémov upravuje smernica Európskeho parlamentu a Rady 2010/40/EÚ o rámci na zavedenie inteligentných dopravných systémov v oblasti cestnej dopravy a na rozhrania s inými druhmi dopravy (ďalej len „smernica o inteligentných dopravných systémoch“).

Vysoká úroveň bezpečnosti systémov inteligentného značenia má v súvislosti s autonómnymi vozidlami dôležitú úlohu, nakoľko autonómne a prepojené vozidlá pre svoje fungovanie komunikujú s rôznymi inteligentnými dopravnými systémami, kedy dochádza k prijímaniu údajov z externého zdroja, ale aj zdieľaniu údajov, ktoré zaznamenáva so vzdialenou treťou stranou pre rôzne účely.

V mnohých prípadoch bude zavádzanie a využívanie aplikácií a služieb inteligentných dopravných systémov zahŕňať aj spracovanie osobných

[42] Usmernenie, s. 9.

[43] Usmernenie, s. 5.

údajov. Problematika ochrany osobných údajov a bezpečnosti je špecificky upravená v čl. 10, v zmysle ktorého je potrebné, aby sa spracovanie osobných údajov realizovalo jednak v súlade s GDPR, ale aj smernicou o súkromí a elektronických komunikáciách.[44] Taktiež sa od členských štátov požaduje, aby boli osobné údaje chránené pred zneužitím vrátane nezákonného prístupu, zmeny alebo straty.

Pri používaní aplikácií inteligentných dopravných systémov by sa mali uplatňovať zásady obmedzenia účelu a minimalizácie údajov a taktiež by sa mala podporovať anonymizácia ako jedna zo zásad zvyšovania ochrany súkromia jednotlivcov.[45]

Z pohľadu komunikácie medzi vozidlami a cestnou infraštruktúrou zohrávajú dôležitú úlohu kooperatívne inteligentné dopravné systémy. Tieto systémy využívajú technológie, ktoré umožňujú cestným vozidlám komunikovať medzi sebou a s cestnou infraštruktúrou vrátane dopravnej signalizácie. Komisia v marci 2019 prijala Delegované nariadenie komisie ktorým sa dopĺňa smernica o inteligentných dopravných systémoch, pokiaľ ide o zavádzanie a prevádzkové využívanie kooperatívnych inteligentných dopravných systémov (ďalej len „delegované nariadenie“).

V cestnej doprave kooperatívne inteligentné dopravné systémy zvyčajne zahŕňajú komunikáciu medzi vozidlami navzájom (V2V), medzi vozidlom a infraštruktúrou (V2I) alebo medzi infraštruktúrami navzájom (I2I) a komunikáciu medzi vozidlami a chodcami alebo cyklistami (Vehicle-to-Everything, V2X).[46]

Služby ktoré sú poskytované prostredníctvom kooperatívnych inteligentných dopravných systémov sú buď založené na otvorenej sieti umožňujúcej komunikáciu medzi stanicami kooperatívnych inteligentných dopravných systémov (ďalej len „stanice KIDS“) spôsobom „všetci všetkým“ (*many-to-many*) alebo na základe rovnocennosti (*peer-to-peer*). Tento prístup znamená, že všetky stanice KIDS si môžu navzájom bezpečne vymieňať

[44] Smernica Európskeho parlamentu a Rady2002/58/ES z 12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách).

[45] Čl. 10 smernice o inteligentných dopravných systémoch.

[46] Delegované nariadenie, s. 1.

správy a nie sú odkázané na výmenu správ len s (jednou) vopred stanovenou stanicou, resp. stanicami.[47]

Stanica KIDS je zostava hardvérových a softvérových komponentov potrebných na zber, uchovávanie, spracovanie, prijímanie a prenos zabezpečených a dôveryhodných správ s cieľom umožniť poskytovanie služby kooperatívnych inteligentných dopravných systémov. V zmysle delegovaného nariadenia sa stanice KIDS namontované vo vozidlách, prenosné alebo namontované popri cestnej infraštruktúre považujú za výrobky, ktoré možno uviesť na trh ako samostatné sústavy alebo ako súčasti väčších zostáv.[48]

V zmysle bodu 25 a 26 preambuly delegovaného nariadenia by sa informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby mali spracúvať za prísneho dodržiavania zásady minimalizácie údajov, len na účely špecifikované v delegovanom nariadení. Taktiež by sa mali ukladať len tak dlho, ako je to potrebné. Bezpečnostné požiadavky na pseudonymizáciu, ktoré sú stanovené v delegovanom nariadení, prispievajú k zníženiu rizika zneužitia údajov. Koncoví používatelia by mali byť jasne a komplexne informovaní o všetkých relevantných informáciách týkajúcich sa spracúvania ich osobných údajov v súlade s GDPR.

Delegované nariadenie sa detailne venuje problematike bezpečnosti v kapitole V, ktorá upravuje bezpečnosť staníc KIDS. Zavádza sa systém EÚ na správu bezpečnostných poverení koordinovaných inteligentných dopravných systémov, ktorý musí spĺňať požiadavky na certifikačnú politiku (príloha III) a bezpečnostnú politiku (príloha IV), v ktorej sa stanovujú požiadavky na riadenie informačnej bezpečnosti v koordinovaných inteligentných dopravných systémoch.[49]

Každý prevádzkovateľ stanice KIDS musí prevádzkovať systém riadenia informačnej bezpečnosti v súlade s normou ISO/IEC 27001 a dodatočnými

[47] Bod 2 preambuly delegovaného nariadenia.

[48] Bod 15 preambuly delegovaného nariadenia.

[49] Čl. 23 delegovaného nariadenia.

požiadavkami uvedenými v bode 1.3.1 prílohy IV delegovaného nariadenia.[50]

V súvislosti so stanicami KIDS si je potrebné uvedomiť, že aj v prípade komunikácie V2I vždy pôjde o výmenu správ medzi jednotlivými stanicami KIDS. Preto, aby vozidlo mohlo komunikovať s inými stanicami KIDS je potrebné, aby takáto stanica bola na vozidle namontovaná.

4.3 KYBERNETICKÁ BEZPEČNOSŤ

Bezpečnosť inteligentných dopravných systémoch upravuje taktiež smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (ďalej len „smernica NIS“). V zmysle smernice sa kybernetická bezpečnosť týka ochrany sietí a informačných systémov, prostredníctvom ktorých sa poskytujú základné služby vo vybraných odvetviach (energetika, bankovníctvo, doprava, zdravotníctvo a pod.), ako aj digitálne služby (online trhovisko, internetový vyhľadávač a služby cloud computingu). V prípade základných služieb ide o služby, ktoré majú zásadný význam z pohľadu zachovania spoločenských a hospodárskych činností.

Prevádzkovatelia inteligentných dopravných systémov v postavení prevádzkovateľov základných služieb sú povinní plniť povinnosti týkajúce sa bezpečnostných opatrení a oznamovania incidentov v zmysle smernice NIS. Uplatňovanie smernice NIS a požiadaviek uložených podľa delegovaného nariadenia sa môže v určitých prípadoch navzájom dopĺňať.

Napriek skutočnosti, že výrobcovia autonómnych vozidiel nie sú v súčasnosti zaradení do jedného z odvetví v zmysle smernice NIS, je možné, že v budúcnosti môže byť v odvetví doprava pridané pododvetvie, ktoré sa bude týkať výrobcov vozidiel, ktoré disponujú systémami automatického riadenia alebo autonómnymi systémami, resp. dodávateľov takýchto systémov. Výrobcovia vozidiel, resp. dodávatelia systémov by v pozícii prevádzkovateľov základných služieb museli spĺňať povinnosti týkajúce sa bezpečnostných opatrení a oznamovania incidentov v zmysle smernice NIS.

[50] Čl. 27 delegovaného nariadenia.

Ďalším legislatívnym aktov z oblasti kybernetickej bezpečnosti, ktorý bol prijatý na úrovni Európskej únie je nariadenie Európskeho parlamentu a Rady o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií (ďalej len „akt o kybernetickej bezpečnosti“), ktorý okrem iného vytvára systém certifikácie v oblasti kybernetickej bezpečnosti, ktorý by mal zabezpečiť dostatočnú úroveň kybernetickej bezpečnosti IKT produktov, postupov a služieb v Európskej únii.

Certifikácia IKT v oblasti kybernetickej bezpečnosti sa stáva veľmi dôležitou otázkou, a to najmä vo vzťahu k zvýšenému používaniu technológií, ktoré požadujú vysokú úroveň kybernetickej bezpečnosti. K odvetviam ako prepojené a autonómne vozidlá, elektronické zdravotnícke pomôcky, riadiace systémy priemyselnej automatizácie a inteligentné siete, kde sa bežne využíva certifikácia, by sa mali v blízkej budúcnosti pridať ďalšie odvetvia.[51]

Certifikát osvedčí, že výrobky a služby IKT, ktoré boli certifikované v súlade s takýmto systémom, spĺňajú stanovené požiadavky na kybernetickú bezpečnosť. Výsledný certifikát bude uznávaný vo všetkých členských štátoch, čo uľahčí podnikom cezhraničné obchodovanie a zákazníkom pochopiť bezpečnostné prvky produktu alebo služby.[52]

Využitie certifikácie kybernetickej bezpečnosti je dobrovoľné, pokiaľ sa to nestanovuje inak v právnych predpisoch Európskej únie alebo vnútroštátnych právnych predpisoch, ktorými sa stanovujú bezpečnostné požiadavky týkajúce sa produktov a služieb IKT. Postupy certifikácie kybernetickej bezpečnosti produktov a služieb IKT, na ktoré sa vzťahuje európsky systém certifikácie kybernetickej bezpečnosti, by mali stratiť účinky od dátumu, ktorý stanoví Komisia vo vykonávacom akte. Okrem toho by členské štáty nemali zavádzať nové vnútroštátne systémy certifikácie kybernetickej

[51] Bod 65 recitálu aktu o kybernetickej bezpečnosti.

[52] Bližšie k systému certifikácie v oblasti kybernetickej bezpečnosti pozri: VOSTOUPAL, J.: *Certifikace kyberbezpečnostních technologií. In* Revue pro právo a technologie. 2019, č. 20, s. 147-268. [on-line]. Dostupné z: https://journals.muni.cz/revue/article/view/12570 [citované 28.9.2020].

bezpečnosti v prípade produktov a služieb IKT, pre ktoré už existuje európsky systém certifikácie kybernetickej bezpečnosti.[53]

5. OCHRANA OSOBNÝCH ÚDAJOV

V tejto časti príspevku sa zameriame na klasifikáciu rôznych aktérov toku údajov na základe modelových situácií uvedených vyššie. V prvom rade považujeme za vhodné uviesť niekoľko poznámok ku osobnej pôsobnosti GDPR a distribúcií zodpovednosti za spracúvanie osobných údajov. Následne stručne charakterizujeme usmernenie Výboru na ochranu údajov (ďalej len „EDPB"), ktoré sa týka spracúvania osobných údajov aj v autonómnych vozidlách.[54]

V poslednej časti aplikujeme relevantný právny rámec na modelové situácie načrtnuté v predchádzajúcich častiach článku a poukážeme na možné aplikačné problémy v kontexte osobnej pôsobnosti GDPR.

5.1 GDPR A OSOBNÁ PÔSOBNOSŤ

Všeobecné nariadenia na ochranu údajov[55] (ďalej len „GDPR") síce neobsahuje výslovne vymedzené ustanovenie s názvom „osobná pôsobnosť," avšak v rámci právneho textu definuje a upravuje rôzne povinnosti súvisiace s aktérmi spracúvania osobných údajov. Ak určitá entita spĺňa požiadavky materiálnej[56] a teritoriálnej pôsobnosti[57] GDPR, je vhodné pristúpiť ku skúmaniu, v akej pozícií sa vlastne nachádza. V tomto kontexte GDPR definuje dvoch kľúčových aktérov spracúvania osobných údajov – prevádzkovateľa (*controller)* a sprostredkovateľa (*processor)* osobných údajov.

[53] Bod 69 recitálu aktu o kybernetickej bezpečnosti.

[54] European Data Protection Board Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications.[Online]. 2020. [cit. 29. 9. 2020] Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en.

[55] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov). In EUR-lex [právní informační system]. Úřad pro publikace Evropské unie. Dostupné z https://eur-lex.europa.eu/legal-content/SK/TXT/?qid=1584526623550&uri=CELEX%3A32016R0679

[56] Článok 2, GDPR.

[57] Článok 3, GDPR.

Správne definovanie entity je osobitne dôležité s ohľadom na distribúciu zodpovednosti za súlad s legislatívnymi požiadavkami na spracúvanie osobných údajov.

5.1.1 POJEM PREVÁDZKOVATEĽ

Prevádzkovateľ je v GDPR legálne definovaný ako *„fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý sám alebo spoločne s inými určí účely a prostriedky spracúvania osobných údajov.“*[58] EDPB vydal nedávno usmernenie[59] k pojmom prevádzkovateľ a sprostredkovateľ.[60] Dané usmernenie implicitne rešpektuje aj novšia judikatúra Súdneho dvora Európskej únie (ďalej len „SDEÚ“) k výkladu daného pojmu.[61]

EDPB vymedzuje päť osobitných prvkov definície prevádzkovateľa: (i) fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt; (ii) ktorý sám alebo spoločne s inými; (iii) určí; (iv) účely a prostriedky; (v) spracúvania osobných údajov.[62] Najdôležitejšie prvky danej definície analyzujeme nižšie.

Prvým aspektom definície je určenie entity, ktorá osobné údaje spracúva. WP29 zvýrazňuje, že v tomto kontexte je potrebné skúmať zaužívané inštitúty súkromného a verejného práva, ktoré by nás mali nasmerovať k fi-

---

[58] Článok 4 (7), GDPR.

[59] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.

[60] Článok 2 d) obsahuje definíciu prevádzkovateľa v tomto znení: *"kontrolór" znamená fyzickú alebo právnickú osobu, verejný orgán, agentúru alebo akýkoľvek iný orgán, ktorý sám, alebo v spojení s inými, určí účely a prostriedky spracovania osobných údajov; tam, kde sú účely a prostriedky spracovania stanovené vnútroštátnymi zákonmi a nariadeniami, alebo zákonmi a nariadeniami spoločenstva, ten, kto spracovanie riadi, alebo konkrétne kritéria pre jeho menovanie, môžu byť navrhnuté na základe vnútroštátneho práva alebo práva spoločenstva“*

[61] Pozri napr. Rozsudok Súdneho dvora zo dňa 5. júna 2018 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein proti Wirtschaftsakademie Schleswig-Holstein GmbH. Vec č. C-210/16.

[62] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z:https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en. S. 9.

nálnemu určeniu konkrétnej entity. Za prevádzkovateľa by mala byť považovaná spoločnosť alebo orgán, nie špecifická osoba v rámci ich štruktúr.[63] SDEÚ v prípade *Google Spain* uviedol, že *„založenie takejto inštitúcie na území členského štátu predpokladá účinné a skutočné vykonávanie činnosti prostredníctvom stabilných dohôd [prostredníctvom stálej prevádzkarne – neoficiálny preklad]“ a že „právna forma takejto inštitúcie, či je to pobočka, alebo dcérska spoločnosť s právnou subjektivitou, nie je určujúcim činiteľom.“*[64] Túto požiadavku v súčasnosti odzrkadľuje Recitál 22 GDPR.[65]

Druhý aspekt reflektuje, či subjektov, ktoré možno považovať za prevádzkovateľov je viacero alebo je len jeden. Tejto problematike sa osobitne venujeme v časti „spoloční prevádzkovatelia“ nižšie.

Najdôležitejším aspektom definície je určenie účelov a prostriedkov spracúvania osobných údajov. EDPB predmetný aspekt diferencuje na problematiku „určenia“ a „účelov a prostriedkov“ spracúvania osobných údajov.

Určenie účelov je potrebné vnímať v kontexte inštitútu prevádzkovateľa, ktorý je dynamický a funkčný, čo v praxi znamená posudzovanie faktických okolností a nie iba formálneho splnenie niekoľkých kritérií.[66] Požiadavka „určenia“ účelov a prostriedkov spracúvania osobných údajov môže vyplávať z troch legitímnych zdrojov. EDPB konkrétne uvádza (i) explicitnú požiadavku ustanovenú právom, (ii) implicitnú požiadavku ustanovenej právom alebo (iii) faktického vplyvu.[67] Pri explicitnej požiadavke upravenej

---

[63] Tamže, s. 10.

[64] Rozsudok Súdneho dvora zo dňa 13. mája 2014 Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mariovi Costejovi Gonzálezovi. Vec č. C-131/12.

[65] Recitál 22, GDPR: *„Každé spracúvanie osobných údajov v kontexte činností prevádzkarne prevádzkovateľa alebo sprostredkovateľa v Únii by sa malo vykonávať v súlade s týmto nariadením bez ohľadu na to, či sa samotné spracúvanie uskutočňuje v Únii. Prevádzkareň znamená efektívny a skutočný výkon činnosti prostredníctvom stálych dojednaní. Právna forma takýchto dojednaní, či už ide o pobočku alebo dcérsku spoločnosť s právnou subjektivitou, nie je v tomto ohľade určujúcim faktorom.“*

[66] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z:https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en. S. 10 - 11.

[67] Tamže.

v právnom poriadku pôjde zväčša o situácie, keď právna norma obsahuje obligáciu zbierať a spracúvať osobné údaje.[68] Implicitná požiadavka na spracúvania osobných údajov spočíva v prirodzenom súvise medzi určitou entitou a spracúvaním osobných údajov, čo je osobitne dôležité v prípadoch, keď právny predpis priamu obligáciu neobsahuje, ale je nepriamo vyplýva zo znenia legislatívneho textu.[69] Tretím zdrojom postavenia prevádzkovateľa môžu byť faktický vplyv a okolnosti daného spracúvania osobných údajov. V tomto kontexte EDPB uvádza zmluvné podmienky ako faktor, ktorý je potrebné brať do úvahy, avšak nie absolútne, nakoľko rozhodujúci je reálny stav a nie ustanovenia v zmluve. Ďalšie faktory, ktoré je možné posudzovať sú stupeň kontroly v rámci spracovateľských operácii, „image" vytvorený voči dotknutým osobám či primerané očakávaní dotknutých subjektov.[70] Subjekt, ktorý má nulový faktický alebo právny vplyv na určenie účelov a prostriedkov spracovania osobných údajov nemôže byť považovaný za prevádzkovateľa.

Určenie účelu spracovania je výsadou prevádzkovateľa. Účel možno zjednodušene vymedziť ako cieľ spracovateľskej operácie. Určenie účelov a prostriedkov spracúvania teda reflektuje „prečo" a „ako" budú osobné údaje spracúvané. Esenciou pri analýze daného faktora je úroveň detailov pri predmetnom determinovaní.[71] Prostriedky spracúvania osobných údajov zahŕňajú technické a organizačné aspekty spracúvania osobných údajov. Môže ísť aj o určenie toho, aké údaje sa budú spracúvať, aké tretie strany

---

[68] Ako príklad zo slovenského právneho poriadku možno uviesť postavenie advokátov v zmysle § 18 ods. 6 zákona č. 586/2003 Z. z. o advokácii a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov: *„Advokát spracúva osobné údaje klientov a iných fyzických osôb v rozsahu nevyhnutnom na účely výkonu advokácie v súlade s týmto zákonom a s osobitným predpisom. Advokát má pri spracúvaní osobných údajov v zmysle prvej vety tohto odseku postavenie prevádzkovateľa podľa osobitného predpisu."*

[69] Ako príklad možno uviesť spracúvanie osobných údajov zamestnávateľom v zmysle zákona č. 311/2001 Z. z. Zákonníka práce.

[70] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z:https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en. S. 12.

[71] Tamže, s. 13.

budú mať k údajom prístup či určenie dôb uchovávania.[72] Prostriedky spracúvania osobných údajov a ich určenie môže byť delegované na sprostredkovateľov, ak hovoríme o organizačných a technických otázkach (software, hardware).

Problematiku (spoločného) vymedzenia účelu ilustruje známy prípad vo veci SWIFT. Spoločnosť SWIFT figurovala ako sprostredkovateľ pri spracúvaní osobných údajov európskych bankových inštitúcií. Zároveň ale bez príkazu európskych bánk sprístupňovala údaje o dotknutých osobách v Európe Ministerstvu financií v Spojených štátoch amerických.

WP29 (Article 29 Data Protection Working Party, predchodca EDPB) vo svojom názore[73] vyslovila záver, že spoločnosť SWIFT na seba delegovala právomoci prevádzkovateľa (poskytnutím údajov o dotknutých osobách) a stala sa tak spoločným prevádzkovateľom spolu s bankovými inštitúciami, ktoré na druhej strane značne zanedbali dohľad nad aktivitami svojho sprostredkovateľa.

5.1.2 POJEM SPOLOČNÍ PREVÁDZKOVATELIA

Ak dvaja alebo viacerí prevádzkovatelia spoločne určia účely a prostriedky spracúvania, sú spoločnými prevádzkovateľmi.[74] S inštitútom spoločných prevádzkovateľov rátala už síce Smernica 95/46/ES v intenciách usmernenia WP29, avšak výslovne zakotvenie daného inštitútu upravuje až GDPR. Nie je dôležitá úroveň prepojenia spoločných prevádzkovateľov (od spoločného zdieľania výkonu všetkých spracovateľských operácii až po zdieľanie výkonu len jednej spracovateľskej operácie).[75] Typickým príkladom spoločných prevádzkovateľov je vedenie databázy dlžníkov viacerými

---

[72] Tamže, s. 13 - 14.

[73] Article 29 Data Protection Working Party Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). 2006. [cit. 29. 9. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf.

[74] Článok 26 ods. 1, GDPR.

[75] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z:https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en. S. 17 a nasl.

entitami napr. vo finančnom sektore. Na tomto mieste je ale potrebné upozorniť na rozdiel medzi spoločnými prevádzkovateľmi a prenosom osobných údajov (napr. cestovná agentúra, ktorá pošle dáta svojich zákazníkom leteckej spoločnosti a hotelovému zariadeniu). Iná by bola situácia, ak by cestovná agentúra, hotel a letecká spoločnosť založila spoločnú databázu manažmentu rezervácii. V takomto prípade by sa jednalo o spoločných prevádzkovateľov.[76]

Napriek výslovnému zakotveniu predmetného inštitútu v GDPR viacerí autori poukazujú na to, že špecifické otázky týkajúce sa alokácie zodpovednosti sú stále predmetom nejasností a diskusií.[77]

5.1.3 POJEM SPROSTREDKOVATEĽ

Sprostredkovateľ je v zmysle článku 4 bodu 8 GDPR *„fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý spracúva osobné údaje v mene prevádzkovateľa.“* Na kvalifikovanie entity ako sprostredkovateľa musia byť kumulatívne splnené dva atribúty. V prvom rade musí ísť o odlišnú entitu od prevádzkovateľa. Druhým kritériom je, že spracúvanie osobných údajov sa vykonáva v mene prevádzkovateľa.[78] Inštitút sprostredkovateľa reflektuje delegáciu resp. poverenie spracúvať osobné údaje na iné entity. Do spracúvania osobných údajov je zároveň možné zapojiť aj ďalších sprostredkovateľov (sub-sprostredkovateľov). Sprostredkovateľ to však môže urobiť iba so súhlasom prevádzkovateľa.[79]

5.1.4 INÉ ENTITY

Okrem kľúčových aktérov spracúvania osobných údajov v podobe prevádzkovateľa a sprostredkovateľ upravuje GDPR definíciu a postavenie ďalších troch entít.

---

[76] Tamže, s. 20 – 21.

[77] Pozri napr. VAN ALSENOY, Brendan: Liability under EU Data Protection Law. *In 7 (2016) JIPITEC 271*.

[78] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z:https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en. S. 24.

[79] Článok 28 ods.4, GDPR.

V prvom rade GDPR na mnohých miestach v legislatívnom texte ustanovuje práva a povinnosti pre dotknuté osoby. GDPR dotknutú osobu definuje ako identifikovanú alebo identifikovateľnú fyzickú osobu, ktorej sa osobné údaje týkajú.[80] Inými slovami, dotknutá osoba je osoba, ktorej osobné údaje sú spracúvané ako napr. bežný užívateľ sociálnej siete, zamestnanec z pohľadu zamestnávateľa alebo zákazník alebo klient elektronického obchodu či služby.

Ďalším pojmom, ktorý GDPR upravuje je príjemca. V zmysle definície je príjemca *„fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorému sa osobné údaje poskytujú bez ohľadu na to, či je treťou stranou.“*[81] Zároveň GDPR obsahuje aj negatívnu definíciu príjemcu týkajúceho sa orgánu verejnej moci pri výkone svojich oprávnení a úloh.[82] Príjemcom tak napr. môže byť sprostredkovateľ alebo poverený zamestnanec prevádzkovateľa.

Posledným pojmom do mozaiky osobnej pôsobnosti GDPR je tretia strana. Tretia je strana je definovaná primárne prostredníctvom negatívnej enumerácie: *„Tretia strana...je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt než dotknutá osoba, prevádzkovateľ, sprostredkovateľ a osoby, ktoré sú na základe priameho poverenia prevádzkovateľa alebo sprostredkovateľa poverené spracúvaním osobných údajov.“*[83]

5.2 ZODPOVEDNOSŤ PRI SPRACÚVANÍ OSOBNÝCH ÚDAJOV

Ak porovnáme znenie Smernice 95/46/ES s GDPR v súvislosti s ustanoveniami týkajúcimi sa zodpovednosti, tie prešli určitými zmenami a na niektorých miestach boli výrazne doplnené. Niektorí autori konštatujú, že režim

[80] Viď článok 4 bod 1, GDPR.

[81] Článok 4 bod 9, GDPR.

[82] Článok 4 bod 8, GDPR: *„Orgány verejnej moci, ktoré môžu prijať osobné údaje v rámci konkrétneho zisťovania v súlade s právom Únie alebo právom členského štátu, sa však nepovažujú za príjemcov; spracúvanie uvedených údajov uvedenými orgánmi verejnej moci sa uskutočňuje v súlade s uplatniteľnými pravidlami ochrany údajov v závislosti od účelov spracúvania.“*

[83] Článok 4 bod 10, GDPR.

zodpovednosti podľa GDPR je veľmi blízko tradičnému ponímaniu opatrení v rámci *tort law* v zmysle angloamerickej právnej tradície.[84]

Článok 82 ods. 2 GDPR obsahuje všeobecnú klauzulu týkajúcu sa zodpovednosti za škodu: *„Každá osoba, ktorá utrpela majetkovú alebo nemajetkovú ujmu v dôsledku porušenia tohto nariadenia, má právo na náhradu utrpenej škody od prevádzkovateľa alebo sprostredkovateľa.“* Podobne ako pri predchádzajúcej právnej úprave, z tohto ustanovenia môžu byť derivované tri podmienky pre uplatnenie zodpovednosti: (i) protiprávnosť, (ii) vznik škody a (iii) príčinná súvislosť.[85] Podmienka protiprávnosti je splnená pri akomkoľvek porušení GDPR. V súvislosti so vznikom škody, GDPR explicitne ustanovuje, že môže ísť o materiálnu alebo nemateriálnu škodu. Príklady materiálnej škody môžu zahŕňať výpoveď z práce, nenaplnenie zmluvy či úpravu zmluvných podmienok v neprospech dotknutej osoby spôsobenú nezákonným spracúvaním osobných údajov. Nemajetkovú ujmu možno ilustrovať na príkladoch úzkosti, diskriminácie či negatívneho obrazu v očiach verejnosti.[86] Poslednou podmienkou pri právnom režime zodpovednosti je príčinná súvislosť medzi protiprávnym konaním a vznikom škody.[87] Pri otázke „kto“ si môže nárok na náhradu škody v zmysle GDPR existujú dve interpretácie, nakoľko legislatíva používa pojem „akákoľvek osoba“. Prvá interpretácia je reštriktívna a hovorí, že škodu si môže nárokovať iba dotknutá osoba v zmysle GDPR. Na strane druhej, existuje skupina autorov, ktorí presadzujú extenzívnejšie prístup v zmysle ktorého si škodu môže nárokovať aj akákoľvek tretia strana.[88] Prikláňame sa k reštriktívnej interpretácií nakoľko iná strana ako dotknutá osoba ťažko úspešne preukáže škodu pri spracúvaní osobných údajov. Je však potrebné zvýrazniť, že

---

[84] TRAKMAN, Leon – WALTERS, Robert – ZELLER, Bruno: Tort and Data Protection Law: Are There Any Lessons to Be Learnt? *In European Data Protection Law Review 4/2019*, s. 506.

[85] Tamže, s. 493 – 495.

[86] Pozri viac v CORDEIRO, A.B. Menezes: Civil Liability for Processing of Personal Data in the GDPR. *In European Data Protection Law Review 4/2019*, s. 495.

[87] Článok 82 ods. 2, GDPR: *„Každá osoba, ktorá utrpela majetkovú alebo nemajetkovú ujmu v dôsledku porušenia tohto nariadenia, má právo na náhradu utrpenej škody od prevádzkovateľa alebo sprostredkovateľa.“*

[88] Pozri viac CORDEIRO, A.B. Menezes: Civil Liability for Processing of Personal Data in the GDPR *In European Data Protection Law Review 4/2019,* s. 495 – 496.

SDEÚ presadzuje princíp kompletnej a účinnej ochrany (*full and effective protection)*[89] pri spracúvaní osobných údajov a v zmysle toho je potrebné akceptovať, že náhrada škody by nemala byť rezervovaná pre dotknuté osoby.

5.2.1 ZODPOVEDNOSŤ PREVÁDZKOVATEĽA

Režim objektívnej zodpovednosti podľa Smernice 95/48/ES ostal v GDPR nezmenený, čo je potvrdené v článku 82 ods. 2 GDPR: *„Každý prevádzkovateľ, ktorý sa zúčastnil na spracúvaní, je zodpovedný za škodu spôsobenú spracúvaním, ktoré bolo v rozpore s týmto nariadením."*

Na tomto mieste si však dovoľujeme zvýrazniť, že z hľadiska povinností prevádzkovateľov GDPR akcentuje princíp zodpovednosti (*accountability*).[90] Princíp zodpovednosti obsahuje dve roviny. V prvej rovine sú prevádzkovatelia povinní demonštrovať súlad s požiadavkami GDPR vo formálnej rovine napr. prostredníctvom vypracovania záznamov o spracovateľských operáciách, plnením informačnej povinnosti či prijatím interných predpisov a pravidiel pre narábanie s osobnými údajmi v rámci organizácie. Druhá rovina reflektuje implementáciu organizačných a technických opatrení do praxe ako napr. manažment identity v rámci automatizovaných počítačových systémov, proces pre nahlasovanie bezpečnostných incidentov v podobe porušení ochrany osobných údajov či kreovanie odlišného prístupu ku osobným údajom vzhľadom na pracovné zaradenie zamestnancov.[91] Tento princíp prakticky znamená, že ak dotknutá osoba poukáže na poru-

[89] Pozri napríklad Rozsudok Súdneho dvora zo dňa 13. mája 2014 Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mariovi Costejovi Gonzálezovi. Vec č. C-131/12; Rozsudok Súdneho dvora Európkej únie zo dňa 5. júna 2018 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein proti Wirtschaftsakademie Schleswig-Holstein GmbH. Vec č. C-210/16 alebo Rozsudok Súdneho dvora zo dňa 10. júla 2018 Tietosuojavaltuutettu za účasti Jehovan todistajat – uskonnollinen yhdyskunta. Vec č. C-25/17.

[90] Pozri článok 5 ods. 2, GDPR.

[91] Podrobnejšie pozri VAN ALSENOY, Brendan – DUMORTIER, Jos: The accountability principle in data protection regulation: origin, development and future directions. *In GUAGNIN, D. – HEMPEL, L. - ILTEN, C. (eds): Managing Privacy Through Accountability*. 2012, Palgrave Macmillian, s. 49 – 82.

šenie GDPR zo strany prevádzkovateľa, dôkazné bremeno sa presúva na stranu prevádzkovateľa, ktorý musí následne preukázať súlad s GDPR.[92]

Prevádzkovateľ sa zodpovednosti môže zbaviť iba v prípadoch udalostí mimo jeho kontrolu. Článok 82 ods. 3 GDPR ustanovuje, že *„prevádzkovateľ…je zbavený zodpovednosti podľa odseku 2, ak sa preukáže, že nenesie žiadnu zodpovednosť za udalosť, ktorá spôsobila škodu.“* Niektorí autori naznačujú, že táto možnosť liberácie by mala byť interpretovaná reštriktívne.[93] Vývoj zodpovedných vzťahov v GDPR odzrkadľuje aj výslovne uznanie výnimiek za cudzí obsah v rámci smernice o elektronickom obchode[94] v článku 2 ods. 4 GDPR.[95] Prakticky to znamená jednotnejší prístup ku otázkam zodpovednosti v rámci európskej legislatívy a posilnenie právnej istoty.[96]

5.2.2 ZODPOVEDNOSŤ SPOLOČNÝCH PREVÁDZKOVATEĽOV

Ako už bolo uvedené vyššie, GDPR výslovne upravuje inštitút spoločných prevádzkovateľov.[97] Spoloční prevádzkovatelia sú povinní vymedziť svoje vzájomné práva a povinnosti v zmysle GDPR transparentným spôsobom. Na tomto mieste si dovoľujeme zvýrazniť, že každý zo spoločných prevádzkovateľ môže byť zodpovedný za škodu v plnom rozsahu. Je však potrebné

---

[92] VAN ALSENOY, Brendan: Liability under EU Data Protection Law. *In 7 (2016) JIPITEC 271*, s. 283.

[93] LAROUCHE, Pierre – PEITZ, Martin – PURTOVA, Nadya: *Consumer Privacy in network industries* – A CERRE Policy Report, 2016, Centre on Regulation in Europe. [Online] 2016. [cit. 29. 9. 2020]. Dostupné z: https://cerre.eu/wp-content/uploads/2016/01/160125_CERRE_Privacy_Final.pdf. S. 58.

[94] Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode). In EUR-lex [právní informační system]. Úřad pro publikace Evropské unie. Dostupné z https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32000L0031&qid=1585224374231&rid=1.

[95] *„Týmto nariadením preto nie je dotknuté uplatňovanie smernice 2000/31/ES, najmä pravidlá týkajúce sa zodpovednosti poskytovateľov služieb informačnej spoločnosti uvedené v článkoch 12 až 15 uvedenej smernice.“*

[96] Napr. CUNHA, A. Maria Viola – MARIN, Luisa – SARTOR, Giovanni: Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web. *In International Data Privacy Law,* Volume 2, Issue 2, 2012, s. 57.

[97] Článok 26 ods. 1, GDPR: *„Ak dvaja alebo viacerí prevádzkovatelia spoločne určia účely a prostriedky spracúvania, sú spoločnými prevádzkovateľmi.“*

poznamenať, že článok 83 GDPR neupravuje špecificky alokáciu zodpovednosti medzi spoločnými prevádzkovateľmi v prípade porušenia GDPR. Dôvody pre zbavenie zodpovednosti a typy odškodnenia sa aplikujú analogicky ako pri prevádzkovateľoch a sprostredkovateľoch.

Inštitút spoločných prevádzkovateľoch a alokácia zodpovednosti boli predmetom viacerých rozhodnutí SDEÚ, najnovšie v prípadoch *Wirtschaftsakademie* a *Fashion ID*, ktoré nadviazali na premisy judikované v prípade *Google Spain*. V rozhodnutí *Google Spain*[98] Luxemburský súd rozhodoval v kontexte spracúvania osobných údajov populárneho internetového vyhľadávača a pôvodného zdroja žurnalistického textu. V tomto prípade uviedol: *„...činnosť vyhľadávača môže významne a vo vzťahu k činnosti editorov webových stránok doplňujúcim spôsobom ovplyvniť základné práva na súkromie a ochranu osobných údajov, poskytovateľ tohto vyhľadávača ako osoba, ktorá určuje ciele a prostriedky tejto činnosti, musí v rámci svojich zodpovedností, kompetencií a možností zaručiť, že táto činnosť spĺňa požiadavky smernice 95/46, aby záruky ňou stanovené mohli mať plný účinok a aby účinná a úplná ochrana dotknutých osôb, a najmä práva na rešpektovanie ich súkromia, mohla byť skutočne dosiahnutá.“*[99] SDEÚ tak diskutovanej kauze zvýraznil, že súlad s pravidlami pre spracúvanie osobných údajov musí byť posúdený prostredníctvom optiky „kompetencií a možností“ prevádzkovateľa. Napriek tomu, že predmetný judikát sa týka pomerne špecifického prevádzkovateľa – internetového vyhľadávača, SDEÚ umožnil interpretovať alokáciu zodpovednosti pomerne extenzívne a otvoril tým pandorinu skrinku pre potenciálne úniky prevádzkovateľov zo zodpovednostných vzťahov.

Prípad *Wirtschaftsakademie*[100] sa skutkovo týkal správneho určenia postavenia správcu fanúšikovskej stránky na sociálnej sieti Facebook (Wirtschaft-

[98] Rozsudok Súdneho dvora zo dňa 13. mája 2014 Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mariovi Costejovi Gonzálezovi. Vec č. C-131/12.

[99] Rozsudok Súdneho dvora zo dňa 13. mája 2014 Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mariovi Costejovi Gonzálezovi. Vec č. C-131/12., bod 38.

[100] Rozsudok Súdneho dvora Európkej únie zo dňa 5. júna 2018 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein proti Wirtschaftsakademie Schleswig-Holstein GmbH. Vec č. C-210/16.

sakademie) a prevádzkovateľa samotnej sociálnej siete (Facebook). Najdôležitejším aspektom rozhodnutia bolo určenie, nakoľko je správca fanúšikovskej stránky zapojený do rozhodovania o účeloch a prostriedkoch spracúvania osobných údajov spolu s Facebookom. Luxemburský súd v úvode rozhodnutia poznamenal, že nie každý užívateľ sociálnej siete bude považovaný za prevádzkovateľa, špecifické postavenie správcu fanúšikovskej stránky vyplýva z toho, že *„správca fanúšikovskej stránky umiestnenej na Facebooku vytvorením takej stránky umožňuje spoločnosti Facebook, aby umiestňoval súbory cookies na počítači alebo akomkoľvek inom zariadení osoby, ktorá jeho fanúšikovskú stránku navštívila, bez ohľadu na to, či táto osoba má alebo nemá účet na Facebooku.“*[101] SDEÚ taktiež poukázal na to, že správca takejto stránky má pomerne veľkú voľnosť pri nastavovaní filtrov na cielene (výber publika) a kritérií na kreovanie štatistík návštevnosti a dosahu stránky.[102] Vzhľadom na tieto okolnosti Luxemburský súd judikoval, že správca fanúšikovskej stránky a Facebook sú na tieto účely spoloční prevádzkovatelia. Zároveň však SDEÚ zvýraznil dôležitosť posúdenia stupňa zodpovednosti vzhľadom na konkrétne štádiá spracúvania osobných údajov: *„...existencia spoločnej zodpovednosti neznamená nevyhnutne rovnakú zodpovednosť rôznych subjektov, ktorých sa týka spracovanie osobných údajov. Tieto subjekty môžu byť naopak zapojené do tohto spracovania v rôznych fázach a stupňoch, takže mieru zodpovednosti každého z nich treba hodnotiť z hľadiska všetkých relevantných okolností prejednávanej veci.“*[103] Doktrína tento prístup a rozhodnutie charakterizovala ako posun z makroskopického pohľadu na mikroskopické nazeranie na spracúvanie osobných údajov.[104] SDEÚ však nechal viaceré otázky otvorené ako napríklad mechanizmus pre určenie zodpovednosti v rámci spoločných prevá-

[101] Tamže, bod 35.

[102] Tamže, bod 36.

[103] Tamže, bod 43.

[104] MAHIEU, René – HOBOKEN VAN, Joris - ASGHARI, Hadi: Responsibility for Data Protection in a Networked World. On the question of the Controller. „Effective and Complete Protection“ and its Application to Data Access Rights in Europe. *In JIPITEC 39, 10 (2019*), s. 48.

dzkovateľov či posudzovanie previazanosti určenia účelov *a* prostriedkov spracúvania.[105]

Podobné závery možno derivovať z prípadu *Fashion ID*.[106] Interpretačný spor sa skutkovo týkal situácie, v ktorej prevádzkovateľ webovej stránky (Fashion ID – online predajca oblečenia) integroval na svojej stránke tlačidlo „LIKE“ napojené na sociálnu sieť Facebook. V tomto kontexte bolo dôležité, že údaje o každom návštevníkovi stránky Fashion ID boli automaticky prenášané sociálnej sieti bez ohľadu na to, či tam daný návštevník mal registrovaný účet alebo nie. Otázka osobnej pôsobnosti legislatívy tak bola znova na stole. SDEÚ opätovne zdôraznil širokú interpretáciu pojmu prevádzkovateľ a nadviazal na rozhodnutie vo veci *Wirtschaftsakademie*. Spoločné určenie účelov a prostriedkov spracúvania osobných údajov bolo založené na počiatkoch spracovateľskej operácie (zbieranie a prenos).[107] Zároveň však súd judikoval, že v rozličných fázach spracúvania je možné viazať odlišný stupeň zodpovednosti aktérom spracúvania osobných údajov.[108]

5.2.3 ZODPOVEDNOSŤ SPROSTREDKOVATEĽA

V porovnaní so Smernicou 95/48/ES sa zákonodarca na úrovni EÚ rozhodol urobiť krok vpred a explicitne upravil povinnosti a súvisiacu zodpovednosť sprostredkovateľov v GDPR. Povinnosti týkajúce sa sprostredkovateľov môžu vyplývať z ustanovení GDPR[109] alebo sprostredkovateľskej zmluvy uzavretej medzi sprostredkovateľom a prevádzkovateľom v zmysle článku 28 ods. 3 GDPR. Z faktického hľadiska sprostredkovateľ vždy koná a spracúva osobné údaje na základe a v mene poverenia od prevádzkovateľa. V prípade deviácie od pokynov sprostredkovateľa prípadne sprostredkovateľskej zmluvy je potrebné riešiť otázky týkajúce sa zodpovednosti.

[105] Tamže, s. 49.

[106] Rozsudok Súdneho dvora Európskej únie zo dňa 29. júla 2019 Fashion ID GmbH & Co.KG proti Verbraucherzentrale NRW eV. Vec č. C-40/17.

[107] Tamže, body 79 – 81.

[108] Tamže, bod 71.

[109] Napríklad povinnosť vypracovať záznamy o spracovateľských operáciách v zmysle článku 30 GDPR, nahlasovať porušenia ochrany osobných údajov prevádzkovateľovi podľa článku 33 ods. 2 GDPR alebo dezignovať do funkcie zodpovednú osobu v zmysle článku 37 GDPR.

Ustanovenia regulujúce zodpovednosť sprostredkovateľov stoja na princípe pomernej zodpovednosti: *„Sprostredkovateľ zodpovedá za škodu spôsobenú spracúvaním, len ak neboli splnené povinnosti, ktoré sa týmto nariadením ukladajú výslovne sprostredkovateľom, alebo ak konal nad rámec alebo v rozpore s pokynmi prevádzkovateľa, ktoré boli v súlade so zákonom.“*[110] GDPR však ustanovuje aj možnosť plnej zodpovednosti sprostredkovateľa, ktorý *„zodpovedá za celú škodu, aby sa dotknutej osobe zabezpečila účinná náhrada.“*[111] Samotné zapojenie sprostredkovateľa do spracúvania osobných údajov však nemusí automaticky znamenať, že v prípade brania na zodpovednosť, tento sprostredkovateľ bude z časti alebo plne zodpovedať za spôsobenú škodu.[112] Vznik škody môže byť pripísaný sprostredkovateľovi iba v prípadoch, ak jeho konanie pri spracúvaní osobných údajov viedlo ku vzniknutej škode na základe porušení ustanovení GDPR alebo toto konanie bolo v rozpore s pokynmi prevádzkovateľa prípadne sprostredkovateľskou zmluvou. Na strane druhej však GDPR neupravuje stupeň a rozsah zodpovednosti a z teoretického hľadiska umožňuje pripísanie celej škody sprostredkovateľovi.[113] Dotknutá osoba má prakticky možnosť vybrať si entitu, u ktorej si škodu bude uplatňovať v prípade, že do spracúvania osobných údajov bol zapojený okrem prevádzkovateľa aj sprostredkovateľ.[114] Navyše, prevádzkovateľ má možnosť regresu (kompenzácií) voči sprostredkovateľovi ak preukáže porušenie GDPR, pokynu prevádzkovateľa či sprostredkovateľskej zmluvy u tohto sprostredkovateľa.[115]

V otázkach typu odškodnenia a liberácie platia rovnaké závery ako pri prevádzkovateľoch.

---

[110] Článok 82 ods. 2, GDPR.

[111] Článok 82 ods. 4, GDPR.

[112] Pozri diskusiu ku prijatiu článku 82 GDPR v VAN ALSENOY, Brendan : Liability under EU Data Protection Law. *In 7 (2016) JIPITEC 271* s. 285.

[113] Tamže, poznámka pod čiarou č. 108.

[114] Článok 82 ods. 4, GDPR: *„Ak sa na tom istom spracúvaní zúčastnil viac než jeden prevádzkovateľ alebo sprostredkovateľ alebo prevádzkovateľ aj sprostredkovateľ spoločne a sú podľa odsekov 2 a 3 zodpovední za škodu spôsobenú spracúvaním, každý z nich zodpovedá za celú škodu, aby sa dotknutej osobe zabezpečila účinná náhrada.“*

[115] Článok 82 ods. 5, GDPR.

5.3 OSOBNÁ PÔSOBNOSŤ GDPR A AUTONÓMNE VOZIDLÁ

Autonómne vozidlá či systémy sú pomerne široko akademicky diskutovanou témou.[116] Snahy o reguláciu autonómnych systémov v podobe technológií na báze umelej inteligencie naberajú na dôležitosti aj v rámci legislatívnych plánov na úrovní EÚ.[117] Svoje usmernenie k danej problematike vydal aj EDPB, ktorý je vedúcou interpretačnou autoritou v oblasti ochrany osobných údajov na úrovní EÚ.

5.3.1 USMERNENIE EDPB

28. januára 2020 vydal EDPB usmernenie o spracúvaní osobných údajov v kontexte prepojených vozidiel a aplikácií súvisiacich s mobilitou (ďalej len „Usmernenie").[118] Ide o verziu pre verejnú konzultáciu, čo znamená, že verejnosť môže k Usmerneniu zasielať pripomienky, ktoré sa môžu premietnuť do finálneho znenia textu. Na ilustráciu komplexu právnych aspektov spracúvania osobných údajov v autonómnych vozidlách je však táto verzia postačujúca.

Štruktúra Usmernenie reflektuje konkrétne aplikačné problémy pri spracúvaní osobných údajov v prepojených vozidlách. Usmernenie sa neza-

---

[116] Napr. POLČÁK, Radim : ODPOVĚDNOST UMĚLÉ INTELIGENCE A INFORMAČNÍ ÚTVARY BEZ PRÁVNÍ OSOBNOSTI. In: http://www.bulletin-advokacie.cz/. [online]. Datum publikování: 30.11.2018. Datum aktualizace [26.3.2020]. Dostupné z:http://www.bulletin-advokacie.cz/odpovednost-umele-inteligence-a-informacni-utvary-bez-pravni-osobnosti; CARP, Jeremy: Autonomous Vehicles: Problems and Principles for Future Regulation. In *University of Pennsylvania Journal of Law & Public Affairs*, Vol. 4, No. 1, 2018; YEEFEN Lim(ed) : *Autonomous Vehicles and the Law: Technology, Algorithms and Ethics*. Edward Elgar Pub. 2018.

[117] Pozri COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Coordinated Plan on Artificial Intelligence; 6.EU High-Level Expert Group on AI Ethics guidelines for trustworthy AI [online]. 2019. [cit. 29. 9. 2020] Dostupné z: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai alebo European Commission: White Paper on Artificial Intelligence: a European approach to excellence and trust. Brussels, 19.2.2020. COM(2020) 65 final. [online]. 2020. [cit. 29. 9. 2020]. Dostupné z: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf.

[118] European Data Protection Board Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications. [Online]. 2020. [cit. 29. 9. 2020] Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en.

meriava výslovne na autonómne vozidlá, ale jeho pôsobnosť možno z časti aplikovať aj na klasické formy vozidiel, ktoré využívajú nové technológie a sú určitým spôsobom pripojené na sieť (*connected vehicles*). Množstvo záverov však bude relevantných práve v súvislosti s autonómnymi vozidlami. Po úvodnej časti a definovaní základných problémov v kontexte ochrany súkromia a osobných údajov nasledujú dve ťažiskové časti. Prvá z nich predstavuje všeobecné odporúčania týkajúce sa kategórií spracúvaných údajov, účelov, zásady minimalizácie údajov, inštitútu špecificky navrhnutej a štandardnej ochrany osobných údajov, plnení informačnej povinnosti, práv dotknutých osôb, prenosu údajov a použití wi-fi technológií.[119] Druhá obsahová časť obsahuje konkrétne prípadové štúdie a konkrétne odporúčania pri spracúvaní osobných údajov v daných situáciách.[120] Z hľadiska zamerania predkladaného príspevku považujeme za vhodné charakterizovať základné postuláty, na ktorých Usmernenie stojí vrátane typov osobných údajov a aplikácií v rámci prepojených vozidiel a základných aktérov ich prevádzkovania.

Usmernenie vo svojom úvode veľmi pragmaticky uvádza, že už aj tradičné vozidlá bez autonómnych systémov sa stávajú „dátovými hubmi.“[121] Na strane druhej, prepojené vozidlá a spracúvanie osobných údajov predstavujú komplexný ekosystém. Tento ekosystém pridáva ku tradičnému poňatiu a účelu automobilu viaceré prvky. Ilustrovať to možno na príkladoch prehrávania hudby podľa nálady vodiča, aktuálne informácie o dopravnej situácií a počasí, systémy asistencie pri vedení vozidla resp. autopilot, meranie výšky poistenia na základe používania automobilu. Ďalej je možné akcentovať možnosti prepojiť vozidlo s ďalšími externými zdrojmi prostredníctvom siete ako prevádzkovateľmi dopravného značenia alebo telekomunikačnými operátormi.[122] Z hľadiska vodiča automobilu je tak

[119] Usmernenie, s. 12 – 21.

[120] Usmernenie, s. 21 – 30.

[121] Usmernenie, s. 3.

[122] Tamže.

možné na základe získaných údajov kreovať profil jeho štýlu vedenia vozidla či vodičských návykov.[123]

Usmernenie sa výslovne venuje spracúvaniu geo-lokalizačných údajov,[124] biometrických údajov[125] a údaje týkajúce sa uznania viny za trestné činy a priestupky.[126] Prirodzene, tieto údaje nie sú jedinými typmi spracúvanými pri prevádzkovaní autonómneho vozidla, avšak vzhľadom na ich osobitosť (citlivosť)[127] EDPB pragmaticky charakterizuje detaily ich spracúvania. Množstvo údajov, ktoré autonómne vozidlo spracúva možno klasifikovať ako osobné údaje v zmysle GDPR, či už ide o priame identifikátory v podobe identity vodiča alebo pasažiera alebo identifikátory nepriame ako štýl vedenia vozidla, prejazdená vzdialenosť či technické údaje týkajúce sa vozidla.[128] Už z vyššie uvedeného výpočtu jednoznačne vyplýva, že v rámci vozidla sú spracúvané osobitné kategórie osobných údajov v zmysle článku 9 ods. 1 GDPR.[129] Z toho priamo vyplýva požiadavka, aby prevádzkovateľ vozidla disponoval niektorou z výnimiek v zmysle článku 9 ods. 2 GDPR pre spracúvanie osobitných kategórií osobných údajov. Nájdenie a aplikácia potenciálne použiteľnej výnimky môže naraziť na pomerne reštriktívne koncipované ustanovenia diskutovaného článku. Vždy bude záležať na konkrétnom účele spracúvania osobných údajov, ale na prvý pohľad sa ako použiteľné výnimky javia životne dôležitý záujem (článok 9 ods. 2 písm. c) GDPR) pri spracúvaní údajov o zdraví vozidla alebo pasažierov a monitorovaní ich životných funkcií a alternatívne výslovný súhlas (článok 9 ods. 2 písm. a) GDPR).

---

[123] Tamže, s. 4.

[124] Tamže, s. 12 - 13

[125] Tamže, s. 13.

[126] Tamže, s. 13 – 14.

[127] K tomu pozri článok 9 GDPR a článok 10 GDPR.

[128] Pozri viac Usmernenie, s. 7 – 8.

[129] Článok 9 ods. 1 GDPR definuje tieto údaje ako také, ktoré *„odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.“*

Z hľadiska rôznych aplikácií a využitia údajov v rámci prepojených vozidiel EDPB demonštratívne spomína šesť oblastí. Prvou je manažment mobility a teda využitie údajov na efektívne vykonanie konkrétnej trasy prostredníctvom údajov o stave vozovky, počasia, hustoty premávky či uzáver. Druhá oblasť je manažment samotného vozidla a spracúvanie údajov, ktorí indikujú vodičom servisný stav vozidla či dáta o používaní vozidla a jeho konkrétnych komponentov. Treťou oblasťou je bezpečnosť na cestách a to v podobe upozornení na externé riziká pri vedení vozidla či automatické volania pri nehodách alebo ukladanie dát v rámci „čiernych skriniek." Štvrtá oblasť predstavuje všetky funkcie určené na „zábavu" v podobe prepojenia mobilných telefónov alebo hot-spotov na účely volania, počúvania hudby, generovania správ či prepojenia na smart-home alebo internet. Piatu oblasť predstavuje spracúvanie údajov na účely plnej alebo čiastočnej asistencie pri vedení vozidla. Napokon, šiesta oblasť sa týka zdravia vodiča ako meranie únavy alebo potreba lekárskej starostlivosti.[130] Vzhľadom na presah jednotlivých oblastí do konkrétnych účelov spracúvania bude nevyhnutné k ich vymedzeniu vždy pristupovať pragmaticky, nakoľko viaceré oblasti budú presahovať do jedného alebo viacerých účelov spracúvania osobných údajov. V zmysle zásady obmedzenia účelu podľa článku 5 ods. 1 písm. b) GDPR sa zdá ako najdôležitejšie precízne upraviť účel týkajúci sa samotného fungovania vozidla a subsumovanie relevantných spracovateľských operácií pod neho. Podľa nášho názoru nemožno všetky uvedené oblasti fungovania vozidla považovať za „nevyhnutné" a aj z hľadiska vymedzenia právneho základu bude preto nevyhnutné medzi rôznymi oblasťami a účelmi rozlišovať.

Už vyššie uvedených typov aplikácií a potenciálne spracúvaných údajov je možné zhrnúť, že pri prevádzke prepojeného vozidla sa k údajom môže dostať potenciálne pomerne veľké množstvo rôznych subjektov od tradičných výrobcov vozidiel až po firmy pôsobiace v digitálnom priemysle. EDPB demonštratívne vymenúva výrobcov vozidiel, výrobcov jednotlivých zariadení, komponentov a ich dodávateľov, autoservisy, predajne automobilov, spoločnosti zaoberajúce sa prenájmom a zdieľaním automobilov,

[130] Usmernenie, s. 7.

správcov vozového parku, poisťovne motorových vozidiel, poskytovateľov zábavy, telekomunikačných operátorov, správcov cestnej infraštruktúry a orgány verejnej moci, ako aj vodičov, majiteľov vozidiel, nájomcov vozidiel či pasažierov.[131] Prakticky sa tvorí pomerne robustný ekosystém entít s prístupom k osobným údajom z jedného vozidla. Tieto otázky sú z hľadiska spracúvania osobných údajov nesmierne dôležité, nakoľko determinujú rozdelenie zodpovednosti za súlad s GDPR a taktiež zodpovednosť za potenciálne porušenie regulácie ochrany osobných údajov.

Z hľadiska konkrétnych aktérov spracúvania osobných údajov EDPB exemplifikatívne určila postavenie v zmysle osobnej pôsobnosti GDPR, avšak prirodzene predmetné postavenie je potrebné vždy posudzovať v konkrétnej situácií a v špecifickom kontexte. Typickými dotknutými osobami by mali byť vodiči, pasažieri a majitelia vozidiel. Prevádzkovateľmi v súvislosti s spracúvaním osobných údajov v prepojených vozidlách môžu byť prevádzkovatelia služieb, ktorí spracúvajú údaje o vozidle za účelom poskytnutia rôznych informácií vodičovi (napr. najkratšia cesta do destinácie, dopravná situácia, servisné upozornenia). Ďalším prevádzkovateľom môže byť poisťovňa, u ktorej je vozidlo poistené či výrobca vozidla, ktoré využíva údaje na vylepšenie komponentov tvoriacich vozidlo. Sprostredkovateľmi môžu byť výrobcovia jednotlivých komponentov, ktorí údaje spracúvajú v mene výrobcov vozidiel. Ako typy príjemcov Usmernenie vymenúva obchodných partnerov poskytovateľov služieb uvedených vyššie, ktorí spracúvajú údaje generované vozidlom.[132] Pri poskytovateľoch externých služieb (ako napr. poisťovní alebo iných) EDPB zvýrazňuje, že jediným príjemcom osobných údajov by mali byť samotný prevádzkovatelia týchto služieb.[133] Totožný záver platí aj pri prenajímateľoch vozidiel a správcov parkovacích miest.[134] V prípade poskytovateľov zdravotnej starostlivosti v urgentných situáciách (tzv. účel 112) by tieto údaje taktiež ne-

[131] Tamže, s. 8.

[132] Tamže, s. 9

[133] Tamže, s. 24.

[134] Tamže.

mali spracúvať a byť prenesené iným subjektom.[135] Pri výskumných účeloch v zmysle článku 89 GDPR (napr. pri výskume nehodovosti) by príjemcom nemal byť žiadny iný subjekt s výnimkou prevádzkovateľa a sprostredkovateľa.[136]

EDPB výslovne spomína aj orgány verejnej moci a tretie strany, ktoré si údaje môžu vyžiadať pri plnení svojich úloh na základe zákonných zmocnení (napr. orgány činné v trestnom konaní prípadne v rámci priestupkového konania).[137]

Možno konštatovať, že diskutované Usmernenie sa konkrétnym aktérom nevenuje veľmi detailne a ponecháva priestor pre aplikačnú prax na vysporiadanie sa s touto otázkou.

5.3.2 APLIKAČNÉ PROBLÉMY (MODELOVÉ SITUÁCIE)

V úvodnej časti predkladaného článku boli definované tri rozmery komunikácie, ktoré sa týkajú autonómneho - prepojeného vozidla. V rámci tejto časti článku poskytneme naše úvahy v kontexte týchto modalít toku dát z hľadiska určenia zodpovednej entity v oblasti ochrany osobných údajov.

Prvou situáciou je pripojenie vozidla na internet, v rámci ktorého využíva rôzne služby (V2I – *Vehicle to Internet*). V tomto postavení je možné analyzovať dve modelové podstaty a to (i) pripojenie ku službe, ktorá je nevyhnutná na fungovanie autonómneho vozidla napr. ku GPS navádzaciemu satelitu a (ii) pripojenie ku aplikáciám, poskytujúcim užívateľom zábavné služby ako napríklad Spotify alebo Netflix. Pri prvej modelovej podstate (služba nevyhnutná na fungovanie autonómneho vozidla) pôjde pravdepodobne o vzťah dotknutá osoba (majiteľ alebo vodič vozidla) a prevádzkovateľ (prevádzkovateľ vozidla). Zaujímavý je však vzťah medzi prevádzkovateľom vozidla a poskytovateľom nevyhnutnej služby. Pri diskusií o tomto vzťahu pred niekoľkým rokmi by sa väčšina komentárov pravdepodobne priklonila ku vzťahu prevádzkovateľ – sprostredkovateľ, nakoľko poskytovateľ nevyhnutnej služby pre fungovanie vozidla by spracúval

[135] Tamže, s. 27.

[136] Tamže, s. 29.

[137] Tamže, s. 9.

osobné údaje v mene prevádzkovateľa vozidla. Tieto závery je však potrebné revidovať vo vzťahu ku rozhodnutia SDEÚ vo veciach *Wirtschaftsakademia* a *Fashion ID*. V spomínanej dvojici prípadov Luxemburský súd zvýraznil princíp plnej a efektívnej ochrany dotknutých osôb a analýzu spracovateľských operácií v mikroskopickom meradle.[138] Ak by sme sa teda v praxi mikroskopicky pozreli na spracovateľské operácie medzi vozidlom a poskytovateľom služby nevyhnutnej na fungovanie vozidla, v niektorých prípadoch môže ísť o spoločných prevádzkovateľoch v zmysle článku 26 GDPR, nakoľko do určitej miery vymedzujú účely a prostriedky spracúvania spoločne. Dopĺňame, že na aplikáciu inštitútu spoločných prevádzkovateľov nie je nevyhnutné výslovné spoločné určenie účelov alebo prostriedkov spracúvania, ale stačí, ak ide o dopĺňajúce (zbiehajúce – *converging decisions*) sa rozhodnutia v rámci spracúvania osobných údajov, ktoré majú hmatateľný vplyv.[139] Nie je preto vylúčené, že v prípade navádzania prepojeného vozidla poskytovateľom nevyhnutnej služby by došlo k naplneniu požiadavky zbiehajúcich sa rozhodnutí na určení účelov a prostriedkov spracúvania a aplikácií inštitútu spoločných prevádzkovateľov. Zodpovednosť by v danom prípade mala byť určená v konkrétnych prípadoch a za konkrétnych okolností.

Druhou modelovou podstatou je pripojenie ku službám, ktoré poskytujú v rámci vozidla zábavu. Sme toho názoru, že v takomto prípade ide o vzťah dotknutá osoba a prevádzkovateľ, pričom prevádzkovateľ autonómneho vozidla by nemal mať *stricto sensu* prístup k údajom získaným poskytovateľom zábavných služieb, nakoľko to nie je nevyhnutné pre fungovanie prepojeného vozidla.

Druhou situáciu je komunikácie vozidiel navzájom (V2V – *Vehicle to Vehicle*), za účelom vedenia vozidla a prevencie proti dopravným nehodám. Sme toho názoru, že v takomto prípade by sa malo pristúpiť ku dôslednej

[138] Rozsudok Súdneho dvora Európkej únie zo dňa 5. júna 2018 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein proti Wirtschaftsakademie Schleswig-Holstein GmbH. Vec č. C-210/16. Bod 43.

[139] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z:https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en. S. 18.

anonymizácií údajov,[140] pričom kvalita dát v tomto nastavení by mala byť zameraná na iné ako osobné údaje (*non-personal data*) týkajúce sa vzdialenosti medzi vozidlami alebo inými technickými údajmi. Pri týchto údajoch by mala byť minimalizovaná možnosť spojenia údajov s konkrétnou dotknutou osobu. Predmetný prístup by prakticky znamenal „únik" z režimu GDPR a bol by v súlade s inštitútom špecificky navrhnutej a štandardnej ochrany údajov v zmysle článku 25 GDPR.[141]

Treťou situáciou je prepojenie vozidla s inými zariadeniami v rámci internetu vecí (V2IoT – *Vehicle to Internet of Things*). V tomto kontexte opätovne vidíme dve modality prepojenia a to medzi vozidlom a (i) inteligentnou cestnou infraštruktúrou a (ii) použitie týchto údajov v konaní o deliktoch orgánmi verejnej moci. Prvou modalitou je spracúvanie údajov vozidla a inteligentnej cestnej infraštruktúry v rámci tzv. kooperatívneho cestného systému (*cooperative – intelligent transportation system*), kde je zmyslom kooperácie prevádzkovateľa vozidla a cestnej infraštruktúry zamedzenie nehodovosti a dodržiavanie regulácie cestnej premávky. V tomto systéme nie je vylúčená ani komunikácia medzi prepojenými vozidlami navzájom.[142] Pri diskusií týkajúce sa pripojenia na inteligentnú cestnú infraštruktúru opätovne vzniká otázka postavenia a zodpovednosti v zmysle GDPR. Pôjde o spoločných prevádzkovateľov osobných údajov alebo samostatných prevádzkovateľov? Podľa nášho názoru je znova možné, že vo svetle nedávnej judikatúry SDEÚ bude musieť prax tento vzťah posudzovať ako spoločných prevádzkovateľov. Tento záver opierame o dva argumenty. Prvým argumentom je, že obaja prevádzkovatelia majú spoločný účel, ktorým je bezporuchový chod cestnej premávky. Tento účel je základnou úlo-

[140] Pozri viac Article 29 Data Protection Working Party: Opinion 05/2014 on Anonymisation Techniques. [online]. 2014. [cit. 29. 9. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[141] Viac v European Data Protection Board: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. [online]. 2020. [cit. 29. 9. 2020]. Dostupné z:https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en.

[142] Pozri vynikajúcu analýzu z pohľadu príčinnej súvislosti spôsobenej škody v ŽOLNERČÍKOVÁ, Veronika. Prokazování příčinné souvislosti u škod způsobených propojenými autonomními vozidly. *Revue pro právo a technologie*. [Online]. 2020, č. 21, s. 129-152. [cit. 2020-09-29]. Dostupné z: https://journals.muni.cz/revue/article/view/13048.

hou prevádzkovateľa inteligentnej infraštruktúry (štát alebo samospráva) a ekonomicky nevyhnutným pre prevádzkovateľa autonómneho vozidla, nakoľko bez rešpektovania diskutovaného aspektu je prakticky nemožné uviesť vozidlo na trh a používať ho. Zároveň prevádzkovatelia využívajú prepojenú infraštruktúru, ktorá navzájom komunikuje. Opätovne tak teda môže ísť o zbiehajúce sa rozhodnutia (*converging decisions*) o účeloch a prostriedkoch spracúvania osobných údajov. Druhým argumentom v prospech predmetnej klasifikácie je samotné rozhodnutie SDEÚ vo veci *Wirtschaftsakademie*. V tomto prípade išlo o to, že správca fanúšikovskej stránky na sociálnej sieti zasadil svoje aktivity do určitých mantinelov (napríklad v podobe špecifikácie cielenia reklamy alebo tvorby štatistík), ktoré mu vytvorila sociálna sieť, z čoho následne profitovali obe entity. Analogicky môže nastať podobná situácia, ak prevádzkovateľ autonómneho vozidla „zasadí“ svoje vozidlo do inteligentnej cestnej infraštruktúry.

Toto riešenie nie je z nášho pohľadu ideálne, nakoľko by vyžadovalo komplexnú revíziu vzťahov medzi prevádzkovateľmi vozidiel a prevádzkovateľmi infraštruktúry v zmysle požiadaviek článku 26 GDPR. Nemožno ale v tejto chvíli precízne prejudikovať, ako sa nastavením pôsobnosti a zodpovednosti v oblasti ochrany osobných údajov v danom nastavení vysporiada prax a judikatúra.

Druhou modalitou je využívanie údajov orgánmi verejnej moci na účely vedenia správnych alebo trestných konaní. V tomto smere figurujú orgány verejnej moci ako príjemcovia a následne v rámci konania samostatní prevádzkovatelia. V tejto súvislosti možno odkázať na nemeckú právnu úpravu, ktorá výslovne reguluje prístup a využitie údajov z tzv. čiernych skriniek autonómnych vozidiel.[143]

[143] § 63a English Translation of the German Road Traffic Act Amendment Regulating the Use of “Motor Vehicles with Highly or Fully Automated Driving Function” from July 17, 2017. CZARNECKI, Krzysztof. English Translation of the German Road Traffic Act Amendment Regulating the Use of “Motor Vehicles with Highly or Fully Automated Driving Function” from July 17, 2017. [Online]. [cit. 2020-09-29]. Dostupné z: https://www.researchgate.net/publication/320813344.

6. ZÁVER

Autonómne vozidlá pre maximálne využitie svojho potenciálu zbierajú, spracúvajú a zdieľajú častokrát aj osobné údaje s externými entitami. Legislatíva na úrovni práva EÚ umožňuje za určitých podmienok schválenie vozidiel s autonómnymi alebo automatizovanými systémami a čiastočne upravuje problematiku ochrany osobných údajov a kybernetickej bezpečnosti. Nariadenie o typovom schválení a najmä k nemu vydané usmernenie týkajúce sa výnimiek na schválenie automatizovaných vozidiel obsahuje usmernenia o inštalovaní nahrávacieho zariadenia, tak aby boli dodržané právne predpisy EÚ o ochrane údajov a boli chránené konkrétne informácie pred manipuláciou. Z pohľadu infraštruktúry, s ktorou môžu autonómne vozidlá komunikovať je legislatíva EÚ dosť špecifiká. V zmysle smernice o inteligentných dopravných systémoch a najmä delegovaného nariadenia musia prevádzkovatelia staníc kooperatívnych inteligentných dopravných systémov prevádzkovať systém riadenia informačnej bezpečnosti a taktiež by sa mali uplatniť bezpečnostné požiadavky na pseudonymizáciu údajov. Taktiež platí, že osobné údaje by sa mali spracúvať za prísneho dodržiavania zásady minimalizácie údajov, len na účely špecifikované v delegovanom nariadení. Legislatívne akty EÚ upravujúce problematiku kybernetickej bezpečnosti môžu zabezpečiť dostatočnú úroveň kybernetickej bezpečnosti budúcich technológií, ktoré sa budú používať v autonómnych vozidlách, a to najmä prostredníctvom systému certifikácie IKT produktov, postupov a služieb v EÚ, resp. prostredníctvom plnenia bezpečnostných opatrení v zmysle smernice NIS ak výrobcovia vozidiel alebo dodávatelia systémov budú v pozícii prevádzkovateľov základných služieb.

Z hľadiska postavenia rôznych aktérov spracúvania osobných údajov v autonómnom vozidle sme v prvom rade diskutovali súčasnú interpretáciu pojmov prevádzkovateľ, sprostredkovateľ a ich zodpovednosti v zmysle nedávnej judikatúry SDEÚ. Na základe vymedzenia a analýzy troch modelových situácií sme poukázali na to, že vo viacerých prípadoch spracúvania osobných údajov v rámci prepojeného autonómneho vozidla bude určenie zodpovednej entity nesmierne náročné a to vzhľadom na funkčný a pomerne široký výklad pojmu spoločných prevádzkovateľov z hľadiska

možnosti zbiehajúcich rozhodnutí o účeloch a prostriedkoch spracúvania v rámci diskutovaných vozidiel. Mikroskopický pohľad na spracovateľské operácie optikou SDEÚ nie je najvhodnejším riešením pri vymedzení daných vzťahov v súvislosti s prepojenými vozidlami. Je preto možné, že v budúcnosti dôjde ku veľmi komplikovaným právnym situáciám s nie jednoduchými a pozitívnymi praktickými dôsledkami z hľadiska spracúvania osobných údajov.

7. ZOZNAM LITERATÚRY

[1] MATTESON, S. *Autonomous versus automated: What each means and why it matters*. [online]. Dostupné z: https://www.techrepublic.com/article/autonomous-versus-automated-what-each-means-and-why-it-matters/ [citované 28.9.2020].

[2] TAEIHAGH, A. a SI MIN LIM, H. *Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks.* Transport Reviews, roč. 39. č. 1, 2019, s. 103-128.

[3] POLČÁK, R. *Odpovědnost umělé inteligence a informační útvary bez právní osobnosti.* In Bulletin Advokace 11/2018, s. 24. [on-line]. Dostupné z: http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2018/BA_11_2018_web.pdf. [citované 28.9.2020].

[4] COLLINGWOOD, L. *Privacy implications and liability issues of autonomous vehicles*. In Information & Communications Technology Law, roč. 26. č. 1, 2017, s. 32-45.

[5] KOUROUTAKIS, A. E. *Autonomous Vehicles; Regulatory Challenges and the Response From UK and Germany*. 46 Mitchell Hamline Law Review forthcoming. 2019.

[6] YEEFEN LIM, H. *Autonomous Vehicles and the Law Technology, Algorithms and Ethics.* Edward Elgar Publishing, 2018, 147 s.

[7] SKEETE, JP. Level 5 autonomy: *The new face of disruption in road transport.* In Technological Forecasting and Social Change, Elsevier, roč. 134(C), 2018, s. 22-34.

[8] VOSTOUPAL, J.: *Certifikace kyberbezpečnostních technologií. In* Revue pro právo a technologie. 2019, č. 20, s. 147-268. [on-line]. Dostupné z: https://journals.muni.cz/revue/article/view/12570 [citované 28.9.2020].

[9] CZARNECKI, K. *English Translation of the German Road Traffic Act Amendment Regulating the Use of "Motor Vehicles with Highly or Fully Automated Driving Function" from July 17, 2017* [on-line]. Dostupné z: https://www.researchgate.net/profile/Krzysztof_Czarnecki3/publication/320813344_English_Translation_of_the_German_Road_Traffic_Act_Amendment_Regulating_the_Use_of_Motor_Vehicles_with_Highly_or_Fully_Automated_Driving_Function_from_July_17_2017/links/59fbbe680f7e9b9968bb5a0f/English-Translation-of-the-German-Road-Traffic-Act-Amendment-Regulating-the-Use-of-Motor-Vehicles-with-Highly-or-Fully-Automated-Driving-Function-from-July-17-2017.pdf

[10] International Transport Forum and Corporate Partnership Board: *Autonomous Driving: Regulatory Issues*. 2015. [on-line]. Dostupné z: https://www.itf-oecd.org/sites/default/files/docs/15cpb_autonomousdriving.pdf. [citované 28.9.2020].POLČÁK, R. *Informace a data v právu*. Revue pro právo a technologie 7, 2016, s. 67–91.

[11] Autonomous Vehicles. State of Nevada Register of Administrative Regulations. § 82A. [on-line]. Dostupné z: https://www.leg.state.nv.us/NRS/NRS-482A.html#NRS482ASec036. [citované 28.9.2020].

[12] Nariadene Európskeho parlamentu a Rady (EÚ) 2018/858 z 30. mája 2018 o schvaľovaní motorových vozidiel a ich prípojných vozidiel, ako aj systémov, komponentov a samostatných technických jednotiek určených pre takéto vozidlá a o dohľade nad trhom s nimi, ktorým sa menia nariadenia (ES) č. 715/2007 a (ES) č. 595/2009 a zrušuje smernica 2007/46/ES

[13] Usmernenia týkajúce sa výnimky na schválenie automatizovaných vozidiel EÚ.

[14] Smernica Európskeho parlamentu a Rady 2010/40/EÚ o rámci na zavedenie inteligentných dopravných systémov v oblasti cestnej dopravy a na rozhrania s inými druhmi dopravy.

[15] Delegované nariadenie komisie ktorým sa dopĺňa smernica o inteligentných dopravných systémoch, pokiaľ ide o zavádzanie a prevádzkové využívanie kooperatívnych inteligentných dopravných systémov

[16] Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii

[17] Nariadenie Európskeho parlamentu a Rady o Agentúre EÚ pre kybernetickú bezpečnosť (ENISA), o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií

[18] SAE J3016:Sep 2016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles

[19] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov). In EUR-lex [právní informační system]. Úřad pro publikace Evropské unie. Dostupné z https://eur-lex.europa.eu/legal-content/SK/TXT/?qid=1584526623550&uri=CELEX%3A32016R0679

[20] TRAKMAN, Leon – WALTERS, Robert – ZELLER, Bruno: Tort and Data Protection Law: Are There Any Lessons to Be Learnt? *In European Data Protection Law Review 4/2019*.

[21] CORDEIRO, A.B. Menezes: Civil Liability for Processing of Personal Data in the GDPR *In European Data Protection Law Review 4/2019.*

[22] VAN ALSENOY, Brendan – DUMORTIER, Jos: The accountability principle in data protection regulation: origin, development and future directions. *In GUAGNIN,*

[23] *D. – HEMPEL, L. - ILTEN, C. (eds): Managing Privacy Through Accountability*. 2012, Palgrave Macmillian, s. 49 – 82.

[24] VAN ALSENOY, Brendan: Liability under EU Data Protection Law. *In 7 (2016) JIPITEC 271*.

[25] LAROUCHE, Pierre – PEITZ, Martin – PURTOVA, Nadya: *Consumer Privacy in network industries* – A CERRE Policy Report, 2016, Centre on Regulation in Europe. [Online] 2016. [cit. 29. 9. 2020]. Dostupné z: https://cerre.eu/wp-content/uploads/2016/01/160125_CERRE_Privacy_Final.pdf.

[26] Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode (smernica o elektronickom obchode). In EUR-lex [právní informační system]. Úřad pro publikace Evropské unie. Dostupné z https://eur-lex.europa.eu/legal-content/AUTO/?uri=CELEX:32000L0031&qid=1585224374231&rid=1.

[27] CUNHA, A. Maria Viola – MARIN, Luisa – SARTOR, Giovanni: Peer-to-peer privacy violations and ISP liability: data protection in the user-generated web. *In International Data Privacy Law,* Volume 2, Issue 2, 2012.

[28] Rozsudok Súdneho dvora zo dňa 13. mája 2014 Google Spain SL a Google Inc. proti Agencia Española de Protección de Datos (AEPD) a Mariovi Costejovi Gonzálezovi. Vec č. C-131/12.

[29] MAHIEU, René – HOBOKEN VAN, Joris - ASGHARI, Hadi: Responsibility for Data Protection in a Networked World. On the question of the Controller. „Effective and Complete Protection" and its Application to Data Access Rights in Europe. *In JIPITEC 39, 10 (2019*).

[30] Rozsudok Súdneho dvora Európskej únie zo dňa 29. júla 2019 Fashion ID GmbH & Co.KG proti Verbraucherzentrale NRW eV. Vec č. C-40/17.

[31] European Data Protection Board Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications. [Online]. 2020. [cit. 29. 9. 2020] Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-12020-processing-personal-data-context_en.

[32] Rozsudok Súdneho dvora Európkej únie zo dňa 5. júna 2018 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein proti Wirtschaftsakademie Schleswig-Holstein GmbH. Vec č. C-210/16.

[33] European Data Protection Board Guidelines 07/2020 on the concepts of controller and processor in the GDPR. [Online]. 2020. [cit. 29. 9. 2020]. Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.

[34] Article 29 Data Protection Working Party: Opinion 05/2014 on Anonymisation Techniques. [online]. 2014. [cit. 29. 9. 2020]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[35] European Data Protection Board: Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. [online]. 2020. [cit. 29. 9. 2020]. Dostupné z: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_en.

[36] ŽOLNERČÍKOVÁ, Veronika. Prokazování příčinné souvislosti u škod způsobených propojenými autonomními vozidly. *Revue pro právo a technologie*. [Online]. 2020, č. 21, s. 129-152. [cit. 2020-09-29]. Dostupné z: https://journals.muni.cz/revue/article/view/13048.

[37] CZARNECKI, Krzysztof. English Translation of the German Road Traffic Act Amendment Regulating the Use of "Motor Vehicles with Highly or Fully Automated Driving Function" from July 17, 2017. [Online]. [cit. 2020-09-29]. Dostupné z: https://www.researchgate.net/publication/320813344.

---

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

REVENGE PORN A DEEPFAKES: OCHRANA SOUKROMÍ V ÉŘE MODERNÍCH TECHNOLOGIÍ

MICHAELA DVOŘÁKOVÁ[1]

ABSTRAKT

Rozvoj moderních technologií je neodlučitelně spojen s novými způsoby zásahů do práva na soukromí. V uplynulých letech se mnoho lidí osobně setkalo s jedním z nich, fenoménem přezdívaným revenge porn (anebo obecněji nekonsenzuální pornografie). Po internetu byly totiž šířeny jejich intimní anebo sexuální fotografie či videa, která buďto někdo nedovoleně rozšířil, anebo dokonce i pořídil bez jejich vědomí. Od roku 2017 je hrozba v tomto směru ještě o poznání větší, a to z důvodu rozvoje technologie deepfake, která umožňuje takové záznamy dokonce uměle vytvářet. A přestože představuje i jiná rizika, prozatím se rozšířila převážně v oblasti nedovoleně vytvářených sexuálních záznamů. Téměř kdokoliv tak na internetu může v budoucnu najít pornografické video, v němž účinkuje, aniž by jej kdy natočil. Taková skutečnost pochopitelně zakládá znatelný zásah do práva na soukromí. Otázkami ohledně rozvoje pornografických deepfakes a souvisejícími právními aspekty se tento článek zabývá.

KLÍČOVÁ SLOVA

nekonsenzuální pornografie, revenge porn, technologie deepfake, pornografická deepfake videa, ochrana soukromí, nekontaktní sexuální násilí, image-based sexual abuse (IBSA)

[1] Mgr. Bc. Michaela Dvořáková je doktorandkou na Katedře ústavního práva a politologie Právnické fakulty Masarykovy univerzity a asistentkou soudce Nejvyššího správního soudu, e-mail: 407928@mail.muni.cz.

ABSTRACT

The development of modern technologies is inextricably linked to new means of privacy rights invasions. In recent years, many people have personally experienced one of them, the phenomenon of revenge porn (or more generally non-consensual pornography). Their intimate and/or sexual photographs or video records, which were either shared without their permission, or even taken without their knowledge, were distributed on the Internet. Since 2017, the threat has become even greater, due to the development of deepfake technology allowing to artificially create such recordings. Although it poses risks in different areas as well, it has so far predominantly spread in the area of illicitly created sexual recordings. In the future, almost anyone can find a pornographic video starring himself on the Internet, without him ever making one. Such eventuality naturally constitutes a significant interference with the right to privacy. This article addresses issues regarding the development of pornographic deepfakes and related legal aspects.

KEYWORDS

non-consensual pornography, revenge porn, deepfake technology, deepfake pornography videos, privacy protection, non-contact sexual violence, image-based sexual abuse (IBSA)

1. ÚVOD

V roce 2014 na internet uniklo ohromné množství intimních fotografií stovek slavných žen, které hackeři stáhli z online úložišť, do nichž se nabourali.[2] Tato vysoce medializovaná aféra (přezdívaná *„celebgate“* anebo *„nudegate“*) se stala ukázkou toho, v čem spočívá a jaký účinek má tzv. *revenge porn*, tedy nedovolené šíření sexuálních fotografií či videozáznamů určité osoby. V roce 2019 už bylo možno na internetu zhlédnout slavné he-

[2] LENHART, Amanda; YBARRA, Michelle; PRICE-FEENEY, Myeshia. Nonconsensual Image Sharing: one in 25 Americans has been a victim of “Revenge Porn“. In: *Data & Society Research Institute* [online]. 13. 12. 2016 [cit. 28. 4. 2020], s. 3. Dostupné z: https://datasociety.net/pubs/oh/Nonconsensual_Image_Sharing_2016.pdf

rečky (např. Emmu Watson, Scarlett Johansson,[3] Gal Gadot, Masie Williams, Daisy Ridley a mnoho dalších[4]) v pornografických videích. A to, aniž by jakákoliv taková videa někdy natočily. Objevil se totiž nový inteligentní algoritmus, který umožnil rozvoj tzv. *deepfakes* – vysoce realistických, avšak uměle vytvořených videí. A tato technologie se rozšířila právě v oblasti pornografie.

Co mají oba pojmy, tedy *revenge porn* a pornografická *deepfakes* společného? Zaprvé, z převážné většiny jsou jejich oběťmi ženy.[5] Zadruhé, jejich podstata je velmi obdobná. Zjednodušeně řečeno spočívají v nedovoleném vytváření anebo šíření sexuálních záznamů vyobrazujících osobu, která k jejich vytváření anebo šíření nedala souhlas. Tímto způsobem samozřejmě dochází zejména k podstatnému zásahu do soukromí jednotlivce, který je mnohonásobně zesílen užíváním moderních technologií.[6] Dopady, které takové jednání může mít na životy obětí, jsou přitom podle odborníků srovnatelné s dopady sexuálního zneužívání.[7] Přestože popsaný zásah do soukromí míří do oblasti lidské sexuality a intimní individuality, kterou Evropský soud pro lidská práva (dále "ESLP") nazývá *„nejintimnější sférou jednotlivce“*,[8] neexistuje proti němu účinná, efektivní a rychlá ochrana. Internet totiž nezapomíná.[9] Oběti *revenge porn a* pornografických *deepfakes* tak jsou ponechány v boji s větrnými mlýny. Z popisu jejich zkušeností vy-

---

[3] SPIVAK, Russell. “Deepfakes": The Newest Way to Commit One of the Oldest Crimes. *Georgetown Law Technology Review* [online]. 2019, roč. 3,č. 2 [cit. 27. 4. 2020], s. 345-346. Dostupné z: https://georgetownlawtechreview.org/wp-content/uploads/2019/05/3.1-Spivak-pp-339-400.pdf

[4] Tamtéž, s. 339.

[5] DELFINO, Rebecca. Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn’s Next Tragic Act. *Fordham Law Review* [online]. 2019, roč. 88, 3 [cit. 27. 4. 2020], s. 896. Dostupné z: https://ir.lawnet.fordham.edu/flr/vol88/iss3/2/

[6] Srov. MCGLYNN, Clare; RACKLEY, Erika. Image-Based Sexual Abuse. *Oxford Journal of Legal Studies* [online]. 2017, roč. 37, 3 [cit. 27. 4. 2020], s. 560-561. Dostupné z: https://academic.oup.com/ojls/article-abstract/37/3/534/2965256?redirectedFrom=fulltext

[7] BATES, Samantha. Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors. *Feminist Criminology* [online]. 2017, roč. 12, 1 [cit. 27. 4. 2020], s. 31. Dostupné z: http://journals.sagepub.com/doi/abs/10.1177/1557085116654565

[8] Rozsudek Evropského soudu pro lidská práva ze dne 22. 10. 1981. Dudgeon vs. Spojené království. ECHR 7525/76. In: *HUDOC* [online]. Evropský soud pro lidská práva [cit. 29. 4. 2020], bod 52. Dostupné z: http://hudoc.echr.coe.int/eng?i=001-57473

plývá, až ačkoliv se jim třeba podařilo dosáhnout odstranění jejich nedovoleně šířeného sexuálního záznamu z webových stránek,[10] na nichž byl uveřejněn, nadále žily v nekonečné obavě z toho, kdy a kde se tento materiál zase vynoří.[11] V tomto směru dle svých slov zažívaly pocit ztráty kontroly nad tím, kdo vše záznam uvidí.[12] Mimo jiné i proto se tak mnozí z těch, kteří tento moderní fenomén zažili na vlastní kůži, museli např. stáhnout z veřejného života anebo online prostředí, změnit práci, přestěhovat[13] se či se potýkali s vážnými mentálními problémy.[14] A někteří z nich dokonce spáchali sebevraždu.[15]

Tento článek nejprve popíše, jaké typy jednání lze za nekonsenzuální pornografii označit, v čem spočívají a jakým způsobem k nim může docházet. Poté se bude podrobněji věnovat tématu *deepfake* pornografie, která se zkoumanou problematikou úzce souvisí. Jelikož se v českém právním prostředí jedná o první text, který se pornografickým *deepfake* videím věnuje, pokusí se autorka stručně nastínit i formy zásahu do individuálních práv na straně oběti a prostředky, jimiž se proti tomu lze bránit.

2. *REVENGE PORN* A NEKONSENZUÁLNÍ PORNOGRAFIE

Hned na začátku tohoto článku je nutno vysvětlit užívanou terminologii.[16] Přestože termín *revenge porn* (česky „pornopomsta“) je mezi laickou veřejností extenzivně užíván pro popis všech případů nedovoleného šíření se-

[9] ROSEN, Jeffrey. The Web Means the End of Forgetting. In: *The New York Times Magazine* [online]. 21. 7. 2010 [cit. 27. 4. 2020]. Dostupné z: https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html

[10] Zejména v zahraničí vznikly dokonce specializované webové stránky sloužící pro zveřejňování a sdílení *revenge porn*, tzv. *„revenge porn sites“*. Srov. WINKLEY, Lyndsay; LITTLEFIELD, Dana. Sentence revised for revenge porn site operator. In: *The San Diego Union-Tribune* [online]. 21. 9. 2015 [cit. 27. 4. 2020]. Dostupné z: http://www.sandiegouniontribune.com/sdut-kevin-bollaert-revenge-porn-case-resentencing-2015sep21-story.html

[11] BATES, op. cit., s. 31.

[12] Tamtéž, s. 33-34.

[13] MCGLYNN, RACKLEY, op. cit., s. 545.

[14] BATES, op. cit., s. 31-33.

[15] MCGLYNN, RACKLEY, op. cit., s. 545.

[16] S ohledem na poněkud krkolomné překlady některých pojmů užívá autorka tohoto textu převážně anglickou terminologii.

xuálních záznamů (a v tomto směru představuje určitou mediální zkratku, užitou i v názvu tohoto článku), je vhodnější hovořit buďto o tzv. nekonsenzuální pornografii,[17] anebo tzv. *„image-based sexual abuse"* („IBSA", v překladu „sexuální zneužívání založené na obrazovém znázornění").[18] Poslední uvedený termín nejvíce vystihuje podstatu problému a zároveň zastřešuje naprostou většinu případů nedovoleného vytváření anebo šíření sexuálních záznamů jiné osoby.[19] Pojem *revenge porn* totiž naznačuje, že k jednání dochází za účelem pomsty (*„revenge"*), což může být poněkud zavádějící. Přestože tomu tak mnohdy může být (jak bude rozebráno níže), není to podmínkou ve všech případech, a podle některých autorů není žádoucí užívat pojmosloví zaměřené na úmysl pachatele, a nikoliv na újmu na straně oběti.[20] Není však účelem tohoto článku rozhodnout, který z užívaných pojmů je pro označování zkoumané problematiky vhodnější. Pojmy nekonsenzuální pornografie, *revenge porn* (*largo sensu*, nikoliv pouze za účelem pomsty) a IBSA bude autorka používat jako vzájemná synonyma, a to vzhledem k tomu, že se všechny užívají v zahraničních odborných textech, které se tomuto tématu věnují.[21] K nim přidává ještě další, poněkud deskriptivní pojem „nedovolené šíření sexuálních záznamů".

V čem zkoumaná problematika vlastně spočívá? Nekonsenzuální pornografií je v principu šíření snímků se sexuálním vyobrazením jedince bez jeho souhlasu.[22] Takové jednání můžeme obecně charakterizovat jako jednu z forem nekontaktního sexuálního násilí,[23] která může mít závažné dopady nejen do práv jednotlivce, ale i do jeho postavení v rámci společnosti, dů-

---

[17] CITRON, Danielle Keats; FRANKS, Mary Anne. Criminalizing Revenge Porn. *Wake Forest Law Review* [online]. 2014, roč. 49, [cit. 27. 4. 2020], s. 346. Dostupné z: http://repository.law.miami.edu/cgi/viewcontent.cgi?article=1059&context=fac_articles

[18] MCGLYNN, RACKLEY, op. cit., s. 535-544.

[19] Tamtéž, s. 536-537.

[20] Tamtéž.

[21] Terminologickou problematiku zkoumaného tématu blíže vysvětlují HENRY, Nicola; FLYNN, Asher; POWELL, Anastasia. *Responding to 'revenge pornography': Prevalence, nature and impacts* [online]. Canberra: Australian Research Council, 2019 [cit. 27. 4. 2020], s. 12-14. Dostupné z: https://www.crg.aic.gov.au/reports/CRG_08_15-16-FinalReport.pdf

[22] FRANKS, Mary Anne. Combating Non-Consensual Pornography: A Working Paper. In: *SSRN* [online]. 7. 9. 2014 [cit. 27. 4. 2020], s. 3. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2336537

stojnosti a pocitu vlastní hodnoty. Tento zásah je obzvlášť citlivý, neboť se dotýká lidské sexuality, touhy po vlastním sebeurčení a mnohdy i ohrožení na pocitu osobního bezpečí, a to dokonce i v reálném, fyzickém světě. Skutečnost, že se po internetu mohou šířit vaše intimní anebo sexuálně explicitní snímky a videa (ať už skutečná, nebo uměle vytvořená) se tedy zásadně liší např. od neoprávněného nakládání s osobními údaji či od pomluvy,[24] a to kvůli tomu, že podstata tohoto jednání leží právě v oné sexuální oblasti. Jednoduše řečeno, pokud by obsah nekonsenzuální pornografie nezobrazoval něco, co je běžně cizím očím skryto a co je považováno ryze za soukromé, nebyl by tento typ jednání natolik populární a nezpůsoboval by tak závažnou újmu na straně obětí.

Z amerického výzkumu z roku 2017 vyplynulo, že 8 % všech dotázaných v minulosti čelilo nedovolenému šíření svých intimních či sexuálních záznamů a dalším 5 % dotázaných bylo takovým jednáním alespoň vyhrožováno.[25] Zároveň se ukázalo, že se oběťmi tohoto jednání stávají výrazně častěji ženy[26, 27] anebo příslušníci LGBT komunity.[28] Mnohdy navíc nezůstane „jen“ u samotného šíření takového typu záznamu, často musí oběti čelit dalším souvisejícím projevům, kterými může být ponižování, šikana, nedovolené pronásledování, vyhrožování či vydírání. Oběti uveřejnění nekonsenzuální pornografie jsou mnohdy navíc vystaveny množství verbálního násilí, které má nejen dehonestující charakter, ale může ob-

[23] POWELL, Anastasia; HENRY, Nicola. *Sexual Violence in a Digital Age* [online]. Basingstoke: Palgrave Macmillan, 2017 [cit. 27. 4. 2020], s. 61. Dostupné z: https://link.springer.com/book/10.1057%2F978-1-137-58047-4

[24] V tomto kontextu je nutno vysvětlit, že právě tyto skutkové podstaty spadají do Hlavy II dílu 2 zákona č. 40/2009 Sb., trestního zákoníku, která mj. zajišťuje ochranu osobnosti, soukromí a listovního tajemství.

[25] EATON, Asia A.; JACOBS, Holly; RUVALCABA, Yanet. 2017 Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration. A Summary Report. In: *Cyber Civil Rights Initiative* [online]. ©2017 [cit. 27. 4. 2020], s. 11. Dostupné z: https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf

[26] EATON, JACOBS a RUVALCABA, op. cit., s. 12, anebo MCGLYNN, RACKLEY, op. cit., s. 544.

[27] Někteří autoři však upozorňují, že se oběťmi uveřejnění nekonsenzuální pornografie stávají obdobně často i muži. V jejich případě ale dochází výrazně méně častěji k vyhrožování z uveřejnění těchto záznamů. Viz LENHART, YBARRA a PRICE-FEENEY, op. cit., s. 5.

[28] Tamtéž.

sahovat i výhružky znásilněním.[29] Ti, kteří se stanou oběťmi tohoto jednání, tak zažívají skutečný strach, někteří se obávají vycházet z domu[30] a často musí měnit své životy a zažité zvyky. Bývalá americká kongresmanka Katie Hill rezignovala na svůj mandát poté, co bulvární a pravicová média zveřejnila intimní fotografie, na nichž je zobrazena se svou bývalou podřízenou. V poslední řeči na půdě Sněmovny reprezentantů uvedla, že úřad opouští kvůli *„tisícům odporných, vyhrožujících e-mailů, hovorů a zpráv,"* které v ní vyvolaly *„strach o vlastní život a život jejích blízkých."* Dodala, že je vyděšená, neboť poprvé od uveřejnění uvedených snímků opustila svůj byt.[31]

Oběti IBSA se také musí často vypořádat s posttraumatickým syndromem, úzkostí, depresemi a sebevražednými tendencemi, nikoliv nepodobnými stavům, které zažívají oběti fyzických sexuálních útoků.[32] Jak bylo navíc zmíněno v úvodu, některé příběhy obětí nekonsenzuální pornografie dokonce končí předčasnou smrtí. Například Italka Tiziana Cantone spáchala v roce 2016 sebevraždu poté, co se stala předmětem širokého virálního posměchu kvůli obsahu uniklého soukromého videa, na kterém provozuje sexuální aktivity a které se stalo internetovou senzací.[33] Lze zmínit i dva případy z roku 2013. Sedmnáctiletá Brazilka Julia Rebecca se oběsila po úniku své sexuální nahrávky[34] a stejně starý Daniel Perry ze Skotska skočil z mostu pod tlakem vydírání uveřejnění jeho explicitní nahrávky, kterou útočníci lstí pořídili přes online aplikaci *Skype*.[35]

---

[29] CITRON, FRANKS, op. cit., s. 353.

[30] Tamtéž, s. 351.

[31] GESSEN, Masha. The Terrorization of Katie Hill. In: *The New Yorker* [online]. 5. 11. 2019 [cit. 27. 4. 2020]. Dostupné z: https://www.newyorker.com/news/our-columnists/the-terrorization-of-katie-hill

[32] BATES, op. cit., s. 31-33.

[33] REYNOLDS, James. Italy's Tiziana: Tragedy of a woman destroyed by viral sex video. In: *BBC* [online]. 13. 2. 2017 [cit. 27. 4. 2020]. Dostupné z: http://www.bbc.com/news/world-europe-38848528

[34] BERGER, Miriam. Brazilian 17-Year-Old Commits Suicide After Revenge Porn Posted Online. In: *BuzzFeed News* [online]. 20. 11. 2013 [cit. 27. 4. 2020]. Dostupné z: https://www.buzzfeed.com/miriamberger/brazilian-17-year-old-commits-suicide-after-revenge-porn-pos?utm_term=.lxoO1z9r4#.txZ2n7aGr

Z popsaných případů se může zdát, že se tento fenomén České republice vyhýbá. Bohužel tomu tak není, přestože se mu zde nedostává takové pozornosti jako v zahraničí. V roce 2013 vzniklo na sociální síti Facebook několik stránek, jejichž účelem bylo sdílet uživateli zaslané fotografie tzv. „roztahovaček" (údajně promiskuitních dívek z okolí). Tyto stránky byly vždy zaměřeny na určitou lokalitu, zejména konkrétní město (např. „brněnské roztahovačky") a na nich uveřejněné fotografie zobrazovaly dívky (často středoškolačky, některé mladší 15 let) nahé, obnažené či v jiných vyzývavých pózách. Tyto fotografie doprovázely i hanlivé komentáře k vyobrazeným dívkám, případně přímé odkazy na jejich facebookové profily.[36] Facebook tyto stránky následně na základě oznámení zrušil, nicméně bulvární média v mezičase stihla o celé záležitosti na svých portálech informovat jako o senzaci, přičemž články doplnila těmito nedovoleně uveřejněnými fotografiemi. Po zrušení facebookých stránek některá z těchto médií dokonce dále čtenáře odkázala na nově vzniklé internetové stránky, kam byly fotografie přesunuty.[37] Policie také v posledních letech opakovaně upozorňuje na riziko zneužití intimních fotografií zaslaných v soukromé konverzaci anebo jinak zpřístupněných, které mohou být šířeny anebo mohou vést k vydírání oběti vyhrožováním jejich zveřejněním. Z webových stránek Policie ČR je patrné, že i u nás k jednání spadajícímu pod nekonsenzuální pornografii dochází poměrně často.[38] Jelikož však může nabývat různých podob a jejich vzájemná souvislost nemu-

[35] SMITH-SPARK, Laura; VANDOORNE, Saskya. Reports: Teen Daniel Perry commits suicide over Skype blackmail scam. In: *CNN* [online]. 16. 8. 2013 [cit. 27. 4. 2020]. Dostupné z: https://edition.cnn.com/2013/08/16/world/europe/uk-cyber-blackmail-suicide/index.html

[36] ŽLÁBKOVÁ, Ludmila. Snímky polonahých dívek od zhrzených partnerů zaplavily český internet. In: *Novinky.cz* [online]. 9. 11. 2014 [cit. 27. 4. 2020]. Dostupné z: https://www.novinky.cz/internet-a-pc/352987-snimky-polonahych-divek-od-zhrzenych-partneru-zaplavily-cesky-internet.html

[37] Například server pořadu Prásk televize Nova.cz s článkem nazvaným „*Kam zmizely všechny roztahovačky?*", který je dnes již nedostupný. Srov. DVOŘÁKOVÁ, Michaela. *Právo na informační sebeurčení a nedovolené šíření sexuálních záznamů* [online]. Brno, 2018 [cit. 29. 4. 2020]. Diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Kateřina ŠIMÁČKOVÁ, s. 20. Dostupné z: https://is.muni.cz/th/t361z/

sí být zřejmá, následující podkapitola vymezí, jaké všechny druhy jednání pod nekonsenzuální pornografii neboli tzv. *„image-based sexual abuse“* patří.

2.1 TYPOLOGIE *„IMAGE-BASED SEXUAL ABUSE“*

Jednání naplňující podstatu IBSA[39] může mít typově tři různé formy: 1) vytváření sexuálních záznamů bez souhlasu vyobrazené osoby, 2) zveřejnění, šíření anebo sdílení sexuálních záznamů bez souhlasu vyobrazené osoby, 3) vyhrožování zveřejněním, šířením anebo sdílením sexuálních záznamů jiné osoby.[40] V praxi nebývají mnohdy tyto druhy odděleny, naopak dochází k jejich vzájemné kombinaci a zároveň k prolínání s dalšími níže popsanými kategoriemi. K tomu je ještě nutno dodat, že ačkoliv k těmto druhům jednání může docházet i bez užití moderních technologií,[41] jejich všudypřítomná dostupnost je značně usnadňuje a urychluje.[42]

IBSA lze dále rozlišovat[43] z hlediska okolností, za nichž k předmětnému jednání dochází. První skupinu tak tvoří jednání spočívající v určité „vztahové odplatě“,[44] v tomto případě se tedy jedná o *revenge porn stricto sensu*. Typickým příkladem je, že osoba v průběhu vztahu zašle partnerovi své intimní fotografie, který je po následném rozchodu rozešle jiným lidem

---

[38] Srov. Např.: JANDA, Petr. Zneužití fotografie. In: *Policie České republiky – KŘP Královéhradeckého kraje* [online]. 7. 3. 2012 [cit. 29. 4. 2020]. Dostupné z: https://www.policie.cz/clanek/zneuzite-fotografie.aspx; MATZNER, Jiří. Vydírá expřítelkyni zveřejněním intimních fotografií. In: *Policie České republiky – KŘP Jihočeského kraje* [online]. 3. 5. 2015 [cit. 29. 4. 2020]. Dostupné z: http://www.policie.cz/clanek/vydira-expritelkyni-zverejnenim-intimnich-fotografii.aspx; BURÝŠKOVÁ, Lenka. Vydíral ženu přes facebook. In: *Policie České republiky – KŘP Královéhradeckého kraje* [online]. 2. 9. 2016 [cit. 29. 4. 2020]. Dostupné z: http://www.policie.cz/clanek/vydiral-zenu-pres-facebook.aspx; KYŠNEROVÁ, Simona. Vydíral ji jejími nahými fotkami. In: *Policie České republiky – KŘP Zlínského kraje* [online]. 12. 1. 2017 [cit. 29. 4. 2020]. Dostupné z: http://www.policie.cz/clanek/vydiral-ji-jejimi-nahymi-fotkami.aspx; ZÁMEČNÍK, Petr. Začalo to nevinně. In: *Policie České republiky – KŘP Jihomoravského kraje* [online]. 23. 3. 2018 [cit. 29. 4. 2020]. Dostupné z: https://www.policie.cz/clanek/zacalo-to-nevinne.aspx; DRAHOKOUPILOVÁ, Lenka. Prozrazení hesla se jí nevyplatilo. In: *Policie České republiky – KŘP Jihomoravského kraje* [online]. 12. 12. 2019 [cit. 29. 4. 2020]. Dostupné z: https://www.policie.cz/clanek/prozrazeni-hesla-se-ji-nevyplatilo.aspx

[39] Autorka typologie, z níž tento článek vychází, používá pro nedovolené šíření sexuálních záznamů pojem IBSA, proto se v této podkapitole jedná o převažující termín popisující zkoumané jednání. Jak však bylo vysvětleno výše, jedná se významově o synonymum k pojmům nekonsenzuální pornografie anebo *revenge porn*. Viz POWELL, HENRY, op. cit., s. 120-132.

[40] Tamtéž, s. 120.

(např. přátelům, rodině či zaměstnavateli vyobrazené osoby), anebo je zveřejní na sociální sítě či jiné internetové stránky.[45] Samozřejmě se však může jednat i o jiné situace, významným faktorem však je vzájemný vztah mezi tím, kdo se IBSA v tomto případě dopouští, a jeho obětí.[46] V tomto případě tak lze předpokládat jako hlavní motiv snahu oběti co nejvíce ublížit. Proto nezřídka dochází i ke zveřejnění jejích osobních anebo kontaktních údajů (případně odkazů na profil na sociální síti),[47] či dokonce falešných „pornoinzerátů" nabízejících sexuální služby.[48] To umožňuje, aby jiné osoby oběť IBSA kontaktovaly, případně se vůči nim dopouštěly nedovoleného pronásledování (tzv. *stalkingu*).[49]

---

[41] Již v 80. letech 20. stol. zavedl například americký magazín *Hustler's* rubriku nazvanou *„Beaver Hunt"*, do které čtenáři přispívali fotografiemi nahých žen ze svého okolí. Viz LEWENDOWSKI, Amanda. Our Best Weapon Against Revenge Porn: Copyright Law?. In: *The Atlantic* [online]. 4. 2. 2014 [cit. 29. 4. 2020]. Dostupné z: https://www.theatlantic.-com/technology/archive/2014/02/our-best-weapon-against-revenge-porn-copyright-law/283564/

[42] POWELL, HENRY, op. cit., s. 120.

[43] V úvahu připadají i další různá dělení, např. z hlediska formy šíření záznamu (např. soukromou zprávou, zveřejněním na veřejné internetové stránce, zveřejněním na osobním profilu na sociální síti), nebo třeba z hlediska toho, nakolik „nahá" a sexuálně explicitně vyobrazená osoba na záznamu je, případně při jaké činnosti (např. ve sprše anebo při sexuálním aktu). Srov.: HENRY, FLYNN, POWELL, op. cit., s. 14.

[44] Tamtéž.

[45] POWELL, HENRY, op. cit., s. 121.

[46] Srov. BATES, op. cit., s. 29.

[47] Podle amerického výzkumu z roku 2013 bylo v 60 % případů *revenge porn* zveřejněno celé jméno vyobrazené osoby, v 50 % právě odkaz na profil na sociálních sítích. Ve 20 % případů bylo zveřejněno telefonní číslo oběti, v 15 % pak adresa jejího bydliště či pracoviště. Srov. 2013 NCP Study Results. In: *Cyber Civil Rights Initiative* [online]. ©2018 [cit. 27. 4. 2020]. Dostupné z: https://www.cybercivilrights.org/wp-content/uploads/2016/11/NCP-2013-Study-Research-Results-1.pdf

[48] Na tomto místě je samozřejmě nutno připomenou kauzu bývalého fotbalisty Tomáše Řepky, který společně se svou současnou přítelkyní vytvořil na internetu falešný inzerát nabízející sexuální služby pod jménem své bývalé manželky. Za to a další trestnou činnost byl v roce 2019 odsouzen k nepodmíněnému trestu odnětí svobody. Více viz: Tomáš Řepka půjde do vězení, odvolací soud mu zvýšil trest. In: *iROZHLAS* [online]. 30. 4. 2019 [cit. 30. 4. 2020]. Dostupné z: https://www.irozhlas.cz/sport/fotbal/tomas-repka-vezeni-odvolaci-soud-2-roky-sparta-praha-zpronevera_1904301028_vman

[49] Jedna z žen, která se stala obětí IBSA, popsala, že za ní domů chodili cizí muži žádající o sexuální aktivity. Jeden z nich se k ní vloupal a škrtil ji. Její bývalý přítel těmto mužům totiž rozesílal její nahé fotografie a adresu bydliště společně s nabídkou sexu. Viz BATES, op. cit., s. 32.

Dalším druhem IBSA je sexuální vydírání neboli *„sextortion“*.[50] Jeho předmětem je vyhrožování zveřejněním anebo šířením sexuálních fotografií či videozáznamů, na nichž je daná osoba vyobrazena. Ta je tak nucena např. k zaslání dalšího (třeba i více „odvážného“) materiálu, k osobnímu setkání, anebo nezřídka i k fyzickým sexuálním aktivitám.[51, 52] Tuto formu IBSA (v podobě vydírání a následném zveřejnění zaslaných snímků) mohli diváci vidět v dokumentárním filmu *V síti* tvůrců Víta Klusáka a Barbory Chalupové, který se zabývá sexuálními predátory vyhledávajícími na internetu nezletilé děti. Odborníci upozorňují, že právě v případě dětí představuje sexuální vydírání závažné riziko, neboť jsou snáze manipulovatelné a neumějí se proti takovému jednání samy bránit.[53] Pro úplnost je nutno dodat, že tato forma IBSA spadá pod obecnou problematiku vydírání, ke které dochází i v jiných oblastech lidského života. I v tomto případě je však dopad takového vydírání specifický tím, že se dotýká velmi citlivé otázky lidské sexuality.

Mezi IBSA dále spadá tzv. sexuální voyeurismus (ve smyslu užívání moderních technologií, nikoliv pouhého pozorování jiných osob). Ten spočívá ve vytváření intimních, sexuálních, sexuálně explicitních anebo pornografických materiálů vyobrazujících osobu, která k jejich vytvoření neudělila souhlas. Projevuje se dále tím, že v jeho případě schází úmysl, aby se oběť o tomto jednání dozvěděla.[54] Takový záznam má sloužit spíše pro privátní účely (zejména sexuální gratifikaci), a to buďto pro toho, kdo jej

---

[50] POWELL, HENRY, op. cit., s. 120-132.

[51] CITRON, Danielle Keats. Sexual Privacy. *The Yale Law Journal* [online]. 2018-2019, roč. 128, 7 [cit. 29. 4. 2020], s. 1924. Dostupné z: https://www.yalelawjournal.org/article/sexual-privacy

[52] Viz např.: LADMANOVÁ, Dana. Důvěřivé ženy. In: *Policie České republiky – KŘP Plzeňského kraje* [online]. 27. 12. 2017 [cit. 29. 4. 2020]. Dostupné z: http://www.policie.cz/clanek/duverive-zeny.aspx

[53] Podle výzkumu Centra prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého se pouze necelých 33 procent dětí svěří jiné osobě s tím, že někdo zneužil jejich intimní fotografie. Viz KOPECKÝ, Kamil; SZOTKOWSKI, René. Sexting a rizikové seznamování českých dětí v kyberprostoru. Výzkumná zpráva. In: *Univerzita Palackého v Olomouci ve spolupráci se společností 02 Czech Republic* [online]. ©2017 [cit. 29. 4. 2020]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/96-sexting-a-rizikove-seznamovani-2017/file

[54] POWELL, HENRY, op. cit., s. 120-132.

vytvořil, anebo i pro další osoby. Do této kategorie spadají záznamy ze skrytých kamer (např. v převlékárnách či převlékacích kabinkách, anebo pořízené skrytou kamerou při konsenzuální sexuální aktivitě), tajné sledování jiných osob skrze webkameru[55] anebo získání nedovoleného přístupu k intimním anebo sexuálním záznamům jiné osoby (např. „nabouráním" se do soukromého úložiště). Ve všech těchto případech je z povahy věci zřejmé, že k takto vytvořenému záznamu vyobrazená osoba neudělila souhlas, neboť o něm zpravidla vůbec neví.[56] U jejich vytváření je typické, že k nim dochází v situaci, kdy má oběť buďto očekávání soukromí a z něj plynoucího bezpečí (v případě „nabourání" počítačové webkamery[57] anebo nafilmování konsenzuální sexuální aktivity bez vědomí jednoho ze zúčastněných), anebo sice na veřejném místě, avšak za očekávání určitého soukromí (např. skrytá kamera umístěná v převlékárně či převlékací kabince). V tomto bodě se však poněkud odlišuje další typ jednání spadající pod sexuální voyeurismus, kterým je tzv. *„upskirting"* a tzv. *„down-blousing"*.[58] V obou těchto případech jde o pořizování fotografií či videozáznamů těla jiné osoby pod oblečením (pod sukní, resp. za výstřihem), a to většinou mobilním telefonem na veřejném místě,[59] např. v hromadných dopravních prostředcích anebo na eskalátorech. Tyto záznamy tedy sice vznikají na místě, na němž nelze příliš soukromí očekávat, avšak způsobem, který na-

[55] O takovém případě u nás rozhodoval Nejvyšší soud. Jednalo se o to, že pronajímatel bytu umístil za zrcadlem v koupelně zařízení umožňující sledování nájemníků bez jejich vědomí a souhlasu za účelem vlastního sexuálního uspokojování. Srov. usnesení Nejvyššího soudu ze dne 14. 7. 2015, sp. zn. 4 Tdo 843/2015.

[56] MCGLYNN, RACKLEY, op. cit., s. 543.

[57] V již zmiňovaném filmu *V síti* popsala jedna z hereček, že když jí bylo 12 let, naboural se jí starší muž do webkamery. Přes tu ji bez jejího vědomí sledoval a potají nahrával, a to při převlékání či masturbaci. Později vyžadoval osobní schůzku a když dívka nepřišla, začal ji těmito záznamy vydírat. Viz HLAVÁČOVÁ, Veronika; DUCHKOVÁ, Anna. Internetový sexuální predátor se mi naboural do webkamery a sledoval, jak se převlékám, říká Monika. In: *iROZHLAS* [online]. 2. 3. 2020 [cit. 29. 4. 2020]. Dostupné z: https://www.irozhlas.cz/zivotni-styl/spolecnost/internetovy-sexualni-predator-serial-pojd-si-semnou-psat-webkamera-v-siti_2003021909_jgr

[58] CITRON, op. cit., s. 1914.

[59] KIRCHENGAST, Tyrone; CROFTS, Thomas. The legal and policy contexts of 'revenge porn' criminalisation: the need for multiple approaches. *Oxford University Commonwealth Law Journal* [online]. 2019, roč. 19, 1 [cit. 28. 4. 2020], s. 5. Dostupné z: https://www.tandfonline.com/doi/abs/10.1080/14729342.2019.1580518?journalCode=rouc20

rušuje hranice mezi tím, co je i ve veřejném prostoru soukromé, a tím, co je ve veřejném prostoru veřejné. Záznam nahého těla vyfoceného pod oblečením je v tomto směru porušením soukromí vyobrazené osoby i přesto, že vznikl na veřejném místě, neboť i ve veřejném prostoru existuje sféra soukromí,[60, 61] která není určena očím veřejnosti, pokud se člověk nerozhodne ji veřejnosti odhalit.[62,63]

Další kategorií IBSA je tzv. *„sexploitation"*. Ta může kloubit výše uvedené případy, avšak takto získané sexuální záznamy zveřejňuje, šíří anebo sdílí za účelem zisku.[64] Za tímto záměrem vznikly v zahraničí mnohé specializované internetové stránky. Například na serveru *UGotPosted.com* byly zveřejňovány sexuální záznamy vyobrazující osoby, které k tomu neudělily souhlas, a to společně s jejich osobními a kontaktními informacemi. Když následně tyto osoby žádaly o jejich smazání, server je odkazoval na stránku *ChangeMyReputation.com*, která po nich za stažení materiálu požadovala zaplatit stovky dolarů.[65] V tomto kontextu je zároveň nutno podotknout, že k *„sexploitation"* může docházet i na známých pornografických stránkách, neboť v kategorii amatérských videí je mnohdy velmi obtížné, anebo dokonce nemožné odlišit konsenzuálně natočená videa od těch nekonsenzuálních.[66]

Na závěr této typologie z hlediska okolností vzniku IBSA rozlišit ještě jeden, nejvíce znepokojující typ. Tím je záznam, distribuce anebo vy-

---

[60] K tomu srov. NISSELBAUM, Helen. Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy* [online]. 1998, roč. 17, 5/6 [cit. 29. 4. 2020], s. 559-596. Dostupné z: https://www.jstor.org/stable/3505189?seq=1#metadata_info_tab_contents

[61] K tomu dále srov. rozsudek Evropského soudu pro lidská práva ze dne 28. 1. 2003. Peck vs. Spojené království. ECHR 44647/98. In: *HUDOC* [online]. Evropský soud pro lidská práva [cit. 29. 4. 2020], bod 62. Dostupné z: http://hudoc.echr.coe.int/eng?i=001-60898

[62] Danielle Citron zdůrazňuje, že takové jednání odnímá obětem „sexuální svobodu", neboť podrývá jejich osobní rozhodnutí skrýt své genitálie a ňadra před zraky veřejnosti. V důsledku toho tak nemají kontrolu nad svou sexuální autonomií a konsentem. CITRON, op. cit., s. 1914.

[63] K tomu dále srov. MCGLYNN, RACKLEY, op. cit., s. 542-543.

[64] POWELL, HENRY, op. cit., s. 128.

[65] Tamtéž, s. 128-129.

[66] Tamtéž, s. 129.

hrožování zveřejněním sexuálního napadení. Odborníci upozorňují, že taková forma IBSA je na vzestupu a stává se z ní určitý trend, byť doposud neexistují spolehlivá data, která by tyto závěry prokazovala.[67] Již několik zahraničních medializovaných kauz znásilnění však bylo buďto doprovázeno přímým *„livestreamingem“* (živým vysíláním na sociálních sítích),[68] anebo následným šířením fotografií anebo videozáznamu útoku na internetu.[69] V těchto případech samozřejmě dochází k ohromnému zásahu do práv oběti již samotným sexuálním napadením. Tento zásah je však sekundárně doprovázen dalším ponížením, obtěžováním a viktimizací obětí, v důsledku čehož některé z těchto obětí čelí i vyhrožování smrtí.[70] Zároveň je i v tomto případě z povahy věci zřejmé, že oběť k vytvoření takového záznamu nedala souhlas.

V kontextu *revenge porn* a nekonsenzuální pornografie často zaznívá námitka, že si za uveřejnění anebo šíření svých sexuálních snímků a videí mohou mnohé oběti samy, neboť jej neměly nikomu posílat,[71] neměly jej vytvářet a měly dbát o to, aby nemohly být vytvořeny ani jiným způsobem. Na základě výše uvedeného je však zřejmé, že je naprosto lichá, právně irelevantní a spočívá v pouhé diskreditaci a sekundární viktimizaci těchto obětí (obecně je tzv. *„victim blaming“ u* případů *revenge porn* poměrně obvyklý). Jednak jsou mnohé z těchto obětí nezletilé děti,[72] v jejichž případě je namístě vyšší míra ochrany jejich práv. A dále, což je pro tento článek

[67] Tamtéž, s. 130.

[68] Např.: ENGLAND, Charlotte. Teenager jailed for broadcast of girl's rape on online Periscope app. In: *The Independent* [online]. 15. 2. 2017 [cit. 28. 4. 2020]. Dostupné z: http://www.independent.co.uk/news/world/americas/teenager-marina-lonina-livestream-rape-17-year-old-friend-periscope-app-sentence-prison-columbus-a7581196.html

[69] Viz např.: Steubenville Ohio School Footballers Guilty of Rape. In: *BBC* [online]. 17. 3. 2013 [cit. 29. 4. 2020]. Dostupné z: https://www.bbc.com/news/world-us-canada-21823042; SANGHANI, Radhika. Chrissy Chambers: 'My rape became revenge porn in the UK'. In: *The Telegraph* [online]. 17. 6. 2015 [cit. 29. 4. 2020]. Dostupné z: https://www.telegraph.co.uk/women/womens-life/11677742/YouTube-Chrissy-Chambers-My-rape-became-revenge-porn-in-the-UK.html

[70] MCGLYNN, RACKLEY, op. cit., s. 540.

[71] Autorky Citron a Franks namítají, že by společnost neměla vinit oběti nekonsenzuální pornografie za to, že důvěřovaly blízké osobě a předaly jí intimní snímky, pokud zároveň chrání například oběti zneužití citlivých informací finančními poradci. CITRON, FRANKS, op. cit., s. 348.

podstatnější, ani sebeopatrnější osoba se nemůže zcela vyhnout tomu, aby se obětí nekonsenzuální pornografie rovněž stala. Mezi IBSA totiž přirozeně spadají i případy, kdy sexuální záznam nedovoleně vyobrazující konkrétní osobu není reálný, avšak jako reálný se jeví. Do této kategorie můžeme zařadit jak fotomontáže, tak zejména pornografická *deepfakes* – realistická, avšak uměle vytvořená videa. Těm se tento článek bude věnovat podrobněji.

3. PORNOGRAFICKÁ *DEEPFAKE* VIDEA

Problematika pornografických *deepfakes* se od doposud rozebíraných případů do určité míry liší, byť se jedná o úzce související fenomén, jehož důsledky jsou ze své podstaty obdobné. Technologie *deepfake* vznikla v roce 2017[73] *a* spočívá ve vytváření ultrarealistických nepravých videí[74] osob, jejichž hlava je (velmi zjednodušeně řečeno) vložena namísto hlavy jiné osoby (tzv. *„face swap“*).[75] Strojové učení přitom umožňuje nejen velmi uvěřitelné splynutí obrazu, ale zejména i převzetí pohybů, drobné mimiky a gest vyobrazené osoby. Stačí tedy skloubit cílové video – pro účely tohoto článku vybrané pornografické video – s množstvím snímků a videozáznamů (datasetem, tzv. *„face setem“*) osoby, kterou do tohoto videa chceme zakomponovat.[76] Výsledkem tak je pornografická nahrávka, která na první

[72] Srov. např.: MORAVČÍK, Ondřej. Když čtrnáctiletá Kristýna… In: *Policie České republiky – KŘP Královéhradeckého kraje* [online]. 20. 3. 2019 [cit. 29. 4. 2020]. Dostupné z: https://www.policie.cz/clanek/kdyz-ctrnactileta-kristyna.aspx; KOZUMPLÍKOVÁ, Monika. Než pošleš nahou fotku, přemýšlej!. In: *Policie České republiky – KŘP Zlínského kraje* [online]. 31. 10. 2019 [cit. 29. 4. 2020]. Dostupné z: https://www.policie.cz/clanek/nez-poslesnahou-fotku-premyslej.aspx; SCHNEEWEISSOVÁ, Barbora. Sedmadvacetiletý muž několik let přes sociální sítě obtěžoval nezletilé dívky. In: *Policie České republiky – KŘP Středočeského kraje* [online]. 25. 11. 2019 [cit. 29. 4. 2020]. Dostupné z: https://www.policie.cz/clanek/sedmadvacetilety-muz-nekolik-let-pres-socialni-site-obtezoval-nezletile-divky.aspx; JIROUŠKOVÁ, Pavla. Láska přes internet nedopadla dobře. In: *Policie České republiky – KŘP Moravskoslezského kraje* [online]. 26. 11. 2019 [cit. 29. 4. 2020]. Dostupné z: https://www.policie.cz/clanek/laska-pres-internet-nedopadla-dobre.aspx

[73] DELFINO, op. cit., s. 893.

[74] HARRIS, Douglas. Deepfakes: False Pornography Is Here and the Law Cannot Protect You. *Duke Law & Technology Review* [online]. 2019, roč. 17, 1 [cit. 28. 4. 2020], s. 99. Dostupné z: https://scholarship.law.duke.edu/dltr/vol17/iss1/4/

[75] Tamtéž.

pohled vytváří dojem toho, že v ní účinkuje někdo, kdo ji však nikdy nenatočil.

Přestože má technologie *deepfake* širší uplatnění[77] a představuje riziko[78] i v jiných oblastech,[79] podle odborných odhadů tvoří až 96 % všech *deepfake* videí pornografická *deepfakes*.[80] Stejně jako v ostatních případech IBSA se jejich oběťmi stávají převážně ženy – v tomto případě dokonce ve 100 % všech pornografických *deepfakes*.[81] Internetovým uživatelům tak tato technologie umožňuje vytvářet pornografické nahrávky žen, které by si přáli vidět nahé.[82] Většinou jsou jimi celebrity,[83] a to z prostého důvodu – jejich *„face set"* je snadno dostupný, neboť internet je plný jejich fotografií.[84] Vznikají však samozřejmě i pornografická *deepfakes* s ženami, které slavné nejsou. Tvůrci těchto videí si vybírají převážně své známé, kamarádky, spolužačky či bývalé přítelkyně.[85,86] K usnadnění vytváření takových videí jim slouží jak aplikace, které dokáží automaticky shromáždit a propojit fotografie z profilu vytipované osoby na sociálních sítích,[87] tak veřejně dostupné rady a návody.[88] Doposud jsou sice mnohá takto vytvářená videa rozmazaná či nedokonalá z hlediska uvěřitelnosti,[89] lze však předpokládat, že další rozvoj této technologie povede k jejich vylepšení.[90]

---

[76] Technologie vytváření *deepfakes* se zakládá na pokročilém strojovém učení, v tomto případě hovoříme o tzv. *„deep learning"*. Více o tom, jak funguje, viz SPIVAK, op. cit.

[77] Tato technologie nabízí i pozitivní možnosti užití, např. pro filmový průmysl.

[78] Na rizika *deepfakes* poukázal např. americký komik Jordan Peele, který prostřednictvím této technologie vytvořil falešný projev bývalého prezidenta Baracka Obamy. Viz GSTALTER, Morgan. 'Obama' Voiced by Jordan Peele in PSA Video Warning About Fake Videos. In: *The Hill* [online]. 17. 4. 2018 [cit. 29. 4. 2020]. Dostupné z: https://thehill.com/blogs/in-the-know/in-the-know/383525-obama-voiced-by-jordan-peele-in-psa-video-warning-about-fake

[79] Riziku *deepfake* videí pro společnost a demokracii se obecně věnují např. CHESNEY, Robert; CITRON, Danielle Keats. Deep Fakes: A Looming Crisis for National Security, Democracy and Privacy? *California Law Review* [online]. 2019, roč. 107, 6 [cit. 29. 4. 2020]. Dostupné z: http://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security/

[80] RAFFAGHELLO, Ida a kol. What Does a Feminist Approach to Deepfake Pornography Look Like?. In: *Masters of Media* [online]. 24. 10. 2019 [cit. 28. 4. 2020]. Dostupné z: https://mastersofmedia.hum.uva.nl/blog/2019/10/24/what-does-a-feminist-approach-to-deepfake-pornography-look-like/

[81] RAFFAGHELLO, op. cit.

Následující podkapitoly se budou věnovat otázce, jakou újmu pornografická *deepfake* videa vyobrazeným osobám způsobují. Na tomto místě je třeba pouze velmi krátce uvést, že obětí se nestává pouze osoba, jejíž podoba je ve videu užita (tedy osoba, které „patří hlava"),[91] byť ta je samozřejmě postižena nejvíce – kdokoliv ji totiž může rozpoznat. Druhou obětí je ale i osoba, která byla zobrazena v původním videu (tedy osoba, které „patří tělo"),[92] a která jej většinou natočila zcela konsenzuálně (a třeba i za úplatu).[93] Pravděpodobně však aktérka původního videa neudělila souhlas k tomu, aby bylo zobrazováno pouze její nahé tělo, a namísto její hlavy byla vložena hlava jiné osoby.[94] V tomto směru lze dle názoru autorky tohoto článku uvažovat o zásahu do lidské důstojnosti, neboť se jedná do určité míry o objektivizaci. Upravené *deepfake* video může navíc zasahovat i do autorských práv k původnímu videu, obzvlášť pokud se jednalo o profesionální pornografické video. Nicméně jakkoliv tato rovina rovněž otevírá zajímavé otázky, bude se tento text dále věnovat pouze zásahu do práv osoby, jejíž hlava je ve výsledném *deepfake* videu zobrazena.

---

[82] Jedna americká novinářka podotkla, že *„deepfakes vznikla jako způsob, jak si přivlastnit ženská těla"*. Viz COLE, Samantha. Deepfakes Were Created As a Way to Own Women's Bodies—We Can't Forget That. In: *Vice* [online]. 19. 4. 2018 [cit. 30. 4. 2020]. Dostupné z: https://www.vice.com/en_us/article/j5kk9d/deepfakes-were-created-as-a-way-to-own-womens-bodieswe-cant-forget-that-v25n2

[83] DELFINO, op. cit., s. 894.

[84] Srov. HARRIS, op. cit., s. 100.

[85] Tamtéž, s. 101.

[86] V tomto směru se tak může jednat o IBSA ve formě „vztahové odplaty", nikoliv nepodobné *revenge porn stricto sensu.*

[87] Po vzniku prvních pornografických *deepfakes* v roce 2017 se objevila online aplikace FakeApp, která jejich snadné vytváření sama umožňovala. DELFINO, op. cit., s. 893, anebo HARRIS, op. cit., s. 101.

[88] HARRIS, op. cit., s. 101.

[89] DOLD, Kristen. Face-Swapping Porn: How a Creepy Internet Trend Could Threaten Democracy. In: *Rolling Stone* [online]. 17. 4. 2018 [cit. 29. 4. 2020]. Dostupné z: https://www.rollingstone.com/culture/culture-features/face-swapping-porn-how-a-creepy-internet-trend-could-threaten-democracy-629275/

[90] SIVAK, op. cit., s. 349.

[91] DELFINO, op. cit., s. 898.

[92] Tamtéž.

Zkuste si nyní na okamžik představit, že se touto osobou stanete vy. Že někdo zneužije vaše fotky, které jste nahráli na své sociální sítě, a které vás vyobrazují v naprosto normálních životních situacích, a které nejsou ani intimní či lechtivé, natož pak sexuálně explicitní. Najednou se na internetu objeví pornografické video s vaší podobou, byť s jiným tělem. Po prvním zhlédnutí okamžitě víte, že je uměle vytvořené, že jste jej nikdy nenatočili. Ví to ale stejně dobře všichni vaši známí, kolegové anebo rodinní příslušníci, kteří jej také viděli anebo dokonce šířili? A i přesto, že je toto video falešné a nezobrazuje při sexuálních aktivitách vaše skutečné nahé tělo (ve skutečnosti zobrazuje neexistující osobu, neboť hlava a tělo k sobě nepatří[95]), necítili byste v takové situaci značný zásah do svých práv a do své osobnosti? Tento popis je samozřejmě velmi sugestivní, avšak ilustruje, v jaké pozici se oběti pornografických *deepfakes* ocitají. Z hlediska zkoumání zásahu do práv vyobrazené osoby je přitom nutno odlišit případný[96] zásah spočívající v samotném vytvoření pornografického *deepfake* videa od zásahu, k němuž dojde jeho zveřejněním, sdílením či šířením. Ze své podstaty se totiž jedná o velmi rozdílné situace.

3.1 VYTVOŘENÍ PORNOGRAFICKÉHO *DEEPFAKE*

Zásah založený pouhým vytvořením pornografického *deepfake* je poněkud problematický. Z hlediska obecné roviny nekonsenzuální pornografie může k IBSA docházet samotným nedovoleným vytvořením intimního či sexuálního záznamu, a to způsoby, které tento text popisuje výše. V těchto ostatních případech však k vytvoření dochází buďto narušením důvodně očekávaného soukromí (blíže viz podkapitola 2.1.), anebo zneužitím bezbrannosti oběti (typicky v případech záznamu sexuálního napadení). Při

[93] Ačkoliv se tomu článek nebude dále věnovat, lze si představit i situaci, kdy *deepfake* video nebude založeno na „běžném“ komerčním pornografickém videu, ale např. na nahrávce znásilnění či jiných nekonsenzuálních sexuálních aktivit. Takové video, které by samo o sobě představovalo formu IBSA, pak může být dále zneužíváno ve vztahu k dalším osobám.

[94] DELFINO, op. cit., s. 898.

[95] DELFINO, op. cit., s. 897.

[96] Lze si představit i situaci, kdy pornografické *deepfake* video vznikne se souhlasem vyobrazené osoby, aniž by jí nutně způsobovalo újmu na právech.

vzniku pornografického *deepfake* videa nedochází ani k jedné z těchto situací. Tvůrce takového videa pro jeho vytvoření většinou používá fotografie vytipované oběti, které jsou běžně dostupné na internetu a sociálních sítích. K tomuto materiálu si tedy zpravidla nezjedná přístup způsobem, který by sám o sobě představoval zásah do soukromí na nich vyobrazené osoby, ani nijak nezneužije její bezbrannosti.

I přesto však může být samotné vytvoření pornografického *deepfake* videa zásahem do soukromí jednotlivce, konkrétněji do jeho práva na informační sebeurčení. Byť je toto právo [které je v našem právním řádu garantováno v čl. 10 odst. 3 Listiny základních práv a svobod („LZPS“)[97]] obvykle spojováno s možností jednotlivce rozvíjet se a seberealizovat se v lidské společnosti,[98] lze jej chápat i jinak. Právo na informační sebeurčení (stejně jako právo na soukromí obecně[99]) v sobě totiž obsahuje nejen složku externí, pod níž si můžeme představit možnost kontroly, jaké informace, komu, za jakých okolností a jakým způsobem jsou šířeny a sdíleny (o čemž bude pojednávat další podkapitola). Obsahuje i složku interní, která existuje sama o sobě, bez ohledu na interakci s jinými lidmi. Tou je předpoklad pro individuální sebeurčení jednotlivce, tedy jeho vnitřní kapacita pro sebeuvědomění a sebedefinici, a dále možnost prožití života v souladu se svou vlastní vůlí. Jednoduše řečeno, informační sebeurčení (resp. soukromí) v sobě zahrnuje předpoklad pro existenci lidí jakožto individuálních osobností, jejichž lidství je respektováno.[100] Právě v tomto ohledu může vytváření *deepfake* pornografie představovat zásah do práva na informační sebeurčení, neboť tento respekt k sebeurčení jiných lidí (kteří nechtějí být v pornografickém videu vyobrazeni) narušuje.

---

[97] Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění ústavního č. zákona 162/1998 Sb.

[98] Srov. rozhodnutí Spolkového ústavního soudu SRN ze dne 15. 12. 1983, BVerfGE 65, 1, body 94-97. In: OpenJur [online]. 2012 [cit. 29. 4. 2020]. Dostupné z: https://openjur.de/u/268440.html

[99] WAGNEROVÁ, Eliška. Právo na soukromí: Kde má být svoboda, tam musí být soukromí. In: ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí*. Brno: Masarykova univerzita, 2011, s. 54.

[100] K tomu blíže vit REIMAN, Jeffrey H. Privacy, Intimacy and Personhood. *Philosophy and Public Affairs* [online]. 1976, roč. 6, 1 [cit. 26. 9. 2020], s. 38-44. Dostupné z: https://www.jstor.org/stable/2265060?seq=1

Vytvoření pornografického *deepfake* videa může dále zasahovat do práv na ochranu osobnosti člověka ve smyslu § 81 až § 90 zákona č. 89/2012 Sb., občanského zákoníku (jejichž ústavní garance má rovněž oporu v čl. 10 LZPS). Konkrétně se tento zásah může projevovat manipulací s volně dostupnými fotografiemi za účelem vytvoření konkrétního videa. Tímto způsobem však dochází k zásahu spočívajícího primárně v tom, že byla nedovoleně užita podoba určité osoby, nikoliv v tom, že byla užita právě pro vytvoření pornografického *deepfake*. Autorka tohoto článku se tedy přiklání k závěru, že pouhé vytvoření takového umělého pornografického videa zobrazujícího konkrétní osobu nepředstavuje o mnoho větší zásah než jakékoliv jiné nedovolené nakládání s její podobou, a to i přesto, že ji výsledné video zobrazuje v sexuálně explicitních scénách. Pokud však výsledné video není dále jakkoliv šířeno, může být považováno toliko za oplzlé či nemorální,[101] avšak nepředstavuje takový zásah do práv osoby v něm vyobrazené, jako je tomu v případě jiných typů IBSA. I s ohledem na to, že se o něm oběť (anebo kdokoliv jiný) vůbec nemusí dozvědět, se vytvoření pornografického *deepfake*, které není dále šířené nebo zpřístupněné, v podstatě příliš neliší od sexuálních fantazií, které jednotlivec může mít ohledně jiných lidí.[102] Tento závěr je nicméně otevřen širší diskuzi, která může být ovlivněna dalším rozvojem pornografických *deepfake* videí a způsobu jejich vytváření.

V kontextu vytváření těchto videí nelze dále pominout to, že vytvořené pornografické *deepfake* video nemusí vždy sloužit pouze k sexuální gratifikaci jeho tvůrce – může být samozřejmě užito i za účelem vydírání zobrazené osoby, a to vyhrožováním jeho uveřejnění.[103] Tím spíš, pokud by oběť vyobrazovalo obzvlášť ponižujícím způsobem, např. v extrémně násilné, pedofilní či zoofilní pornografické nahrávce.[104] Takové jednání spadá mezi jiné formy IBSA popsané výše (zejména *„sextortion“*) a zároveň svou

[101] HARRIS, s. 125.

[102] ÖHMAN, Carl. Introducing the pervert's dilemma: a contribution to the critique of Deepfake Pornography. *Ethics and Information Technology* [online]. 2019 [cit. 29. 4. 2020]. Dostupné z: https://link.springer.com/article/10.1007/s10676-019-09522-1

[103] HARRIS, op. cit., s. 102.

[104] Srov. CHESNEY, CITRON, op. cit., s. 1773.

povahou zasahuje do trestněprávní roviny. V takovém případě však k tomuto odvozenému zásahu dochází až vydíráním vyobrazené osoby, nikoliv samotným vytvořením daného videa. Z hlediska existence pornografického *deepfake* videa tedy zpravidla dochází k významnému zásahu do individuálních práv až v okamžiku, kdy jej může zhlédnout někdo jiný.

3.2 ZVEŘEJNĚNÍ, SDÍLENÍ ČI ŠÍŘENÍ PORNOGRAFICKÉHO *DEEPFAKE*

Na tomto místě je důležité si uvědomit, že aby pornografické *deepfake* zasahovalo do práv vyobrazené osoby, není nutno, aby bylo nutně šířeno veřejně. Stejně jako u jiných výše popsaných druhů *revenge porn* ke vzniku újmy postačí, je-li sdíleno kupříkladu ve skupině známých, v určitém úzkém kolektivu (školním, pracovním apod.), či je-li zasláno vybraným osobám jako třeba zaměstnavateli anebo klientovi dotyčné osoby. Taková forma může být s ohledem na okolnosti pro většinu lidí zpravidla dokonce horší, než kdyby se pornografické *deepfake* video s nimi jako aktéry šířilo internetem anonymně, a pravděpodobnost rozpoznání by tak byla nižší (což samozřejmě neplatí v případě známých celebrit).

V první řadě je nutno zdůraznit, že šíření falešného pornografického *deepfake* videa představuje citelný zásah do lidské důstojnosti. Lidská důstojnost je totiž bezpochyby narušena tehdy, je-li šířen videozáznam vyobrazující člověka, jehož podoba na nahrávce činí více či méně obscénní akty, k nimž tento skutečný člověk neudělil souhlas. Jedním z důvodů, které mohou v tomto směru vyobrazenému člověku způsobit újmu, je možnost vidět sám sebe (resp. svou podobu) vykonávat činnosti, které by normálně nevykonával, anebo by je nevykonával zpodobněným způsobem, případně s konkrétním člověkem (jiným aktérem původního pornografického videa). V tomto směru se zásah do lidské důstojnosti do určité míry prolíná s výše popsaným právem na informační sebeurčení, neboť je tímto způsobem s člověkem (resp. jeho podobou) nakládáno jako s objektem, nikoliv subjektem. Pokud osoba, která je v *deepfake* pornu vyobrazena, nikdy žádné pornografické video nenatočila, představuje její „vložení“ do takového uměle vytvořeného videa nerespektování volby dané osoby neúčinkovat

v pornografickém videu, které je přístupné jiným lidem.[105] Tímto způsobem je narušována kontrola jednotlivců nad tím, zdali budou, anebo nebudou vyobrazeni při sexuálních aktivitách. Možnost jejich sebeurčení a „vlastnění" sebe sama (konkrétně své podoby) před ostatními lidmi je značně zasažena, kvůli čemuž je tak nutně zasažena i jejich lidská důstojnost.

Samozřejmě se nabízí otázka, nakolik závažný zásah do práv vyobrazeného člověka *deepfake* pornografie skutečně představuje. Nelze totiž zapomínat na to, že se jedná o uměle vytvořená videa – videomontáže – která jsou do určité míry srovnatelná s profesionálními fotomontážemi (opomeňme na okamžik, že i fotomontáže mohou představovat zásah do práv člověka). Zaprvé, je třeba si uvědomit, že se může jednat o velmi kvalitně a realisticky zpracované videomontáže, jejichž uvěřitelnost bude s vývojem užívaných technologií větší a větší. Už dnes tak může být těžké rozlišit, která pornografická videa jsou skutečná (a osoby na nich vyobrazené je za účelem zveřejnění natočily vědomě a dobrovolně, pokud se nejedná o *revenge porn* či záznam sexuálního napadení) a která jsou uměle vytvořená. Tím spíše, že se jedná o nový fenomén, tudíž nejsme doposud zvyklí u realisticky se tvářících videí kriticky přemýšlet nad jejich pravdivostí (a nutno dodat, že v segmentu pornografie to pro mnohé diváky ani není podstatné). Právě realističnost a uvěřitelnost výsledného videa je tím nejproblematičtějším a nejvážnějším aspektem technologie *deepfake*, a tedy i *deepfake* pornografie. Tento aspekt ale současně představuje důvod jejího úspěchu. Věříme tomu, co vidíme[106] – a pokud vidíme video (tedy nikoliv jeden statický snímek, který lze v grafických programech upravit snadno), které pů-

[105] Je možno se zamyslet, zdali by bylo stejně závažným zásahem do lidské důstojnosti vytvoření pornografického *deepfake* videa, do něhož by byla vložena „hlava" jiné pornoherečky, která běžně taková videa natáčí. Je to samozřejmě diskuzní otázka, autorka tohoto článku se nicméně domnívá, že v takovém případě by se rovněž o zásad do lidské důstojnosti jednalo, avšak byl by menší. Spočíval by zřejmě pouze v tom, že autor daného videa vyobrazenou pornoherečku objektivizoval a zobrazil ji způsobem, který nerespektuje její individualitu (to, jak v pornografických videích skutečně vystupuje). Odlišný případ by však pravděpodobně nastal tehdy, pokud by autor tuto pornoherečku nechal „účinkovat" např. v pedofilním, zoofilním anebo jinak problematickém pornu, pokud daný druh videí netočí a nikdy netočila. Takový případ by mohl představovat zásah do lidské důstojnosti srovnatelný s tím, pokud by vyobrazenou osobou byl kdokoliv jiný.

sobí autenticky, nevykazuje známky parodie či zfalšování a pravdivost jeho obsahu není přinejmenším nepředstavitelná, není těžké mu uvěřit.[107]

S tím souvisí i způsob, jakým se zveřejnění či šíření pornografických *deepfakes* dotýká práva na soukromí. Skutečnost, že jiní lidé mohou takové video zhlédnout a případně mu uvěřit, vážně zasahuje do osobnostních práv ve smyslu čl. 10 odst. 1 LZPS, tedy konkrétně práva na ochranu cti, dobré pověsti a jména člověka (která spadají pod ochranu soukromí *largo sensu*). Ústavní soud ve své judikatuře dovodil, že tyto chráněné hodnoty představují důležitou a integrální součást důstojnosti člověka (ve smyslu jeho váženosti) a formují základ mnoha rozhodnutí činěných členy demokratické společnosti. Jsou-li jednou pošpiněny, mohou být poškozeny navždy, obzvlášť není-li dotyčnému dána možnost rehabilitace.[108] Právě neefektivita této možnosti obětem *deepfake* pornografie nejvíce ztěžuje nastalou situaci, neboť si lze jen těžko představit, že by mohly oběti ve snaze o nápravu vlastní cti a pověsti přesvědčovat každého, kdo „jejich" video zhlédl, že není skutečné. Naopak si ale lze představit, že tato forma pošpinění cti a dobré pověsti určité osoby může mít dopad nejen do individuálních práv, ale i do kolektivních zájmů společnosti.[109] Může totiž mj. vést i k ovlivnění výsledků voleb a jiných politických procesů, a tedy fungování demokracie jako takové.[110] Pokud by se např. před volbami objevilo pornografické video, v němž by figuroval některý z kandidátů (prav-

[106] K zastaralosti fráze „uvěřím, až to uvidím na vlastní oči" blíže viz HALL, Holly Kathleen. Deepfake Videos: When Seeing Isn't Believing. *Catholic University Journal of Law and Technology* [online]. 2018, roč. 27, 1 [cit. 27. 9. 2020], s. 51-76. Dostupné z: https://scholarship.law.edu/cgi/viewcontent.cgi?article=1060&context=jlt

[107] Podle výzkumů patří mezi faktory zvyšující uvěřitelnost falešných *deepfake* videí (nikoliv konkrétně pornografických) plynulost videa způsobená realističností dané technologie a známost vyobrazené osoby. K tomu blíže viz VACCARI, Christian; CHADWICK, Andrew. Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. *Social Media + Society* [online]. 2020, roč. 6, 1 [cit. 27. 9. 2020], s. 2. Dostupné z: https://journals.sagepub.com/doi/pdf/10.1177/2056305120903408

[108] Nález Ústavního soudu ze dne 11. 11. 2005, sp. zn. I. ÚS 453/03, část IV.

[109] K tzv. „kolektivní újmě" nebo „kulturní újmě" způsobené nekonsenzuální pornografií srov. MCGLYNN, RACKLEY, op. cit., s. 544, 549-551, 561.

[110] Na možnost ovlivňování výsledků voleb prostřednictvím (nikoliv přímo pornografických) *deepfake* videí upozorňují Citron a Chesney. Viz CHESNEY, CITRON, op. cit., s. 22-23.

děpodobně spíše kandidátka s ohledem na genderovou nevyrovnanost IBSA), je možné, že by se určitá část voličů rozhodla jej z těchto důvodů nevolit – a to bez ohledu na to, že by se jednalo o uměle vytvořené manipulativní *deepfake* video.[111]

Z hlediska zásahu do osobní cti a dobré pověsti člověka je potřeba se ještě krátce zamyslet nad následujícím: byl by zásah do těchto práv osoby vyobrazené na zveřejněném nebo jinak šířeném *deepfake* pornografickém videu stejně velký, pokud by jeho autor zároveň uvedl, že je dané video falešné, tedy uměle vytvořené (a šíří jej např. za účelem pomsty)? Bezpochyby by i v tomto případě bylo možno hovořit o zásahu do lidské důstojnosti – vyobrazená osoba by byla objektivizována, byla by narušena možnost jejího individuálního sebeurčení neúčinkovat v pornografických videích a mohla by vidět „sama sebe" při obscénních činnostech. Je však představitelné, že zásah do její cti a dobré pověsti by byl umenšen přiznáním nepravdivosti daného videa.[112]

Vedle zásahu do uvedených osobnostních práv je samozřejmě potřeba se zabývat i tím, jakým způsobem zveřejnění, sdílení či šíření pornografického *deepfake* videa zasahuje do soukromí vyobrazené osoby *stricto sensu*. Předně dochází společně se šířením vytvořeného videa i k neoprávněnému šíření její podoby (viz § 85 odst. 1 občanského zákoníku). Otázkou je, zdali je

[111] Obdobné situaci čelila americká kandidátka na prezidentku Hillary Clinton v roce 2016. Na několika pornografických stránkách se objevilo video (nikoliv *deepfake*, tato technologie tou dobou ještě neexistovala), které ji mělo údajně vyobrazovat při sexu v hotelovém pokoji s černošským mužem, přičemž bylo video doplněno popisky jako „takto Hillary Clinton získává černošské hlasy". Video údajně nepůsobilo příliš autentickým dojmem a ti, kteří jej zhlédli, byli skeptičtí vůči tomu, že by se skutečně jednalo o Hillary Clinton. Pokud by se jednalo o *deepfake* video, jeho autentičnost by mohla být výrazně větší, a kredibilita kandidátky naopak o poznání menší. Je nutno zároveň v tomto kontextu dodat, že není prokázáno, že by šíření tohoto videa (které je dodnes na internetu dohledatelné) způsobilo následné vítězství Donalda Trumpa. Bylo však naopak prokázáno, že za šířením videa stála ruská agentura Internet Research Agency. Viz COLLINS, Ben. Russia-linked account pushed fake Hillary Clinton sex video. In: *NBC News* [online]. 11. 4. 2018 [cit. 29. 4. 2020]. Dostupné z: https://www.nbcnews.com/tech/security/russia-linked-account-pushed-fake-hillary-clinton-sex-video-n864871

[112] Záměrně se zde neuvádí, že by k němu vůbec nedošlo – jak je popsáno výše v tomto článku, internet nezapomíná. Lze tedy předpokládat že by se takové video šířilo i dále, mimo rámec jeho původního sdílení. K zásahu do těchto práv by tak v budoucnu mohlo dojít, pokud by zveřejněné video zhlédl a uvěřil mu někdo, kdo o jeho kontextu nic neví.

však zásah do soukromí jednotlivce větší proto, že je jeho podoba vyobrazena právě v pornografickém videu, anebo zdali hranice zásahu do soukromí v tomto směru končí právě neoprávněným nakládáním s podobou konkrétní oběti. Autorka tohoto článku se domnívá, že zásah do soukromí jedince je větší právě kvůli tomu, že se jedná o jeho vyobrazení v pornografickém videu. Tento jedinec, resp. jeho podoba, je ve výsledném videu nucen velmi objektivizujícím způsobem činit něco, co se běžně odehrává „za zavřenými dveřmi" a co je samotnou podstatou lidské intimity a sexuality. Zahraniční odborná literatura v tomto kontextu dokonce hovoří o zásahu do „sexuální autonomie a sexuálního projevu,"[113] „sexuální integrity a identity"[114] či „sexuálního soukromí".[115] *Deepfake* pornografie tak způsobuje zásah do samotného jádra pojmu soukromí,[116] a to do tzv. *„nejintimnější osobní sféry jednotlivce"* ve smyslu judikatury ESLP.[117] Jak již totiž bylo zmíněno, soukromí má i interní složku, která se nejvíce projevuje v osobní soukromé sféře.[118] Podle ESLP mohou do této osobní sféry jednotlivce (chráněné čl. 8 Úmluvy o ochraně lidských práv a základních svobod[119]) spadat mj. i aspekty sociální identity a sexuálního života člověka.[120] Podle Ústavního soudu

[113] MCGLYNN, RACKLEY, op. cit., s. 548-549.

[114] ŠEPEC, Miha. Revenge Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence Pornography or Non-Consensual. *International Journal of Cyber Criminology* [online]. 2019, roč. 13, 2 [cit. 29. 4. 2020], s. 421. Dostupné z: https://www.cybercrimejournal.com/MihaSepecVol13Issue2IJCC2019.pdf

[115] CITRON, op. cit., s. 1874.

[116] Pro určení toho, co lze ještě interpretovat jako „soukromí", slouží podle Michala Bartoně vazba na ochranu lidské důstojnosti jako zachování určující meze – existuje tak blízký vztah mezi ochranou soukromí a ochranou lidské důstojnosti. BARTOŇ, Michal a kol. *Základní práva.* Praha: Leges, 2016, s. 284.

[117] Rozsudek Evropského soudu pro lidská práva ze dne 22. 10. 1981. Dudgeon vs. Spojené království, op. cit., bod 52.

[118] Srov. WAGNEROVÁ, Eliška. Právo na soukromí v širším smyslu. In: WAGNEROVÁ, Eliška a kol. *Listina základních práv a svobod: komentář.* Praha: Wolters Kluwer ČR, 2012, s. 282.

[119] Úmluva o ochraně lidských práv a základních svobod Rady Evropy ze dne 4. 11. 1950, ve znění Protokolů 11 a 14, s Protokoly 1, 4, 6, 7, 12 a 13. In: *Evropský soud pro lidská práva* [online]. Evropský soud pro lidská práva [cit. 30. 4. 2020]. Dostupné z: http://www.echr.coe.int/Documents/Convention_CES.pdf

[120] Rozsudek Evropského soudu pro lidská práva ze dne 4. 12. 2008. S. a Marper vs. Spojené království. ECHR 30562/04 a 30566/04. In: *HUDOC* [online]. Evropský soud pro lidská práva [cit. 29. 4. 2020], bod 66. Dostupné z: http://hudoc.echr.coe.int/eng?i=001-90051

navíc spadají pod rozsah tzv. nejintimnější sféry jednotlivce i informace o sexualitě člověka. Ve vztahu k této nejintimnější sféře se navíc zvyšuje míra ochrany soukromí a důstojnosti,[121] což souvisí s tím, o jak citlivou oblast se jedná a k nakolik závažné újmě může zásahem do této sféry dojít.

Přirozeně se nabízí namítnout, že ze skutečného „soukromí" osoby vyobrazené v pornografickém *deepfake* je uveřejněna pouze její podoba (hlava). Oproti jiným případům IBSA není např. vyobrazeno reálné nahé tělo oběti anebo není oběť vyobrazena při konkrétních sexuálních aktivitách, které by skutečně vykonávala. Je třeba jasně zdůraznit, že šíření skutečného pornografického videa vyobrazující osobu, která k takovému jednání nedala souhlas, představuje bezpochyby zásadně větší zásah do jejího soukromí, než je tomu v případě falešných *deepfakes*. Bylo by však chybou domnívat se, že v jejich případě není soukromí jednotlivce vůbec zasaženo. Jak již bylo zmíněno, jedním z aspektů práva na soukromí je totiž i právo na informační sebeurčení. Jak konstatoval německý Spolkový soud, který v roce 1983 tento koncept představil, nemá-li jedinec jistotu, jaké informace jsou o jeho osobě sdělovány, ovlivňuje taková skutečnost svobodu jeho rozhodování o sobě samém.[122] Ústavní soud v nálezu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, zároveň potvrdil, že obecnou funkcí práva na respekt k soukromému životu je možnost zajistit prostor pro rozvoj a realizaci individuální osobnosti. Ztráta kontroly nad informacemi, které jsou o nás dostupné, by však takové možnosti seberealizace ve společnosti zabránila.[123]

To lze vztáhnout i na šíření uměle vytvořených pornografických *deepfake* videí, která se jeví být skutečným záznamem dotyčné osoby. Tato videa totiž zasahují do toho, jak se dané osoby chtějí realizovat a jak se chtějí prezentovat na veřejnosti. Autorka tohoto článku se domnívá, že v případě

[121] Nález Ústavního soudu ze dne 20. 12. 2016, sp. zn. Pl. ÚS 3/14.

[122] Rozhodnutí Spolkového ústavního soudu SRN ze dne 15. 12. 1983, BVerfGE 65, 1, op. cit., bod 94.

[123] Srov. ROUVROY, Antoinette; POULLET, Yves. The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: GUTWIRTH, Serge et kol. (ed.). *Reinventing Data Protection?* [online]. Dordrecht: Springer, 2009, s. 51. Dostupné z: https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_2

deepfake pornografie – právě s ohledem na citelnost a povahu jejích dopadů na život vyobrazené osoby – je namístě ochranu vztáhnout i na úzce chápaný pojem soukromí, a to konkrétně ve smyslu sexuálního soukromí. Zaprvé, jak je uvedeno výše, tato oblast soukromí podléhá zvýšené míře právní ochrany. Zadruhé, zveřejnění *deepfake* pornografického videa může nejen snižovat osobní čest a dobrou pověst na něm vyobrazené osoby, ale zejména učiní otázku jejího sexuálního života „veřejným tématem".[124] Tato osoba tak pravděpodobně bude (ve snaze vyvrátit pravdivost videa) nucena hovořit o svém sexuálním životě s lidmi, jimž by tuto oblast vlastního soukromí normálně neodhalovala, anebo způsobem, jakým by tak běžně nečinila. V tomto směru se *deepfake* pornografie liší od jiných druhů *deepfake* videí – i tato ostatní videa (např. falešné politické projevy) mohou zásadně zasáhnout do osobnostních práv člověka, který se stal jejich obětí, a jeho váženost může být významně zasažena. Zřejmě však nebude vzniklou újmu vnímat natolik niterně, jako pokud bude v důsledku zveřejnění „jeho" *deepfake* porna veřejně rozvířena otázka projevů jeho sexuality. A již popsaná realističnost a explicitnost tohoto typu videí tento dopad zásadně zesiluje.

Jelikož *deepfake* pornografie nepředstavuje reálné záznamy skutečných lidí, liší se od ostatních typů IBSA právě v tom, že se její obětí může stát prakticky kdokoliv. Jak se tedy proti ní lze bránit?

3.3 PROSTŘEDKY OBRANY PROTI PORNOGRAFICKÝM *DEEPFAKES*

Na tomto místě je nejprve je třeba uvést, že z důvodu absence české odborné literatury k tomuto tématu anebo soudně řešených případů jsou dále popisované prostředky ochrany pouze předpokládané, doposud neozkoušené. Jelikož však lze očekávat, že se i v České republice v dohledné době tyto případy objeví (stejně jako se zde objevují jiné formy *revenge porn*), pokusí se autorka na tomto místě shrnout možnosti, kterými se teoreticky lze proti *deepfake* pornografii bránit. V mnohém se jedná o stejné nástroje, které mohou sloužit i k ochraně proti jiným formám nekonsenzuální porno-

[124] Nejenom ve smyslu „celospolečenským tématem", postačí, bude-li toto téma určitým způsobem rezonovat v kolektivu přátel, kolegů, známých apod. vyobrazené osoby.

grafie. A bohužel je potřeba dodat, že se nejedná o příliš efektivní prostředky obrany.[125]

Jedním z nich může být civilní žaloba na ochranu osobnosti, a to zejména ve smyslu práva na ochranu podoby a soukromí (ve smyslu § 84 až § 90 občanského zákoníku). Jeho obsahem je jednak zákaz zásahu do soukromí jiného člověka, a to mj. pořizováním, využíváním anebo šířením záznamů o jeho soukromém životě. Obsahem práva na ochranu podoby člověka pak je zákaz zachycení podoby a další nakládání s ní bez svolení vyobrazené osoby. Judikatura Nejvyššího soudu v tomto směru vymezuje jak pozitivní komponentu tohoto práva (dispoziční právo každé osoby zachytit svou podobu a udělovat jiným osobám souhlas k jejímu zachycení), tak i negativní (možnost bránit se proti neoprávněnému zachycení podoby, právě tak jako proti jejímu neoprávněnému rozšiřování ze strany jiného subjektu).[126] Oproti jiným případům nekonsenzuální pornografie, kdy může být vyobrazeno např. pouze tělo, nikoliv obličej (a osoba je tedy na základě této podoby hůře identifikovatelná[127]), je v případě oběti pornografického *deepfake* vyobrazena právě jen její tvář. Tato osoba je tudíž rozpoznatelná velmi snadno. Rozhodne-li se proti tomu, kdo vytvořené *deepfake* video šíří, bránit touto cestou, může se dožadovat a) upuštění od neoprávněného zásahu do individuálních práv (žaloba negatorní), b) odstranění závadného stavu (žaloba restituční) a c) náhradu škody a nemajetkové újmy včetně uzpůsobených duševních útrap (žaloba satisfakční).[128]

V úvahu samozřejmě dále připadá i rovina trestního práva. V případě zveřejnění, šíření anebo sdílení pornografického *deepfake* videa lze uvažovat o naplnění skutkové podstaty trestného činu poškození cizích práv podle § 181 zákona č. 40/2009 Sb., trestního zákoníku. Samotná podstata *deepfake* pornografie totiž spočívá ve snaze vyvolat dojem, že vyobrazený

[125] K tomu blíže viz DVOŘÁKOVÁ, op. cit., s. 55-80.

[126] Rozsudek Nejvyššího soudu ze dne 27. 5. 2015, sp. zn. 30 Cdo 5216/2014.

[127] Podle názoru autorky v případě *revenge porn* k zásahu do práv jednotlivce dojde i tehdy, jsou-li sdíleny záznamy, na nichž není vidět hlava dotyčného. Byť samozřejmě bude takový zásah pro daného člověka méně nepříjemný (lidé, kteří neznají jeho nahé tělo, jej nebudou schopni rozpoznat), právně relevantní přesto bude. K tomu blíže viz DVOŘÁKOVÁ, op. cit., s. 58.

[128] § 82 a § 2956 občanského zákoníku. Tyto nároky lze požadovat i společně.

uměle vytvořený záznam je skutečný, v důsledku čehož může být tímto jednáním naplněna zákonná podmínka „uvedení někoho v omyl“.[129] Případně může připadat v úvahu naplnění skutkové podstaty trestného činu pomluvy podle § 184 trestního zákoníku, pokud by bylo šířené *deepfake* pornografické video považováno za *„sdělení nepravdivého údaje, který je způsobilý značnou měrou ohrozit vážnost* [dotyčného jedince] *u spoluobčanů, zejména poškodit jej v zaměstnání, narušit jeho rodinné vztahy nebo způsobit mu jinou vážnou újmu“*.[130] Pokud by vytvořené *deepfake* video znázorňovalo např. zoofilní anebo pedofilní pornografii, bylo by dále na místě aplikovat § 191 (šíření pornografie) a § 192 (výroba a jiné nakládání s dětskou pornografií) trestního zákoníku. Stejně tak by bylo možno shledat naplnění jiných skutkových podstat, pokud by byla osoba např. vydírána ze šíření *deepfake* pornografie, která by ji vyobrazovala. To už se však poněkud míjí se samotnou podstatou zkoumané problematiky. Z uvedených důvodů je tedy autorka tohoto článku pevně přesvědčená, že by bylo vhodnější a systematičtější, pokud by byl trestní zákoník rozšířen o nové skutkové podstaty, které by výslovně pokrývaly problematiku IBSA a zdůrazňovaly specifický zásah do sexuálního soukromí jednotlivce. K tomuto názoru ji vede především skutečnost, že zahraniční právní úpravy již v uplynulých letech na rozšíření *revenge porn* reagovaly jeho kriminalizací,[131] a mnozí odborníci zdůrazňují, že je třeba obdobně postupovat i v případě *deepfake* pornografie.[132]

Vzhledem k tomu, že se však pornografická *deepfake* videa (stejně jako jiné druhy nekonsenzuální pornografie) šíří internetem lavinovitě a nejsou

[129] Tato skutková podstata je nejčastěji užívána i v jiných případech *revenge porn*. K tomu viz DVOŘÁKOVÁ, op. cit., s. 74-75.

[130] V tomto kontextu přichází samozřejmě v úvahu otázka svobody projevu a její případná kolize s individuálními právy jiné osoby. Tento článek se tomu podrobněji věnovat nebude, k tomu srov. DVOŘÁKOVÁ, op. cit., s. 46-53. Blíže se této otázce přímo ve vztahu k pornografickým *deepfakes* věnují FRANKS, Mary Anne; WALDMAN, Ari Ezra. Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions. *Maryland Law Review* [online]. 2019, roč. 78, 4 [cit. 29. 4. 2020]. Dostupné z: https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3835&context=mlr

[131] Např. Izrael, Spojené království, Kanada, Francie anebo mnohé státy Spojených států amerických. Srov. DVOŘÁKOVÁ, op. cit., s. 81-82.

[132] K tomu viz DELFINO, op. cit., HARRIS, op. cit., anebo FRANKS, WALDMAN, op. cit.

omezena na území České republiky, je nutno se zabývat i prostředky obrany, které lze najít na nadnárodní úrovni. Těmi jsou v rámci Evropské unie zejména právo být zapomenut[133, 134] anebo požadavek vůči provozovateli internetové stránky na odstranění pornografického *deepfake* videa (tzv. *„notice and take down“*), které se na ní vyskytuje.[135, 136] Nicméně nejúčinnějšími prostředky proti této formě IBSA stejně bezesporu je, pokud provozovatelé internetových stránek (zejména sociálních sítí anebo pornografických webů) brání uveřejňování pornografických *deepfakes* svými vlastními prostředky, jako tak činí např. Facebook,[137] Reddit, Twitter anebo Pornhub.[138] To však nemůže zabránit jejich šíření jinými prostředky.

Na závěr této kapitoly je vhodno ještě dodat, že se v poslední době objevily i různé další návrhy, jak lze nedovolenému šíření *deepfake* porna zabránit. Jedním z těchto návrhů je např. úvaha o vytvoření „feministické aplikace“ pro vytváření pornografických *deepfake* videí, která by umožňovala na jedné straně za finanční odměnu nahrávat vlastní *„face sety“* (soubor fotografií), a na druhé straně na základě těchto datasetů vytvářet

[133] Ve smyslu čl. 17 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES In: *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=CS, a dále ve smyslu rozsudku Soudního dvora (velkého senátu) ze dne 13. 5. 2014 ve věci C-131/12, Google Spain and Google.

[134] K tomu srov. např. MESARČÍK, Matúš; ZIMEN, Ondrej. Deep fakes a ochrana súkromia. *Acta Facultatis Iuridicae Universitatis Comenianae* [online]. 2019, roč. 38, 2 [cit. 29. 4. 2020]. Dostupné z: https://afi.flaw.uniba.sk/index.php/AFI/article/view/65

[135] Ve smyslu čl. 14 směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. 6. 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu. In: *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32000L0031&from=EN

[136] Ve vnitrostátním právu je pak tzv. *„notice and take down“* systém upraven § 5 odst. 1 písm. b) zákona č. 480/2004 Sb., o některých službách informační společnosti, který uvedenou směrnici 2000/31/ES implementuje.

[137] Facebook nezakázal pouze pornografická *deepfakes*, ale veškerá takto uměle vytvořená videa. Viz SHEAD, Sam. Facebook to ban ‘deepfakes‘. In: *BBC* [online]. 7. 1. 2020 [cit. 29. 4. 2020].Dostupné z: https://www.bbc.com/news/technology-51018758

[138] HARRIS, op. cit., s. 101-102.

konsenzuální pornografická *deepfakes*.[139] Dalším návrhem je určitá forma „digitálního podpisu", který by se vepsal do jakéhokoliv natočeného videa. Podle toho by bylo možno poznat, je-li nahrávka autentická, anebo byla dále měněna či uměle spojena s jinou.[140] Oba tyto návrhy však mohou fungovat jen v případě, kdy tvůrce anebo „divák" bude dbát o to, aby nedošlo k zásahu do ničích práv. Z toho důvodu je jejich využití pro boj s nekonsenzuální pornografií spíše nepravděpodobné a obětem této nové formy IBSA příliš nepomůže.

4. ZÁVĚR

Nekonsenzuální pornografie může mít mnoho podob, a to od pořízení fotografie nahého člověka prostřednictvím skryté kamery pro osobní účely, až po zveřejnění a sdílení videozáznamu znásilnění. Co mají tyto jednotlivé formy společného, je to, že mohou mít v různé míře závažnosti obdobný dopad na život oběti jako skutečný sexuální útok, a to i přes svou „nefyzickou" formu. Jedná se tedy o nekontaktní sexuální násilí, které lze dokonce označit za formu sexuálního zneužití[141] (*„image-based sexual abuse"*). Mezi těmito druhy jednání se značně vymyká rozvoj *deepfake* pornografie, která se objevila v roce 2017 a velmi rychle se rozšířila. Jejím prostřednictvím lze jednak vytvářet falešná, avšak realistická pornografická videa znázorňující ženy, kterým chce tvůrce takového záznamu ublížit z osobních důvodů, dále slavné ženy, které si internetoví uživatelé přejí vidět nahé, anebo např. političky, které má takové video zdiskreditovat. Důvodů samozřejmě může být nespočet a tato nová technologie k jejich naplnění poskytuje velmi snadný způsob. Právní aspekty *deepfake* porna se v zahraničních odborných kruzích v uplynulých měsících hojně diskutují. České republice se však doposud tyto otázky vyhýbají – nutno podotknout, že zřejmě i proto, že se jí prozatím vyhýbá existence popsaného problému jako takového.

[139] Více viz RAFFAGHELLO a kol., op. cit.

[140] LIN, Herb; HOLLAND, Hank J. The Danger of Deepfakes: Responding to Bobby Chesney and Danielle Citron. In: *Lawfare* [online]. 27. 2. 2018 [cit. 29. 4. 2020]. Dostupné z: https://www.lawfareblog.com/danger-deepfakes-responding-bobby-chesney-and-danielle-citron

[141] CITRON, FRANKS, op. cit., s. 362.

Je však namístě zdůraznit slovo prozatím. Stejně jako se zde objevují i jiné formy nekonsenzuální pornografie, je možno očekávat i rozšíření *deepfake* pornografie. S ohledem na popsanou závažnost újmy, kterou šíření takových nahrávek může způsobovat, je tedy třeba, aby na to právní řád byl schopen efektivně reagovat.

5. LITERATURA

5.1 MONOGRAFIE

[1] BARTOŇ, Michal a kol. *Základní práva.* 1. vydání. Praha: Leges, 2016, 608 s. ISBN 978-80-7502-128-1.

[2] HENRY, Nicola; FLYNN, Asher; POWELL, Anastasia. *Responding to 'revenge pornography': Prevalence, nature and impacts* [online]. 1. vydání. Canberra: Australian Research Council, 2019 [cit. 27. 4. 2020], 126 s. ISBN 978-1-925304-14-5. Dostupné z: https://www.crg.aic.gov.au/reports/CRG_08_15-16-FinalReport.pdf

[3] POWELL, Anastasia; HENRY, Nicola. *Sexual Violence in a Digital Age* [online]. 1. vydání. Basingstoke: Palgrave Macmillan, 2017 [cit. 27. 4. 2020], 317 s. ISBN 978-1-137-58047-4. Dostupné z: https://link.springer.com/book/10.1057%2F978-1-137-58047-4

5.2 KAPITOLA Z MONOGRAFIE

[4] WAGNEROVÁ, Eliška. Právo na soukromí v širším smyslu. In: WAGNEROVÁ, Eliška a kol. *Listina základních práv a svobod: komentář.* 1. vydání. Praha: Wolters Kluwer ČR, 2012, s. 277-299. ISBN 978-80-7357-750-6.

5.3 PŘÍSPĚVKY VE SBORNÍKU

[5] ROUVROY, Antoinette; POULLET, Yves. The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In: GUTWIRTH, Serge et kol. (ed.). *Reinventing Data Protection?* [online]. 1. vydání. Dordrecht: Springer, 2009, s. 45-76. ISBN 978-1-4020-9498-9. Dostupné z: https://link.springer.com/chapter/10.1007/978-1-4020-9498-9_2

[6] WAGNEROVÁ, Eliška. Právo na soukromí: Kde má být svoboda, tam musí být soukromí. In: ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí.* 1. vydání. Brno: Masarykova univerzita, 2011, s. 49-62. ISBN 978-80-210-5449-3.

5.4 KVALIFIKAČNÍ PRÁCE

[7] DVOŘÁKOVÁ, Michaela. *Právo na informační sebeurčení a nedovolené šíření sexuálních záznamů* [online]. Brno, 2018 [cit. 29. 4. 2020]. Diplomová práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Kateřina ŠIMÁČKOVÁ, 117 s. Dostupné z: https://is.muni.cz/th/t361z/

5.5 ČLÁNKY Z ODBORNÝCH PUBLIKACÍ

[8] BATES, Samantha. Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors. *Feminist Criminology* [online]. 2017, roč. 12, 1 [cit. 27. 4. 2020] s. 22-42. ISSN: 1557-086X. Dostupné z: http://journals.sagepub.com/doi/abs/10.1177/1557085116654565

[9] CITRON, Danielle Keats. Sexual Privacy. *The Yale Law Journal* [online]. 2018-2019, roč. 128, 7 [cit. 29. 4. 2020], s. 1870-1960. ISSN: 1939-8611. Dostupné z: https://www.yalelawjournal.org/article/sexual-privacy

[10] CITRON, Danielle Keats; FRANKS, Mary Anne. Criminalizing Revenge Porn. *Wake Forest Law Review* [online]. 2014, roč. 49, [cit. 27. 4. 2018], s. 345-391. ISSN: 0043-003X. Dostupné z: http://repository.law.miami.edu/cgi/viewcontent.cgi?article=1059&context=fac_articles

[11] DELFINO, Rebecca. Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act. *Fordham Law Review* [online]. 2019, roč. 88, 3 [cit. 27. 4. 2020], s. 887-938. ISSN: 0015-704X. Dostupné z: https://ir.lawnet.fordham.edu/flr/vol88/iss3/2/

[12] FRANKS, Mary Anne; WALDMAN, Ari Ezra. Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions. *Maryland Law Review* [online]. 2019, roč. 78, 4 [cit. 29. 4. 2020], s. 892-898. ISSN: 0025-4282 Dostupné z: https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=3835&context=mlr

[13] HALL, Holly Kathleen. Deepfake Videos: When Seeing Isn't Believing. *Catholic University Journal of Law and Technology* [online]. 2018, roč. 27, 1 [cit. 27. 9. 2020], s. 51-76. ISSN: 1068-5871. Dostupné z: https://scholarship.law.edu/cgi/viewcontent.cgi?article=1060&context=jlt

[14] HARRIS, Douglas. Deepfakes: False Pornography Is Here and the Law Cannot Protect You. *Duke Law & Technology Review* [online]. 2019, roč. 17, 1 [cit. 28. 4. 2020], s. 99-127. ISSN: 2328-9600 Dostupné z: https://scholarship.law.duke.edu/dltr/vol17/iss1/4/

[15] CHESNEY, Robert; CITRON, Danielle Keats. Deep Fakes: A Looming Crisis for National Security, Democracy and Privacy? *California Law Review* [online]. 2019, roč. 107, 6 [cit. 29. 4. 2020], s. 1753-1820. ISSN: 1942-6542. Dostupné z: http://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security/

[16] KIRCHENGAST, Tyrone; CROFTS, Thomas. The legal and policy contexts of 'revenge porn' criminalisation: the need for multiple approaches. *Oxford University Commonwealth Law Journal* [online]. 2019, roč. 19, 1 [cit. 28. 4. 2020], s. 1-29. ISSN: 1757-8469. Dostupné z: https://www.tandfonline.com/doi/abs/10.1080/14729342.2019.1580518?journalCode=rouc20

[17] MCGLYNN, Clare; RACKLEY, Erika. Image-Based Sexual Abuse. *Oxford Journal of Legal Studies* [online]. 2017, roč. 37, 3 [cit. 6. 4. 2020], s. 534-561. ISSN: 1464-3820. Dostupné z: https://academic.oup.com/ojls/article-abstract/37/3/534/2965256?redirectedFrom=fulltext

[18] MESARČÍK, Matúš; ZIMEN, Ondrej. Deep fakes a ochrana súkromia. *Acta Facultatis Iuridicae Universitatis Comenianae* [online]. 2019, roč. 38, 2 [cit. 29. 4. 2020] s. 227-242. ISSN: 1336-6912. Dostupné z: https://afi.flaw.uniba.sk/index.php/AFI/article/view/65

[19] NISSELBAUM, Helen. Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy* [online]. 1998, roč. 17, 5/6 [cit. 29. 4. 2020], s. 559-596. ISSN: 0167-5249. Dostupné z: https://www.jstor.org/stable/3505189?seq=1#metadata_info_tab_contents

[20] ÖHMAN, Carl. Introducing the pervert's dilemma: a contribution to the critique of Deepfake Pornography. *Ethics and Information Technology* [online]. 2019 [cit. 29. 4. 2020]. ISSN: 1572-8439. Dostupné z: https://link.springer.com/article/10.1007/s10676-019-09522-1

[21] REIMAN, Jeffrey H. Privacy, Intimacy and Personhood. *Philosophy and Public Affairs* [online]. 1976, roč. 6, 1 [cit. 26. 9. 2020], s. 26-44. ISSN: 1088-4963. Dostupné z: https://www.jstor.org/stable/2265060?seq=1

[22] SPIVAK, Russell. "Deepfakes": The Newest Way to Commit One of the Oldest Crimes. *Georgetown Law Technology Review* [online]. 2019, roč. 3, 2 [cit. 27. 4. 2020], s. 339-400. Dostupné z: https://georgetownlawtechreview.org/wp-content/uploads/2019/05/3.1-Spivak-pp-339-400.pdf

[23] ŠEPEC, Miha. Revenge Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence Pornography or Non-Consensual. *International Journal of Cyber Criminology* [online]. 2019, roč. 13, 2 [cit. 29. 4. 2020], s. 418-438. ISSN: 0974-2891. Dostupné z: https://www.cybercrimejournal.com/MihaSepecVol13Issue2IJCC2019.pdf

[24] VACCARI, Christian; CHADWICK, Andrew. Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. *Social Media + Society* [online]. 2020, roč. 6, 1 [cit. 27. 9. 2020], s. 1-12. ISSN: 2056-3051. Dostupné z: https://journals.sagepub.com/doi/pdf/10.1177/2056305120903408

5.6 ELEKTRONICKÉ ZDROJE

[25] 2013 NCP Study Results. In: *Cyber Civil Rights Initiative* [online]. ©2018 [cit. 27. 4. 2020]. Dostupné z: https://www.cybercivilrights.org/wp-content/uploads/2016/11/NCP-2013-Study-Research-Results-1.pdf

[26] BERGER, Miriam. Brazilian 17-Year-Old Commits Suicide After Revenge Porn Posted Online. In: *BuzzFeed News* [online]. 20. 11. 2013 [cit. 27. 4. 2020]. Dostupné z: https://www.buzzfeed.com/miriamberger/brazilian-17-year-old-commits-suicide-after-revenge-porn-pos?utm_term=.lxoO1z9r4#.txZ2n7aGr

[27] BURÝŠKOVÁ, Lenka. Vydíral ženu přes facebook. In: *Policie České republiky – KŘP Královéhradeckého kraje* [online]. 2. 9. 2016 [cit. 29. 4. 2020]. Dostupné z: http://www.policie.cz/clanek/vydiral-zenu-pres-facebook.aspx

[28] COLE, Samantha. Deepfakes Were Created As a Way to Own Women's Bodies—We Can't Forget That. In: *Vice* [online]. 19. 4. 2018 [cit. 30. 4. 2020]. Dostupné z: https://www.vice.com/en_us/article/j5kk9d/deepfakes-were-created-as-a-way-to-own-womens-bodieswe-cant-forget-that-v25n2

[29] COLLINS, Ben. Russia-linked account pushed fake Hillary Clinton sex video. In: *NBC News* [online]. 11. 4. 2018 [cit. 29. 4. 2020]. Dostupné z: https://www.nbcnews.com/tech/security/russia-linked-account-pushed-fake-hillary-clinton-sex-video-n864871

[30] DOLD, Kristen. Face-Swapping Porn: How a Creepy Internet Trend Could Threaten Democracy. In: *Rolling Stone* [online]. 17. 4. 2018 [cit. 29. 4. 2020]. Dostupné z: https://www.rollingstone.com/culture/culture-features/face-swapping-porn-how-a-creepy-internet-trend-could-threaten-democracy-629275/

[31] DRAHOKOUPILOVÁ, Lenka. Prozrazení hesla se jí nevyplatilo. In: *Policie České republiky – KŘP Jihomoravského kraje* [online]. 12. 12. 2019 [cit. 29. 4. 2020]. Dostupné z: https://www.policie.cz/clanek/prozrazeni-hesla-se-ji-nevyplatilo.aspx

[32] EATON, Asia A.; JACOBS, Holly; RUVALCABA, Yanet. 2017 Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration. A Summary Report. In: *Cyber Civil Rights Initiative* [online]. ©2017 [cit. 27. 4. 2020], 28 s. Dostupné z: https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf

[33] ENGLAND, Charlotte. Teenager jailed for broadcast of girl's rape on online Periscope app. In: *The Independent* [online]. 15. 2. 2017 [cit. 28. 4. 2020]. Dostupné z: http://www.independent.co.uk/news/world/americas/teenager-marina-lonina-livestream-rape-17-year-old-friend-periscope-app-sentence-prison-columbus-a7581196.html

[34] FRANKS, Mary Anne. Combating Non-Consensual Pornography: A Working Paper. In: *SSRN* [online]. 7. 9. 2014 [cit. 27. 4. 2020], 17 s. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2336537

[35] GESSEN, Masha. The Terrorization of Katie Hill. In: *The New Yorker* [online]. 5. 11. 2019 [cit. 27. 4. 2020]. Dostupné z: https://www.newyorker.com/news/our-columnists/the-terrorization-of-katie-hill?utm_campaign=falcon&utm_source=facebook&utm_social-type=owned&mbid=social_facebook&utm_medium=social&utm_brand=tny&fbclid=IwAR01EotER_bQTgbX5dqMmKMqlU84hNshdxAqDM08LV9pCxAAuA-ucHp506s

[36] GSTALTER, Morgan. 'Obama' Voiced by Jordan Peele in PSA Video Warning About Fake Videos. In: *The Hill* [online]. 17. 4. 2018 [cit. 29. 4. 2020]. Dostupné z: https://thehill.com/blogs/in-the-know/in-the-know/383525-obama-voiced-by-jordan-peele-in-psa-video-warning-about-fake

[37] HLAVÁČOVÁ, Veronika; DUCHKOVÁ, Anna. Internetový sexuální predátor se mi naboural do webkamery a sledoval, jak se převlékám, říká Monika. In: *iROZHLAS* [online]. 2. 3. 2020 [cit. 29. 4. 2020]. Dostupné z: https://www.irozhlas.cz/zivotni-styl/spolecnost/internetovy-sexualni-predator-serial-pojd-si-se-mnou-psat-webkamera-v-siti_2003021909_jgr

[38] JANDA, Petr. Zneužití fotografie. In: *Policie České republiky – KŘP Královéhradeckého kraje* [online]. 7. 3. 2012 [cit. 29. 4. 2020]. Dostupné z: https://www.policie.cz/clanek/zneuzite-fotografie.aspx

[39] JIROUŠKOVÁ, Pavla. Láska přes internet nedopadla dobře. In: *Policie České republiky – KŘP Moravskoslezského kraje* [online]. 26. 11. 2019 [cit. 29. 4. 2020]. Dostupné z: https://www.policie.cz/clanek/laska-pres-internet-nedopadla-dobre.aspx

[40] KOPECKÝ, Kamil; SZOTKOWSKI, René. Sexting a rizikové seznamování českých dětí v kyberprostoru. Výzkumná zpráva. In: *Univerzita Palackého v Olomouci ve spolupráci se společností 02 Czech Republic* [online]. ©2017 [cit. 29. 4. 2020]. Dostupné z: https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/96-sexting-a-rizikove-seznamovani-2017/file

[41] KOZUMPLÍKOVÁ, Monika. Než pošleš nahou fotku, přemýšlej!. In: *Policie České republiky – KŘP Zlínského kraje* [online]. 31. 10. 2019 [cit. 29. 4. 2020]. Dostupné z: https://www.policie.cz/clanek/nez-posles-nahou-fotku-premyslej.aspx

[42] KYŠNEROVÁ, Simona. Vydíral ji jejími nahými fotkami. In: *Policie České republiky – KŘP Zlínského kraje* [online]. 12. 1. 2017 [cit. 29. 4. 2020]. Dostupné z: http://www.policie.cz/clanek/vydiral-ji-jejimi-nahymi-fotkami.aspx

[43] LADMANOVÁ, Dana. Důvěřivé ženy. In: *Policie České republiky – KŘP Plzeňského kraje* [online]. 27. 12. 2017 [cit. 29. 4. 2020]. Dostupné z: http://www.policie.cz/clanek/duverive-zeny.aspx

[44] LENHART, Amanda; YBARRA, Michelle; PRICE-FEENEY, Myeshia. Nonconsensual Image Sharing: one in 25 Americans has been a victim of "Revenge Porn". In: *Data & Society Research Institute* [online]. 13. 12. 2016 [cit. 28. 4. 2020], 8 s. Dostupné z: https://datasociety.net/pubs/oh/Nonconsensual_Image_Sharing_2016.pdf

[45] LEWENDOWSKI, Amanda. Our Best Weapon Against Revenge Porn: Copyright Law?. In: *The Atlantic* [online]. 4. 2. 2014 [cit. 29. 4. 2020]. Dostupné z: https://www.theatlantic.com/technology/archive/2014/02/our-best-weapon-against-revenge-porn-copyright-law/283564/

[46] LIN, Herb; HOLLAND, Hank J. The Danger of Deepfakes: Responding to Bobby Chesney and Danielle Citron. In: Lawfare [online]. 27. 2. 2018 [cit. 29. 4. 2020]. Dostupné z: https://www.lawfareblog.com/danger-deepfakes-responding-bobby-chesney-and-danielle-citron

[47] MATZNER, Jiří. Vydírá expřítelkyni zveřejněním intimních fotografií. In: *Policie České republiky – KŘP Jihočeského kraje* [online]. 3. 5. 2015 [cit. 29. 4. 2020]. Dostupné z: http://www.policie.cz/clanek/vydira-expritelkyni-zverejnenim-intimnich-fotografii.aspx

[48] MORAVČÍK, Ondřej. Když čtrnáctiletá Kristýna… In: *Policie České republiky – KŘP Královéhradeckého kraje* [online]. 20. 3. 2019 [cit. 29. 4. 2020]. Dostupné z: https://www.policie.cz/clanek/kdyz-ctrnactileta-kristyna.aspx

[49] RAFFAGHELLO, Ida a kol. What Does a Feminist Approach to Deepfake Pornography Look Like?. In: *Masters of Media* [online]. 24. 10. 2019 [cit. 28. 4. 2020]. Dostupné z: https://mastersofmedia.hum.uva.nl/blog/2019/10/24/what-does-a-feminist-approach-to-deepfake-pornography-look-like/

[50] REYNOLDS, James. Italy's Tiziana: Tragedy of a woman destroyed by viral sex video. In: *BBC* [online]. 13. 2. 2017 [cit. 27. 4. 2020]. Dostupné z: http://www.bbc.com/news/world-europe-38848528

[51] ROSEN, Jeffrey. The Web Means the End of Forgetting. In: *The New York Times Magazine* [online]. 21. 7. 2010 [cit. 27. 4. 2020]. Dostupné z: https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html

[52] SANGHANI, Radhika. Chrissy Chambers: 'My rape became revenge porn in the UK'. In: *The Telegraph* [online]. 17. 6. 2015 [cit. 29. 4. 2020]. Dostupné z: https://www.telegraph.co.uk/women/womens-life/11677742/YouTube-Chrissy-Chambers-My-rape-became-revenge-porn-in-the-UK.html

[53] SCHNEEWEISSOVÁ, Barbora. Sedmadvacetiletý muž několik let přes sociální sítě obtěžoval nezletilé dívky. In: *Policie České republiky – KŘP Středočeského kraje* [online]. 25. 11. 2019 [cit. 29. 4. 2020]. Dostupné z: https://www.policie.cz/clanek/sedmadvacetiletymuz-nekolik-let-pres-socialni-site-obtezoval-nezletile-divky.aspx

[54] SHEAD, Sam. Facebook to ban 'deepfakes'. In: *BBC* [online]. 7. 1. 2020 [cit. 29. 4. 2020]. Dostupné z: https://www.bbc.com/news/technology-51018758

[55] SMITH-SPARK, Laura; VANDOORNE, Saskya. Reports: Teen Daniel Perry commits suicide over Skype blackmail scam. In: *CNN* [online]. 16. 8. 2013 [cit. 27. 4. 2020]. Dostupné z: https://edition.cnn.com/2013/08/16/world/europe/uk-cyber-blackmail-suicide/index.html

[56] Steubenville Ohio School Footballers Guilty of Rape. In: *BBC* [online]. 17. 3 2013 [cit. 29. 4. 2020]. Dostupné z: https://www.bbc.com/news/world-us-canada-21823042

[57] Tomáš Řepka půjde do vězení, odvolací soud mu zvýšil trest. In: *iROZHLAS* [online]. 30. 4. 2019 [cit. 30. 4. 2020]. Dostupné z: https://www.irozhlas.cz/sport/fotbal/tomas-repka-vezeni-odvolaci-soud-2-roky-sparta-praha-zpronevera_1904301028_vman

[58] WINKLEY, Lyndsay; LITTLEFIELD, Dana. Sentence revised for revenge porn site operator. In: The San Diego Union-Tribune [online]. 21. 9. 2015 [cit. 27. 4. 2020]. Dostupné z: http://www.sandiegouniontribune.com/sdut-kevin-bollaert-revenge-porn-case-resentencing-2015sep21-story.html

[59] ZÁMEČNÍK, Petr. Začalo to nevinně. In: *Policie České republiky – KŘP Jihomoravského kraje* [online]. 23. 3. 2018 [cit. 29. 4. 2020]. Dostupné z: https://www.policie.cz/clanek/zacalo-to-nevinne.aspx

[60] ŽLÁBKOVÁ, Ludmila. Snímky polonahých dívek od zhrzených partnerů zaplavily český internet. In: *Novinky.cz* [online]. 9. 11. 2014 [cit. 27. 4. 2020]. Dostupné z: https://www.novinky.cz/internet-a-pc/352987-snimky-polonahych-divek-od-zhrzenych-partneru-zaplavily-cesky-internet.html

5.7 ROZHODNUTÍ ČESKÝCH SOUDŮ

[61] Nález Ústavního soudu ze dne 11. 11. 2005, sp. zn. I. ÚS 453/03.

[62] Nález Ústavního soudu ze dne 20. 12. 2016, sp. zn. Pl. ÚS 3/14.

[63] Rozsudek Nejvyššího soudu ze dne 27. 5. 2015, sp. zn. 30 Cdo 5216/2014.

[64] Usnesení Nejvyššího soudu ze dne 14. 7. 2015, sp. zn. 4 Tdo 843/2015.

5.8 ROZHODNUTÍ SOUDNÍHO DVORA EU

[65] Rozsudek Soudního dvora (velkého senátu) ze dne 13. 5. 2014 ve věci C-131/12, Google Spain and Google, ECLI EU:C:2014:317.

5.9 ROZHODNUTÍ EVROPSKÉHO SOUDU PRO LIDSKÁ PRÁVA

[66] Rozsudek Evropského soudu pro lidská práva ze dne 22. 10. 1981. Dudgeon vs. Spojené království. ECHR 7525/76. In: *HUDOC* [online]. Evropský soud pro lidská práva [cit. 29. 4. 2020]. Dostupné z: http://hudoc.echr.coe.int/eng?i=001-57473

[67] Rozsudek Evropského soudu pro lidská práva ze dne 28. 1. 2003. Peck vs. Spojené království. ECHR 44647/98. In: *HUDOC* [online]. Evropský soud pro lidská práva [cit. 29. 4. 2020]. Dostupné z: http://hudoc.echr.coe.int/eng?i=001-60898

[68] Rozsudek Evropského soudu pro lidská práva ze dne 4. 12. 2008. S. a Marper vs. Spojené království. ECHR 30562/04 a 30566/04. In: *HUDOC* [online]. Evropský soud pro lidská práva [cit. 29. 4. 2020]. Dostupné z: http://hudoc.echr.coe.int/eng?i=001-90051

5.10 ROZHODNUTÍ ZAHRANIČNÍHO SOUDU

[69] Rozhodnutí Spolkového ústavního soudu SRN ze dne 15. 12. 1983, BVerfGE 65, 1. In: *OpenJur* [online]. 2012 [cit. 29. 4. 2020]. Dostupné z: https://openjur.de/u/268440.html

5.11 PRÁVNÍ PŘEDPISY ČR

[70] Usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění ústavního č. zákona 162/1998 Sb.

[71] Zákon č. 480/2004 Sb., o některých službách informační společnosti.

[72] Zákon č. 40/2009 Sb., trestní zákoník.

[73] Zákon č. 89/2012 Sb., občanský zákoník.

5.12 PRÁVNÍ PŘEDPISY EU

[74] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. 4. 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES. In: *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679&from=CS

[75] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. 6. 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu. In: *EUR-lex* [právní informační systém]. Úřad pro publikace Evropské unie. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32000L0031&from=EN

5.13 MEZINÁRODNÍ SMLOUVY

[76] Úmluva o ochraně lidských práv a základních svobod Rady Evropy ze dne 4. 11. 1950, ve znění Protokolů 11 a 14, s Protokoly 1, 4, 6, 7, 12 a 13. In: *Evropský soud pro lidská práva* [online]. Evropský soud pro lidská práva [cit. 30. 4. 2020]. Dostupné z: http://www.echr.coe.int/Documents/Convention_CES.pdf

https://doi.org/10.5817/RPT2020-2-3

YOUTUBE, CONTENT ID A TVORBA UŽIVATELŮ VE SVĚTLE ČLÁNKU 17 DSM SMĚRNICE

JELIZAVETA LAŠKEVIČOVÁ[1]

ABSTRAKT

Příspěvek na příkladu YouTube jako typické upload-platformy zkoumá dvě cesty nabízené článkem 17 DSM směrnice, jak zachovat soulad sdílení uživatelského obsahu s právem duševního vlastnictví za podmínek nového režimu odpovědnosti upload-platforem. Jedno z nabízených východisek v důsledku vede k zavedení systémů automatizovaného rozpoznávání obsahu. Nástroj Content ID vyvinutý YouTube má předpoklady stát se určujícím pro stanovení standardu, který musí takové systémy splňovat. Proto lze na jeho příkladu hodnotit, zda je cesta filtrování obsahu vhodná pro spravedlivé vyvážení rozličných zájmů zúčastněných subjektů. V příspěvku bude seznáno, že nástroje automatického rozpoznávání obsahu jsou problematické, a bude diskutována německá cesta implementace, která kreativně využívá druhou možnost, tedy získání svolení nositelů práv, pro zavedení nové výjimky. Závěrem bude nastíněn význam německé výjimky pro budoucí efektivní licencování děl za podmínek odstavců 1 a 2 článku 17 DSM směrnice formou zákonné licence.

KLÍČOVÁ SLOVA

článek 17 DSM směrnice, YouTube, Content ID, UGC, výjimky a omezení, filtrování obsahu, licencování

[1] Jelizaveta Laškevičová, studentkou pátého ročníku Právnické fakulty Univerzity Karlovy. Kontaktní e-mail: liz.lashkevich@gmail.com.

ABSTRACT

The article, using the example of YouTube as a typical upload platform, examines the two ways offered by Article 17 of the DSM Directive on how to keep the sharing of user-generated content in line with intellectual property rights under the new upload platform liability regime. One of the offered solutions leads to the introduction of automated content recognition systems. The Content ID system developed by YouTube has the capacity to become a standard for such systems. Therefore, its example can be used to assess whether a content-filtering path is appropriate for striking a fair balance of the different interests of stakeholders. The paper will recognize that automatic content recognition tools are problematic, and will discuss the German path of implementation, which creatively uses the second option, i.e. obtaining the consent of rights holders, to introduce a new exception. The article ends with a discussion of the importance of the German exception to the future effective licensing of protected works under the conditions of paragraphs 1 and 2 of Article 17 of the DSM Directive, which could take form of a statutory licence.

KEYWORDS

article 17 DSM Directive, YouTube, Content ID, UGC, exceptions and limitations, upload filters, licensing

1. ÚVOD

Článek 17 DSM směrnice[2] přináší výrazné změny pro tzv. upload-platformy, které stojí na pomezí mezi klasickými poskytovateli hostingových služeb požívajícími *safe harbour* a poskytovateli *on-demand* služeb, kteří plně odpovídají za jimi zpřístupňovaný obsah. Upload-platformy jsou zásadním prvkem participativního webu, protože vytvářejí prostředí pro tvorbu nového obsahu a sociální interakce. Typickým představitelem těchto platforem je YouTube. Vzhledem k množství nahrávaného obsahu (v březnu 2019 bylo každou minutu na YouTube nahráváno cca 500 hodin videa)[3] a množství odběratelů (mezi lety 2018 a 2019 narostl počet kanálů na YouTube,

[2] Směrnice (EU) 2017/790 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES.

které mají více než 1 milion odběratelů, o 50 %)[4] jde o platformu, která je pro fungování participativního webu velmi podstatná.

YouTube, který původně nabízel téměř výlučně uživatelský obsah, se díky povaze svých služeb potýkal se značnými problémy v oblasti porušování autorského práva.[5] V reakci na konflikty s nositeli práv začal YouTube vyvíjet systém automatizovaného rozpoznávání obsahu Content ID, jehož prostřednictvím nyní probíhá 98 % správy autorských práv na YouTube.[6]

Článek 17 DSM směrnice zakotvuje nový režim odpovědnosti upload-platforem a nabízí dvě východiska, jak zachovat soulad sdílení uživatelského obsahu s právem duševního vlastnictví. Implementací můžou národní zákonodárci podpořit jedno z těchto řešení na úkor druhého a tak ovlivnit, kterou cestu bude praxe spíš využívat. Jedno z nabízených východisek v důsledku vede k zavedení systémů automatizovaného rozpoznávání obsahu, jak bude demonstrováno níže. Proto lze na příkladu Content ID jako typického zástupce těchto systémů zkoumat, zda je tato cesta vhodná zejména z hlediska ochrany práv uživatelů. V příspěvku bude seznáno, že nástroje automatického rozpoznávání obsahu jsou problematické, a bude diskutována německá cesta implementace, která kreativně využívá druhou možnost, tedy získání svolení nositelů práv, pro zavedení nové výjimky. Závěrem bude nastíněn význam německé výjimky pro budoucí efektivní licencování děl za podmínek odstavců 1 a 2 článku 17 DSM směrnice formou zákonné licence.

---

[3] JOHNSON, Eric. Full Q&A: YouTube CEO Susan Wojcicki talks about child safety, the Google walkout, and AI on Recode Decode [online]. 2019 [cit. 27.09.2020]. Dostupné z: https://www.vox.com/podcasts/2019/3/11/18259303/youtube-susan-wojcicki-child-comments-videos-google-walkout-kara-swisher-decode-podcast-interview

[4] *Öffentliche Konsultation zur Umsetzung der EU-Richtlinie imUrheberrecht (DSM-RL (EU) 2019/790)* [online]. Google a YouTube, 2019. s. 17. [cit. 23.09.2020]. Dostupné z: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Konsultation_Umsetzung_EU_Richtlinien_Urheberrecht.html?nn=6712350

[5] BURGESS, Jean a Joshua GREEN. *YouTube: Online Video and Participatory Culture*. Polity Press, 2018. s. 35.

[6] *How Google Fights Piracy* [online]. 2018. s. 13. [cit. 24.09.2020]. Dostupné z: https://www.blog.google/documents/27/How_Google_Fights_Piracy_2018.pdf

2. CHARAKTERISTIKA UŽIVATELSKÉ TVORBY

V posledních letech zaznamenala kreativita uživatelů na upload-platformách nevídaný rozmach. Důvodem je dostupnost velkého množství děl, ze kterých mohou uživatelé čerpat, v digitální podobě, dále také rozvoj nástrojů, pomocí kterých je obsah vytvářen, a rozšířenost širokopásmového internetu.[7] OECD vnímá obsah vytvářený uživateli (*user created content* nebo *user generated content,* dále jen „UGC") jako jeden ze základních prvků participativního webu a stanovuje tři vlastnosti, které jsou pro něj charakteristické – nutnost zpřístupnění veřejnosti (byť se může jednat o úžeji vymezenou veřejnost jako např. určitou komunitu), vynaložení tvůrčího úsilí (ačkoli míra kreativity se může u jednotlivých výtvorů velmi lišit) a vytvoření mimo profesní rámec (*creation outside of professional routines and practices*).[8]

Tvorba uživatelů může na sebe brát různé podoby, každopádně se často neobejde bez prvků, které jsou chráněny autorským právem. Někdy sledují výpůjčky uživatelů účely předvídané zákonnými výjimkami a omezeními autorského práva jako karikatura, parodie či recenze, jindy jde o transformativní užití jiného rázu, např. tzv. *meme* – existující dílo (typicky fotografie, obraz nebo video) kreativně pozměněné tak, aby vyvolávalo komický efekt, které se organicky šíří na sociálních sítích.[9] Zejména v případě relativně nových fenoménů jako *memes* není lehké určit, zda užití původního díla je ospravedlněno výjimkou pro parodii nebo karikaturu či nikoli. Hranice mezi zákonem uznávanými a novými formami transformativního užití díla je tedy v dnešní době poměrně tenká.

Co do právního rámce obsahu vytvářeného uživateli, v některých případech bude požívat ochrany poskytované systémem výjimek a omezení au-

---

[7] WONG, Mary W. S. „Transformative" User-Generated Content in Copyright Law: Infringing Derivative Works or Fair Use? *Vanderbilt Journal of Entertainment & Technology Law*. 2009, roč. 11, č. 4. s. 1077 – 1079.

[8] OECD, Graham VICKERY a Sacha WUNSCH-VINCENT. *Participative Web and User-Created Content* [online]. 2007. s. 18. [cit. 26.09.2020]. Dostupné z: https://www.oecd-ilibrary.org/content/publication/9789264037472-en

[9] Pro další definice viz např. https://www.merriam-webster.com/dictionary/meme nebo https://dictionary.cambridge.org/dictionary/english/meme.

torského práva. Tyto výjimky a omezení byly z různých důvodů společností uznány jako prospěšné a hodné ochrany (přispívají např. k zachování kulturní rozmanitosti, rozvoji vědy nebo uplatňování svobody projevu). Vycházejí ze základních práv a svobod zakotvených mj. v Listině základních práv Evropské Unie (dále jen"LZPEU"), ve většině případů ze svobody umění a věd dle článku 13. Některé výjimky jako parodie nebo karikatura mají rovněž silný politický podtext a jsou proto úžeji spjaty se svobodou projevu a informací zaručenou článkem 11 LZPEU.

Na evropské úrovni jsou výjimky a omezení autorského práva upraveny zejména ve článku 5 InfoSoc směrnice[10] obsahujícím výčet výjimek a omezení, které členské státy mohou, ale nemusejí, implementovat. Aby mohly být využívány, musejí výjimky v každém konkrétním případě projít tzv. třístupňovým testem. Třístupňový test zahrnuje podmínky, které musí být splněny kumulativně. Za prvé lze výjimky a omezení uplatnit v určitých zvláštních případech. Za druhé, užití díla by nemělo být v rozporu s běžným způsobem užití díla. Za třetí, užitím díla nesmějí být nepřiměřeně dotčeny oprávněné zájmy autora.

Jiná transformativní užití této ochrany nepožívají. Důvodem může být skutečnost, že jsou relativně nová, takže zatím nebyla reflektována v právní úpravě. Zejména užití, která vykazují vysokou míru kreativity a transformace původního obsahu a jsou společensky prospěšná, mají teoretické předpoklady se stát součástí evropského systému výjimek a omezení, nicméně problém s jejich zakotvením v InfoSoc směrnici spočívá v tom, že katalog výjimek a omezení ve článku 5 InfoSoc směrnice je taxativní a, byť toto je poněkud zjednodušující tvrzení, evropské autorské právo dosud spočívalo na širokém výkladu výlučných práv autora a restriktivní interpretaci výjimek a omezení autorského práva.[11]

---

[10] 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.

[11] Např. rozsudek SDEU (čvrtého senátu) ze dne 16. 7. 2009 ve věci C-5/08, *Infopaq*, body 56-57, rozsudek SDEU (třetího senátu) ze dne 21. 10. 2010 ve věci C-467/08, *Padawan*, bod 36, rozsudek SDEU (třetího senátu) ze dne 26. 4. 2012 ve věci C 510/10, *DR a TV 2 Denmark*, bod 36 , Rozsudek SDEU (čtvrtého senátu) ze dne 10. 4. 2014 ve věci C 435/12, *ACI Adam*, body 33 - 34.

Nicméně probíhá normativní diskuze o významu UCG pro svobodu projevu.[12] Obsah vytvářený uživateli se stal nástrojem názorového sebevyjádření jednotlivců, kteří se z pasivních konzumentů mění v aktivní tvůrce a účastníky společenské diskuze. V USA zaznívají názory, že UGC má přímou vazbu na svobodu projevu zakotvenou v Prvním dodatku, protože naplňuje účel této svobody, kterým je rozvoj demokratické participativní kultury.[13] Jako příklad lze uvést videa vytvářená na podporu určité politické kampaně, pomocí kterých mohou jednotlivci obeznámit se svým názorem širokou veřejnost. Proto je třeba přizpůsobit koncepci svobody projevu novým poměrům a zejména zabránit tomu, aby práva duševního vlastnictví působila jako překážka pro šíření kulturních fenoménů.[14]

Střet svobody projevu a práva duševního vlastnictví se také promítnul do rozsudků Evropského soudu pro lidská práva ve věcech Ashby Donald proti Francii[15] a Neij proti Švédsku.[16] V těchto rozsudcích ESLP vyjádřil myšlenku, že svoboda projevu je výchozím bodem, od kterého se právo duševního vlastnictví odchyluje.[17] Na rozdíl od tradičního pojetí práva duševního vlastnictví ESLP chápe svobodu projevu jako vnější limit práva autorského a práv souvisejících, který je schopen ospravedlnit užití děl, která porušují tato práva.[18]

---

[12] Pro detailní přehled viz LEE, Yin Harn. *Copyright and Freedom of Expression: A Literature Review* [online]. CREATe, 2015. s. 119 an. [cit. 24.09.2020]. Dostupné z: DOI:10.5281/zenodo.18132

[13] BALKIN, Jack. Digital speech and democratic culture: A theory of freedom of expression for the information society. *New York University Law Review*. 2004, roč. 79. s. 33 –38.

[14] Ibid. s. 53.

[15] Rozsudek ESLP ze dne 10. 1. 2013 ve věci *Ashby Donald a další proti Francii*, stížnost č. 36769/08.

[16] Rozsudek ESLP ze dne 19. 2. 2013 ve věci *Neij a Sunde Kolmisoppi proti Švédsku*, stížnost č. 40397/12.

[17] GEIGER, Christophe a Elena IZYUMENKO. Copyright on the Human Rights' Trial: Redefining the Boundaries of Exclusivity Through Freedom of Expression. *IIC - International Review of Intellectual Property and Competition Law*. 2014, roč. 45. s. 325.

[18] QUINTAIS, João. *Copyright in the Age of Online Access: Alternative Compensation Systems in EU Law*. Wolters Kluwer, 2017. s. 255.

3. ČLÁNEK 17 DSM SMĚRNICE: KONEC BEZPEČNÉHO PŘÍSTAVU

Jak již bylo zmíněno v úvodu, DSM směrnice mění právní status YouTube. Článek 2 odst. 6 DSM směrnice zavádí novou kategorii poskytovatele služeb pro sdílení obsahu online (dále jen „poskytovatel"), jímž je míněn poskytovatel služby informační společnosti, jehož hlavním účelem nebo jedním z hlavních účelů je uchovávat velký počet děl chráněných autorským právem nebo jiných předmětů ochrany nahrávaných jeho uživateli a zpřístupňovat je veřejnosti, přičemž poskytovatel tato díla a jiné předměty ochrany uspořádává a propaguje za účelem zisku. Z této definice jsou vyňaty některé subjekty jako např. neziskové online encyklopedie, nezisková vzdělávací a vědecká úložiště, platformy pro vývoj a sdílení softwaru s otevřeným zdrojovým kódem.

Podle odstavce 1 článku 17 DSM směrnice poskytovatelé provádějí sdělení veřejnosti nebo zpřístupnění veřejnosti pro účely této směrnice, pokud poskytují veřejnosti přístup k dílům chráněným autorským právem nebo jiným předmětům ochrany nahraným svými uživateli. Podle odstavce 3 článku 17 DSM směrnice se v takovém případě na poskytovatele nevztahuje omezení odpovědnosti podle článku 14 odst. 1 EC směrnice.[19] Článek 17 DSM směrnice tedy zakotvuje primární odpovědnost poskytovatele za obsah nahrávaný uživateli.

4. DVĚ CESTY IMPLEMENTACE

Článek 17 DSM směrnice dává poskytovatelům dvě možnosti, jak předejít odpovědnosti za sdílení uživatelského obsahu. První možností zakotvenou v odstavcích 1 a 2 článku 17 DSM směrnice je získání svolení nositelů práv, které se rovněž bude automaticky vztahovat i na nekomerční aktivity uživatelů. Druhou možností obsaženou v odstavci 4 článku 17 DSM směrnice je prokázat, že poskytovatel „vynaložil veškeré úsilí k získání svolení" a že „ v souladu s vysokými odvětvovými standardy odborné péče vynaložil veškeré úsilí k zajištění nedostupnosti děl [...], o nichž mu nositelé práv po-

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

skytli relevantní informace“. V případě oznámení nositelů práv o obsahu porušujícím jejich práva se aktivuje *notice and takedown* mechanismus nejspíše inspirovaný článkem 512 Digital Millenium Copyright Act.

Ačkoli odstavec 8 článku 17 DSM směrnice stanovuje, že uplatňování článku 17 nesmí vést k žádným povinnostem v oblasti dohledu, a navzdory moderačnímu pravidlu zakotvenému v odstavci 5 článku 17 DSM směrnice, druhá možnost zjevně vede k uplatňování systémů automatizovaného rozpoznávání obsahu. Pro tento závěr svědčí objem obsahu nahrávaného uživateli – jak už bylo zmíněno výše, v březnu 2019 bylo každou minutu na YouTube nahráváno cca 500 hodin videa. Evropská komise sice ve svém konzultačním dokumentu uvádí, že členské státy by při implementaci neměly podmínit prokazování „vynaložení veškerého úsilí“ ze strany poskytovatelů nasazením určité technologie,[20] není však jasné, jakým způsobem by jinak měli poskytovatelé dostát svým povinnostem podle odstavce 4 článku 17 DSM směrnice.

5. CONTENT ID

5.1 CONTENT ID JAKO STANDARD

Google s oblibou představuje ContentID jako jeden z nejdokonalejších nástrojů svého druhu, což není překvapivé, uvážíme-li, že do vývoje Content ID bylo investováno přes 90 milionů dolarů.[21] Databáze Content ID obsahuje přes 80 milionů referenčních souborů.[22] Jak poznamenává Tóth, za účelem efektivního zajištění nedostupnosti chráněných děl budou mít poskytovatelé zájem o nasazení nejmodernějších preventivních technologií.[23] Přihlédneme-li zároveň ke znění odstavce 4 článku 17 DSM směrnice, který

[20] *Targeted consultation addressed to the participants to the stakeholder dialogue on Article 17 of the Directive on Copyright in the Digital Single Market* [online]. Evropská komise, [cit. 24.09.2020]. Dostupné z: https://ec.europa.eu/eusurvey/runner/4fd43123-6008-a214-f572-4ecd331b9e0e

[21] *Öffentliche Konsultation zur Umsetzung der EU-Richtlinie imUrheberrecht (DSM-RL (EU) 2019/790)*. op. cit.

[22] *How Google Fights Piracy*. op. cit. s. 14.

[23] TÓTH, Andrea. Algorithmic Copyright Enforcement and AI: Issues and Potential Solutions through the Lens of Text and Data Mining. *Masaryk University Journal of Law and Technology*. 2019, roč. 13. s. 376.

vyžaduje soulad s „vysokými odvětvovými standardy odborné péče“, se tedy dá předpokládat, že Content ID a podobné systémy automatického rozpoznávání obsahu budou pro vytyčení těchto standardů určující. Z tohoto důvodu je nyní namístě tento systém stručně představit a na jeho příkladu rovněž prozkoumat nevýhody systémů automatického rozpoznávání obsahu zejména ve vztahu k uživatelům tvořícím obsah.

Princip Content ID je takový, že videa nahraná na YouTube jsou porovnávána s databází referenčních souborů poskytnutých nositeli autorských práv. Databáze systému Content ID obsahuje více než 80 milionů referenčních souborů, což z ní činí největší databázi na světě. Content ID využívá technologie *fingerprinting*. Tato technologie zkoumá vlastnosti samotného média (např. noty u zvukového záznamu) místo toho, aby zkoumala a porovnávala bity souboru, do kterého je obsah zakódován. *Fingerprint* konkrétního zvukového záznamu tedy bude obsahovat takové informace jako intenzita různých frekvencí v určitém časovém intervalu. Vzhledem k tomu, že *fingerprinting* využívá algoritmů, které zpracovávají charakteristiky média obsaženého v souboru (např. sled frekvencí ve skladbě), je omezen na konkrétní typ obsahu a je nutné mít odlišné nástroje pro videa, zvukové záznamy a další typy médií.[24]

Po uplatnění nároku k videu má nositel práv tři možnosti: dostávat příjmy z reklam videa, ponechat video přístupným a sledovat statistiku prohlížení nebo zablokovat video na YouTube úplně. YouTube poté uplatní u tohoto obsahu preferovanou akci nositele práv. Nicméně nejčastějším scénářem je zpeněžení. V roce 2017 se nositelé práv rozhodli zpeněžit 90 % všech nároků v systému Content ID. V hudebním průmyslu se nositelé práv rozhodli zpeněžit více než 95 % nároků na ID obsahu. Během posledních 5 let vyplatil YouTube nositelům práv využívajícím Content ID více než 3 miliardy dolarů.[25]

[24] ENGSTROM, Evan a Nick FEAMSTER. *The Limits of Filtering* [online]. Engine, 2017. s. 13 - 15. [cit. 28.05.2020]. Dostupné z: https://www.engine.is/the-limits-of-filtering

[25] *How Google Fights Piracy*. op. cit. s. 13.

5.2 ÚSKALÍ CONTENT ID

I přes soustavné zdokonalování a značné investice vykazuje Content ID určité nedostatky. Některé mají příčinu v současném stavu technologického rozvoje, jiné plynou z povahy systémů automatizovaného rozpoznávání obsahu. Hlavní potíží je skutečnost, že Content ID z principu nerozlišuje účel, za jakým došlo k užití cizího díla. Content ID umožňuje nositelům práv k autorskému dílu automaticky identifikovat, jestli jsou ve videu použity prvky, které jsou totožné s jejich obsahem. Na základě této identifikace následně dojde ke vznesení nároku. To, že systém správně určí shodu, však samo o sobě neznamená, že jde o neoprávněné užití. Během dialogu Komise a zúčastněných stran na základě odstavce 10 článku 17 DSM směrnice bylo zástupci šesti poskytovatelů systémů automatizovaného rozpoznávání obsahu potvrzeno, že jejich systémy nedokážou zohlednit kontext, ve kterém dochází k užití, a jako takové nemohou stanovit, zda užití spadá do rámce výjimky nebo omezení či nikoli.[26] Nadto se určité množství obsahu vytvořeného uživateli pohybuje na hraně zákonem uznávaných výjimek a omezení a automatizovaný filtrovací systém není způsobilý rozlišovat jemné nuance. Tak například k rozpoznání, že se jedná o parodii, zejména takovou, která není ostentativní, ale je vystavěna na rafinovaném smyslu pro humor, je potřeba humoru rozumět. Poněkud znepokojující je v tomto ohledu myšlenka, že když i zástupci poskytovatelů nejpoužívanějších systémů na trhu vyjadřují pochybnosti ohledně rozlišovacích schopností svých systémů, což teprve nástroje menších a méně významných poskytovatelů, kteří navíc v souladu s uplatňováním zásady přiměřenosti dle odstavce 5 článku 17 DSM směrnice zřejmě nemusejí prokazovat tak striktní dodržování „vysokých standardů odvětvové péče“?

Dalším úskalím, u kterého je však naděje, že je odstranitelné v čase, je poměrně velké množství neoprávněně vznesených nároků. Neoprávněnost má původ jak v technické nepřesnosti samotného systému automatizované-

[26] KELLER, Paul. Article 17 stakeholder dialogue: What we have learned so far – Part 1 - Kluwer Copyright Blog. In: Kluwer Copyright Blog [online]. 2020 [cit. 28.05.2020]. Dostupné z: http://copyrightblog.kluweriplaw.com/2020/01/13/article-17-stakeholder-dialogue-what-we-have-learned-so-far-part-1/?doing_wp_cron=1590693562.1587688922882080078125

ho rozpoznávání obsahu,[27] tak v ne vždy efektivním odhalení podvodných, neopodstatněných či excesivních nároků. Dle YouTube je 99,7 % Content ID nároků technicky správných, tedy nárokovaný obsah skutečně vykazuje shodu s referenčními soubory v databázi Content ID.[28] Nicméně podle empirických studií je přítomnost žadatelů o stažení obsahu ve zlé víře motivovaných například obtěžováním konkurence, umlčením kritiků či poškozením dobré pověsti poskytovatele nezanedbatelná.[29]

Následující skupina problémů se týká znevýhodnění uživatelů-jednotlivců, kteří na YouTube sdílejí vlastní obsah. Jedním problémem je jednostranné určení osudu díla, které bylo shledáno porušujícím, ze strany YouTube a nositelů práv. Byť obecně lze monetizaci obsahu považovat za kladnou stránku Content ID, protože takovým způsobem je přístup k obsahu zachován, je monetizace problematická z toho důvodu, že funguje jako zpětné udělování licence k užití autorskoprávně chráněného obsahu. Jednak takovou možnost licencování evropské právo vůbec nepředvídá, jednak jsou podmínky takové licenční smlouvy diktovány nositeli práv a uživatel nemá možnost namítat jejich nepřiměřenost nebo vůbec nějak o nich jednat.[30]

Další skutečností, která může posílit obavy o zachování dostupnosti uživatelského obsahu, je překvapivý výsledek využití Content ID nositeli práv, kdy podle výsledků empirických studií přistupovali britští nositelé práv k odstraňování napadených videí na YouTube v rozporu s argumenty, které namítali proti zavedení výjimky z autorského práva ve prospěch uživatelů.[31] Deklarované obavy se týkaly zachování ochrany tržní hodnoty děl, ohrožení integrity původního díla uživatelským obsahem apod. Ze studie však vyplynulo, že nositelé práv nechávali smazat obsah, který nebyl

---

[27] URBAN, Jennifer M., Joe KARAGANIS a Brianna L. SCHOFIELD. Notice and takedown: Online service provider and rightsholder accounts of everyday practice. *Journal of the Copyright Society of the USA*. 2017, roč. 64, č. 3. s. 392.

[28] *How Google Fights Piracy*. op. cit. s. 25.

[29] URBAN, Jennifer M., Joe KARAGANIS a Brianna L. SCHOFIELD. *Notice and takedown: Online service provider and rightsholder accounts of everyday practice*. op. cit. s. 396.

[30] TÓTH, Andrea. *Algorithmic Copyright Enforcement and AI: Issues and Potential Solutions through the Lens of Text and Data Mining*. s. 376.

[31] V daném případě šlo o zavedení výjimky pro účely parodie.

populární a tudíž ani komerčně významný, což mohlo poškodit zejména uživatele-jednotlivce, a ponechávali dostupnými a zpeněžovali virální videa.[32]

Uživatele by mohla také poškozovat skutečnost, že uplatnění systémů automatizovaného rozpoznávání obsahu k vymáhání práv nositelů mění výchozí nastavení – jestliže dříve byl chráněný obsah dostupný, dokud nebylo shledáno, že porušuje práva nositelů, je nyní běžně obsah odstraněn, ledaže by byl schválen nositelem práv.[33] Zejména ve světle nového pojetí odpovědnosti poskytovatele zaváděného článkem 17 DSM směrnice hrozí, že poskytovatelé budou inklinovat k blokování obsahu, aby naplnili pojem vynaložení „veškerého úsilí". Zárukou proti *overblockingu* by měl být odstavec 7 článku 17 DSM směrnice, který proklamuje, že spolupráce mezi poskytovateli služeb pro sdílení obsahu online a nositeli práv nesmí vést k omezování dostupnosti děl nahraných uživateli, na která se vztahuje výjimka nebo omezení včetně výjimky pro parodii. Vzhledem k tomu, že toto prohlášení není doprovázeno žádnými konkrétními opatřeními na omezení excesivní cenzury obsahu, zdá se, že poskytovatelé postrádají motivaci znepřístupňovat obsah selektivně a k *overblockingu* docházet bude.[34]

Ačkoli Content ID je využíván dobrovolně, v obecné rovině je zavádění systémů automatizovaného rozpoznávání obsahu problematické také z důvodů rozporu takové povinnosti se základními právy. Nesoulad uložení obecné monitorovací povinnosti poskytovateli služeb informační společnosti s jeho právem na podnikání a s právy uživatelů na respektování soukromí a na ochranu osobních údajů už byl reflektován v judikatuře

[32] ERICKSON, Kristofer a M KRETSCHMER. „This Video is Unavailable": Analyzing Copyright Takedown of User-Generated Content on YouTube. *JIPITEC : Journal of Intellectual Property, Information Technology and E-Commerce Law*. 2018, roč. 9. s. 21 - 24.

[33] ELKIN-KOREN, Niva. Fair Use by Design. *UCLA Law Review* [online]. 2017, roč. 64, č. 22. s. 1082. [cit. 24.09.2020]. Dostupné z: https://ssrn.com/abstract=3217839

[34] SENFTLEBEN, Martin. Bermuda Triangle – Licensing , Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market ". *SSRN Electronic Journal*. 2018. s. 8.

Soudního dvora Evropské unie.[35] V rozsudku SABAM[36] se kolektivní správce domáhal uložení povinnosti filtrování obsahu společnosti Netlog, která na svých stránkách umožňovala uživatelům sdílení hudby, filmů, fotografií a dalšího obsahu. Díla, k nimž spravoval práva SABAM, měla být znepřístupněna. Soudní dvůr Evropské unie seznal, že uložení takové časově neomezené povinnosti v oblasti dohledu by výrazně zasáhlo do svobody podnikání společnosti Netlog a do svobody projevu a informací uživatelů platformy Netlog.[37] Pokud by se však plnění povinností uložených článkem 17 DSM směrnice prostřednictvím Content ID stalo „vysokým odvětvovým standardem odborné péče", ostatní poskytovatelé by byli touto okolností nuceni k zavedení podobných systémů.

6. DRUHÁ CESTA

Vzhledem k výše diskutované problematičnosti systémů automatizovaného rozpoznávání obsahu se zdá být vhodnější cesta získání svolení nositelů práv. Tato možnost má také určité nevýhody. Jádrem těchto problémů je otázka, jak efektivně získat svolení nositelů práv pro tak veliké množství děl. První možností, kterou přímo nabízí alinea 2 odstavce 1 článku 17 DSM směrnice, je uzavření licenční smlouvy. Status quo pro většinu online užití děl je individuální výkon výlučných práv.[38] S výjimkou licencí typu *creative commons* je získávání takových licencí náročné a nákladné a navíc s ohledem na množství licencí, které je třeba získat, těžko uskutečnitelné.

Nabízí se tedy tzv. systémy náhradních odměn *(alternative compensation systems),* jejichž podstatou je, že dávají přednost zpřístupnění díla za přiměřenou odměnu před tradičním modelem výlučného výkonu práv a jejich vymáhání v případě porušení.[39] Zahrnují dobrovolnou, rozšířenou a povinnou

---

[35] Viz např. rozsudek SDEU (třetího senátu) ze dne 24. 11. 2011 ve věci C-70/10, *Scarlet Extended a* rozsudek SDEU (čtvrtého senátu) ze dne 27. 3. 2014 ve věci C-314/12, *UPC Telekabel*.

[36] Rozsudek SDEU (třetího senátu) ze dne 16. 2. 2012 ve věci C-360/10, *SABAM*.

[37] Ibid. body 46 – 50.

[38] QUINTAIS, João. *Copyright in the Age of Online Access: Alternative Compensation Systems in EU Law*. s. 87.

[39] Ibid.

kolektivní správu a zákonné licence. S ohledem na obšírnost tématu kolektivní správy se tento příspěvek dále zaměří zejména na možnost zavedení zákonných licencí.

7. PŘEDPOKLADY PRO ZAVEDENÍ ZÁKONNÉ LICENCE

Při řešení problému získání svolení nositelů práv přichází v úvahu také zavedení nové zákonné licence, která by v souladu s recitálem 74 DSM směrnice měla být úplatná. Tato možnost ovšem předpokládá, že článek 17 DSM směrnice poskytuje členským státům dostatečný manévrovací prostor při implementaci směrnice, protože v dosavadní úpravě článku 5 InfoSoc směrnice byl výčet výjimek a omezení taxativní, jak už bylo zmíněno. Kromě toho výjimky a omezení dle InfoSoc směrnice musí splňovat podmínky tříkrokového testu. Pokud by však článek 17 DSM směrnice nepodléhal režimu InfoSoc směrnice, nevztahovala by se na něj ani tato omezení.

Není tedy překvapující, že vztah článku 17 DSM směrnice a režimu InfoSoc směrnice se stal předmětem akademické debaty.[40] Šlo o to, zda právo na „sdělení veřejnosti nebo zpřístupnění veřejnosti pro účely této směrnice" v odstavci 1 článku 17 DSM směrnice je právem na sdělování veřejnosti ve smyslu článku 3 InfoSoc směrnice nebo zda je vůči němu ve vztahu speciality, či snad jde o právo *sui generis*. Již zmiňovaný konzultační dokument Evropské komise postavil najisto, že článek 17 DSM směrnice je *lex specialis* ke článku 3 InfoSoc směrnice.[41] Ve prospěch tohoto závěru svědčí jedinečná regulační technika článku 17 DSM směrnice, která místo přiznání výlučného práva nositeli práv (jako to dělá InfoSoc směrnice) stanovuje, že poskytovatel potřebuje svolení nositele práv, protože jinak zasahuje do práva nositele, a koncipuje složitý mechanismus odpovědnosti poskytovatele spolu

[40] HUSOVEC, Martin a João QUINTAIS. How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms. *SSRN Electronic Journal*. 2019.; Art. 17 DSMCD: a class of its own? How to implement Art. 17 into the existing national copyright acts, including a comment on the recent German Discussion Draft - Part 1. In: *Kluwer Copyright Blog* [online]. 16. 7. 2020 [cit. 25.09.2020]. Dostupné z: http://copyrightblog.kluweriplaw.com/2020/07/16/art-17-dsmcd-a-class-of-its-own-how-to-implement-art-17-into-the-existing-national-copyright-acts-including-a-comment-on-the-recent-german-discussion-draft-part-1/

[41] *Targeted consultation addressed to the participants to the stakeholder dialogue on Article 17 of the Directive on Copyright in the Digital Single Market*. op. cit. s. 4.

se stížnostním mechanismem uživatelů. Takovou úpravu nezná ani světové, ani evropské právo autorské.[42] Rovněž jazykovým výkladem odstavce 1 článku 17 DSM směrnice, který stanoví, že poskytovatelé provádějí sdělení veřejnosti nebo zpřístupnění veřejnosti „pro účely této směrnice", lze dospět k tomu, že režim článku 17 DSM směrnice stojí stranou systému InfoSoc směrnice. Vzhledem k tomu, že je článek 17 DSM směrnice *lex specialis*, neplatí pro něj *numerus clausus* výjimek a omezení stanovený článkem 5 InfoSoc směrnice. Tímto jsou tedy, zdá se, otevřeny dveře pro různá jiná řešení než licenční smlouva.

8. DER DEUTSCHE WEG

Německé Spolkové ministerstvo spravedlnosti a ochrany spotřebitele zveřejnilo 24. června 2020 návrh druhého zákona k přizpůsobení autorského práva digitálnímu vnitřnímu trhu. Tento návrh počítá s přijetím nového zákona o autorskoprávní odpovědnosti poskytovatelů služeb pro sdílení obsahu online (*Gesetz über die urheberrechtliche Verantwortlichkeit von Diensteanbietern für das Teilen von Online-Inhalten,* dále jen „UrhDaG"). § 6 UrhDaG zavádí novou výjimku z autorského práva pro „mechanicky přezkoumatelná zákonem povolená užití"[43]:

(1) Je přípustné sdělování veřejnosti a pro tento účel potřebné rozmnožování autorskoprávně chráněných děl a částí děl pro nekomerční účely v následujícím rozsahu:

1. až 20 sekund téhož filmu nebo pohyblivé obrazové sekvence,
2. až 20 sekund téhož zvukového záznamu,
3. až 1000 znaků téhož textu,
4. fotografii nebo grafiku s objemem dat až 250 kB.

[42] *Entwurf eines Zweiten Gesetzes zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarktes* [online]. 2020. s. 34. [cit. 23.09.2020]. Dostupné z: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/DiskE_II_Anpassung%20Urheberrecht_digitaler_Binnenmarkt.pdf?__blob=publicationFile&v=2

[43] UrhDaG rozlišuje užití, jejichž přípustnost nelze posoudit prostřednictvím stávajících technických prostředků (protože zatím nejsou tak dokonalé) a užití, jejichž soulad s autorskými právy lze posoudit pomocí systémů automatizovaného rozpoznávání obsahu.

(2) Odstavce 1 se použije, pokud neexistuje žádné smluvní užívací právo povolující užití dle odstavce 1 a pokud se nejedná o zákonem povolené užití podle § 5.[44]

Podle § 7 odstavce 2 UrhDaG je poskytovatel povinen poskytnout nositeli práv přiměřenou odměnu za užití podle § 6 UrhDaG. Nová zákonná výjimka tedy naplňuje požadavek úplatnosti vyplývající z recitálu 74 DSM směrnice. § 9 UrhDaG v souladu s odstavcem 2 článku 17 DSM směrnice vztahuje svolení, které platí pro poskytovatele, na nekomerční úkony uživatelů.

Podle důvodové zprávy k UrhDaG je účelem této výjimky zohlednění soudobých obchodních praktik, kdy pro reklamní účely jsou bezúplatně zpřístupňovány např. úryvky knih nebo trailery,[45] a také ochrana obsahu vytvořeného uživateli.[46]

9. ZÁKONNÁ LICENCE PRO UCG?

I přes svůj úzký záběr má německá výjimka význam – její zavedení je v důvodové zprávě podepřeno přesvědčivou argumentací, že zavádět další výjimky a omezení v režimu článku 17 DSM směrnice je v souladu s evropským právem. Ukazuje tedy cestu pro další výjimky v rámci speciálního režimu článku 17 DSM směrnice. Takovou výjimkou by mohla být celoevropská úplatná zákonná licence pro užití chráněných děl s cílem vytváření UGC splňující charakteristiky definované OECD (viz část 2 tohoto příspěvku), tedy zejména určitý stupeň kreativní transformace původního obsahu a vytvoření mimo rámec profesní aktivity (slovy DSM směrnice pokud uživatelé „nejednají v rámci podnikatelské činnosti a pokud jejich činnost nevytváří významné příjmy“). V souladu s odstavcem 2 článku 17 DSM by

[44] § 5 UrhDaG, který odkazuje na výjimky a omezení autorského práva zakotvené v německém autorském zákoně (Urheberrechtgesetz) a stanovuje, že je přípustné sdělování veřejnosti a rozmnožování autorskoprávně chráněných děl pro účely citace, karikatury, parodie a další účely zakotvené v německém autorském zákoně. Nutno poznamenat, že výjimka pro parodii, karikaturu a pastiš bude do německého práva implementována teprve v souvislosti s přijetím DSM směrnice.

[45] *Entwurf eines Zweiten Gesetzes zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarktes*. op.cit. s. 88.

[46] Ibid. s. 2.

povinnost vyplácet nositelům práv náhradní odměnu spočívala na poskytovateli.

Obecné výhody zákonné licence jako formy licencování nejlépe vyvstanou v kontrastu ke kolektivní správě, která je teritoriálně rozdrobená a v některých oblastech jako např. v audiovizi není pro online práva zavedena. Dobrovolná a do jisté míry i rozšířená kolektivní správa navíc trpí tím, že nositelé práv se mohou rozhodnout pro *opt-out*. Možnost zastřešující licence se tedy ve mnoha evropských státech zdá být neuskutečnitelná.[47] Nicméně k tomu, aby bylo řešení navrhované odstavcem 2 článku 17 DSM směrnice efektivní, je tento zastřešující efekt licencování nezbytný. Navíc poskytovatelé nemohou předvídat, jaká díla uživatelé nahrají, a tudíž ani to, čí svolení by měla být získána.

Zákonná licence pro obsah vytvářený uživateli by také mohla pomoci docílit rovnováhy mezi právem duševního vlastnictví a svobodou projevu a informací, kterou uživatelé často realizují právě prostřednictvím svých aktivit na YouTube a podobných platformách. Zavedení této zákonné licence by zabránilo *overblockingu* hrozícímu zejména v důsledku uplatnění systémů automatizovaného rozpoznávání obsahu (viz část 5.2 tohoto příspěvku) a dalším negativním důsledkům vymáhání autorských práv a práv souvisejících, které by mohly vést k erozi participativního webu. Zároveň by zákonná licence zohledňovala také zájmy nositelů práv, kterým by se dostalo spravedlivé náhradní odměny.

10. ZÁVĚR

Jak Senftleben výstižně definoval problém článku 17 DSM směrnice, jeho ustanovení dohromady vytvářejí neurčitý prostor podobný Bermudskému trojúhelníku, jehož stranami jsou licencování, filtrování a problematika uživatelského obsahu. Ačkoli jádro tohoto příspěvku se zabývalo důvody, proč místo používání systémů automatizovaného rozpoznávání obsahu bude zejména z hlediska uživatelů vhodnější se vydat cestou licencování, a následně teoretickými předpoklady vytvoření nové výjimky v rámci reži-

[47] SENFTLEBEN, Martin. *Bermuda Triangle – Licensing , Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market "*. op. cit. s. 4.

mu článku 17 DSM směrnice, doufejme, že ve výsledku byl (byť poněkud schematicky) nastíněn jeden z bezpečných směrů vyplutí z těchto temných vod.

11. SEZNAM ZDROJŮ

11.1 LITERATURA

[1] BALKIN, Jack. Digital speech and democratic culture: A theory of freedom of expression for the information society. *New York University Law Review*. 2004, roč. 79, s. 1–58.

[2] BURGESS, Jean a Joshua GREEN. *YouTube: Online Video and Participatory Culture*. 2. vyd. Polity Press, 2018. ISBN 978-0-7456-6019-6.

[3] ELKIN-KOREN, Niva. Fair Use by Design. *UCLA Law Review* [online]. 2017, roč. 64, č. 22 [cit. 24.09.2020]. Dostupné z: https://ssrn.com/abstract=3217839

[4] ENGSTROM, Evan a Nick FEAMSTER. *The Limits of Filtering* [online]. Engine, 2017 [cit. 28.05.2020]. Dostupné z: https://www.engine.is/the-limits-of-filtering

[5] ERICKSON, Kristofer a M KRETSCHMER. „This Video is Unavailable": Analyzing Copyright Takedown of User-Generated Content on YouTube. *JIPITEC : Journal of Intellectual Property, Information Technology and E-Commerce Law*. 2018, roč. 9

[6] GEIGER, Christophe a Elena IZYUMENKO. Copyright on the Human Rights' Trial: Redefining the Boundaries of Exclusivity Through Freedom of Expression. *IIC - International Review of Intellectual Property and Competition Law*. 2014, roč.45, s. 316–342.

[7] HUSOVEC, Martin a João QUINTAIS. How to License Article 17? Exploring the Implementation Options for the New EU Rules on Content-Sharing Platforms. *SSRN Electronic Journal*. 2019, s. 1–27.

[8] JOHNSON, Eric. Full Q&A: YouTube CEO Susan Wojcicki talks about child safety, the Google walkout, and AI on Recode Decode [online]. 2019 [cit. 27.09.2020]. Dostupné z: https://www.vox.com/podcasts/2019/3/11/18259303/youtube-susan-wojcicki-child-comments-videos-google-walkout-kara-swisher-decode-podcast-interview

[9] KELLER, Paul. Article 17 stakeholder dialogue: What we have learned so far – Part 1 - Kluwer Copyright Blog. In: *Kluwer Copyright Blog* [online]. 2020 [cit. 28.05.2020]. Dostupné z: http://copyrightblog.kluweriplaw.com/2020/01/13/article-17-stakeholder-dialogue-what-we-have-learned-so-far-part-1/?doing_wp_cron=1590693562.1587688922882080078125

[10] LEE, Yin Harn. *Copyright and Freedom of Expression: A Literature Review* [online]. CREATe, 2015 [cit. 24.09.2020]. Dostupné z: DOI:10.5281/zenodo.18132

[11] OECD, Graham VICKERY a Sacha WUNSCH-VINCENT. *Participative Web and User-Created Content* [online]. 2007 [cit. 26.09.2020]. Dostupné z: https://www.oecd-ilibrary.org/content/publication/9789264037472-en

[12] QUINTAIS, João. *Copyright in the Age of Online Access: Alternative Compensation Systems in EU Law*. Wolters Kluwer, 2017. ISBN 978-90-411-8667-6.

[13] SENFTLEBEN, Martin. Bermuda Triangle – Licensing , Filtering and Privileging User-Generated Content Under the New Directive on Copyright in the Digital Single Market ". *SSRN Electronic Journal*. 2018, s. 1–18.

[14] TÓTH, Andrea. Algorithmic Copyright Enforcement and AI: Issues and Potential Solutions through the Lens of Text and Data Mining. *Masaryk University Journal of Law and Technology*. 2019, roč. 13, s. 361.

[15] URBAN, Jennifer M., Joe KARAGANIS a Brianna L. SCHOFIELD. Notice and takedown: Online service provider and rightsholder accounts of everyday practice. *Journal of the Copyright Society of the USA*. 2017, roč. 64, č. 3, s. 317–410.

[16] WONG, Mary W. S. „Transformative" User-Generated Content in Copyright Law: Infringing Derivative Works or Fair Use? *Vanderbilt Journal of Entertainment & Technology Law*. 2009, roč. 11, č. 4, s. s. 1075-1139.

[17] Art. 17 DSMCD: a class of its own? How to implement Art. 17 into the existing national copyright acts, including a comment on the recent German Discussion Draft - Part 1. In: *Kluwer Copyright Blog* [online]. 16. 7. 2020 [cit. 25.09.2020]. Dostupné z: http://copyrightblog.kluweriplaw.com/2020/07/16/art-17-dsmcd-a-class-of-its-own-how-to-implement-art-17-into-the-existing-national-copyright-acts-including-a-comment-on-the-recent-german-discussion-draft-part-1/

[18] *Entwurf eines Zweiten Gesetzes zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarktes* [online]. 2020. s. 34. [cit. 23.09.2020]. Dostupné z: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/DiskE_II_Anpassung%20Urheberrecht_digitaler_Binnenmarkt.pdf?__blob=publicationFile&v=2

[19] *How Google Fights Piracy* [online]. 2018 [cit. 24.09.2020]. Dostupné z: https://www.blog.google/documents/27/How_Google_Fights_Piracy_2018.pdf

[20] *Öffentliche Konsultation zur Umsetzung der EU-Richtlinie im Urheberrecht (DSM-RL (EU) 2019/790)* [online]. Google a YouTube, 2019 [cit. 23.09.2020]. Dostupné z: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/Konsultation_Umsetzung_EU_Richtlinien_Urheberrecht.html?nn=6712350

[21] *Targeted consultation addressed to the participants to the stakeholder dialogue on Article 17 of the Directive on Copyright in the Digital Single Market* [online]. Evropská komise, [cit. 24.09.2020]. Dostupné z: https://ec.europa.eu/eusurvey/runner/4fd43123-6008-a214-f572-4ecd331b9e0e

11.2 JUDIKATURA

[21] Rozsudek SDEU (čvrtého senátu) ze dne 16. 7. 2009 ve věci C-5/08, *Infopaq*, ECLI:EU:C:2009:465.

[22] Rozsudek SDEU (třetího senátu) ze dne 21. 10. 2010 ve věci C-467/08, *Padawan*, ECLI:EU:C:2010:620.

[23] Rozsudek SDEU (třetího senátu) ze dne 26. 4. 2012 ve věci C 510/10, *DR a TV 2 Denmark*, ECLI:EU:C:2012:244.

[24] Rozsudek SDEU (čtvrtého senátu) ze dne 10. 4. 2014 ve věci C 435/12, *ACI Adam*, ECLI:EU:C:2014:254.

[25] Rozsudek SDEU (třetího senátu) ze dne 24. 11. 2011 ve věci C-70/10, *Scarlet Extended,* ECLI:EU:C:2011:771.

[26] Rozsudek SDEU (čtvrtého senátu) ze dne 27. 3. 2014 ve věci C-314/12, *UPC Telekabel*, ECLI:EU:C:2014:192.

[27] Rozsudek SDEU (třetího senátu) ze dne 16. 2. 2012 ve věci C-360/10, *SABAM*, ECLI: EU:C:2012:8.

[28] Rozsudek ESLP ze dne 10. 1. 2013 ve věci Ashby Donald a další proti Francii, stížnost č. 36769/08.

[29] Rozsudek ESLP ze dne 19. 2. 2013 ve věci Neij a Sunde Kolmisoppi proti Švédsku, stížnost č. 40397/12.

---

https://doi.org/10.5817/RPT2020-2-4

MODELOVÁNÍ PRÁVNÍCH NOREM NA ÚROVNI VĚT

JAKUB MICHÁLEK[1]

ABSTRAKT

Hypotézy norem složené z více podmínek jsou v právním řádu natolik rozsáhlé, že jejich sestavení je časově i intelektuálně náročné, a tudíž v řadě případů může jejich praktickou aplikaci podpora automatizovaného systému významně usnadnit, zlevnit a zkvalitnit. Takový systém ovšem vyžaduje nejprve model právních norem. V tomto článku explicitně formuluji hypotézy některých právních norem z oblasti práva na informace, a to konkrétně k hmotněprávním důvodům poskytování informací, poskytování utajovaných informací, poskytování informací o platech z veřejných prostředků a vydání rozhodnutí o odmítnutí žádosti o informace. Metodu v úvodu zasazuji do kontextu a dále ukazuji, jakou mají právní normy strukturu, definuji jejich funkční a strukturní vzorce na úrovni vět a navrhuji postup pro sestavení řetězce vyplývání a jeho pokrácení. Popisuji, jak se individualizací, prokázáním skutkového stavu a výběrem z alternativ tvoří z normy argument.

KLÍČOVÁ SLOVA

právní norma, model právních norem, právo na informace, právní informatika

ABSTRACT

Hypotheses of norms which consist of several conditions are in the legal order so extensive that their compilation is a challenge of both time and intellect. There-

[1] Mgr. et Mgr. Jakub Michálek, Autor studuje doktorské studium Právnické fakulty UK v Praze a dále působí jako místopředseda ústavně právního výboru Poslanecké sněmovny PČR. Vedle toho je také spoluautorem novely zákona č. 106/1999 Sb., o svobodném přístupu k informacím. E-mail: jakub.michalek@pirati.cz

fore in many cases the support of an automated decision system can make things significantly easier, cheaper and better. Such a system, however, requires a model of legal norms. In this article I present the explicit hypotheses of some legal norms from the field of free access to information in Czech law, such as material reasons for providing information in general, providing classified information, providing information on the salaries paid from public funds and issuing a decision on the rejection of an information request. In the introduction, I put the method in context and then show the structure of legal norms, define their functional and structural formulas at the level of sentences, and propose a procedure for assembling the chain of inference and its contraction. I describe how individualization, proving facts and choosing from alternatives translate the norm to an argument.

KEYWORDS

legal norm, model of legal norms, free access to information, legal informatics

1. ÚVOD

Cílem tohoto článku je poskytnout základní model hmotného práva v informačním zákoně[2], a to pomocí explicitní reprezentace norem na úrovni gramatických vět a jejich logické struktury.

Hmotným právem mám na mysli objektivní právo vyplývající z té části informačního zákona, která odpovídá na otázku, zda informace lze poskytnout či nikoliv (§ 7 až 12 cit. zákona). Zákon vedle toho rovněž obsahuje ustanovení informativní (§ 1), terminologické (§ 3), kompetenční (§ 2 odst. 1 vedlejší věta, § 20 odst. 5), působnostní (§ 2 odst. 3, § 20 odst. 1 až 3, § 22), aplikační (§ 20 odst. 4) a procesní (§ 4a a násl., § 13 a násl.).

V další části textu předpokládám, že je problém působnosti vyřešen – použitelnost níže uvedených právních předpisů presumuji.[3] Zaměřuji se jen

[2] Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění účinném k 1. 1. 2020 po novele provedené zákonem č. 111/2019 Sb.

[3] Jde o působnost právní normy zakotvenou např. v § 2 odst. 3 (věcná působnost), § 20 odst. 1 až 3, § 22 (časová působnost) nebo územní působnost. V tomto textu také předpokládáme vyřešení otázky personální působnosti (tj. určení povinného subjektu podle § 2 odst. 1 až 2).

na takto identifikovaný soubor norem (dále také „zkoumaný úsek práva“). Proto jsou příklady zjednodušené a nezahrnují např. otázky časové působnosti norem, které by v reálném nasazení bylo nutné doplnit do hypotézy, nicméně pro názornost výkladu s nimi zde nepočítám.

2. KONTEXT MODELU ZKOUMANÉHO ÚSEKU PRÁVA

K modelování práva jako informačního systému lze přistoupit např. z pohledu lingvistického či z pohledu formálně logického. Zatímco lingvistika akcentuje jazykové vyjádření a jeho parametry (viz např. Cvrčkova právní statistika[4]), logický pohled vyjadřuje vztahy mezi výroky, případně normami, ve zvolené logice (viz např. Štěpánova učebnice[5]). Cvrček[6] pak odlišuje deskriptivní část právní informatiky a tzv. modelování právního usuzování. Knapp[7] podobně rozlišuje tři úrovně právní informace, a to indikativní (uvedení adresy dokumentu), reproduktivní (uvedení obsahu) a deduktivní (podává informaci *quid iuris*). Všichni zmínění autoři mají v závěru na mysli totéž a právě na deduktivní úroveň právní informace, faktografickou povahu, logický pohled či v mém pojetí **modelování zkoumaného úseku práva** se v tomto článku zaměřuji.

K modelování práva lze používat modely, které mají různou úroveň abstrakce a typicky také jí nepřímo úměrnou náročnost simulace na počítači. Rád bych, aby na můj model nebyla kladena přehnaná očekávání, protože jde oblast zkoumání, která je pro právní informatiku stále nová. Model musí být přiměřeně rozsáhlý a zjednodušený, aby bylo vůbec možné dosáhnout výsledku v dohledné době. Musím předeslat, že řada poznatků v tomto článku se může jevit jako zcela samozřejmá, což však při dobrém modelu není nedostatkem modelu, ale jeho předností. Přesto je nutno tyto poznatky výslovně popsat, aby byly při modelování práva na počítači explicitně zachyceny.

---

[4] CVRČEK, F.: *Právní informatika*. Plzeň: Ústav státu a práva AV ČR ve spolupráci s Vydavatelstvím a nakladatelstvím Aleš Čeněk, 2010, s. 342.

[5] ŠTĚPÁN, J. *Logika a právo.* Praha: Beck, 2001, s. 25 a násl.

[6] CVRČEK, F., op. cit., s. 342.

[7] KNAPP, V.: *Teorie práva*. Plzeň: Západočeská univerzita, 1994, s. 155-156.

Jen s normativními pravidly uvedenými v zákonech nelze dospět k algoritmu právního posuzování.[8]

Proto:

- Používám klasické vymezení práva jako souboru norem vyvozených z právních předpisů (pramenů práva) interpretovaných ve světle judikatury soudů, případně doktríny. Snažím zachovat co nejvěrnější korespondenci mezi modelem a textem právního předpisu s přihlédnutím k jeho interpretaci judikaturou,[9] případně doktrínou. Při reprezentaci judikátů zaznamenávám právě ty skutkové okolnosti případu, které jsou relevantní. Za vhodnou ucelenou reprezentaci těchto znalostí považuji komentářovou literaturu.
- Pokud jde o paragraf, větu či jinou jednotku normativní části pramene práva, mluvím o „ustanovení". Některé strukturální prvky norem lze vyvodit přímočaře z textu právního předpisu či jiného pramene práva, případně z jejich soudní interpretace, pak jde o normy exponované. Některé strukturální prvky norem je nutné dovodit z kontextu nebo jsou předpokládány, potom mluvíme o presuponovaných prvcích.
- Vedle toho musí algoritmus zohlednit otevřenost některých rozhodovacích procesů,[10] v případě informačního práva hmotného například posouzení fakultativnosti[11] odepření informace (podle § 11 odst. 1 „Povinný subjekt *může* omezit poskytnutí informace, pokud …"). Normy regulující správního uvážení v případě tzv. nevázané pravomoci mohou být obsaženy v judikatuře soudů.

Dále budu mluvit o explicitní formulaci norem, která je systémem formálně standardizovaných vět specializovaného právního jazyka. Převod

[8] CVRČEK, F., op. cit., s. 342, KRECHT, J., op. cit., s. 136.

[9] MICHÁLEK, J. Co je právo a jak ho můžeme modelovat. *Právník. Teoretický časopis pro otázky státu a práva*, 2020, 159.4: 321-341, s. 333.

[10] BOGUSZAK, J., ČAPEK, J., a GERLOCH, A.: *Teorie práva*. Druhé, přepracované vydání. Praha: ASPI, 2004, s. 166 a násl.

[11] FUREK, A., ROTHANZL, L.: *Zákon o svobodném přístupu k informacím. Komentář*. 2. vyd. Praha: Linde, 2012, s. 405, a tam citovaný rozsudek NSS ze dne 2. 7. 2008, č. j. 1 As 44/2008-116.K dispozici je i novější vydání komentáře z roku 2016.

ustanovení do explicitní formulace nazývám explikací.[12] Některé základní práce v oboru logického programování práva modelují úsek práva logickým programem v predikátové logice.[13] Přehled tzv. právních expertních systémů by si zasloužil samostatný článek. Lze však zde shrnout, že již od 80. let minulého století se pravidelně objevují nové pokusy o počítačový model určitého úseku práva, aniž by se však kterýkoliv z nich významně rozšířil do praxe (specifické postavení mají programy navázané na kryptoměny, které však byly zase zasaženy bezpečnostními problémy).[14] Na rozdíl od nich v tomto článku uvažuji pouze strukturu práva na úrovni normativních a deskriptivních vět, které jsou spojeny podmiňovacími, slučovacími a vylučovacími spojkami, tedy v podstatě jakéhosi normativního ekvivalentu výrokové logiky.[15]

Bylo by naivní a nemístné se domnívat, že sebelepší model poskytne i vhled do úvah o interpretaci a tvorbě práva, ať už zákonného či soudcovského. Tyto rozhodovací procesy totiž mají výrazně otevřený charakter a je na první pohled zřejmé, že v nich mohou hrát silnou roli mimoprávní činitele.[16] Soustřeďme se tedy na tu část právního systému, kterou modelovat můžeme. Aby byl model prakticky užitečný, je vhodné ho spojit s určitou funkcí, přičemž se nabízejí dva základní problémy, a to zdůvodňování a odvozování.[17] Každý model dává smysl a je navrhován ve vztahu

---

[12] KRECHT, J.: *Normativní regulace.* Praha: Ediční středisko PF UK, 1997,, s. 135. K explikaci srovnej také ŠPIRUDA, A.: *Teorie právních norem*. Dizertační práce. Brno: Masarykova univerzita, 2011, s. 74 a násl. Dostupný na https://is.muni.cz/th/p04a3/Teorie_pravnich_norem.pdf [citováno 2. června 2020].

[13] SERGOT, M. J., et al.: The British Nationality Act as a logic program. In: *Communications of the ACM*, 1986, 29.5: 370-386. BENCH-CAPON, T. J. M., ROBINSON, G. O., ROUTEN, T. W., SERGOT, M. J. Logic Programming for Large Scale Applications in Law: A Formalisation of Supplementary Benefit Legislation. In: *Proceedings of the 1st international conference on Artificial intelligence and law*. ACM, 1987, s. 190-198.

[14] Design právních expertních systémů se již v některých západních technologicko-právních centrech stal součástí výuky. Viz například ROSTAIN, T., SKALBECK, R., MULCAHY, K. G.: Thinking Like a Lawyer, Designing Like an Architect: Preparing Students for the 21st Century Practice. *Chi.-Kent L. Rev.*, 2012, **88**: 743.

[15] Při dokončování tohoto článku jsem se seznámil s tím, že před deseti lety již něco podobného zkoušel v letech 2006 až cca 2009 Michael Poulshock: Project Hammurabi History. Dostupný na https://github.com/foundation-for-computable-law/hammurabi/wiki/Project-History [citováno 2. června 2020].

k problému, který řeší.[18] Pak se případně ukáže, že je některá část modelu použitelná i při řešení jiného problému. V tomto článku model zkoumaného úseku práva použiju na problém zpětného vyhledávání, který spočívá v hledání zdůvodnění vybrané teze (např. zda mají být informace žadateli odepřeny kvůli ochraně utajovaných informací). Problém zpětného vyhledávání zahrnuje následující kroky:

1. Vymezit si tezi,[19] pro kterou budeme hledat podmínky, ze kterých teze vyplyne
2. Neautomatizovatelná část (tvorba právního komentáře):
   - Najít a sepsat relevantní části právních předpisů pro budoucí aplikaci práva na zkoumaném úseku práva
   - Identifikovat právní předpisy regulující danou situaci (věc, čas a místo) a vybrat potřebná ustanovení
   - Identifikovat podklady k interpretaci (judikaturu, literaturu, např. komentář)
   - Interpretací a explikací dospět k modelu práva na daném úseku – typicky ve struktuře elementární normy antecedent/konsekvent[20] v explicitní formulaci
3. Automatizovatelná část (zpětné vyhledání):

---

[16] Podrobněji viz teoretická část MICHÁLEK, op. cit., s. 325. Jistě všichni známe nesmyslná rozhodnutí úřadů či soudů, kde je argumentace odůvodnění zjevně neimplikuje výrok rozhodnutí. Totéž se běžně děje v politickém systému. I v autoritativní právní argumentaci někdy můžeme nalézt vadu (měřeno převažující shodou diskursu), která má psychologickou příčinu. Za prvé se lidský mozek vyvinul tak, aby rozhodovaly automatické procesy včetně limbického systému (slon) a argumentace neokortexu (jezdec) tomu pomáhala, viz HAIDT, J.: *Morálka lidské mysli*. Nakladatelství dybbuk: Praha, 2013, s. 61 a následující. Druhý efekt cituje CARNEGIE, D.: *Jak získávat přátele a působit na lidi.* Nakladatelství Dobrovský, Praha, 2012, s. 174: *„J. Pierpont Morgan došel v jedné své analýze k závěru, že lidé mají obvykle dva důvody pro to, co udělali: První bývá ten, který zní dobře, a druhý je pak ten skutečný.*"

[17] ŠTĚPÁN, J., op. cit., s. 17, a s tím korespondující motivace adresátů norem, viz MICHÁLEK, op. cit., 322.

[18] PELÁNEK, R.: *Modelování a simulace komplexních systémů.* Brno: Masarykova univerzita, 2011, s. 45. Dostupné také z: http://radekpelanek.cz/dokumenty/ms-web.pdf.

[19] ROSTAIN, T., et al., op. cit., s. 747, mluví v rámci designu expertních systémů o „základní otázce" (*fundamental question*).

[20] DVOŘÁK, J., ŠVESTKA, J., ZUKLÍNOVÁ, M.: *Občanské právo hmotné 1*. Praha: Wolters Kluwer, 2017, s. 131.

- Ukázat, jak z elementárních norem sestavit řetězec vyplývání pro testovanou tezi
- Provést pokrácení řetězce vyplývání, kde je to možné
- Zobrazit předcházející normy
- Výběrem splněných podmínek hypotézy získat strukturu argumentu

4. Neautomatizovatelná část (aplikace práva):
   - Subsumpce skutkových podstat u vybraných podmínek

V následujících částech stručně rozebírám relevantní ustanovení zákona, modeluji související elementární normu (kurzívou) a zapisuji elementární i složené normy pomocí vzorců.

3. HMOTNĚ PRÁVNÍ DŮVODY POSKYTNUTÍ INFORMACÍ

3.1 VYMEZENÍ TESTOVANÉ TEZE

Uvažme, že účelem modelu práva na informace je pomoci uživateli odpovědět na otázku, zda lze informace poskytnout.

Odpověď na tuto otázku, stejně jako to bývá u řady jiných důležitých otázek adresátů právních norem, není výslovně zakotvena v právním předpise, ale je nutné ji dovodit. Ačkoliv je volba libovolná, kvůli jednoduchosti může být často vhodnější formulovat otázky pozitivně, v tomto případě v souladu se základní otázkou občana jako primárního adresáta právních norem. Cílem adresáta normy totiž primárně bude dosáhnout poskytnutí informace, proto je na místě formulovat cíl, u jehož určení máme volnost, pozitivně.

Právo občana na informace je zakotveno v čl. 17 odst. 1, 5 Listiny základních práv a svobod (dále jen „Listina“) a informace se podle tohoto ustanovení poskytují, není-li stanoveno jinak, jak potvrdil i Ústavní soud.[21] Čl. 17 odst. 4 Listiny vymezuje legitimní hodnoty, kvůli nimž lze omezit poskytování informací. Konkrétní podmínky pak stanoví zákon č. 106/1999

[21] Nález Ústavního soudu sp. zn. III.ÚS 28/96 ze dne 16. 5. 1996.

Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a související judikatura.

V případě práva na informace vycházím při zpracování modelu z komentáře Adama Furka a Lukáše Rothanzla,[22] ale také novější judikatury. Zohledňuji také později provedené změny práva, vydání Obecného nařízení o ochraně osobních údajů (nařízení č. 2016/679, dále jen „GDPR“[23]) a zákona č. 111/2019 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů (změnový zákon k GDPR).

Hlavní otázku, tedy zda bude požadovaná informace poskytnuta, lze reformulovat: jsou dány hmotněprávní důvody poskytnutí informace? Otázka vychází z ustanovení § 2 zákona o svobodném přístupu k informacím (zákon č. 106/1999 Sb., dále jen „InfZ“); dispozice příslušné normy je pak testovanou tezí. Protože pro tento článek je naplnění § 12 ústřední otázkou, mluvím o tam obsažené normě dále v článku také jako o „hlavní“ normě.

§ 12 InfZ
„Všechna omezení práva na informace provede povinný subjekt tak, že poskytne požadované informace včetně doprovodných informací po vyloučení těch informací, u nichž to stanoví zákon. (…)“

Toto základní ustanovení provádí zmíněný základní ústavní princip, že požadované informace se poskytují po vyloučení informací, u nichž to stanoví zákon. Do explicitní formulace tohoto ustanovení je však třeba převést i presuponované části logického modelu práva, které vyplývají z významu pojmů a explikace sdělného textu právního předpisu. Zákon stanoví povinnost odepření různými výrazy, které lze shrnout pod doktrinální pojem hmotněprávních důvodů neposkytnutí informace, například „neposkytne“, „zákon se nevztahuje“, „ustanovení se netýká“, věta se nepoužije“, viz dále. Zvláštní pozornost je třeba věnovat fakultativnímu omezení práva

[22] FUREK, A., ROTHANZL, L., op. cit.

[23] 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).

na informace v § 11 odst. 1 InfZ, které je spojeno se správním uvážením, viz judikát citovaný u fakultativnosti odepření výše, z něhož vyplývá speciální test proporcionality doplňující hlavní normu.

3.2 EXPLICITNÍ FORMULACE NORMY

Pojem **elementární norma**,[24] označuje normu tvořenou následkem (konsekventem, typicky dispozicí), případně také předpokladem (antecendentem, hypotézou), který se skládá z jedné nebo více podmínek. Elementární norma může tvořit celou právní normu jako regulativ chování,[25] ale také může vyjadřovat jen některou její část (např. působnost jako část hypotézy, okolnosti a postupy zohledňované při aplikaci, které mohou původní význam ustanovení výrazně modifikovat).

K explicitní formulaci norem nejprve několik formálních poznámek, aby byl další text srozumitelný. Explicitní formulace norem jsou v tomto článku vysázeny kurzívou, abych je odlišil od zbytku textu. Aby byl zřetelný rozdíl označení právních ustanovení od právních norem, je za normou lomítko. Vyplývá-li z ustanovení více norem jako v tomto případě, používám římskou číslici, např. zde § 12/I. Lomítko i římskou číslici lze vynechat, nehrozí-li záměna.

Dispozici normy označíme *D*, hypotézu *H* a její jednotlivé podmínky číslovkami 1, 2, 3 atd.; podmínky jsou dále strukturované (nicméně norma níže zatím neobsahuje explicitní formulaci všech podmínek). V textu používám konvenci, že při vnořování připojuji další body, tedy například podmínku částečné informační povinnosti ve výčtu níže značím 5.2. Pokud je třeba odkazovat na část konkrétní normy § 12 InfZ/ v explikaci, používám syntaxi § 12/*D* InfZ pro dispozici, § 12/*H* InfZ pro hypotézu a § 12/5.2 InfZ pro podmínku 5.2 hypotézy.

Explicitním výčtem antecedentů z textu zákona lze normu § 12 InfZ shrnout[26] takto:

---

[24] BOGUSZAK a kol.: *Teorie práva*, op. cit., s. 83.

[25] Regulací chování pak v nejširším významu mám na mysli také pravidla regulující výklad či aplikaci jiných právních norem – v této souvislosti se také mluví o metanormách; srovnej můj předchozí článek, s. 337 an.

§ 12/ InfZ

Hmotněprávní důvody poskytnutí informace povinným subjektem jsou dány ***právě tehdy, pokud*** **současně**

1. ***není pravda, že***
   zákon se na poskytování informace nevztahuje
2. *informace se vztahuje k působnosti povinného subjektu*
3. ***není pravda, že***
   povinnost poskytovat informace se informace netýká
4. ***není pravda, že***
   povinný subjekt informaci neposkytne
5. ***alternativně***
   1. *povinný subjekt má úplnou povinnost poskytovat informace*
   2. *je dána částečná informační povinnost povinného subjektu ve vztahu k informaci*
6. ***alternativně***
   1. ***není pravda, že***
      povinný subjekt informaci může odepřít
   2. ***současně***
      1. *povinný subjekt informaci může odepřít*
      2. *na odepření informace je legitimní zájem s ohledem na čl. 17 Listiny práv a svobod*
      3. *nutnost ochrany informace s ohledem na legitimní zájem s ohledem na konkrétní okolnosti převažuje nad právem na informace*

Norma má základní dvoudílnou strukturu logické funkce $H = H(1, \ldots, 6) \Rightarrow D$. V § 12 InfZ/ je mezi D a H nejen vztah implikace $\Rightarrow$, ale též

[26] V tento okamžik jde o instruktivnost výkladu, takže nevylučuji, že jsou i další důvody odepření informace. Pokud jde o formalizaci explicitní formulace norem, během recenzního řízení k tomuto článku jsem se seznámil s tím, že obdobné metody byly použity ve tvorbě legislativy, viz ALLEN, Layman E.; ENGHOLM, C. Rudy. Normalized legal drafting and the query method. *J. Legal Educ.*, 1977, 29: 380.

ekvivalence $D \Leftrightarrow H$. Je tomu tak proto, že předpokládáme, že výčet důvodů odepření je úplný, protože jsme vyhledali všechny výskyty v legislativním textu a judikatuře. Nicméně důkladnějším rozborem, např. rozepsáním implicitních podmínek vyplývajících z působnosti normy, by patrně bylo možné najít další podmínky. Pro $D \Rightarrow H$ platí také obměněná implikace $\neg H \Rightarrow \neg D$. Tím bychom dostali formulaci bližší legislativnímu textu, ale z hlediska použitelnosti pro adresáta norem o něco méně názornou.

Logickou strukturu (vzorec) normy můžeme také zachytit podrobněji. Podobně jako u chemických sloučenin, tak i u prvků hypotézy určité normy můžeme uvést funkční a strukturní vzorec, které mohou být užitečné z hlediska stručnosti, použití logických operací nebo znázornění struktury.

3.3 FUNKČNÍ VZOREC

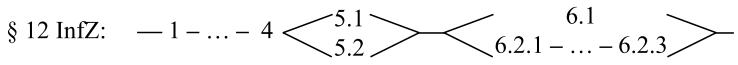
Plnou logickou strukturu výše uvedené hypotézy H lze vystihnout funkčním vzorcem (dispozici normy pro jednoduchost vynecháváme):

§ 12 InfZ: $H = 1$ **&** ... **&** 4 **&** (5.1 | 5.2) **&** [6.1 | (6.2.1 **&** ... **&** 6.2.3)],

kde **&** je symbol operace současného splnění (logického násobení) a | je symbol operace alternativy (logického sčítání).

3.4 STRUKTURNÍ VZOREC

Logickou strukturu § 12 lze zapsat do grafu, ve kterém vybíráme pro platný argument právě jednu cestu zleva doprava, který je strukturním vzorcem normy:



4. POSKYTNUTÍ UTAJOVANÉ INFORMACE

Vezmu si nejprve za příklad jeden z jednodušších, a to výluku z práva na informace ve vztahu k utajovaným informacím. V níže uvedeném výčtu

jsem shromáždil relevantní ustanovení pro posouzení otázky, jaké informace lze z hlediska informačního práva hmotného poskytnout. Velká část obsahu je v zákoně č. 412/2005 Sb., o ochraně utajovaných informací, v účinném znění (dále jen „ZUI“).

§ 7 InfZ

„Je-li požadovaná informace v souladu s právními předpisy označena za utajovanou informaci, k níž žadatel nemá oprávněný přístup, povinný subjekt ji neposkytne. (…)“

Explicitní formulace:

Povinný subjekt neposkytne informaci, ***pokud současně***

- informace je označena za utajovanou informaci
- žadatel nemá oprávněný přístup k informaci
- informace je označena za utajovanou informaci v souladu s právními předpisy

Funkční vzorec této normy zapisujeme:

$$\S\ 7/\mathrm{I.\ InfZ}: H = 1\ \&\ \ldots\ \&\ 3.$$

§ 2 ZUI písm. a)

„Pro účely tohoto zákona se rozumí

a) utajovanou informací informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací,“

Informace je označena za utajovanou informaci v souladu s právními předpisy ***právě tehdy, pokud současně***

1 ***alternativně***

1. vyzrazení nebo zneužití informace může způsobit újmu zájmu České republiky

2. vyzrazení nebo zneužití informace může být pro zájem České republiky nevýhodné

2 informace je druhu, který je uveden v seznamu utajovaných informací podle nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací

Obdobně u výše uvedených případů můžeme uvést funkční a strukturní vzorce této elementární normy:

§ 2 písm. a) ZUI: $H = (\ 1.1 \mid 1.2\ )\ \mathbf{\&}\ 2.$

§ 3 ZUI
„Újmou zájmu České republiky se pro účely tohoto zákona rozumí poškození nebo ohrožení zájmu České republiky.“

Tato norma je legální definicí pojmu újma zájmu České republiky, se kterým pracují jiné normy (§ 2 písm. a) ZUI) a je možné tuto definici do těchto norem přímo dosadit.

Vyzrazení nebo zneužití informace může způsobit újmu zájmu České republiky ***právě tehdy, pokud*** *vyzrazení nebo zneužití informace může způsobit poškození nebo ohrožení zájmu České republiky*

4.1 ŘETĚZEC VYPLÝVÁNÍ

Je zřejmé, že uvedená ustanovení na sobě nejsou nezávislá, ale konsekventy elementárních norem splývají s antecendenty jiných norem, tedy normy na sebe navazují a tvoří řetězec vyplývání navazujících norem (normativní komplex), který je druhem sekvence.[27] Návaznost norem označuji symbolem implikace nahoru „⇑“ od konsekventu předcházející normy směrem k antecedentu navazující normy (prostřední část). Dvě navazující normy lze složit, tedy z tranzitivity implikace (hypotetického sylogismu) odvodit, že z hypotézy předcházející normy vyplývá dispozice navazující normy, a výsledná norma bude také platná.

[27] ŠPIRUDA, op. cit., s. 61 a násl. K uvedené úvaze je třeba dodat, že v návaznosti (dosazení) musí být zachován i normativní mód, tedy nelze zaměňovat výroky o bytí a mětí.

Pokrácení řetězce vyplývání. Je však třeba říci, že dvě navazující elementární normy obecně nelze jednou složenou normou *ekvivalentně* nahradit, aby byla zachována informační hodnota. Vypuštěním prostřední části se totiž ztrácí možnost, aby byla tato část naplněna jiným způsobem. Přitom v obecném popisu musíme počítat s tím, že právní řád může obsahovat alternativní způsoby naplnění hypotézy navazující normy, ať už z jiných právních norem či napřímo.

- **Ekvivalence**. Pokud tomu však není a implikace je současně ekvivalencí, kterou značím „⇳“, například pokud je předcházející norma zákonnou definicí nebo jedinou normou s danou prostřední částí jako konsekventem, lze řetězec vyplývání *pokrátit*, podobně jako se krátí zlomky, a získat tak složenou normu.
- **Jednostranná implikace**. Naopak typicky nepůjde pokrácení provést u zákonných domněnek, kdy lze naplnit hypotézu navazující normy také napřímo nebo existuje více norem s danou prostřední částí jako konsekventem. V takovém případě je vhodné pracovat s řetězcem vyplývání bez pokrácení.

Pokud navazující elementární normy uspořádáme pod sebe (najdeme je zpětným vyhledáváním neboli *backtrackingem*), dostaneme následující řetězec vyplývání, který zachycuje explicitní formulaci právní normy:

§ 7/I InfZ (normativní komplex)

Povinný subjekt neposkytne informaci, ***pokud*** **současně**

1. *informace je označena za utajovanou informaci*
2. *žadatel nemá oprávněný přístup k informaci*
3. *informace je označena za utajovanou informaci v souladu s právními předpisy*

   ⇳ § 2 ZUI

   Informace je označena za utajovanou informaci v souladu s právními předpisy ***právě tehdy, pokud***

   současně

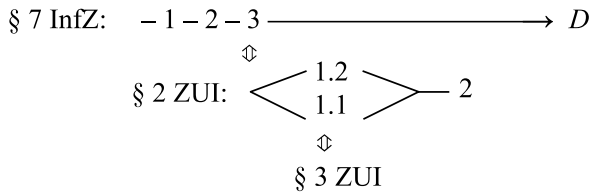
   1. **alternativně**
      1. *vyzrazení nebo zneužití informace může způsobit újmu zájmu České republiky*

⇳ ***§ 3 ZUI***
Vyzrazení nebo zneužití informace může způsobit újmu zájmu České republiky ***právě tehdy, pokud***
vyzrazení nebo zneužití informace může způsobit poškození nebo ohrožení zájmu České republiky

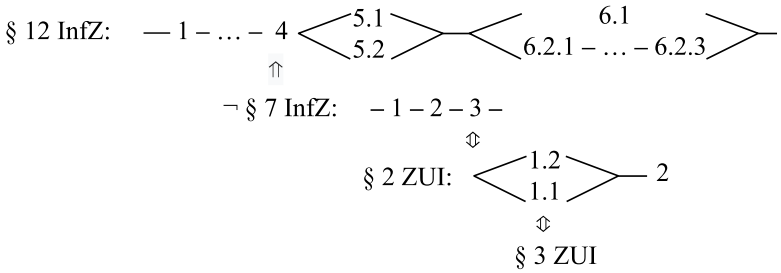
2. *vyzrazení nebo zneužití informace může být pro zájem České republiky nevýhodné*

2. informace je druhu, který je uveden v seznamu utajovaných informací podle nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací

Tento normativní komplex můžeme zapsat pomocí strukturního vzorce následovně:



Analogicky můžeme tento výsledek označit do strukturního vzorce právní normy, kde je formulace explicitní vzhledem k podmínce 4 hypotézy hlavní normy:



přičemž v tomto strukturním vzorci značí symbol „¬“ negaci dané strukturní části. V tomto případě vyjadřuje, že jako podmínka 4 v hypotéze hlavní normy vystupuje negace konsekventu normy § 7 InfZ. Tímto způsobem by bylo analogicky možné znázornit úplnou explicitní formulaci § 12 InfZ.[28]

Jak jsem uvedl v části o hmotněprávních důvodech poskytnutí informace, pro dovození toho, že má být informace odepřena z důvodu utajení (možná teze povinného subjektu), stačí ukázat splnění negace podmínky 4 hlavní normy, tedy splnění hypotézy § 7 InfZ.

Pokud provedeme výše naznačené pokrácení, tedy zohledníme vždy poslední antecedent v každé předcházející ekvivalentní normě, dostaneme následující složenou normu:

§ 7 InfZ/ (pokrácená složená norma)

Povinný subjekt neposkytne informaci, ***pokud***

současně

1. *informace je označena za utajovanou informaci*
2. *žadatel nemá oprávněný přístup k informaci*
3. ***alternativně***
    1. *vyzrazení nebo zneužití informace může způsobit poškození nebo ohrožení zájmu České republiky*
    2. *vyzrazení nebo zneužití informace může být pro zájem České republiky nevýhodné*
4. *informace je druhu, který je uveden v seznamu utajovaných informací podle nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací*

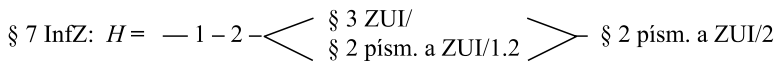
Ke složené normě můžeme také dospět úpravou funkčního vzorce, tj. dosazením:

[28] Jak to tak bývá, situace je ve skutečnosti ještě složitější, protože § 12 ve skutečnosti nelze takto zjednodušeně aplikovat, protože jeho dikce nemluví o jediné informaci, která se posuzuje, ale předvídá proces vyloučení informací, kde jsou hmotněprávní důvody odepření informace. Proto musí povinný subjekt posuzovat, která část požadované informace vykazuje tuto překážku a pouze v tomto rozsahu nelze informace poskytnout.

§ 7 InfZ: H = 1 **&** 2 **&** 3
= 1 **&** 2 **&** (§ 2 písm. a ZUI/ (1.1 | 1.2) **&** 2)
= 1 **&** 2 **&** ((§ 3/ ZUI | § 2 písm. a ZUI/1.2) **&**
& § 2 písm. aZUI/2),

přičemž je použita konvence, že u písmen v označení normy se ve vzorci nepíše závorka, aby nedocházelo k záměně s logickými závorkami, a číslo podmínky vždy odkazuje k poslední zmíněné normě na dané úrovni uzávorkování.

Výsledná složená norma má po pokrácení podstatně jednodušší strukturu:



Úředníkovi, který má hypotézu informaci z důvodu utajení neposkytnout, pak zbývá pouze ověřit a odůvodnit, že jsou naplněny podmínky pokrácené hypotézy a má vysokou míru jistoty, že vydá rozhodnutí se správnou strukturou argumentu. Přitom požadovaný počet podmínek hypotézy je nejmenší možný. Tím není vyloučeno, že špatně zjistí skutkový stav či pochybí při subsumpci skutkového stavu nebo bude mít nesprávný právní názor.

5. POSKYTNUTÍ INFORMACE O PLATU

Velmi častý důvod pro odepření informací v podobě ochrany osobních údajů má nejsložitější právní úpravu, přičemž pro názornost se soustředím na ve veřejném prostoru populární problém poskytování informací o platech zaměstnanců veřejné správy. Úředník reprezentující povinný subjekt musí aplikovat informační zákon, přímo použitelné nařízení GDPR, prováděcí zákon č. 110/2019 Sb., o zpracování osobních údajů, zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě (dále jen „ZFK“) a judikaturu Ústavního a Nejvyššího správního soudu.

§ 8a odst. 1 InfZ

„Informace týkající se osobnosti, projevů osobní povahy, soukromí fyzické osoby a osobní údaje povinný subjekt poskytne jen v souladu s právními předpisy, upravujícími jejich ochranu.“

Jde o alternativní podmínku hlavní normy, která se týká ochrany soukromí, přičemž ji nebudeme rozepisovat celou, nýbrž se zaměříme zejména na otázku poskytování informací o platech. Při formulaci § 8a odst. 1 můžeme vzít v úvahu výjimku uvedenou v odstavci 3 anebo tuto výjimku řešit zvlášť. Elementární normu lze v první zmíněné možné explikaci formulovat takto:

Povinný subjekt neposkytne informaci, ***pokud***

současně

1 alternativně

1. informace se týká osobnosti, projevů osobní povahy nebo soukromí fyzické osoby

2. informace je osobním údajem

2 poskytnutí informace by bylo v rozporu s právním předpisem, který upravuje její ochranu

3 není pravda, že

alternativně

1. pro informaci je stanovena výjimka týkající se příjemců veřejných prostředků

2. pro informaci je stanovena výjimka týkající se veřejně činných osob

Funkční vzorec této normy lze zapsat:

§ 8a odst. 1/ InfZ: $H = (1.1 \mid 1.2) \;\&\; 2 \;\&\; \neg (3.1 \mid 3.2)$ (*)

čl. 4 bod 1 nařízení GDPR

„Pro účely tohoto nařízení se rozumí osobními údaji 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“

Tuto definici je nutné rozvést do dvou elementárních norem (část před středníkem a po), které definují pojmy použité v jiných právních předpisech, a to osobní údaje a subjekt údajů. Elementární normy označíme římskými číslicemi.

I.

Informace je osobním údajem ***právě tehdy, pokud***

současně

1. *informace je o fyzické osobě*
2. ***alternativně***
    1. *fyzická osoba je identifikovaná*
    2. *fyzická osoba je identifikovatelná*

II.

Fyzická osoba je identifikovatelná ***právě tehdy, pokud***

fyzickou osobu 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

§ 8b odst. 1, 3 InfZ

„*Povinný subjekt poskytne základní osobní údaje o osobě, které poskytl veřejné prostředky.*“

Uvedené ustanovení je výjimkou *lex specialis* z pravidla § 8a, které je samo výjimkou z poskytování informací. Proto je vhodné tuto výjimku formulovat explicitně, přičemž je nutné zohlednit ustanovení odstavce 2 (vý-

jimka z výjimky z výjimky), a to výslovným odkazem. Judikaturou[29] bylo dovozeno, že plat poskytnutý zaměstnanci za jeho práci státem, je nutné považovat za poskytnuté veřejné prostředky.

Pro informaci je stanovena výjimka týkající se příjemců veřejných prostředků ***právě tehdy, pokud***

současně

1. *informace je základním osobním údajem o osobě*
2. *povinný subjekt poskytl příjemci veřejné prostředky*
3. ***není pravda, že***
   na informaci se výjimka týkající se příjemců veřejných prostředků nevztahuje

§ 8b odst. 2 InfZ

„Ustanovení [§ 8b] odstavce 1 se nevztahuje na poskytování veřejných prostředků podle zákonů v oblasti sociální, poskytování zdravotních služeb, hmotného zabezpečení v nezaměstnanosti, státní podpory stavebního spoření a státní pomoci při obnově území.“

Na informaci se výjimka týkající se příjemců veřejných prostředků nevztahuje, ***pokud***

informace se týká jen poskytování veřejných prostředků podle zákonů v oblasti sociální, poskytování zdravotních služeb, hmotného zabezpečení v nezaměstnanosti, státní podpory stavebního spoření nebo státní pomoci při obnově území

§ 8b odst. 3 InfZ

„Základní osobní údaje podle odstavce 1 se poskytnou pouze v tomto rozsahu: jméno, příjmení, rok narození, obec, kde má příjemce trvalý pobyt, výše, účel a podmínky poskytnutých veřejných prostředků.“

Informace je základním osobním údajem o osobě, ***pokud***

[29] Rozsudek Nejvyššího správního soudu ze dne 27. 5. 2011, č. j. 5 As 57/2010-79, s. 7.

informace je jménem, příjmením, rokem narození, obcí, kde má fyzická osoba trvalý pobyt, nebo výše, účel či podmínka poskytnutých veřejných prostředků fyzické osobě

§ 2 písm. a), g) ZFK
„Pro účely tohoto zákona se rozumí

a) orgánem veřejné správy organizační složka státu, která je účetní jednotkou podle zvláštního právního předpisu, státní příspěvková organizace, státní fond, územní samosprávný celek, městská část hlavního města Prahy, příspěvková organizace územního samosprávného celku nebo městské části hlavního města Prahy a jiná právnická osoba zřízená k plnění úkolů veřejné správy zvláštním právním předpisem nebo právnická osoba zřízená na základě zvláštního právního předpisu, která hospodaří s veřejnými prostředky, (…)

g) veřejnými prostředky veřejné finance, věci, majetková práva a jiné majetkové hodnoty patřící státu nebo jiné právnické osobě uvedené v písmenu a),“

Skutečnost, že se má použít zákon o finanční kontrole vyplývá z citovaného judikátu NSS. Uvedené ustanovení můžeme s ohledem na strukturu a přehlednost rozdělit do dvou elementárních norem:

Povinný subjekt poskytl příjemci veřejné prostředky ***právě tehdy, pokud***
současně

1. *povinný subjekt poskytl příjemci veřejné finance, věci, majetková práva nebo jinou majetkovou hodnotu*
2. *majetková hodnota patřila před poskytnutím státu nebo jiné právnické osobě, která je orgánem veřejné správy ve smyslu zákona o finanční kontrole*

Majetková hodnota patřila před poskytnutím státu nebo jiné právnické osobě, která je orgánem veřejné správy ve smyslu zákona o finanční kontrole, ***pokud***

majetková hodnota patřila před poskytnutím státu nebo státní příspěvkové organizaci, státnímu fondu, územnímu samosprávnému celku, městské části

hlavního města Prahy, příspěvkové organizaci územního samosprávného celku nebo městské části hlavního města Prahy nebo jiné právnické osobě zřízené k plnění úkolů veřejné správy zvláštním právním předpisem nebo právnické osobě zřízené na základě zvláštního právního předpisu, která hospodaří s veřejnými prostředky

Vzhledem k odlišnostem v judikatuře a ve správní praxi (různé názory ÚOOÚ, MVČR, NSS, ÚS)[30] je nezbytné, aby autor komentáře interpretoval rozhodnou judikaturu. S ohledem na postavení Ústavního soudu v čl. 89 odst. 2 Ústavy jsem zvolil doplnění souboru těchto zákonných norem o závěry judikatury ÚS, i když nejsou obsaženy v zákoně a jsou zřejmým extenzivním dotvářením práva ze strany senátu Ústavního soudu.

Platový nález[31]

„Před poskytnutím informací o platu a odměnách zaměstnance, vyžádaných žadatelem na základě ustanovení § 8b zákona o svobodném přístupu k informacím, je nezbytné provést test proporcionality a v jeho rámci posoudit zejména, zda poskytnutí informací je klíčové pro výkon práva žadatele na svobodu projevu, přičemž je třeba zejména zkoumat, zda účelem vyžádání informace je přispět k diskusi o věcech veřejného zájmu, informace samotná se týká veřejného zájmu, žadatel o informaci plní úkoly či poslání dozoru veřejnosti či roli tzv. „společenského hlídacího psa“, informace existuje a je dostupná.“ Poslední 2 podmínky existence a dostupnosti můžeme vypustit z hlediska redundance, protože jde o samostatný důvod odepření informací.[32] Judikát v podstatě modifikuje okruh informací poskytovaných podle § 8b odst. 1, tedy lze ho navázat na podmínku § 8b odst. 1/3.[33]

[30] Srovnej například přehled PÍŠA, R.: „Poskytování informací o platech - případová studie soudů na volném poli.“ *Správní právo*, číslo 8/2018, s. 489 a násl.

[31] Bod 33 nálezu Ústavního soudu ze dne 3. 4. 2018, sp. zn. IV. ÚS 1200/16, bod 125 nálezu ÚS ze dne 17. 10. 2017, sp. zn. IV. ÚS 1378/16 („platového nálezu“).

[32] Rozsudek Nejvyššího správního soudu ze dne 9. 2. 2012, sp. zn. 1 As 141/2011, bod 19. Obě zmíněné podmínky však jsou dále vnitřně strukturované, např. u neexistence nesmí být dovoditelná povinnost informací disponovat.

[33] Samozřejmě bychom mohli jít ještě dále a navázat na tento judikát i upřesňující judikaturu NSS, např. rozsudek ze dne 27. 5. 2020, sp. zn. 2 As 88/2019, body 28 a 30.

I.

Pokud se má povinný subjekt rozhodovat, zda poskytnout informace o platu a odměnách zaměstnance na základě zákona, je povinen provést test proporcionality podle platového nálezu (viz výše).

II.

Na informaci se výjimka týkající se příjemců veřejných prostředků nevztahuje, ***pokud***

současně

1. *byl proveden test proporcionality předvídaný platovým nálezem*
2. *poskytnutí požadované informace by bylo podle platového nálezu nepřiměřené*

III.

Poskytnutí požadované informace by bylo podle platového nálezu nepřiměřené, ***právě tehdy pokud***

není pravda, že

současně

1. *poskytnutí informací je klíčové pro výkon práva žadatele na svobodu projevu*
2. *účelem vyžádání informace je přispět k diskusi o věcech veřejného zájmu*
3. *informace samotná se týká veřejného zájmu*
4. *žadatel o informaci plní úkoly či poslání dozoru veřejnosti či roli tzv. společenského hlídacího psa*

Výše uvedené normy lze opět navázat na sebe a pokrátit, čímž dostaneme následující alternativu hypotézy hlavní normy:

§ 8a odst. 1/ InfZ (pokrácená složená norma)

Povinný subjekt neposkytne informaci, ***pokud***

současně

1. ***alternativně***

    1. informace se týká osobnosti, projevů osobní povahy nebo soukromí fyzické osoby

*2. **současně***

1. informace je o fyzické osobě

*2. **alternativně***

1. fyzická osoba je identifikovaná

2. fyzickou osobu 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

2 poskytnutí informace by bylo v rozporu se právním právním předpisem, který upravuje její ochranu

*3 **není pravda, že***
alternativně

1. současně

1. informace je jménem, příjmením, rokem narození, obcí, kde má fyzická osoba trvalý pobyt, nebo výše, účel či podmínka poskytnutých veřejných prostředků fyzické osobě

*2. **současně***

1. povinný subjekt poskytl příjemci veřejné finance, věci, majetková práva nebo jinou majetkovou hodnotu

2. majetková hodnota patřila před poskytnutím státu nebo státní příspěvkové organizaci, státnímu fondu, územnímu samosprávnému celku, městské části hlavního města Prahy, příspěvkové organizaci územního samosprávného celku nebo městské části hlavního

města Prahy nebo jiné právnické osobě zřízené k plnění úkolů veřejné správy zvláštním právním předpisem nebo právnické osobě zřízené na základě zvláštního právního předpisu, která hospodaří s veřejnými prostředky

3. ***není pravda, že***

alternativně

1. informace se týká jen poskytování veřejných prostředků podle zákonů v oblasti sociální, poskytování zdravotních služeb, hmotného zabezpečení v nezaměstnanosti, státní podpory stavebního spoření nebo státní pomoci při obnově území

2. ***současně***

1. byl proveden test proporcionality předvídaný platovým nálezem

2. ***není pravda, že***

současně

1. poskytnutí informací je klíčové pro výkon práva žadatele na svobodu projevu

2. účelem vyžádání informace je přispět k diskusi o věcech veřejného zájmu

3. informace samotná se týká veřejného zájmu

4. žadatel o informaci plní úkoly či poslání dozoru veřejnosti či roli tzv. společenského hlídacího psa

2. pro informaci je stanovena výjimka týkající se veřejně činných osob

Funkční vzorec hypotézy řešené alternativy v hypotéze hlavní normy dostaneme tak, že do vzorce pro § 8a odst. 1 označeného (*) dosadíme výše zmíněné ekvivalence:

$$
\begin{aligned}
H \quad &= \quad (1.1 \mid 1.2) \,\&\, 2 \,\&\, \neg (3.1 \mid 3.2) \\
&= \quad (1.1 \mid \text{čl. 4 bod 1/I./1 GDPR} \,\&\, (\text{čl. 4 bod 1/I./2.1} \mid \text{čl. 4 bod 1/II. GDPR}) \\
&\quad\; \,\&\, 2 \,\&\, \neg (\text{§ 8b odst. 3 InfZ} \,\&\, (\text{§ 2 písm. g/1 ZFK} \,\&\, \text{§ 2 písm. a}) \,\&\, \\
&\quad\; \neg (\text{§ 8b odst. 2 InfZ} \mid (\text{Platový nález/II./1} \,\&\, \text{Platový nález/III.}))
\end{aligned}
$$

Podle výše vyložených principů by bylo možné nakreslit i strukturní vzorec příslušné hypotézy včetně relevantních navázaných předcházejících norem (§ 2 ZFK) a rovněž zakreslit vztah k podmínce hypotézy hlavní normy § 12/4 InfZ.

Současně by také bylo možné vedle zmíněného pokrácení příslušnou logickou funkci zjednodušit, např. zploštěním vnořených výčtů stejného typu díky asociativnosti operace, vyrušením dvojité negace, propagací negace až směrem k literálům díky využití de Morganových vzorců, roznásobením složených výrazů pomocí distributivního zákona až po případné převedení do disjunktivní normální formy,[34] což však může vytvářet neprakticky dlouhé výrazy. Optimalizace výrazu je otázkou na samostatné pojednání; cílem je vždy najít vyjádření co nejméně náročné na praktické použití.

6. ROZHODNUTÍ O ODMÍTNUTÍ ŽÁDOSTI O INFORMACE

Správní orgán vydává rozhodnutí o odepření informace při naplnění hypotézy normy, která vyplývá z následujícího ustanovení:

§ 15 odst. 1 InfZ

„Pokud povinný subjekt žádosti, byť i jen zčásti, nevyhoví, vydá ve lhůtě pro vyřízení žádosti rozhodnutí o odmítnutí žádosti, popřípadě o odmítnutí části žádosti, s výjimkou případů, kdy se žádost odloží.“

[34] WEISSTEIN, E. W. „Disjunctive Normal Form.“ From MathWorld – A Wolfram Web Resource. Dostupný z: https://mathworld.wolfram.com/DisjunctiveNormalForm.html [cit. 2020-10-25].

Zjednodušeně řečeno je hypotézou této normy, že jsou dány hmotněprávní důvody pro odepření informace. Splněním podmínek pro vydání rozhodnutí se dostáváme do relativně složitého režimu § 20 odst. 4 písm. a) InfZ, podle kterého se rozhodnutí vydává podle zákona č. 500/2004 Sb., správního řádu (dále jen „SpŘ“). Modelování celého správního procesu by překročilo rozsah tohoto článku, opět tedy využiji autorské licence a model zjednoduším.

Povinný subjekt je povinen vydat ve lhůtě pro vyřízení žádosti rozhodnutí o odmítnutí žádosti, ***pokud***

současně

1. ***není pravda, že***
   povinný subjekt žádosti zcela vyhověl
2. ***není pravda, že***
   povinný subjekt žádost odložil

Z výše uvedeného popisu je patrné, že dispozice hlavní normy určuje, jak se má povinný subjekt zachovat, tedy pokud jsou hmotněprávní důvody, má informace poskytnout čili z procesního hlediska žádosti vyhovět. Do § 15 odst. 1 InfZ pak nevstupuje jako hypotéza 1 konsekvent hlavní normy, nýbrž jeho realizace (otázky mětí a bytí je třeba oddělit). Případné porušení normy pak zakládá následky v řízení o odvolání. Povinný subjekt má celou řadu dalších povinností stanovených správním řádem. Správní orgán je např. povinen zjistit skutečný stav věci.[35] Dále má rozhodnutí povinné náležitosti.

§ 68 odst. 2 SpŘ věta prvá

„*Ve výrokové části se uvede řešení otázky, která je předmětem řízení, právní ustanovení, podle nichž bylo rozhodováno, a označení účastníků podle § 27 odst. 1.*“

[35] Stav věci se zjišťuje typicky dokazováním, které je upraveno právem. Současně určitý stav věci je nutný pro určení rozhodného práva (působnosti předpisu). V aplikaci tedy pracujeme s určitou redukcí - pokud jde o právo, pak s výsekem použitelného práva, a pokud jde o skutkový stav, tak s dle práva zjištěnou podobou právně významného úseku reality v dané věci. Tato nuance v propojení práva a skutkového stavu v praxi nepůsobí velké problémy. Je však nezbytné na ni nezapomínat, pokud chceme popsat řešení určité věci před dalším orgánem.

Podle závěru Ministerstva vnitra[36] „předmětem řízení je rozhodování o právech a povinnostech účastníků řízení na základě zjištěného skutkového stavu.“ Ve výrokové části má tedy být uveden výrok o tom, že se žádost odmítá a uvedeno právní ustanovení, podle kterého bylo rozhodnuto (typicky se uvádí pouze označení ustanovení podmínky hlavní normy zakládající hmotněprávní důvod odepření).

Povinný subjekt je povinen uvést ve výrokové části rozhodnutí, že byla žádost odmítnuta, právní ustanovení, podle nichž bylo rozhodováno, a označení účastníků podle § 27 odst. 1, ***pokud***

vydává správní rozhodnutí o odmítnutí žádosti.

6.1 ARGUMENTACE SPRÁVNÍHO ROZHODNUTÍ A INDIVIDUALIZACE NORMY

§ 68 odst. 3 SpŘ věta prvá

„V odůvodnění se uvedou důvody výroku nebo výroků rozhodnutí, podklady pro jeho vydání, úvahy, kterými se správní orgán řídil při jejich hodnocení a při výkladu právních předpisů, a informace o tom, jak se správní orgán vypořádal s návrhy a námitkami účastníků a s jejich vyjádřením k podkladům rozhodnutí.“

Zaměřme se nyní na logickou vrstvu argumentace.[37] Důvody rozhodnutí a úvahy, kterými se přitom řídil, a to jak v hodnocení skutkového stavu, tak při výkladu právních předpisů, lze shrnout tak, že správní orgán potřebuje k danému výroku o povinnosti individualizované vůči osobě identifikovat složenou právní normu $N: H(1, 2, 3, \ldots) \Rightarrow D$, která má příslušnou dispozici, a ověřit naplnění relevantních podmínek složené právní normy 1, 2, …, k. Dostáváme se tak za hranice výrokové logiky k logice predikátové, nicméně vypomůžeme si platným úsudkem, že platí-li dané tvrzení obecně

[36] Ministerstvo vnitra, poradní sbor ke správnímu řádu. Závěr č. 62 ze zasedání poradního sboru ministra vnitra ke správnímu řádu ze dne 26. 11. 2007.

[37] PRAKKEN, H., SARTOR, G. „The Role of Logic in Computational Models of Legal Argument: A Critical Survey.“ *Lecture Notes in Computer Science*, 2002, s. 345.

pro všechny případy, pak platí i pro konkrétní případ, jehož se týká rozhodnutí. Formálně je celý argument dán trojicí podmínek:

Argument zdůvodňuje, že osoba má povinnost jednat způsobem uvedeným v určité dispozici normy,

pokud současně

1. *platí pokrácená složená norma N: H(1, 2, 3, …) ⇒ D,*
2. *taková norma N je na individuální případ použitelná,*
3. *jsou splněny podmínky 1, …, k, které při dosazení do logické funkce příslušné normy vedou k pravdivému závěru.*

Argument typicky zahrnuje soubor podmínek, které mají být splněny kumulativně *A*: 1 **&** … **&** *k* ⇒ *D*; z každé dílčí alternativy hypotézy normy vstupuje do argumentu pouze jedna podmínka.[38]

Odůvodnění by tudíž mělo obsahovat seznam podmínek hypotézy s ohledem na povinnost správního orgánu zjistit skutečný stav věci. Skutková tvrzení a tvrzení o prokázání skutečností důkazy jsou předpoklady individualizovaných norem.[39] Po konstrukci důkazního řetězce můžeme dovršit plně explicitní formulaci argumentu, na základě kterého bude vydáno rozhodnutí v konkrétním případě. Protože taková konstrukce není sdělná, postačí ve většině případů prezentovat podstatu argumentu. Presumování některých částí argumentu však může na druhé straně vytvářet argumentační mezery a způsobovat vady, které činí argument napadnutelným.

Obdobným způsobem lze pokračovat ve vztahu k odvolání, které napadá vady argumentu v rozhodnutí nebo postup, který mu předcházel. Vadou argumentu může být, že rozhodnutí uvádí neúplnou normu, tedy vynechává některou alternativu (využitelnou námitkou), která může závěr argumentu zvrátit, případně nesprávně pracuje s domněnkou, netvrdí splnění určité nezbytné podmínky či ho sice tvrdí, ale nedokazuje, ač je nezbytné ji

[38] Není však vyloučeno, aby argument z důvodů nejistoty či opatrnosti zahrnoval i některé alternativní cesty. Výjimečně může být postaveno na jisto, že některá z alternativ nastala, ale není známo která. To v podstatě koresponduje se situací, kdy pracujeme s normou, u které nedošlo k rozvinutí některé podmínky do alternativ.

[39] Viz § 52 správního řádu věta druhá, podle níž správní orgán vždy provede důkazy, které jsou potřebné ke zjištění stavu věci.

dokázat. Nicméně podrobný rozpis je vzhledem k rozsahu správního řádu nad možnosti tohoto článku.

6.2 PRÁCE S VYVRATITELNOSTÍ

V předchozí podkapitole jsem naznačil místa, která činí argument napadnutelným a vedou k nezbytné relativnosti právních závěrů a nutnosti zajistit autoritativnost právních závěrů procedurálně, tedy ve sporech s více instancemi. Můžeme jistě formulovat jednotlivé podmínky hypotézy a usilovat o explicitní zachycení výjimek z dané normy přidáním dalších podmínek do její hypotézy. Takový model se však stále jeví jako poněkud nepřiměřeně zužující. Už proto, že jak jsem vysvětlil,[40] pracujeme vždy s výsekem práva, takže nemusíme postihnout jiný předpis, z něhož vyplývá jiná rozhodná norma. Navíc může být předpis nepřímo novelizován v budoucnu, případně judikaturou vyložen tak, že ho modifikují obecné principy dobrých mravů, zákazu zneužití práva[41] apod. To je tedy určitým omezujícím faktorem výše uvedeného modelu, který pracuje s explicitními formulacemi norem na úrovni gramatických vět.

Proto by bylo přiléhavější právní logiku modelovat jako součást praktického uvažování vycházející z přirozeného jazyka. Věda ovšem bohužel dosud nedisponuje zcela spolehlivým a prakticky použitelným modelem přirozeného jazyka. Patrně nejlépe lze logickou strukturu právního argumentu vystihnout zamítnutelným usuzováním (*defeasible reasoning*).[42] Podstatou zamítnutelného usuzování je skutečnost, že obsah výroků může být dále modifikován, např. specifičtějším výrokem, takže z čistě logického pohledu by nastal spor, ale při zamítnutelném usuzování se upřednostní relevantní námitka, byť není výslovně předvídána. Zamítnutelné usuzování patří do rodiny nemonotónních logik, tedy logik, kde z rozšířené množiny výroků již nelze nutně vyvodit tytéž výroky. Zamítnutelné usuzování je v právu běžné, přičemž konflikty mezi normami se řeší pravidly jako *lex*

[40] MICHÁLEK, op. cit., s. 334.

[41] Rozsudek Nejvyššího správního soudu ze dne 25. 6. 2014, č. j. 6 As 68/2014-21.

[42] ONDRÁČEK, T., ŠTĚPÁNEK, J.: *Nástin koncepce adaptivních logik.* Pro-Fil, vol. 17, no. 1 (2016). ISSN 1212-9097, s. 16–35.

specialis. Vedle toho v oblasti argumentace vzniká díky zamítnutelnému usuzování možnost určitý výrok o právu či o struktuře argumentu (tj. výrok o platnosti řetězce vyplývání) vyvrátit protiargumentem, např. že existuje ten a ten nový předpis, obecný princip či judikát anebo chyba znevěrohodňující závěr. Tyto úvahy pak již v podstatě patří do dialektické vrstvy argumentace.[43]

Nevýhoda zamítnutelného usuzování na druhé straně spočívá v tom, že ho dnes nelze bez dalšího jednoduše modelovat na počítači (či pouze částečně např. koncept *negation as failure* v Prologu[44]), protože jde o postup interpretační, založený mimo jiné na hodnotových úvahách člověka, diskurzu a procedurálním rozměru argumentace. Proto model zachycuje zkoumaný výsek práva explicitně s tím, že umožňuje doplnit specifičtější normy jako další podmínky.

7. ZÁVĚR

Na třech příkladech jsem ukázal, jak lze konstruovat explicitní formulace hypotéz norem. Právní normy jsem namodeloval zejména co do logické struktury podmínek jejich hypotéz. Navrhl jsem funkční a strukturní vzorce jejich textově algoritmické reprezentace. Tyto koncepty mohou být základem jejich počítačového modelování. Vysvětlil jsem, že předcházející a navazující normy lze někdy pokrátit, díky čemuž se složené normy zjednoduší. Také jsem popsal vznik argumentu z explicitní formulace normy, a to výběrem z alternativ a individualizací. Mnou navržená metoda je sice na té nejnižší úrovni komplexity modelování práva, pokud jde o jeho faktografickou povahu, přesto lze výsledné závěry využít pro netriviální praktický účel, a to automatizaci norem na úrovni vět. Celý obor deduktivní roviny právní informace se teprve rozvíjí a dosud nemá jasné zakotvení a ani není zřejmé, nakolik bude perspektivní. Přesto články jako tento mohou přispět rozvoji právního modelování, které může jednou výrazně zlevnit a zrychlit vymahatelnost práva. Další zkoumání co do hloubky bude

[43] PRAKKEN, H., SARTOR, G., op. cit., s. 348.

[44] SERGOT, M. J., et al., op. cit., s. 379 a násl.

vyžadovat problematika vyvratitelnosti a struktury norem na úrovni slov a co do rozsahu modelování dalších postupů v řízení podle správního řádu.

8. SEZNAM LITERATURY

[1] ALLEN, Layman E.; ENGHOLM, C. Rudy. Normalized legal drafting and the query method. *J. Legal Educ.*, 1977, 29: 380.

[2] BENCH-CAPON, T. J. M., ROBINSON, G. O., ROUTEN, T. W., SERGOT, M. J. Logic Programming for Large Scale Applications in Law: A Formalisation of Supplementary Benefit Legislation. In: *Proceedings of the 1st international conference on Artificial intelligence and law*. ACM, 1987.

[3] BOGUSZAK, J., ČAPEK, J., a GERLOCH, A.: *Teorie práva*. Druhé, přepracované vydání. Praha: ASPI, 2004.

[4] CARNEGIE, D.: *Jak získávat přátele a působit na lidi.* Nakladatelství Dobrovský, Praha, 2012.

[5] CVRČEK, F.: *Právní informatika*. Plzeň: Ústav státu a práva AV ČR ve spolupráci s Vydavatelstvím a nakladatelstvím Aleš Čeněk, 2010.

[6] DVOŘÁK, J., ŠVESTKA, J., ZUKLÍNOVÁ, M.: *Občanské právo hmotné 1*. Praha: Wolters Kluwer, 2017.

[7] FUREK, A., ROTHANZL, L.: *Zákon o svobodném přístupu k informacím. Komentář.* 2. vyd. Praha: Linde, 2012.

[8] HAIDT, J.: *Morálka lidské mysli*. Nakladatelství dybbuk: Praha, 2013.

[9] KNAPP, V.: *Teorie práva*. Plzeň: Západočeská univerzita, 1994.

[10] KRECHT, J.: *Normativní regulace.* Praha: Ediční středisko PF UK, 1997.

[11] MICHÁLEK, J. Co je právo a jak ho můžeme modelovat. *Právník. Teoretický časopis pro otázky státu a práva*, 2020, 159.4: 321-341.

[12] ONDRÁČEK, T., ŠTĚPÁNEK, J.: *Nástin koncepce adaptivních logik.* Pro-Fil, vol. 17, no. 1 (2016). ISSN 1212-9097, s. 16–35.

[13] PELÁNEK, R.: *Modelování a simulace komplexních systémů.* Brno: Masarykova univerzita, 2011

[14] PÍŠA, R.: „Poskytování informací o platech - případová studie soudů na volném poli.“ *Správní právo*, číslo 8/2018.

[15] PRAKKEN, H., SARTOR, G. „The Role of Logic in Computational Models of Legal Argument: A Critical Survey.“ *Lecture Notes in Computer Science*, 2002.

[16] ROSTAIN, T., SKALBECK, R., MULCAHY, K. G.: Thinking Like a Lawyer, Designing Like an Architect: Preparing Students for the 21st Century Practice. *Chi.-Kent L. Rev.*, 2012, **88**: 743.

[17] ŠPIRUDA, A.: *Teorie právních norem*. Dizertační práce. Brno: Masarykova univerzita, 2011.

[18] SERGOT, M. J., et al.: The British Nationality Act as a logic program. In: *Communications of the ACM*, 1986, 29.5: 370-386.

[19] ŠTĚPÁN, J. *Logika a právo.* Praha: Beck, 2001, s. 25 a násl.

[20] WEISSTEIN, E. W. „Disjunctive Normal Form.“ From MathWorld – A Wolfram Web Resource. Dostupný z: https://mathworld.wolfram.com/DisjunctiveNormalForm.html [cit. 2020-10-25].

---

https://doi.org/10.5817/RPT2020-2-5

NESNESITELNÁ LEHKOST ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ORGÁNY VEŘEJNÉ SPRÁVY[1]

JAKUB MÍŠEK,[2] VOJTĚCH BARTOŠ[3]

ABSTRAKT

Zákon o zpracování osobních údajů přinesl některá specifická pravidla pro zpracování osobních údajů ze strany orgánů veřejné moci a veřejných subjektů. Jedním z těchto specifik je nemožnost uložit těmto subjektům správní sankci v případě porušení pravidel ochrany osobních údajů. Autoři tohoto článku se zaměřili na existenci a dosavadní aplikaci této výjimky ze sankční pravomoci ze strany Úřadu pro ochranu osobních údajů. Předkládají přehled dosavadní rozhodovací praxe úřadu a podrobují ji kritické analýze. Tuto analýzu pak zasazují do obecnějšího teoretického rámce důležitého pro pochopení fungování regulace ochrany osobních údajů v rámci Obecného nařízení o ochraně osobních údajů. Konkrétně se věnují sankce v regulaci vystavěné na performativních pravidlech, tak jako je tomu v případě Obecného nařízení. Autoři dovozují konkrétní negativní důsledky současné právní úpravy a její aplikace v konkrétních případech a přicházejí s návrhy řešení spočívajícího v legislativních úpravách i změně interpretace současného znění zákona.

KLÍČOVÁ SLOVA

osobní údaje, GDPR, orgán veřejné moci, správní sankce

[1] Tento článek vznikl v rámci projektu "Právo a technologie VIII" (MUNI/A/0989/2019). Autoři dále děkují recenzentům za cenné rady a postřehy.

[2] JUDr. MgA. Jakub Míšek, Ph.D., odborným asistentem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontakt: jakub.misek@law.muni.cz.

[3] Mgr. Vojtěch Bartoš, interním doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity. Kontakt: vojtech.bartos@seznam.cz.

ABSTRACT

The Personal Data Processing Act introduced some specific rules for the processing of personal data by public authorities and public entities. One of these specifics is the impossibility of imposing an administrative sanction on these entities in the event of a breach of personal data protection rules. The authors of this article focused on the existence and current application of this exception to the sanctioning power by the Office for Personal Data Protection. They present an overview of the Office's current decision-making practice and subject it to critical analysis. They then place this analysis in a more general theoretical framework important for understanding the functioning of personal data protection regulation within the General Data Protection Regulation. Specifically, they address sanctions in regulation based on performance-based rules, as is the case with the General Data Protection Regulation. The authors derive specific negative consequences of the current legislation and its application in specific cases and come up with proposals for a solution consisting in legislative regulations and a change in the interpretation of the current wording of the law.

KEYWORDS

personal data, GDPR, public authority, administrative sanction

1. ÚVODEM

Reforma ochrany osobních údajů, jakkoli vzhledem ke komplikované situaci ePrivacy nařízení v celé své šíři doposud nedokončená, se překlopila do své aplikační fáze, kdy můžeme začít postupně pozorovat a vyhodnocovat její dopady a účinky. Přímá aplikace nařízení č. 2016/679 (obecné nařízení o ochraně osobních údajů, dále „Obecné nařízení“) začala v květnu 2018 a po značných porodních bolestech český zákonodárce doručil o necelý rok později i národní harmonizační předpis v podobě zákona

č. 110/2019 Sb., o zpracování osobních údajů (dále „ZZOÚ“).[4] Jeho legislativní proces byl problematický již v době přípravy vládního návrhu, který Legislativní rada vlády v únoru 2018 vrátila Ministerstvu vnitra z důvodu nízké kvality návrhu k přepracování. Upravená verze byla schválena Vládou 21. 3. 2018[5] a odeslána do Poslanecké sněmovny v podobě dvou sněmovních tisků č. 138, který přinášel návrh zákona o zpracování osobních údajů, a 139, který navrhoval nutné změny do celé řady souvisejících předpisů.[6] Návrhy pak byly schváleny a poslány prezidentovi k podpisu až poté, co došlo k jejich vrácení Sněmovně Senátem. Nestandardní situaci nového národního předpisu ochrany osobních údajů korunoval fakt, že jeho účinnost byla stanovena na den vyhlášení ve sbírce zákonů, což se stalo 24. 4. 2019.

ZZOÚ bohužel obsahuje řadu problematických ustanovení rovněž po věcné stránce. Některé z nich jsou pouze nepochopitelné, úsměvně, ale v zásadě neškodné. Obecné nařízení v omezeném rozsahu umožňuje národním zákonodárcům, aby specifické otázky upravili, dle lokálních potřeb. Příkladem takového ustanovení je čl. 6 odst. 2 Obecného nařízení, dle kterého mohou členské státy zavést pravidla, která specifikují požadavky na zpracování prováděná na základě právních titulů plnění povinnosti, nebo provádění úkolu ve veřejném zájmu a při výkonu veřejné moci (čl. 6 odst. 1 písm. c) a e) Obecného nařízení). Český zákon však v § 5 obsahuje jen prosté konstatování, že správce osobních údajů je „*oprávněn zpracovávat osobní údaje, pokud je to nezbytné pro splnění a) povinnosti, která je správci uložena právním předpisem, nebo b) úkolu prováděného ve veřejném zájmu*

[4] Tento zákon dále upravuje dílčí část implementace tzv. policejní směrnice (směrnice EU č. 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) a zpracování osobních údajů, na které evropské právo nedopadá.

[5] Viz ODOK [online, vid. 30. 10. 2020]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5

[6] Detailní průběh legislativního procesu je k nalezení online na stránkách Parlamentu ČR [online, vid. 30. 10. 2020]. Dostupné z: https://www.psp.cz/sqw/historie.sqw?t=138&o=8.

nebo při výkonu veřejné moci, kterým je správce pověřen."[7] Jde tedy o naprosto prázdné a zbytečné ustanovení, protože toto oprávnění vyplývá již přímo z Obecného nařízení. Stejně bizarně pak působí § 66 odst. 7 ZZOÚ, který uvádí: „*Souhlas subjektu údajů udělený podle zákona č. 101/2000 Sb. se považuje za souhlas podle nařízení Evropského parlamentu a Rady (EU) 2016/679, ledaže způsob jeho udělení nebyl v souladu s tímto nařízením.*"[8] Důvod existence takového ustanovení je možné jen hádat.

Zákon ovšem obsahuje i poměrně zásadní problémy, které svým působením snižují úroveň ochrany osobních údajů dotčených subjektů. Jako příklad je možné uvést ustanovení § 10, který zakládá výjimku z povinnosti provádět posouzení vlivu na zpracování osobních údajů před jeho zahájením, pokud je zpracování prováděno na základě zákonné povinnosti. Detailnější analýza reálných dopadů zmíněného ustanovení leží daleko za hranicí tohoto článku, ale již na základě zběžné úvahy je možné identifikovat několik základních nedostatků této koncepce. Za prvé, hodnocení dopadů prováděné v rámci legislativního procesu se zásadně liší od hodnocení dopadů, které provádí správce údajů pro konkrétní zpracování.[9] Je z principu abstraktní na rozdíl od nutně velmi konkrétního hodnocení správce, který musí zvážit rovněž konkrétní technologie, organizační zajištění v rámci své instituce a obdobně. Za druhé, zákonodárce zcela opomenul, že velké množství procesů zpracování osobních údajů je založeno předpisy, které vznikly v době, kdy ještě nebyl v průběhu legislativního procesu tak vysoký standard na hodnocení dopadů chystané legislativy na soukromí. Konečně za třetí, ustanovení zcela pomíjí, že hodnocení rizik je středobodem regulace ochrany osobních údajů podle Obecného nařízení.[10] Správce údajů musí alespoň základní hodnocení rizik provést vždy. Výjimka se však týká pouze posouzení dopadů podle čl. 35 Obecného nařízení, a to navíc jen před zaha-

[7] Viz § 5 ZZOÚ.

[8] Viz § 66 odst. 7 ZZOÚ.

[9] Srovnej např. Van Dijk, N., Gellert, R., Rommetveit, K. A risk to a right? Beyond data protection risk assessments. *Computer Law & Security Review*. 2016, č. 2.

[10] Viz Quelle, C. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. *European Journal of Risk Regulation*. 2018, č. 3.

jením zpracování. Hodnocení dopadů je však nutné provádět průběžně. Výsledkem aplikace § 10 je tak nutně buď naprosté zmatení dotčených správců údajů, nebo porušení základních stavebních kamenů, na kterých právní úprava zpracování osobních údajů spočívá.

Podle našeho názoru však jeden z nejzásadnějších problémů nové české regulace spočívá v ustanovení § 62 odst. 5, který stanoví, že Úřad pro ochranu osobních údajů (dále ÚOOÚ) „*upustí od uložení správního trestu také tehdy, jde-li o správce a zpracovatele uvedené v čl. 83 odst. 7 nařízení Evropského parlamentu a Rady (EU) 2016/679*“.[11] Odkazované ustanovení Obecného nařízení uvádí, že členské státy mohou stanovit „*další pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě*“.[12] Jinými slovy, námi analyzované a kritizované ustanovení českého zákona zamezuje udělení správní pokuty za porušení povinností vyplývajících z Obecného nařízení orgánům veřejné moci a veřejným subjektům.[13] Uvedená výjimka byla do textu návrhu zákona na základě senátního návrhu a byla odůvodněna tím, že v případě veřejnoprávních správců osobních údajů jsou finanční sankce zbytečné, protože se jedná pouze o přelévání rozpočtových položek „z jedné kapsy do druhé“.[14] Již dosavadní aplikační zkušenost, byť stále ještě pochopitelně limitovaná dobou, která od nabytí účinnosti nového zákona uplynula, ukazuje, že uvedený argument není platný a zákonodárce bohužel prokázal, že nezhodnotil vhodnost a dů-

[11] Viz § 62 odst. 5 ZZOÚ.

[12] Viz čl. 83 odst. 7 Obecného nařízení. Možnost zavedení této výjimky je v Obecném nařízení přítomná proto, že některé ze členských států Unie mají specifická pravidla pro udělování správních sankcí orgánům veřejné správy. V kontextu českého práva je však praxe udělování finančních sankcí orgánům veřejné správy a veřejným subjektům zcela běžná, jak ukazuje například rozhodovací praxe ÚOOÚ z doby minulé právní úpravy, nebo rozhodovací praxe Úřadu pro ochranu hospodářské soutěže. Rovněž z tohoto hlediska je tak zavedení diskutované výjimky do ZZOÚ jen stěží obhajitelné.

[13] Ekvivalentní výjimka je přítomná rovněž v § 61 odst. 3 ZZOÚ, která vylučuje udělení sankce stejnému okruhu subjektů v případě, že jimi dojde k porušení zákazu zveřejnění osobních údajů stanovenému jiným právním předpisem. Z hlediska zaměření tohoto článku se dále zaměřujeme na § 62 odst. 5, naše závěry jsou však aplikovatelné i na ustanovení § 61 odst. 3.

sledky této úpravy v celé její šíři. Prozatím se navíc tomuto problému věnovalo dle našeho názoru méně pozornosti, než si zaslouží.[15]

V tomto článku kriticky analyzujeme současnou situaci. Druhá část článku představí případy, v nichž doposud ÚOOÚ upustil podle ustanovení § 62 odst. 5 od udělení sankce. Třetí část rozhodovací praxi komentuje a upozorňuje na závažná systematická i praktická pochybení, která jsou s ní spojena. Čtvrtá část pak nabízí možná řešení identifikovaného problému, a to jak *de lege lata*, tak *de lege ferenda*.

2. DOSAVADNÍ ROZHODOVACÍ PRAXE ÚOOÚ

Od účinnosti ZZOÚ uplynul již téměř rok a půl a je tak možné začít balancovat a hodnotit, jak se jeho aplikace projevuje v praxi. Když se podíváme na aplikaci jeho § 62 odst. 5, ÚOOÚ vydal ke dni přípravy tohoto článku

[14] Senátor Michael Canov, autor pozměňovacího návrhu, nezbytnost změny odůvodnil na jednání pléna následovně: „*[…] Já se přiznám, že jsem očekával, opravdu jsem očekával, že totéž* [zakázání pokut] *udělá česká vláda. Přece všichni víme, jak u nás máme všichni byrokracie z Bruselu plné zuby. I ti největší příznivci EU prostě poukazují na to, jak je ta byrokracie hrozná, s kterou se zabýváme. A zde dostala česká vláda jedinečnou možnost od Evropského parlamentu a rady, aby orgány veřejné moci a veřejné subjekty osvobodila od správních pokut a ona to neučinila. Pokud v budoucnu bude kdokoli nadávat na ten Brusel, co je to zase za, s prominutím to slovo, buzeraci a šikanu, tak ho opravte. Ne Brusel, to my tady v ČR v čele s vládou si to děláme sami, jak už říkal Honza Horník. Sami. Proč to asi Evropský parlament a rada umožnil ve svém nařízení? No protože to má logiku. Je to vlastně přehazování peněz z jedné kapsy do druhé. Někdo namítne, a co se bude dělat, když tedy nebudou správní pokuty? No ty povinnosti platí. Pracovníci orgánu veřejné moci jsou pracovníci, kteří za porušení můžou dostat výpověď, můžou být potrestáni oni osobně. Ale jaký má smysl se tady upokutovat a upeněžovat tam a zpátky? Co se asi stane, když dostane ministerstvo financí pokutu dva miliony? Tak jí vláda dá dva miliony, zaplatí pokutu a zpátky, že jo. To jsou ty státní organizace.*“ Senát [online, vid. 30. 10. 2020]. Dostupné z: https://www.senat.cz/xqw/xervlet/pssenat/hlasovani?action=steno&O=12&IS=6167&D=30.01.2019#b19565.

[15] Komentář publikovaný v nakladatelství C.H. Beck pouze konstatuje, že ÚOOÚ od potrestání upustí, a zmiňuje odůvodnění o přelévání finančních prostředků od jednoho orgánu k druhému (viz Vlachová, B., Maisner, M. § 61 Porušení zákazu zveřejnění osobních údajů a § 62 Přestupky správců a zpracovatelů. In: Vlachová, B., Maisner, M. *Zákon o o zpracování osobních údajů*. 1. vydání. Praha: Nakladatelství C. H. Beck, 2019, s. 126-132). Naopak komentář publikovaný v nakladatelství Wolters Kluwer nabízí poměrně precizní vymezení pojmu veřejný subjekt (Nulíček, M. et al. *Zákon o zpracování osobních údajů*. Praha: Wolters Kluwer ČR, 2019. In: ASPI [právní informační systém]). Z časopisecké produkce je možné zmínit snad jen text Marka Moravce, který se tématu lehce dotýká (viz Moravec, M. Základní otázky zpracování osobních údajů ve veřejné správě. *Právní rozhledy*. 2020, č. 17.)

celkem 10 rozhodnutí, v rámci kterých upustil od uložení správního trestu dle § 62 odst. 5 ZZOÚ.[16] Jedná se o 7 prvostupňových rozhodnutí a 3 druhostupňová rozhodnutí, jež byla vydána v časovém rozmezí od 20. 5. 2019 do 21. 10. 2020 a tato rozhodnutí budou předmětem další analýzy. Naše analýza se přitom věnuje aplikaci § 62 odst. 5 ZZOÚ, a to jak z hlediska intertemporálního, tak také z hlediska jeho osobní působnosti.

2.1 PROBLÉM INTERTEMPORALITY

Vzhledem k tomu že ZZOÚ nabyl účinnosti dne 24. 4. 2019, je zřejmé, že některá z vydaných rozhodnutí byla vyústěním šetření, resp. správních řízení, zahájených ještě za účinnosti předchozí právní úpravy. Jako první z otázek, které se nabízejí k prozkoumání, jsou tak intertemporální účinky ZZOÚ. Ustanovení § 66 odst. 5 ZZOÚ stanoví, že řízení zahájená podle zákona č. 101/2000 Sb., která nebyla pravomocně skončena přede dnem nabytí účinnosti tohoto zákona, se dokončí podle zákona č. 101/2000 Sb. Jeden ze základních principů trestání obsažený v čl. 40 odst. 6 Listiny základních práv a svobod (jehož použitelnost byla soudně dovozena i ve správním trestání)[17] nicméně stanoví, že je-li pozdější zákon pro pachatele činu příznivější, posuzuje se trestnost a ukládá se trest podle tohoto pozdějšího zákona. Obdoba tohoto principu je obsažena také v § 2 odst. 1 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich. ÚOOÚ tedy s vědomím uvedeného vyřešil příslušné intertemporální kauzy v zásadě dvojím způsobem.

První způsob řešení je patrný v případech druhostupňových rozhodnutí, které tehdejší předsedkyně ÚOOÚ potvrdila v rozsahu výroku o spáchání přestupku (a tedy i jeho kvalifikace dle staré právní úpravy), a které nicméně změnila v rozsahu výroku o trestu, od jehož uložení upustila dle nové právní úpravy.[18] Druhý způsob se pak týkal případů, kdy ke změně právní

[16] Tato rozhodnutí byla získána na základě žádosti dle zákona o svobodném přístupu k informacím ke dni 15. 10. 2020.

[17] Viz např. rozsudek Nejvyššího správního soudu ze dne 27. 10. 2004, sp. zn. 6 A 126/2002 a rozsudek ze dne 13. 6. 2008, čj. 2 As 9/2008 – 77.

[18] Viz rozhodnutí ÚOOÚ ze dne 20. 5. 2019, čj. UOOU-01894/18-18 a rozhodnutí ze dne 22. 5. 2019, čj. UOOU-03469/18-19.

úpravy došlo ještě před vydání prvostupňového rozhodnutí. Tehdy ÚOOÚ používá jak pro kvalifikaci skutku, tak pro výrok o trestu (tj. upuštění od jeho uložení) již novou právní úpravu.[19]

S popsaným postupem ze strany ÚOOÚ, kdy dochází podle nové úpravy k upuštění od potrestání, je zřejmě nutné obecně souhlasit vzhledem k pozitivně právní úpravě stanovené ZZOÚ. Důsledky § 62 odst. 5 ZZOÚ jsou skutečně pro pachatele přestupků příznivější oproti původní právní úpravě, neboť omezují dozorový orgán toliko na možnost konstatovat spáchání přestupku a znemožňují mu za takovéto jednání udělit veřejnoprávní sankci. Na druhou stranu, jak bude ukázáno dále, je otázkou, nakolik je taková aplikace vhodná z hlediska efektivního fungování systému ochrany osobních údajů jako takového. Nehledě na to, samotné konstatování porušení ZZOÚ má samozřejmě nemalý význam pro případné řízení o nároku na náhradu škody podle čl. 82 Obecného nařízení.

2.2 OTÁZKY OSOBNÍ PŮSOBNOSTI § 62 ODST. 5 ZZOÚ

Druhým a snad i zajímavějším problémem, který se v souvislosti s dosavadní aplikací § 62 odst. 5 nabízí, je rozsah osob, které do této výjimky z ukládání veřejnoprávní sankcí za porušení Obecného nařízení spadají. Samotné ustanovení českého ZZOÚ je provedením výjimky stanovené v čl. 83 odst. 7 Obecného nařízení, dle které může každý členský stát stanovit pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě.

Před závorku je potřeba vytknout, že Obecné nařízení hovoří o výjimce z ukládání správních pokut, zatímco ZZOÚ přikazuje upustit od uložení správního trestu. Česká národní úprava je tak jednoznačně širší než výjimka stanovená Obecným nařízením, a tedy je již zde namístě se ptát, zda je takováto národní úprava vůbec souladná s požadavky evropského práva.[20]

[19] Viz rozhodnutí ÚOOÚ ze dne 21. 5. 2019, čj. UOOU-08109/18-3 a rozhodnutí ze dne 22. 5. 2019, čj. UOOU-08729/18-3.

[20] Tento samostatný problém však není předmětem této případové studie.

Pokud jde o subjekty, u nichž má docházet k upuštění od ukládání správních trestů, odkazuje § 62 odst. 5 ZZOÚ přímo na čl. 83 odst. 7 Obecného nařízení, a tedy jedná se o orgány veřejné moci a veřejné subjekty usazené v členském státě. V rámci analyzovaných případů se ÚOOÚ nepouští prakticky do žádné argumentace nebo interpretace těchto pojmů a ve svých rozhodnutích v podstatě jen kategoricky konstatuje, že příslušný správce nebo obviněný je buď orgánem veřejné moci nebo veřejným subjektem. V případech, kdy ÚOOÚ rozhodoval o porušení Obecného nařízení ze strany ústředních orgánů státní správy v jejichž čele je člen vlády, ve smyslu zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy, nemůže být patrně skutečně pochyb, že se tato výjimka uplatní (konkrétně se jednalo o případy Ministerstva vnitra a Ministerstva dopravy),[21] a to navíc při výkonu jejich pravomocí.

Obdobně málo pochyb vzbuzující je případ týkající se České školní inspekce.[22] Česká školní inspekce je dle § 173 školského zákona správní úřad s celostátní působností, který je organizační složkou státu a účetní jednotkou. V tomto případě ÚOOÚ posuzoval zpracování osobních údajů Českou školní inspekcí při výkonu jejích zákonných pravomocí, a závěr úřadu, že „*obviněná je orgán veřejné moci*“, pročež bylo upuštěno od uložení trestu, se tak zdá jako nesporný.

Z hlediska výkladu § 62 odst. 5 ZZOÚ dle úmyslu zákonodárce, jenž se dá zjistit z parlamentní rozpravy, pak také nevzbuzuje pochybnosti, že ÚOOÚ tuto výjimku použil v případě, kdy shledal porušení Obecného nařízení ze strany samospráv. Konkrétně se jednalo o čtyři případy, kdy k porušení Obecného nařízení došlo ze strany obcí.[23] Obce jsou územní samosprávné společenství občanů a veřejnoprávní korporace, přičemž příslušné orgány obce vykonávají veřejné pravomoci svěřené jim právním řádem, zejména pak zákonem č. 128/2000 Sb., o obcích (obecní zřízení), a dalšími

[21] Rozhodnutí ÚOOÚ ze dne 22. 5. 2019, čj. UOOU-08729/18-3, ze dne 6. 6. 2019, čj. UOOU-03469/18-19 a ze dne 5. 12. 2019, čj. UOOU-09383/18-17.

[22] Rozhodnutí ÚOOÚ čj. UOOU-01132/19-3 ze dne 11. 6. 2019.

[23] Rozhodnutí ÚOOÚ čj. UOOU-01894/18-18 ze dne 20. 5. 2019, čj. UOOU-08109/18-3 ze dne 21. 5. 2019, čj. UOOU-00909/20-3 ze dne 21. 5. 2020 a čj. UOOU-00371/20-5 ze dne 29. 6. 2020.

právními předpisy a jsou tak v tomto ohledu nepochybně orgány veřejné moci se všemi důsledky, a to bez ohledu na to, zda jednají v samostatné nebo přenesené působnosti.

Zajímavým a odlišným případem v řadě rozhodnutí ÚOOÚ je však rozhodnutí z června tohoto roku, v rámci kterého bylo upuštěno od uložení správního trestu statutárnímu městu.[24] V tomto případě totiž na rozdíl od zbylých tří rozhodnutí došlo k upuštění od uložení trestu za porušení Obecného nařízení zcela mimo výkon pravomocí, tedy veřejnoprávních funkcí obce. Příslušné porušení Obecného nařízení shledal ÚOOÚ v tom, že pracovnice obce předala nájemci nebytových prostor ve vlastnictví obce seznam členů společenství vlastníků pro účely získání souhlasu s nájmem těchto prostor. Jednalo se tedy o čistě soukromoprávní záležitost, kdy město nakládalo se svým majetkem a v rámci těchto majetkoprávních dispozic zpracovávalo osobní údaje způsobem, který dle názoru ÚOOÚ porušoval Obecné nařízení. ÚOOÚ v tomto rozhodnutí však neuvádí žádnou argumentaci, která by naznačovala jakoukoliv úvahu nad tímto aspektem. Z toho se tedy dá usuzovat, že ÚOOÚ interpretuje rozsah výjimky spíše široce a využívá její jednoduchou aplikaci založenou na celkové povaze správce údajů. Pokud se správce definičně vejde do konceptu orgánu veřejné moci nebo veřejného subjektu, jak je chápe ÚOOÚ, úřad výjimku aplikuje. ÚOOÚ ve všech těchto rozhodnutích pouze lakonicky konstatuje že správce, či obviněný je orgánem veřejné moci, a proto ve smyslu příslušného ustanovení upouští od uložení trestu. Funkčnímu pojetí pojmu „orgán veřejné moci“ pak nepřisuzuje vůbec žádnou relevanci. I na základě ustálené praxe Soudního dvora Evropské Unie (dále „SDEU“), dle které se jakékoli výjimky z režimu ochrany osobních údajů mají interpretovat spíše úzce,[25] se však domníváme, že by bylo vhodné, kdyby rozhodovací praxe ÚOOÚ funkční aspekt v budoucnu adresovala, neboť v případě, kdy orgány veřejné moci (nota bene od státu odlišné veřejnoprávní korporace) zpra-

[24] Rozhodnutí ÚOOÚ čj. UOOU-00371/20-5 ze dne 29. 6. 2020.

[25] Srovnej například bod 47 rozsudku Soudního dvora Evropské unie ze dne 6. 11. 2003 ve věci C-101/01 - Bodil Lindqvist, bod 35 rozsudku Soudního dvora Evropské unie ze dne 11. 12. 2014 ve věci C-212/13 – Ryneš a bod 47 rozsudku Soudního dvora Evropské unie ze dne 14. 2. 2019 ve věci C-345/17 – Buivids.

covávají osobní údaje zcela mimo svou veřejnoprávní působnost, tedy čistě za „soukromými" účely, nedává prakticky žádný smysl, proč by měly být zvýhodňovány oproti jiným správcům a zpracovatelům do té míry, že v zásadě požívají beztrestnosti ve smyslu § 62 odst. 5 ZZOÚ.

Velmi specifická a s ohledem na aplikaci § 62 odst. 5 ZZOÚ přinejmenším sporná jsou pak tři rozhodnutí týkající se základní školy, veřejné vysoké školy a České televize.[26] Ve všech těchto případech ÚOOÚ bez dalšího aplikoval předmětnou výjimku a upustil od uložení trestu. Tato tři rozhodnutí pojí společně skutečnost, že šetřené subjekty ÚOOÚ nekvalifikuje jako orgány veřejné moci, nýbrž jako veřejné subjekty. Pojem veřejný subjekt nemá v českém právním řádu legální ani doktrinálně obecně akceptovanou definici a v tomto případě se jedná o pojem evropského práva, konkrétně používaný na několika místech Obecného nařízení. Jako takový by měl tedy nést specifický evropskoprávní (nikoliv tedy primárně národní) význam, a vycházíme-li z premisy racionálního zákonodárce používajícího jeden pojem pro označení jednoho právního institutu, jeho interpretace v rámci Obecného nařízení, ZZOÚ a mezi těmto předpisy navzájem by měla být v zásadě shodná.

Z tohoto hlediska ke snaze o vyložení pojmu veřejný subjekt přistupuje alespoň v náznaku i ÚOOÚ, když pro výklad používá argument § 14 ZZOÚ, jenž se týká povinnosti jmenovat pověřence pro ochranu osobních údajů. Úprava § 14 ZZOÚ navazuje na čl. 37 odst. 1 písm. a) Obecného nařízení, který stanovuje povinnost jmenovat pověřence právě orgánům veřejné moci a veřejným subjektům. Ustanovení § 14 je pak jakýmsi legislativním „vysvětlením" (nebo snad pokusem o legální definici?) pojmu veřejný subjekt, když stanoví, že povinnost jmenovat pověřence pro ochranu osobních údajů podle čl. 37 odst. 1 písm. a) *„[…] mají kromě orgánů veřejné moci také orgány zřízené zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu"*.[27] Bokem stojí otázka, zda je vůbec souladné s principem přednosti evropského práva, aby členský stát takovýmto způsobem definoval nebo legislativně

[26] Rozhodnutí ÚOOÚ čj. UOOU-01131/19-3 ze dne, čj. UOOU-03305/20-5 ze dne a čj. UOOU-04272/20-3 ze dne 21. 10. 2020.

[27] Viz § 14 ZOOÚ.

zasahoval do pojmů obsažených v přímo aplikovatelném unijním právním předpisu.[28] Nicméně nehledě na to, ÚOOÚ používá toto ustanovení bez dalších úvah nebo argumentace k odůvodnění, proč v daném případě Česká televize je veřejným subjektem, a tedy proč v jejím případě upouští od uložení pokuty. Bez zajímavosti není ani to, že v chronologickém pořadí tří rozhodnutí týkajících se veřejných subjektů, a nikoliv orgánů veřejné moci, je případ České televize až tím posledním. V předchozích dvou případech ÚOOÚ (tj. v případě základní školy a veřejné vysoké školy) se spokojí s pouhým konstatováním, že „*obviněná je veřejným subjektem*".

3. MOŽNOST BEZTRESTNÉHO CHYBOVÁNÍ?

V minulé části tohoto článku byly představeny případy, ve kterých doposud ÚOOÚ upustil od udělení sankce na základě § 62 odst. 5 ZZOÚ. Hlavní problémy této úpravy je dle našeho názoru možné shrnout do dvou okruhů. Prvním je samotná otázka vymezení subjektů, na které analyzovaná výjimka dopadá. Druhým je pak efektivita působení systému ochrany osobních údajů jako taková.

3.1 ROZSAH APLIKACE VÝJIMKY

Je nasnadě, že vymezení osobní působnosti výjimky § 62 odst. 5 ZZOÚ není vůbec tak zřejmé, jak jej ÚOOÚ ve svých rozhodnutích prezentuje. Za veřejný subjekt by si totiž bez jakékoli další argumentace nebo stanovení jakýchkoli konkrétních kritérií každý mohl dosadit významně odlišnou množinu osob. I pokud však vezmeme argument § 14 ZZOÚ, tak tento hovoří o orgánech zřízených zákonem. Pojem orgán je přitom nerozlučně svázán s vrchnostenským výkonem veřejné moci. V takovém případě pak ale školy ani Česká televize nejsou svou povahou orgány, které by za svůj primární cíl měly autoritativní rozhodování o veřejných subjektivních

[28] Zde je možné upozornit jen na to, že původní verze návrhu ZZOÚ, kterou Ministerstvo vnitra předložilo Legislativní radě vlády pokus o definici obsahovala, a právě tato definice (resp. její nevhodnost, jelikož jde o pojem evropského práva) byla jedním z důvodů, proč LRV návrh zákona vrátila ministerstvu k přepracování. Viz Aplikace ODOK [online, vid. 30. 10. 2020]. Dostupné z: https://apps.odok.cz/veklep-detail?pid=KORNAQCDZPW5.

právech a povinnostech. Dá se samozřejmě říci, že pojem orgán je nevhodně použitým termínem, a tedy že jedná v zásadě o legislativní chybu. Místo toho by se dal použít termín veřejný subjekt, nebo správce údajů. I v takovém případě jsou však další vyčtená kritéria nedostatečná a pokud by měla být bez dalších úvah vodítkem pro určení subjektů, kterým nemohou být ukládány pokuty, vedlo by to při jejich mechanické aplikaci k absurdním výsledkům zakládajícím zjevnou nerovnost mezi některými srovnatelnými subjekty.

Příkladem by mohla být třeba Všeobecná zdravotní pojišťovna.[29] Svou funkcí a povahou přinejmenším hybridní subjekt, který je ale v mnoha aspektech zcela srovnatelný se svými plně soukromoprávními konkurenty. Z logiky rozhodnutí ÚOOÚ by však vyplývalo, že VZP jakožto zákonem zřízenému subjektu plnícímu zákonem stanovené úkoly ve veřejném zájmu nemůže být uložen správní trest za porušení Obecného nařízení (na rozdíl od ostatních komerčních pojišťoven). Takový závěr by však dle našeho názoru byl nepřípustný přinejmenším s ohledem na princip rovnosti a zákaz diskriminace. Obdobných příkladů by se samozřejmě dalo najít víc. Konec konců už třeba samotná oblast školství může být z tohoto hlediska problematická. Znamená závěr ÚOOÚ, že např. soukromé vysoké školy, resp. jiné vzdělávací instituce v obdobném postavení, jež nejsou zřízeny zákonem, mohou být (na rozdíl veřejně zřizovaných škol) pokutovány? Nebo by snad ÚOOÚ v takovém případě přistoupil na funkční vymezení role dotčeného povinného subjektu a v případě výkonu povinností vyplývajících ze zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů by bylo od udělení pokuty upuštěno, zatímco v ostatních případech zpracování by již pokuta udělena být mohla?

Logika argumentu ÚOOÚ, že veřejným subjektem je takový subjekt, který plní nějakou specifickou (veřejně důležitou) funkci, se zdá být alespoň částečně funkční (tj. zohledňující právě tuto specifickou funkci) - proto ÚOOÚ upouští od uložení trestů právě např. u veřejných vzdělávacích institucí. Problém ovšem spočívá v tom, že jde o obdobný argument, který

[29] Shodně viz důvodová zpráva k zákonu č. 110/2019 Sb. a Nulíček et al. *Zákon o zpracování osobních údajů*. In ASPI [právní informační systém].

v případě orgánů veřejné moci ÚOOÚ zjevně odmítl uplatnit, když upustil od uložení sankce obci, která jednala zcela mimo výkon svých veřejných pravomocí. Zdá se být vnitřně nesouladné, že při interpretaci jednoho z dvojice velmi úzce spojených pojmů označujících osoby, které mají být vyňaty ze sankční pravomoci ÚOOÚ tuto logiku funkčního výkonu činnosti alespoň implicitně odmítá a u druhého ji explicitně aplikuje.

Z hlediska hodnocení rozhodovací praxe ÚOOÚ je nutné konstatovat, že argumentace dozorového orgánu týkající se aplikace a výkladu pojmů orgán veřejné moci a zejména pak veřejný subjekt je ve většině případů zcela absentující, z čehož vyplývá, že správní rozhodnutí je tak v tomto pro výrok o uložení trestu zcela klíčovém ohledu nepřezkoumatelné. Navíc, a to je z hlediska aplikace výrazně problematičtější, ani přezkoumáno ve většině případů nebude. Účastník řízení, tedy kontrolovaný, totiž v takovém případě opravný prostředek jen sotva podá. V kontextu správního řízení tak zbývá maximálně přezkumné řízení ve smyslu § 94 a následujících zákona č. 500/2004 Sb., správní řád, k jehož zahájení může dát podnět například dotčený subjekt údajů, případně pak stížnost ve smyslu § 175 Správního řádu s možností následné soudní ochrany.

V případě, kdy už ÚOOÚ alespoň nějaký argument předkládá, je pak jeho argumentace dle našeho názoru nedostatečná, vnitřně rozporná a při jejím domyšlení do důsledků nesprávná, zejména proto že zakládá zásadní nerovnost mezi jinak srovnatelnými správci či zpracovateli osobních údajů. Konečně je nutné rovněž upozornit na to, že široká interpretace jakýchkoli výjimek z dopadu právní úpravy ochrany osobních údajů je v rozporu s ustálenou rozhodovací praxí SDEU, který opakovaně uvádí, že je nezbytné zajistit vysokou úroveň ochrany osobních údajů.[30] I v tomto ohledu se pak dle našeho názoru interpretační přístup ÚOOÚ ocitá za hranicí eurokonformního výkladu.

[30] Viz například bod 27 rozsudku SDEU ze dne 11. 12. 2014 ve věci C-212/13 - Ryneš, případně bod 66 rozsudku SDEU ze dne 13. 5. 2014 ve věci C-131/12 - Google Spain.

3.2 SANKCE JAKO KLÍČOVÁ SOUČÁST PRÁVNÍ ÚPRAVY V OBECNÉM NAŘÍZENÍ

I pokud se přeneseme přes právě uvedené nedostatky ve vymezení subjektů, na které výjimka dopadá, mnohem větší problém spočívá v existenci uvedené výjimky jako takové, protože zcela popírá základní regulatorní koncepci a zásady, které byly evropským zákonodárcem pro Obecné nařízení zvoleny. Obecné nařízení je svojí povahou performativní regulace,[31] tedy způsob stanovení povinností, kde není určen konkrétní postup, který musí povinný subjekt dodržet, aby měl jistotu, že naplní svoji *compliance* povinnost. Namísto toho zákonodárce pouze stanoví cíl, kterého má být povinnými subjekty dosaženo.[32] Tento cíl je pak vymezen prostřednictvím zásady odpovědnosti formulované v čl. 5 odst. 2 Obecného nařízení a principu regulace postavené na míře rizika, který je zakotven v čl. 24 Obecného nařízení. Dle něj má správce povinnost dodržet požadavky kladené Obecným nařízením úměrně riziku, které zpracování osobních údajů představuje. Pro plné uvedení kontextu je nezbytné věnovat se alespoň stručně roli, kterou princip odpovědnosti v současné regulaci ochrany osobních údajů hraje.

Předně je třeba zdůraznit, že označení „princip odpovědnosti" není bohužel přesné, protože významově neodpovídá anglické jazykové verzi Obecného nařízení, které jej uvádí jako „*principle of accountability*".[33] Pojem „odpovědnost" v českém právním kontextu obecně označuje „*povinnost snést zákonem danou újmu* [sankci] *v případě, že nastane zákonem stanovená*

[31] Polčák, R. et al. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*. 2019, č. 1.

[32] Viz Coglianese, C. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*. 2017, č. 3, s. 531–532.

[33] V kontextu ochrany osobních údajů nejde zcela o novinku, protože byť na normativní úrovni byla zásada odpovědnosti ve smyslu *accountability* zavedena až Obecným nařízením, prvně se objevuje již v Pravidlech OECD z roku 1980, která v čl. 14 obsahují stručné zanesení zásady odpovědnosti ve znění: „ A *data controller should be accountable for complying with measures which give effect to the principles stated above.*" Čl. 14 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *Oecd.org* [online, vid. 30. 10. 2020]. Jedná se o poslední článek druhé části Doporučení, která je tak formulována analogicky k čl. 5 Obecného nařízení.

skutečnost“.[34] To však mnohem přesněji odpovídá anglickému výrazu „*liability*“.[35] Pojem *accountability* nese primárně významové konotace, že povinný subjekt *za něco* aktivně odpovídá, tedy že zaručuje, že určitý postup nebo fungování věci je v pořádku. Zároveň s tím pojem *accountability* nese význam *zodpovídání se vůči někomu*, tedy nějaké autoritě, která má nad povinným subjektem moc nebo dozor. Richard Mulgan toto dobře shrnuje: „*The concept of 'account-ability' includes an implication of potentiality, literally an 'ability' to be called to 'account'. It may thus refer to the potential for external scrutiny under which most expert professionals work, however independent they may be in their day-to-day decisions. Every medical doctor, for instance, knows that any action he or she takes (or does not take) could potentially become the object of disciplinary investigation or a legal action. In this respect, professionals are literally accountable in their professional actions because they are able to be called to account later for any of their actions.*“[36] Jádro principu odpovědnosti ve smyslu *accountability* leží v povinnosti být schopen prokázat, že jsou vyžadované povinnosti korektně plněny již v průběhu zpracování osobních údajů. Zásada odpovědnosti správce je tak často poměrně nepřesně omezována na povinnost vést záznamy o zpracování a být schopný prokázat, že správce postupuje v souladu s Obecným nařízením.[37] Zásada odpovědnosti ve smyslu *accountability* má však výrazně větší dosah v celém systému ochrany osobních údajů. Představuje totiž fundamentální posun od statického chápání zpracování osobních údajů jako držby informací zafixované okamžikem začátku jejich zpracování[38] k mnohem vhodnějšímu chápání osobních údajů jako procesu probíhajícího

[34] Knapp, V. *Teorie práva*. Praha: C.H. Beck, 1995, s. 200.

[35] Srovnej Liability. *The Law Dictionary* [online, vid. 30. 10. 2020].

[36] Mulgan, R. 'Accountability': An Ever-Expanding Concept? *Public Administration*. 2000, č. 3, s. 560.

[37] Srovnej např. Nulíček, M. et al. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. In ASPI [právní informační systém].

[38] Nedostatky tohoto přístupu k osobním údajů dobře shrnuje Polčák. Viz Polčák, R. Getting European Data Protection Off the Ground. *International Data Privacy Law*. 2014 [cit. 30. 10. 2020]. idpl.oxfordjournals.org

v čase, který se vyvíjí, mění a správce údajů se mu musí přizpůsobovat a na nastalé změny reagovat.[39]

Aby správce osobních údajů splnil povinnosti, které mu ze zásady odpovědnosti ve smyslu *accountability* vyplývají, nestačí, aby měl dokonale zpracované dokumenty o jím prováděném zpracování osobních údajů. Je zcela nezbytné, aby závěry z těchto dokumentů byly opravdu uvedeny do praxe. Ruku v ruce se zásadou *accountability* jde fakt, že Obecné nařízení je regulace postavená na hodnocení rizika, které chystané nebo probíhající zpracování osobních údajů představuje pro práva a zájmy fyzických osob.[40] Čl. 5 odst. 2 ve spojení s čl. 24 Obecného nařízení je tak nezbytné vykládat tak, že stanoví správci údajů povinnost připravit a zabezpečit proces zpracování tak, aby odpovídal míře rizika, kterou dané zpracování pro dotčené fyzické osoby[41] představuje.[42] V tom pak spočívá podstata právní úpravy ochrany osobních údajů jako performativní regulace. Jinými slovy, čím je zpracování rizikovější, tím více povinností a tím větší nároky jsou na správce kladeny a naopak, pokud je zpracování méně rizikové, jsou nižší i požadavky na naplnění dostatečného splnění požadavků Obecného nařízení. Tato regulatorní konstrukce umožňuje, aby obecný předpis, jako je Obecné nařízení, mohl být aplikován na široké spektrum zcela rozličných povinných subjektů,[43] povinností z něj vyplývající byly pro všechny z nich přiměřené a efektivní a zároveň zajistily vysokou úroveň ochrany dotčených

---

[39] Srovnej shodně Míšek, J. *Osobní údaje v čase a prostoru* [online]. Brno, 2020 [vid. 30. 10. 2020]. Dostupné z: <https://is.muni.cz/th/wpa9m/>. Disertační práce. Masarykova univerzita, Právnická fakulta, s. 144.

[40] Ke konceptu rizika pro práva více viz např. Böröcz, I. Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras. *European Data Protection Law Review*. 2016, č. 4.

[41] Záměrně na tomto místě nepoužíváme pojem subjekt údajů, protože zajištěním efektivní aplikace Obecného nařízení jsou chráněny i další fyzické osoby, jak je možné vyčíst například z textace čl. 6 odst. 1 písm. f), ze čl. 35 odst. 1 Obecného nařízení.

[42] Viz Quelle, C. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. *European Journal of Risk Regulation*. 2018, č. 3, s. 502–526.; Nulíček et al. *GDPR - obecné nařízení o ochraně osobních údajů*. In ASPI [právní informační systém]. Detailně též Míšek, J. *Osobní údaje v čase a prostoru* [online]. Brno, 2020 [vid. 30. 10. 2020]. Dostupné z: <https://is.muni.cz/th/wpa9m/>. Disertační práce. Masarykova univerzita, Právnická fakulta, s. 146 a následující.

fyzických osob. Rizikovost zpracování působí jako modifikátor, který může přidat správci nové povinnosti,[44] nebo naopak stanoví možnost nějaké povinnosti nevykonávat.[45] Rizikovost zpracování rovněž působí jako modifikátor míry důslednosti, s jakou správce musí své povinnosti plnit.[46] Zásada *accountability* ve spojení s hodnocením rizik tak vlastně umožňuje správci údajů, aby si sám nastavil, jaké konkrétní povinnosti bude jakým konkrétním způsobem plnit. Podmínkou, kterou pak musí splnit je, aby ve výsledku zpracovával osobní údaje tak, že toto zpracování představuje minimální riziko pro práva a svobody fyzických osob.

Nezbytným předpokladem efektivního fungování performativní regulace je důsledná kontrola a vymáhání povinností, které z ní vyplývají.[47] Dozorový úřad totiž nekontroluje jen to, jakým způsobem správce údajů fakticky postupuje, ale rovněž zda si svoje povinnosti nastavil odpovídajícím způsobem vzhledem k riziku prováděného zpracování. Performativní regulace nabízí povinným subjektům velkou míru flexibility. Daní za to však je reálné

---

[43] Obecné nařízení dopadá na veškeré zpracování osobních údajů, pokud není z jeho aplikace vyloučeno, bez ohledu na velikost povinného subjektu, nebo rizikovost zpracování, které provádí. Ať už se jedná o technologické giganty jako je Facebook a Google, nebo malé živnostníky, kteří prodávají med na Šumavě a vedou si tabulku se jmény stálých zákazníků, Obecné nařízení se aplikuje.

[44] Jako klasický příklad je možné uvést povinnost provést posuzování vlivu zpracování podle čl. 35, které má správce povinnost provést až pokud „*je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob*“. Dále můžeme zmínit čl. 34, který v případě vysokého rizika zakládá povinnost správce informovat přímo subjekty údajů o události porušení ochrany osobních údajů.

[45] Jako příklad výjimky z povinnosti při nízkém riziku můžeme zmínit výjimku z informační povinnosti podle čl. 11 Obecného nařízení, případně výjimku stanovenou v čl. 27, dle které nemusí v případě nízkého rizika správce, který nesídlí na území Unie, jmenovat svého zástupce.

[46] Jako příklad je možné uvést zásadu přesnosti ve smyslu čl. 5 odst. 1 písm. d) Obecného nařízení. Všeobecně platí, že správce musí zajistit, že zpracovává přesné osobní údaje. Zcela jinou míru důslednosti a nezbytné investice však musí vynaložit v případech, kdy jde o zpracování na jehož základě se rozhoduje o právech a povinnostech fyzických osob, a kdy jde o informativní zpracování počtu návštěvníků na webové stránce.

[47] Viz Coglianese. *The Limits of Performance-Based Regulation*, s. 551.; May, P. J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. *Law & Policy*. 2003, č. 4, s. 397.

zajištění toho, že se povinný subjekt bude zodpovídat (bude *accountable*) externímu subjektu, tedy zejména dozorovému úřadu.

Zajištění vymáhání práva, jako jedné z nezbytných podmínek toho, abychom o daném regulatorním rámci mohli jako o právu vůbec hovořit, formuloval již Lon Fuller.[48] Pro performativní regulaci to však platí o to více. Dozor a možné sankce jsou naprosto klíčovou součástí celého systému ochrany osobních údajů, bez které regulace nemůže efektivně fungovat. Flexibilita umožněná performativní regulací a zajištění fungování této regulace prostřednictvím dozoru a sankcí jsou dvěma stranami téže mince. To ostatně potvrzuje samotné Obecné nařízení, když na několika místech jasně formuluje, že sankce by měly v každém případě „*účinné, přiměřené a odrazující*“.[49] Stejná textace se konkrétně objevuje v čl. 84 Obecného nařízení, který v odst. 1 uvádí, že pokud se členské státy rozhodnou stanovit autonomní pravidla pro udělování správních pokut orgánům veřejné moci a veřejným subjektům podle čl. 83 odst. 7 (tak jak to učinil český zákonodárce), musí stanovit „*pravidla pro jiné sankce, jež se mají ukládat za porušení tohoto nařízení… a učinit veškerá opatření nezbytná k zajištění jejich uplatňování. Tyto sankce musí být účinné, přiměřené a odrazující*“. Český zákonodárce však tento požadavek nesplnil.

Pokud takové sankce nebudou, bude správcům a zpracovatelům údajů celá právní úprava doslova pro smích. Jako krásnou ukázku, byť samozřejmě anekdotickou, je možné uvést argumentaci Ministerstva vnitra, kterou použilo v jednom z námi analyzovaných rozhodnutí.[50] Ministerstvo se snažilo přesvědčit ÚOOÚ, že by věc „*měla být odložena, případně mělo být postupováno podle § 60 zákona č. 110/2019 Sb. a obě strany neměly být zbytečně zatěžovány,*“[51] protože vedení řízení v rámci § 62 odst. 5 ZZOÚ je „zatěžující a nehospodárné“, jelikož stejně nemůže být uložená jakákoli sankce. Takovou intepretaci však ÚOOÚ jednoznačně odmítl. V tomto ohledu je nutné podpořit ÚOOÚ v tom, že nerezignoval zcela na prošetřování činností zpra-

[48] Fuller, L. L. *The morality of law*. New Haven: Yale University Press, 1978, s. 39.

[49] Viz body odůvodnění č. 151 a 152 a čl. č. 83 a 84 Obecného nařízení.

[50] Viz rozhodnutí ÚOOÚ ze dne 5. 12. 2019, čj. UOOU-09383/18-17.

[51] Tamtéž s. 5.

cování dotčených analyzovanou výjimkou a nadále alespoň vydává rozhodnutí, ve kterých porušení norem Obecného nařízení formuluje. Jak bylo již zmíněno výše, význam takových rozhodnutí pro případné následné spory o náhradu škody je zjevný.

Analyzovaná právní úprava § 62 odst. 5 ZZOÚ je však od základu chybná, podrývá zásadní regulatorní principy, na kterých je Obecného nařízení vystavěno a jako taková je v rozporu s požadavky, které evropská legislativa na členské státy klade. To pak platí, že analyzovaná výjimka cílí primárně právě na státní instituce, u kterých můžeme oprávněně požadovat vysoký standard plnění jejich zákonných povinností. Není navíc ani možné tvrdit, že by naplňovala argumentaci předkladatele, se kterou byla do zákona vložena, tedy že sankce postrádají smysl, protože jde jen o „přesypávání z jedné kapsy do druhé“. Jak bylo ukázáno výše, řada správců, kteří do současného rozsahu aplikace výjimky spadají, mají rozpočty od státu oddělené. Krom toho i v případech centrálních úřadů veřejné správy mají sankce význam. Tyto orgány mají určité rozpočtové možnosti a jejich součástí není placení pokut za porušení zákonných povinností. Proto i v těchto případech mohou být finanční sankce účelné.

4. SPRÁVNÉ ŘEŠENÍ V NEDOHLEDNU

Jak bylo popsáno výše, máme za to, že hlavní problém analyzovaného ustanovení spočívá v jeho samotné existenci v této podobě. I přes výhrady k dosavadní interpretaci ze strany ÚOOÚ je třeba uznat, že se ÚOOÚ musí pohybovat v legislativou vymezeném rámci. Z tohoto hlediska je tedy nezbytné hledat příčinu současného neuspokojivého stavu na straně zákonodárce spíše než u ÚOOÚ. Jako ideální řešení se proto nabízí, aby zákonodárce ustanovení § 62 odst. 5 (a § 61 odst. 3, protože jak bylo předesláno v úvodu tohoto textu, vše, co je řečeno k prvně jmenovanému, se týká i tohoto) zrušil, případně zásadně upravil do takové podoby, která by byla v souladu s regulatorním rámcem Obecného nařízení. Dle našeho názoru by vhodná úprava mohla spočívat v limitaci výše sankce, jak ostatně bylo upraveno ve vládní podobě návrhu ZZOÚ. Druhou variantou pak může být opravdu vyloučení možnosti uložení sankce vybraným správcům údajů, ale

takové řešení není možné ani vhodné dělat plošně pouhým překopírováním textu Obecného nařízení. Bylo by nezbytné vhodně zacílit a taxativně specifikovat subjekty, u kterých by taková právní úprava byla odůvodnitelná. Dále by bylo vhodné pro zajištění souladu s regulatorním rámcem Obecného nařízení zahrnout do rozhodovacího algoritmu rovněž aspekt rizikovosti zpracování. Na zpracování, která představují vysoké riziko pro práva a zájmy fyzických osob, by tak výjimka nedopadala, zatímco na zpracování nízkoriziková by dopadnout mohla. Je nad rámec tohoto textu vytvářet seznam vhodných kandidátů správců údajů, nebo typů zpracování, i vzhledem k tomu, že se domníváme, že by v první řadě ustanovení vylučující sankce vůbec nemělo být v zákoně přítomné. Zcela jistě však víme, že ministerstva, v čele s Ministerstvem vnitra, které je jedním z největších správců osobních údajů v České republice, by na takovém seznamu ve většině rozsahu svých činností nebyla.

Legislativní změna je však zatím v nedohlednu i vzhledem k relativnímu mládí analyzované právní úpravy a poměrně pochopitelnému obecnému odporu zákonodárce pravidla často měnit a tím snižovat právní jistotu. Následující část článku proto zkoumá možnosti, které se pro alespoň částečné řešení současné situace nabízejí i bez legislativní změny.

4.1 INTERPRETACE, ANEB „VYŠŠÍ BERE“

První možnou cestou, která by mohla zmírnit nežádoucí dopady existence ustanovení § 62 odst. 5 ZZOÚ je jeho vhodná interpretace. Domníváme se proto, že ÚOOÚ by v rámci své rozhodovací činnosti měl hledat takovou interpretaci platné legislativy, která nebude a *priori* zakládat nerovnosti, bude logicky koherentní a v neposlední řadě také souladná s evropským právem. Z tohoto hlediska je poměrně podstatné, že ÚOOÚ používá jako základní východisko své interpretace veřejného subjektu § 14 ZZOÚ. Tímto ustanovením se český zákonodárce sice patrně chtěl pokusit definovat pojem veřejný subjekt obsažený v čl. 37 odst. 1 písm. a) Obecného nařízení, nicméně z hlediska evropského práva tato snaha nedává žádný smysl. Zaprvé, pojmy Obecného nařízení, resp. v zásadě všech evropských předpisů, je obecně potřeba vnímat jako autonomní pojmy evropského

práva a není možné je svazovat národními definicemi. Opačný přístup by v tomto případě odporoval podstatě unifikace národního práva členských států přímo účinným právním předpisem EU a také principu přednosti evropského práva. Zadruhé, samotné Obecné nařízení nedává národnímu zákonodárci ani v čl. 37 ani na jiném místě zmocnění k takovéto "implementaci" pojmu veřejný subjekt do národního právního řádu. Zatřetí, samotné Obecné nařízení neobsahuje žádné ustanovení, které by dávalo sebemenší vodítko pro pojetí pojmu veřejný subjekt právě tak, jak je předkládán v § 14 ZZOÚ. Toto národní ustanovení, resp. jeho aplikace ze strany ÚOOÚ v kontextu čl. 62 odst. 5 ZOOÚ, přitom evidentně zasahuje do požadavku účinných, přiměřených a odrazujících pokut dle č. 83 odst. 9 Obecného nařízení. Tím se národní právní úprava, resp. současná správní praxe ÚOOÚ dostává do přímého konfliktu s požadavky práva EU.

Z ustálené judikatury SDEU vyplývá, že členské státy (včetně jejich správních orgánů) jsou povinny při aplikaci práva dát přednost přímo účinnému právnímu předpisu evropského práva před konfliktním pravidlem práva národního.[52] Soudní dvůr také jednoznačně říká, že také správní orgány mají jednoznačnou povinnost nepoužít vnitrostátní právní předpisy odporující unijnímu právu.[53] Z hlediska evropského práva by tedy ÚOOÚ v žádném případě neměl volit takovou aplikaci ZZOÚ, kdy interpretací § 62 odst. 5 ZZOÚ ve smyslu § 14 ZZOÚ dojde k závěru, že všechny subjekty zřízené zákonem, které plní zákonem stanovené úkoly ve veřejném zájmu nemohou být nijak sankcionovány za porušení Obecného nařízení. Takováto aplikace národního práva je totiž v rozporu s požadavky evropského práva. Namísto toho by ÚOOÚ měl argumentovat přímým účinkem Obecného nařízení, od § 14 odhlédnout, resp. jej neaplikovat a pro výklad pojmu veřejný subjekt zvolit eurokonformní obsah. Je pravdou, že tento přístup by zpočátku vykazoval nižší právní jistotu pro adresáty normy, avšak při zvolení transparentní metodologie a podrobné

[52] Rozsudek ESD ze dne 22. 6. 1989, ve věci C-103/88 *Fratelli Constanzo SpA proti Comune di Milano* a navazující judikatura.

[53] Viz např. bod 38 rozsudku SDEU ze dne 4. 12. 2018, ve věci C-378/17 *Minister for Justice and Equality a Commissioner of the Garda Síochána*.

argumentace ÚOOÚ v jeho rozhodnutích by právní jistota mohla být relativně brzy významně zvýšena.

Jednou z možností, jak by pojem veřejný subjekt mohl být vykládán, je např. výklad "funkční" (jak byl popsán výše), respektive pohled rozlišující mezi veřejnoprávním a soukromoprávním účelem zpracování osobních údajů. Tedy o veřejný subjekt jde tehdy, pokud v kontextu daného zpracování osobních údajů plní veřejnoprávní funkci. Takový výklad by umožňoval vyšší míru flexibility s ohledem na okolnosti konkrétního případu, jelikož na rozdíl od současného přístupu by subjekty zřízené zákonem mohly být v některých případech sankcionovány (zejména tam, kde neexistuje spravedlivý důvod pro odlišné zacházení oproti "soukromým" subjektům). Ilustrací tohoto přístupu by bylo alternativní rozhodnutí v případu UOOU-00371/20-5, kdy statutární město pochybilo při zpracování osobních údajů v rámci soukromoprávních dispozic se svým majetkem. V takovém případě by na základě funkčního přístupu mohlo být konstatováno, že příslušný správce vykonává čistě soukromoprávní funkci a neexistuje důvod pro jeho odlišení od jakýchkoliv jiných správců, kteří by se při nakládání se svým majetkem dopustili stejného pochybení. Statutární město by v takovém případě nebylo považováno za veřejný subjekt ve smyslu § 62 odst. 5 ZZOÚ.

Dalším z pomocných znaků, který by bylo možné aplikovat při „funkčním výkladu" pro rozlišení zda je § 62 odst. 5 ZZOÚ aplikovatelný, který by se držel logiky a systematiky samotného Obecného nařízení, je rozlišování veřejných subjektů dle toho, na základě jakého právního titulu příslušné (ne)sankcionované zpracování provádělo. Tam, kde se jedná o zpracování zejména dle čl. 6 odst. 1 písm. c) nebo e), existuje důvod se domnívat, že zpracování provádí správce v postavení veřejného subjektu. Pro orgány veřejné moci a veřejné subjekty bude totiž typické právě takovéto zpracování. Na druhou stranu, nemůže jít samozřejmě o jediné hodnotící kritérium. Pokud bychom se spolehli jen na tento aspekt, mohlo by dojít k obtížím spojeným s tím, že řada soukromých správců provádí často a pravidelně zpracování na základě zákona a žádným způsobem se přitom neblíží svou povahou nebo povahou své činnosti orgánům veřejné moci nebo veřejným subjektům. V takových případech by také neexistoval

spravedlivý důvod pro vyloučení příslušných správců ze sankční pravomoci ÚOOÚ. Typicky by se jednalo o zpracování v rámci osobních údajů v kontextu zaměstnání, plnění daňových povinností, archivačních povinností, atp. což jsou běžné agendy, v rámci kterých soukromí správci zpracovávají osobní údaje z titulu plnění zákonných povinností.

Konečně i samotné ustanovení § 14 by bylo možné interpretovat jiným způsobem, který by reflektoval tento funkční přístup a zároveň byl eurokonformní. Na tuto definici by se totiž zcela jistě bylo možno dívat jako na souhrn tří znaků, jež musí být kumulativně splněny, aby bylo možno daného správce považovat za veřejný subjekt. Správce by vždy musel (i) být zřízen zákonem, (ii) plnit zákonem stanovené úkoly (tj. jednat na základě zákona) a (iii) jednat ve veřejném zájmu (tj. nikoliv při plnění soukromých zájmů). V rámci této interpretace by tedy musel ÚOOÚ rovněž vždy zejména dbát na to, jakou příslušný (zákonem zřízený) správce plnil funkci. Zda k příslušnému zpracování osobních údajů došlo v rámci jednání na základě zákona a zda směřovalo k naplňování veřejného zájmu. Tento přístup by tak do značné míry odpovídal na shora nastíněnou kritiku dosavadního přístupu ÚOOÚ a více by odpovídal smyslu čl. 83 odst. 7. Ten má totiž umožnit členským státům začlenění sankcí za porušení Obecného nařízení do jejich specifického (zejm. neobsahujícího finanční pokuty) domácího sankčního mechanismu vůči orgánům státu (resp. relativně úzce vymezenému okruhu subjektů, jež mají nějaké významné veřejné postavení, pro které jsou postaveny mimo běžný systém administrativních pokut), spíše než plošně vyčlenit ze sankčního mechanismu Obecného nařízení všechny subjekty, jež se v nějakém ohledu dají charakterizovat jako veřejné. Jako každá výjimka z pravidla i tato by měla být interpretována co nejúžeji, aby skrze ni nedocházelo k systematickému tunelování základního pravidla.

4.2 CO SI ČLOVĚK NEUDĚLÁ SÁM…

Pro úplnost na samém závěru tohoto textu je vhodné připomenout, že dozorový úřad (a jeho sankce) není jediným externím subjektem, kterému se má ve smyslu zásady *accountability* správce údajů zodpovídat. Určitá forma do-

hledu, respektive zajištění transparentnosti zpracování,[54] je zajištěna možností subjektu údajů vykonávat svá práva a dovolat se přímé soudní ochrany. V případě zpracování osobních údajů v kontextu výkonu veřejné správy však může být často možnost aplikace práv subjektů údajů fakticky omezena, například v podobě nemožnosti dovolat se práva na výmaz. Konečně, i v případě, že právo subjektu údajů opravdu svědčí, a správce údajů odmítne jeho výkon, nehrozí mu ze strany ÚOOÚ žádná sankce.

Jedinou reálnou možností, kterou tak v současné době subjekt údajů pro zajištění svých práv vyplývajících z Obecného nařízení má, je přímá soudní ochrana zaručená čl. 79 Obecného nařízení, dle kterého má „*každý subjekt údajů právo na účinnou soudní ochranu, pokud má za to, že jeho práva podle tohoto nařízení byla porušena v důsledku zpracování jeho osobních údajů v rozporu s tímto nařízením*“.[55] Jakkoli toto ustanovení přináší (alespoň teoretické) zvýšení úrovně ochrany subjektů údajů oproti stavu před účinností Obecného nařízení, je jeho praktická aplikace problematická. Hlavním důvodem je zejména jeho dosavadní neprobádanost, protože (alespoň pokud je nám známo) doposud na jeho základě české soudy nerozhodovaly. Samostatnou otázkou pak zůstává, podle jakých procesních předpisů se bude v takových řízeních postupovat, což je jedna z otázek, které rovněž ZZOÚ neřeší, byť by mohl. Nabízí se řízení o ochraně před nezákonným zásahem, pokynem nebo donucením správního orgánu podle § 82 a následujících zákona č. 150/2002 Sb., soudní řád správní.[56] V případě, že v důsledku zpracování osobních údajů prováděném při výkonu veřejné moci vznikne subjektu údajů újma, bude věcně postupovat v souladu se zákonem č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád).

[54] K transparentnosti jako jednomu ze základních cílů právní úpravy ochrany osobních údajů viz např. Hert, P. De. Gutwirth, S. Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power. In: Claes, E.; Duff, A.; Gutwirth, S., eds. *Privacy and the criminal law*. Antwerp: Intersentia, 2006, s. 77–78 a Lynskey, O. Deconstructing Data Protection: The ‘added-Value’ of a Right to Data Protection in the Eu Legal Order. *International & Comparative Law Quarterly*. 2014, č. 3, s. 595.

[55] Viz čl. 79 odst. 1 Obecného nařízení.

[56] Shodně též Moravec. *Základní otázky zpracování osobních údajů ve veřejné správě*.

Další zatím neprobádanou otázkou zůstává, zda pouhé porušení norem Obecného nařízení, tedy pouhé protiprávní zpracování osobních údajů, může v kontextu českého soudního výkladu konstituovat újmu. Jakkoli například Ústavní soud vyzdvihuje zásadní důležitost informačního soukromí a informačního sebeurčení,[57] jehož jsou osobní údaje přímým odrazem, není nám známo žádné české rozhodnutí, ve kterém by pro založení újmy postačovalo pouhé protiprávní zpracování osobních údajů.[58] Situace se navíc komplikuje tím, že pokud ÚOOÚ zachová širokou interpretaci pojmu veřejný subjekt, a bude tak dopadat i na v zásadě soukromoprávní zpracování osobních údajů, nebude se v případných řízeních o přímé ochraně subjektů údajů postupovat jen podle těchto předpisů, ale v úvahu budou připadat rovněž relevantní ustanovení týkající se civilního soudního řízení.

Již jen z tohoto velmi stručného přehledu je znatelné, že jakkoli je nutné vítat snahu evropského zákonodárce o posílení práv subjektu údajů prostřednictvím jednoznačně formulované možnosti přímé soudní ochrany, není možné pro její složitost a dosavadní nejednoznačnost očekávat, že by dokázala efektivně nahradit nedostatek v podobě absentujících sankcí dle § 62 odst. 5 ZZOÚ.

5. ZÁVĚREM

Existence výjimky z ukládání sankcí stanovená § 62 odst. 5 (a § 61 odst. 3) ZZOÚ představuje dle našeho názoru zásadní pochybení, které nikdy neměmě-

[57] Viz např. bod 30 rozhodnutí Data retention I, ve kterém Ústavní soud uvádí: „*Pokud jednotlivci nebude garantována možnost hlídat a kontrolovat obsah i rozsah osobních dat a informací jím poskytnutých, jež mají být zveřejněny, uchovány či použity k jiným než původním účelům, nebude-li mít možnost rozpoznat a zhodnotit důvěryhodnost svého potenciálního komunikačního partnera a případně tomu uzpůsobit i své jednání, pak nutně dochází k omezení až potlačování jeho práv a svobod a nelze tak již nadále hovořit o svobodné a demokratické společnosti. Právo na informační sebeurčení (informationelle Selbstbestimmung) je tak nezbytnou podmínkou nejen pro svobodný rozvoj a seberealizaci jednotlivce ve společnosti, nýbrž i pro ustavení svobodného a demokratického komunikačního řádu. Zjednodušeně řečeno, v podmínkách vševědoucího a všudypřítomného státu a veřejné moci se svoboda projevu, právo na soukromí a právo svobodné volby chování a konání stávají prakticky neexistujícími a iluzorními.*“ Viz Nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl.ÚS 24/10, č. N 52/60 SbNU 625.

[58] Inspiraci k podobným závěrům je však možné nabírat v zahraničí, konkrétně ve Velké Británii, viz rozhodnutí Royal Courts of Justice, Strand, London zde dne 8. 10. 2018, sp. zn. [2018] EWHC 2599 (QB).

lo najít cestu do českého právního řádu.[59] V tomto článku jsme identifikovali tři hlavní problémy, které analyzovaná právní úprava představuje.

Prvním a z hlediska regulace ochrany osobních údajů jako takové zcela nejzásadnějším problémem je, že vyloučení uložení sankcí bez adekvátní náhrady, v podobě úpravy, která by byla účinná, přiměřená a odrazující, je v příkrém rozporu s principem performativní regulace, na kterém je prostřednictvím zásady *accountability* správce Obecné nařízení vystavěno. Bez efektivního dohledu se nemohou projevit benefity flexibility, které zásada *accountability* a hodnocení rizik přináší. Naopak, právní rámec ochrany osobních údajů se bez efektivního dozoru a vymáhání stává prázdnou skořápkou, fíkovým listem, který jen zcela neefektivně překrývá nekorektní, chybné a neproporcionální zpracování osobních údajů. Druhý problém spočívá v nejasném vymezení osobní působnosti analyzované výjimky. Ukázali jsme, že již dosavadní rozhodovací praxe ÚOOÚ v této oblasti představuje do budoucna potenciální riziko. To spočívá zejména v přílišné šíři aplikace předmětné výjimky, a to jak z hlediska toho, na které správce dopadá (jako jsou například školská zařízení), tak z hlediska činností, v jejichž případech není ospravedlnitelné, aby veřejnoprávní správce požíval takové výhody oproti typově obdobným zpracováním prováděným jinými subjekty (např. zpracování osobních údajů, které je ve svém základu soukromoprávního charakteru). Třetí důvod zásadní defektnosti analyzované výjimky spatřujeme v tom, že ani neplní účel, který byl při jejím přijímání proklamován jako důvod její existence, tedy aby se zabránilo zbytečnému přesypávání financí „z *jedné kapsy do druhé*“. Jak vyplývá z druhého problému, v případě, že bude dopad výjimky interpretován široce, může jít často o naprosto rozdílné kapsy, různých svrchníků zcela odlišných osob. Krom toho, i v případě, že by došlo k uložení sankce orgánu veřejné správy, který je přímo financován z veřejného rozpočtu, má takové uložení sankce význam z hlediska dopadů na rozpočtovou kázeň daného orgánu. Odstrašující aspekt sankce je tak bezpochyby přítomný.

[59] S trochou nadsázky by se dalo označit za ukázkový příklad nesystematické „lidové kreativity“, které jsou občas bohužel čeští poslanci a senátoři schopni.

Pokud uvažujeme o variantách řešení této situace, nabízí se poměrně přirozeně varianty *de lege ferenda* a *de lege lata*. Legislativní řešení by dle našeho názoru bylo ideální, jakkoli je spíše v brzké době neočekáváme vzhledem k obvyklé nechuti zákonodárce měnit teprve nedávno zavedenou úpravu. Jako nejvhodnější se nám jeví odstranění výjimky § 62 odst. 5 (a § 61 odst. 3) ZZOÚ a ponechání plné aplikace režimu sankcí podle Obecného nařízení. Aspekty případu, které ÚOOÚ musí při řešení kauzy brát v potaz,[60] ruku v ruce s rozsahem možných udělených sankcí, nabízí dostatečně flexibilní nástroj, který umožňuje adekvátní aplikaci vzhledem ke všem myslitelným případům zpracování osobních údajů v kontextu veřejné správy. Je-li Obecné nařízení, včetně jeho systému sankcí, dostatečně flexibilním předpisem, aby efektivně regulovalo zpracování prováděné technologickými giganty na jedné straně a malými živnostníky na straně druhé, není moc důvod, proč by nemohlo být použito pro efektivní regulaci Ministerstva vnitra a zároveň malé obce o padesáti obyvatelích. V případě, že by se zákonodárce rozhodl přeci jen využít možnosti zavést výjimku, kterou mu Obecné nařízení nabízí v čl. 83 odst. 7, je nutné, aby taková právní úprava byla ve svém důsledku účinná, přiměřená a odrazující. Jako vhodné se jeví zastropování výše možné udělené sankce, případně zavedení aspektu rizika zpracování osobních údajů pro práva a zájmy fyzických osob, jako flexibilní proměnné, na základě které by bylo možné aplikovatelnost výjimky stanovit.

V případě řešení *de lege lata* máme k dispozici dvě cesty. První spočívá v zajištění práv subjektů údajů prostřednictvím přímé soudní ochrany. Ta se však na základě prvotního prozkoumání nejeví jako příliš efektivní, i vzhledem k značné procesní složitosti a nevyjasněnosti. Druhá cesta, kterou je dle našeho názoru nezbytné se co nejrychleji vydat, je interpretační posun ze strany ÚOOÚ, a případně správních soudů v následných řízeních, které takový posun nutně vyvolá. Jakékoli výjimky z režimu ochrany osobních údajů musí být vykládány co nejvíce restriktivně. To pak platí o to více v případě výjimky, která efektivně zapříčiňuje nefunkčnost celé oblasti zpracování osobních údajů, a která tím pádem vede k zásadnímu

[60] Viz čl. 83 odst. 2 Obecného nařízení.

snížení standardu ochrany subjektů údajů. ÚOOÚ by měl brát v potaz nejen povahu daného povinného subjektu, ale rovněž funkční povahu probíhající zpracování. Vhodnou cestou tak může být například identifikace dotčených subjektů na základě kumulativního splnění tří podmínek, dle kterých by pro aplikaci výjimky správce vždy musel (i) být zřízen zákonem, (ii) plnit zákonem stanovené úkoly (tj. jednat na základě zákona) a (iii) jednat ve veřejném zájmu (tj. nikoli při plnění soukromých zájmů). ÚOOÚ je v současné době v samých počátcích tvorby své rozhodovací praxe v této oblasti. Při dobré argumentaci v odůvodnění svých rozhodnutí a vytvoření transparentní metodologie určování správců údajů, kteří se do rozsahu výjimky vejdou, může ÚOOÚ svojí činností alespoň částečně v mezích možného překonat nedostatky, které tato právní úprava přinesla. Uvědomujeme si, že se nejedná o snadný úkol. Na druhou stranu, právě z toho důvodu plní ÚOOÚ v kontextu státní správy tak zásadní roli v podobě nezávislého dozorového úřadu, který má chránit fyzické osoby i před nekorektním zpracováním ze strany státu. To je role, na kterou ÚOOÚ nesmí rezignovat.

6. POUŽITÁ LITERATURA

[1] Böröcz, I. Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras. *European Data Protection Law Review*. 2016, č. 4, s. 467–480.

[2] Coglianese, C. The Limits of Performance-Based Regulation. *University of Michigan Journal of Law Reform*. 2017, č. 3, s. 525–564.

[3] Van Dijk, N., Gellert, R., Rommetveit, K. A risk to a right? Beyond data protection risk assessments. *Computer Law & Security Review*. 2016, č. 2, s. 286–306.

[4] Fuller, L. L. *The morality of law*. New Haven: Yale University Press, 1978.

[5] Hert, P. De. Gutwirth, S. Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power. In: Claes, E.; Duff, A.; Guthwirth, S., eds. *Privacy and the criminal law*. Antwerp: Intersentia, 2006, 199 s. ISBN 978-90-5095-545-4.

[6] Knapp, V. *Teorie práva*. Praha: C.H. Beck, 1995. Právnické učebnice.

[7] Lynskey, O. Deconstructing Data Protection: The 'added-Value' of a Right to Data Protection in the Eu Legal Order. *International & Comparative Law Quarterly*. 2014, č. 3, s. 569–597.

[8] May, P. J. Performance-Based Regulation and Regulatory Regimes: The Saga of Leaky Buildings. *Law & Policy*. 2003, č. 4, s. 381.

[9] Míšek, J. *Osobní údaje v čase a prostoru* [online]. Brno, 2020 [vid. 30. 10. 2020]. Dostupné z: <https://is.muni.cz/th/wpa9m/>. Disertační práce. Masarykova univerzita, Právnická fakulta.

[10] Moravec, M. Základní otázky zpracování osobních údajů ve veřejné správě. *Právní rozhledy*. 2020, č. 17, s. 576–583.

[11] Mulgan, R. 'Accountability': An Ever-Expanding Concept? *Public Administration*. 2000, č. 3, s. 555–573.

[12] Nulíček, M. et al. *Zákon o zpracování osobních údajů*. Praha: Wolters Kluwer ČR, 2019. In ASPI [právní informační systém].

[13] Nulíček, M. et al. *GDPR - obecné nařízení o ochraně osobních údajů*. Praha: Wolters Kluwer, 2017. In ASPI [právní informační systém].

[14] Polčák, R. Getting European Data Protection Off the Ground. *International Data Privacy Law*. 2014 [cit. 30. 10. 2020]. idpl.oxfordjournals.org

[15] Polčák, R. et al. Virtualizace právních vztahů a nové regulatorní metody v pozitivním právu. *Právník*. 2019, č. 1, s. 86–98.

[16] Quelle, C. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability and Risk-based Approach. *European Journal of Risk Regulation*. 2018, č. 3, s. 502–526.

[17] Vlachová, B., Maisner, M. Zákon o zpracování osobních údajů. 1. vydání. Praha: Nakladatelství C. H. Beck, 2019, 163 s. ISBN 978-80-7400-760-6.

[18] Organizace pro hospodářskou spolupráci a rozvoj. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. *Oecd.org* [online, vid. 30. 10. 2020]. Dostupné z: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotection ofprivacyandtransborderflowsofpersonaldata.htm.

[19] Liability. *The Law Dictionary* [online, vid 30. 10. 2020]. Dostupné z: https://thelawdictionary.org/liability/.

https://doi.org/10.5817/RPT2020-2-6

V ČEM SPOČÍVÁ ŠKODLIVÝ NÁSLEDEK POUHÉHO ZÁSAHU DO INFORMAČNÍHO SOUKROMÍ ČLOVĚKA BEZ TOHO, ABY BYLO ČLOVĚKU ZASAŽENO DO DALŠÍCH JEHO PRÁV?[1]

JAN SVOBODA[2]

Soud:	Court of Appeal (Civil Division), Velká Británie
Věc:	Lloyd vs Google, HQ17M01913, ref. A2/2018/2769
Datum:	2. 10. 2019
Dostupnost:	www.pdpjournals.com/docs/888010.pdf

1. ÚVOD

Právo na soukromí, právo na soukromý a rodinný život, právo na informační sebeurčení, právo na informační soukromí a právo na ochranu osobních údajů – to všechno jsou pojmy, které spolu úzce souvisí, avšak až na jednu dvojici (jak bude vysvětleno níže), nejsou zaměnitelné. Do všech z nich, stejně jako do každého práva, lze nicméně zasáhnout, a to způsobem, který může způsobit újmu nositeli těchto práv. Zásahem do jednoho z výše uvedených práv pak často může dojít i k zásahu do práv dalších, a to nejen těch uvedených v tomto článku. Je ale zasažení do práva na informační soukromí, které nezpůsobí zásah do jiného z práv, způsobilé vyvolat škodlivý následek? A pokud ano, v čem tento škodlivý následek spočívá?

[1] Vznik tohoto příspěvku byl podpořen projektem MUNI/A/0989/2019 (Právo a technologie VIII).

[2] Mgr. Jan Svoboda je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity v Brně. Vedle toho působí v mezinárodní advokátní kanceláři PricewaterhouseCoopers Legal. Kontaktní email je jan.svoboda@mail.muni.cz.

Abychom našli odpověď na výše uvedené otázky, je třeba pokusit alespoň nastínit vztah mezi jednotlivými právy, jejichž výčet je uveden na začátku tohoto textu. I proto, že se všechny rozebírané pojmy vztahují k obecné, relativně abstraktní, oblasti lidského žití, není jejich uchopení snadné a na poli právní vědy nenajdeme jejich jednotné definice či stoprocentní shodu na tom, jak si vůči sobě vzájemně stojí a nakolik se překrývají. K popsání jejich vztahu se tak pokusím přistoupit zejména za užití zdrojů, které sám považuji za přesvědčivé a jejichž závěry jsou logicky slučitelné. Nemám však potřebu, a ani nemohu, tvrdit, že jsou jediné přijímané či snad dokonce jediné správné.

Následně pro nalezení odpovědi analyzuji relevantní části dvou nedávných rozhodnutí (jedná se o prvostupňové a druhostupňové rozhodnutí v téže věci) z právního prostředí Velké Británie. Oba se přitom vztahují k evropské úpravě ochrany a zpracování osobních údajů a jsou tedy vhodnými případy pro tento příspěvek. Dále předložím několik příkladů, které charakter zásahu do informačního soukromí člověka blíže ilustrují.

2. INFORMAČNÍ SOUKROMÍ A S NÍM SOUVISEJÍCÍ POJMY

Soukromí, respektive právo na soukromí, bývá popisováno, v závislosti na přístupu k němu, jak ve své práci *„Conceptualizing Privacy“* uvádí D. J. Solove, jako „právo být ponechán sám sobě“,[3] „omezení přístupu k sobě samému“,[4] „utajení“ (respektive možnost utajení),[5] „kontrola nad osobními informacemi“,[6] ale také za užití dalších výrazů a přirovnání.[7] V rámci zde překládaného výkladu pak bude pracováno hned s prvním pojetím práva na soukromí, jakožto s právem být „ponechán sám sobě“, a to zejména proto, že krom řady autorů vycházejících z něho ve svých publikacích jej ve své

[3] Označení bylo přeloženo z anglického *„Right to Be Let Alone“*. Viz SOLOVE, D. J. *Conceptualizing Privacy* [online]. 90 Cal. L. Rev. (2002) s. 1999-1102 [cit. 8. 5. 2020]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103

[4] Označení bylo přeloženo z anglického *„Limited Access to the Self“*. Tamtéž, s. 1102-1105.

[5] Označení bylo přeloženo z anglického *„Secrecy“*. Tamtéž, s. 1105-1109.

[6] Označení bylo přeloženo z anglického *„Control Over Personal Information“*. Tamtéž, s. 1109-1116.

[7] Tamtéž, s. 1116 a násl.

rozhodovací praxi aproboval i náš Ústavní soud. Přístup k právu na soukromí jakožto k právu být ponechán sám sobě můžeme poprvé nalézt v publikaci *„Law of Torts“* z roku 1888 autora T. M. Cooley. O dva roky později stejný přístup k soukromí rozvinuli i S. Warren a L. Brandeis ve své práci „*The Right to Privacy*“, jimž zmíněný popis bývá často nesprávně přisuzován jako těm, kdo jej využili coby první.[8] Ústavní soud pak zmíněný pohled na soukromí odrazil např. ve svém nálezu ze dne 22. 3. 2013, Pl. ÚS 24/10. Překlad do českého jazyka, který Ústavní soud zvolil a v české právní vědě se následně rozšířil, přičemž je používán i v tomto textu, může mít nicméně negativní, nezamýšlené, konotace. Proto lze doporučit jeho výklad provádět vždy ve světle původního anglického sousloví.[9]

S. Warren a L. Brandeis ve své práci „*The Right to Privacy*“ argumentují, že práva související s ochranou soukromí nejsou práva vznikající na základě smlouvy, ale práva „vůči světu“ tedy práva *erga omnes*.[10] Dále uvádějí, že samotný zásah do tohoto soukromí je hodný požadavku odškodnění, neboť sám o sobě působí psychickou újmu.[11]

Právo na soukromí je v České republice v rovině ústavního pořádku chráněno čl. 10 Listiny základních práv a svobod.[12] Již ten nám napoví, že se soukromí skládá mimo jiné ze soukromého a rodinného života (přičemž můžeme říci, že rodinný život je podsložkou života soukromého)[13] a z informačního sebeurčení.[14] Informační sebeurčení tak můžeme považovat, stejně jako činí i E. Wagnerová v rámci komentáře k výše uvedenému předpisu za

[8] Srov. POLČÁK, R.; SVANTESSON, D. *Information Sovereignty – Data, Privacy, Sovereign Powers and the Rule of Law.* Cheltenham: Edward Elgar Publishing, 2017, s. 82.

[9] Srozumitelný přehled přístupu k pojmu soukromí nabízí J. MÍŠEK ve své práci *Osobní údaje v čase a prostoru* [online]. Brno, 2020, s. 28-35 [cit. 8. 5. 2020]. Disertační práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Radim Polčák. Dostupné z: https://is.muni.cz/th/wpa9m/

[10] WARREN,D., BRANDEIS, L. The Right to Privacy. *Harvard Law Review* [online]. 1890, roč. IV, č. 5, s. 213 [cit. 8. 5. 2020]. Dostupné z: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

[11] Tamtéž.

[12] Srov. WAGNEROVÁ, E., In: WAGNEROVÁ, E., a kol. *Listina základních práv a svobod. Komentář.* Praha: Wolters Kluwer, 2011, čl. 10.

[13] Viz čl. 10 odst. 2 Listiny základních práv a svobod a dále pak tamtéž.

[14] Viz čl. 10 odst. 3 Listiny základních práv a svobod a dále pak tamtéž.

součást práva na soukromí. Ústavní soud k právu na informační sebeurčení, které lze, zjednodušeně řečeno, chápat jako možnost kontrolovat informace, případně data, o sobě,[15] uvádí: *„Vedle tradičního vymezení soukromí v jeho prostorové dimenzi (ochrana obydlí v širším slova smyslu) a v souvislosti s autonomní existencí a veřejnou mocí nerušenou tvorbou sociálních vztahů (v manželství, v rodině, ve společnosti) právo na respekt k soukromému životu zahrnuje i garanci sebeurčení ve smyslu zásadního rozhodování jednotlivce o sobě samém. Jinými slovy, právo na soukromí garantuje rovněž právo jednotlivce rozhodnout podle vlastního uvážení, zda, popř. v jakém rozsahu, jakým způsobem a za jakých okolností mají být skutečnosti a informace z jeho osobního soukromí zpřístupněny jiným subjektům.“*[16]

Právo na informační sebeurčení je dle mého názoru, byť jsem si vědom i názorů rozdílných,[17] zaměnitelné s právem na informační soukromí. Obě jsou totiž bezesporu podsložkou soukromí[18] a obě se bezprostředně vztahují ke kontrole dat či informací o dané osobě, a to dat a informací celého spektra lidského soukromí.[19]

Právo na ochranu osobních údajů je pak možné vnímat jako institut sloužící k ochraně všech výše uvedených práv, respektive jako jejich podsložku, s tím, že za stěžejní cíl práva na ochranu osobních údajů lze, alespoň v rámci českého právního prostředí, s odkazem na bod odůvodnění 4 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“), a hlavně pak na § 1 zákona č. 110/2019 Sb., o zpracování

---

[15] Srov. DONÁT, J., Tomíšek, J. *Právo v síti.* Praha: C.H. Beck, 2016, s. 24.

[16] Nález Ústavního soudu ze dne 22. 3. 2013, Pl. ÚS 24/10.

[17] Viz např. MÍŠEK, J. *Osobní údaje v čase a prostoru* [online]. Brno, 2020, s. 36 [cit. 8. 5. 2020]. Disertační práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Radim Polčák. Dostupné z: https://is.muni.cz/th/wpa9m/ nebo POLČÁK, R. *Internet a proměny práva.* Praha: Auditorium, 2012, s. 327.

[18] Srov. SOLOVE, D. J. *Conceptualizing Privacy* [online]. 90 Cal. L. Rev. (2002) s. 1106 [cit. 8. 5. 2020]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103

[19] Srov. KOOPS, B. et al. A *Typology of Privacy* [online]. SSRN Scholarly Paper ID 2754043. Rochester, NY: Social Science Research Network 2016, s. 484 [vid. 8. 5. 2020]. Dostupné z: http://papers.ssrn.com/abstract=2754043

osobních údajů (dále jen „ZZOÚ“) považovat ochranu soukromí. Ustanovení § 1 ZZOÚ přímo říká, že ZZOÚ k naplnění práva každého na ochranu soukromí upravuje práva a povinnosti při zpracování osobních údajů. Ochrana osobních údajů tak vytváří prostor pro ochranu distributivních práv a výkon svobod spjatých s lidským soukromím.

Nyní, když jsme nastínili základní vztah mezi jednotlivými právy a způsob, jakým s nimi bude v rámci tohoto textu pracováno, je vhodné přistoupit ke konkrétnímu případu, který nám rovněž pomůže odpovědět na výše uvedené otázky. Jak bylo avizováno, jedná se o případ řešený před soudy Velké Británie, konkrétně před londýnským Hight Court of Justice, v rámci rozhodnutí č. HQ17M01913 ze dne 8. 10. 2018 a následně před Court of Appeal (Civil Division), a to v rámci rozhodnutí č. HQ17M01913, ref. A2/2018/2769, ze dne 2. 10. 2019. Tato rozhodnutí jsou populárně nazývána dle jejich stran jako *„Lloyd vs Google“*.

3. LLOYD VS GOOGLE - PRVOSTUPŇOVÉ ROZHODNUTÍ

V předmětném rozhodnutí soud projednával žalobu, kterou se pan Lloyd za sebe a další účastníky (4,4 mil uživatelů telefonu typu iPhone)[20] v rámci hromadné žaloby, domáhal odškodnění za újmu. Ta mu měla vzniknut kvůli počínání společnosti Google.[21] Google je společností se sídlem v Kalifornii, a tak musel britský soud rozhodovat o přípustnosti hromadné žaloby. Mezi podmínky pro určení příslušnosti soudu v tomto ohledu patří i skutečnost, zda je s žalobou spojena dostatečná míra pravděpodobnosti na úspěch. Soud tak musí učinit i některé meritorní úvahy.[22] Závěry zde prezentované mohou být v rámci dalšího, již skutečně meritorního, řízení dále změněny. Pro náš výklad není relevantní to, jakou roli v daném sporu hrála problematika hromadných žalob a klasifikace daného sporu pod patřičné řízení. Hromadné žaloby jsou české právní kultuře vzdálené a přes občasné tendence k jejich zavedení je účinná právní úprava dosud nepřipouští.

[20] Viz bod 4 daného rozhodnutí.

[21] Viz bod 1-3 daného rozhodnutí.

[22] Viz bod 45-53 daného rozhodnutí.

Společnost Google zpracovávala informace generované prohlížečem včetně IP adresy daného zařízení a adresy navštívené stránky, a to za užití souboru cookie (tzv. *DoubleClick cookie*). Konečným cílem této aktivity bylo zobrazování personalizované reklamy. Uložení souboru cookie a na to navazující zpracovatelské aktivity byly činěny bez souhlasu a bez vědomí uživatele, tedy subjektu údajů (tzv. *Safari Workaround*).[23]

IP adresa je obecně považována za osobní údaj,[24] stejně tak lze za osobní údaj považovat velkou část souborů cookie nebo údajů na základě nich předávaných, vč. historie stránek. O trendu podřazování širokého spektra údajů pod pojem osobní údaje ve smyslu účinných právních předpisů pak svědčí např. i rozsudek Krajského soudu v Brně ze dne 7. 11. 2018, č j. 31 A 68/2018-177.

Výše nastíněným postupem společnosti Google v období několika měsíců v letech 2011-2012 došlo k porušení povinností § 4 odst. 4 britského Data Protection Act z roku 1998 (dále jen „DPA“), který v dotčeném období představoval transpozici směrnice 95/46/ES. Dle § 13 odst. 1 DPA má fyzická osoba, která utrpěla újmu v důsledku porušení jakékoli povinnosti správce uložené DPA, nárok na odškodnění ze strany správce za tuto újmu. Újma zde má dle žalobce spočívat zejména ve ztrátě kontroly nad osobními údaji.[25] Alternativně žaloba požadovala odškodnění v hodnotě, kterou díky nim Google získal.

Soud však v tomto rozsudku neshledal prosté porušení práva na informační sebeurčení, jak je vymezeno výše v tomto textu,[26] jako způsobilé pro vznik újmy, neboť daná událost se neprojevila zásahem do práva na soukromí daného jedince.[27] Soud mimo jiné uvedl, že nesouhlasí s názorem, že osoba, jejíž údaje byly použity v rozporu se zákonem automaticky utrpí odškodnitelnou újmu, zejména škodu nebo psychickou újmu, na základě

[23] Viz bod 4-8 daného rozhodnutí.

[24] Srov. bod odůvodnění 30 GDPR.

[25] Srov. bod 58 a 59 daného rozhodnutí.

[26] Viz bod 54 daného rozhodnutí.

[27] Srov. bod 56 daného rozhodnutí.

spáchání daného přestupku nebo na základě narušení autonomie, která se k nakládání s osobními údaji vztahuje.[28]

V daném rozhodnutí pak ze strany soudu byla použita řada argumentů pro podložení výše uvedeného závěru. Jedním z nich bylo tvrzení, že někteří lidé mají radost z večírku uspořádaného jakožto překvapení. Dalším pak existence řady dlouhotrvajících vztahů vzniklých díky tomu, že společný přítel dvou osob předal kontakt jedné osoby té druhé bez jejího souhlasu. Na tomto místě je však třeba upozornit, že nelze bez dalšího srovnávat užití osobních údajů pro ryze osobní účely a užití osobních údajů pro zbylé aktivity, zejména pak ty komerční.[29] Dané argumenty tak nelze považovat za relevantní pro tento případ. Nadto je třeba uvést, že spíše než že při výše uvedených případech nevzniká újma (škodlivý následek), nevzniká újma takové intenzity, aby nebyla převážena jinými faktory, v jejichž důsledku na újmu subjekty údajů vlastně zapomenou, čili jim je nezřídka zároveň kompenzována jiným aspektem daného činu.

Výše uvedené závěry pak nepřevzal odvolací soud. Rozdílné posouzení prvostupňovým a druhostupňovým soudem pochopitelně není zvláštností. Svědčí to nicméně o problematičnosti případu a omezené možnosti představit si všechny vztahy a významy relativně abstraktních pojmů uvedených v úvodu tohoto textu, k nimž se více či méně explicitně daná rozhodnutí váží.

4. LLOYD VS GOOGLE – DRUHOSTUPŇOVÉ ROZHODNUTÍ

Odvolací soud otázku, zda je možné poskytnout odškodnění pro samotnou ztrátu kontroly nad daty, aniž by byla způsobena škoda nebo psychická újma, zhodnotil jinak.[30] Vyšel mimo jiné z faktu, že § 13 DPA představuje transpozici směrnice, která byla přijata pro výkon čl. 8 Charty základních práv EU.[31] Předně popsal, že samotná kontrola nad daty představuje určitou hodnotu. Odůvodnil to například tím, že mohou být prodána (nikoli ve

[28] Viz bod 74 daného rozhodnutí.

[29] Srov. např. čl. 2 GDPR.

[30] Bod 70 daného rozhodnutí.

[31] Srov. bod 42 daného rozhodnutí.

smyslu převedení vlastnictví, nýbrž ve smyslu umožnění jejich zpracování). Většinou je možnost zpracovávat data směňována přímo za určitou službu (nikoli tedy za peníze), např. za přístup k wifi či za umožnění využívání určitého programu.[32]

Ve světle výše uvedeného pak odvolací soud rozhodl, že samotná ztráta kontroly nad osobními údaji způsobená porušením správcovy povinnosti dle DPA je způsobilá založit nárok k odškodnění, a to bez nutnosti dalšího dokazování. Dané rozhodnutí tak výrazně posiluje pozici subjektů údajů a ochranu jejich osobních údajů bez ohledu na to, jaké konsekvence porušení správcových povinností na ochranu osobních údajů vyvolalo.

5. CHARAKTER ZÁSAHU DO INFORMAČNÍHO SOUKROMÍ

Ptáme-li se, v čem spočívá škodlivý následek porušení ztráty osobních údajů, je to, jak ukazuje i druhostupňové rozhodnutí Lloyd vs Google, právě ona ztráta kontroly nad těmito daty.

Ztráta kontroly nad vlastními daty nemusí nutně vést například ke zneužití identity, odhalení choulostivých informací pro udržení dobré pověsti, zveřejnění informací zneužitelných v rámci diskriminačních praktik či jiných znatelných zásahů do soukromí. Vždy ale vede k zásahu do svobody vůle. Disponuje-li někdo našimi osobními údaji bez řádného právního důvodu, znemožňuje nám tím nejen možnost mu tyto údaje v budoucnu poskytnout, ale například i možnost s ním souhlas se zpracováním svých údajů za něco směnit.[33] Odpověď na otázku, zda je zasažením do práva na informační soukromí, které nezpůsobí zásah do jiného z práv, způsobilé vyvolat škodlivý následek, je tedy ano.

Omezení svobody vůle pak spočívá i v tom, že své osobní údaje můžeme mít zájem poskytnout pouze takovému správci, kterému důvěřujeme, a to zejména pro jeho reputaci v oblasti zabezpečení těchto údajů.[34] Ve vztahu k zabezpečení pak mohu mít zájem vykonávat určité kontrolní kroky. Ne-

[32] Body 46-47 daného rozhodnutí.

[33] Srov. body 46-47 druhostupňového rozhodnutí Lloyd vs Google.

[34] Srov. kapitola IV oddíl 2 GDPR nebo ÚOOÚ. *Zabezpečení osobních údajů* [online]. Vytvořeno / změněno: 27. 10. 2017 / 25. 4. 2019 [cit. 8. 5. 2020]. https://www.uoou.cz/8-zabezpeceni-osobnich-udaju/d-27282/p1 = 3938

vím-li však, že někdo zpracovává mé osobní údaje, nemohu tuto kontrolu logicky ani vykonávat.

V neposlední řadě pak svoboda vůle bezpochyby zahrnuje i svobodu někoho nepodpořit v jeho činnosti, a to i neposkytnutím svých osobních údajů. Byť jsme nic z výše uvedeného nemuseli mít zájem učinit, neopravňuje toto nikoho nám danou možnost upřít.

Z výše uvedeného je tak patrné, že zásah do informačního soukromí nemusí nutně představovat zásah do soukromého života či do soukromí, vždy ale představuje zásah alespoň do svobody vůle, byť třeba aktuálně nevykonávané/neprezentované. Toto se pokusím uvést na dvou dalších příkladech. První příklad můžeme znát spíše ze cvičení argumentace v oblasti morálních otázek. I když se většinou nepoužívá pro vysvětlování aspektů informačního soukromí, věřím, že se v této oblasti osvědčí. Jedná se o situaci osoby, která se ráda opaluje nepozorována nahá. Činí tak na svém oploceném pozemku, kam za standardních okolností není vidět. Jednoho dne ale na nedalekou lampu vyleze jiná osoba a záměrně ji pozoruje. Nefotí ji a její fotografie tedy logicky ani nijak nemonetizuje. V tomto ohledu jí tak nepřipravuje o zisk. O její zálibě nikomu neříká. Neposkytuje tedy nikomu možnost k užití těchto informací v rámci diskriminace nebo snad, připadalo-li by daného chování někomu z jakéhokoli důvody třeba nemravné, k poškození pověsti. O zneužití identity pak z podstaty věci nemůže být řeč.

Zasahuje však do její svobody vůle. Její první preferencí je totiž opalovat se nahá a nepozorovaná. Druhou pak s největší pravděpodobností není opalovat se nahá a pozorovaná, nýbrž neopalovat se vůbec nebo se opalovat v plavkách.

Odhlédněme teď od toho, že pozorující osoba by jen stěží hledala legitimní důvod pro zásah do informačního soukromí třeba „jen“ z morálního hlediska a zaměřme se na to, že opalující se osobu neupozornila na fakt, že je sledována. Kdyby na ni totiž z lampy zapískala, minimálně by se opalující se osoba oblékla a tím mimo jiné (vlastně znovu) vyjádřila svou vůli komu se (ne)chce při opalování odhalovat.

Aniž by tedy pozorující osoba způsobila efekt zjevně viditelný v soukromí jiného člověka, připravila opalující se osobu o možnost volní reakce

na danou situaci. Dále ji nechala v omylu jejího legitimního očekávání, že má danou situaci fakticky pod kontrolou. Obdobná možnost byla odepřena i uživatelům iPhonu v případě Lloyd vs Google. Je totiž možné předvídat, že by někteří z nich, obdobně k aktu obléknutí, přistoupili k používání jiného telefonu, jiného prohlížeče či k jinému chování na internetu.

Druhý příklad je svým charakterem o něco podobnější tomu z případu Lloyd vs Google. Představme si osobní spis bývalého zaměstnance, pro jehož uchování již neexistuje právní základ. Bývalý zaměstnavatel by tedy měl spis skartovat. Neučiní tak, ale zavře ho do trezoru a kromě samotného uložení údaje v něm obsažené nijak nezpracovává. Uchovává ho nicméně v rozporu s právem. V daném případě zaměstnanec nepřichází o možnost směny svých osobních údajů, neboť zaměstnavatel tyto, vzhledem ke způsobu jejich zpracování, zjevně nepotřebuje. Uložení v trezoru pak nepředstavuje přímé ohrožení ve smyslu možnosti zneužití jeho identity či dalšího zveřejnění jeho osobních údajů. Opět ale dochází ke ztrátě kontroly. Neví-li zaměstnanec o určitém zpracování, nemůže provádět ani výše uvedenou úvahu ve vztahu k zabezpečení a logicky pak ani vykonávat svá práva jakožto práva subjektu údajů. Volní rozhodnutí o tom, jakým způsobem s jeho osobními údaji bude nakládáno, pak bez ohledu na zaměstnancovo další jednání chybí a je tedy opět zasahováno do jeho svobody vůle.

Rozlišujeme-li striktně mezi právy a svobodami, můžeme uzavřít, že zásahem do informačního soukromí, který nepředstavuje zásah do dalších práv, je vždy omezena svoboda vůle. V tom lze tedy spatřovat onen škodlivý následek.

Nadto-lze další škodlivý následek spatřovat v zásahu do systému práva na ochranu osobních údajů, případně do systému práva na informační soukromí. Tyto systémy jsou totiž chráněny řadou komplexních pravidel, přičemž při jejich porušování se přesouváme od zvýšení informovanosti tohoto systému k prvkům nežádoucí entropie a daný systém tak z informačního pohledu strádá. Pracujeme-li s přístupem, že tento systém slouží jako prostředek k ochraně dalších distributivních práv a svobod, tak přesto, že daný zásah do něj nemusí nutně znamenat zásah do dalšího konkrétního

práva, snižuje kvalitu ochranného prostředí jako celku, což může vyústit v intenzivnější škodlivý následek v budoucnosti.

6. ZÁVĚR

V textu byl nejdříve podán výklad pojmu práva na soukromí a s ním souvisejících institutů, včetně popisu jejich vztahu. Uvedeny byly přístupy k pojmu soukromí s důrazem na jeho pojetí formulovaném S. Warrenem a L. Brandeisem.

Pro zodpovězení otázek, zda je zasažení do práva na informační soukromí, které nezpůsobí zásah do jiného z práv, způsobilé vyvolat škodlivý následek a v čem tento škodlivý následek spočívá, bylo rozebráno prvostupňové i druhostupňové rozhodnutí Lloyd vs Google. Na takto podaném výkladu bylo ukázáno, že takový škodlivý následek možné vyvolat je a že tento spočívá zejména v omezení svobody vůle. Pro tento závěr je stěžejní důsledně rozlišovat mezi právy a svobodami.

Nad to byl škodlivý efekt identifikován ve snížení organizovanosti systému ochrany informačního soukromí, který má obecně za cíl chránit další distributivní práva. Toto pak může způsobit dodatečné škodlivé efekty v budoucnu.

Závěrem je myslím vhodné připomenout hysterii okolo blížící se použitelnosti GDPR v roce 2018. Ta mohla řadu subjektů údajů nepochybně utvrdit v důležitosti těchto údajů takovým způsobem, že je zcela legitimní očekávat, že jim prostý zásah do informačního soukromí způsobí psychickou újmu, byť třeba nepodloženou zásahem do dalších práv.

7. ZDROJE:

7.1 ODBORNÁ LITERATURA:

[1] DONÁT, J., Tomíšek, J. *Právo v síti.* Praha: C.H. Beck, 2016, 352 s., ISBN 978-80-7400-610-4.

[2] KOOPS, B. et al. A *Typology of Privacy* [online]. SSRN Scholarly Paper ID 2754043. Rochester, NY: Social Science Research Network 2016, 93 s. [vid. 8. 5. 2020]. Dostupné z: http://papers.ssrn.com/abstract=2754043

[3] MÍŠEK, J. *Osobní údaje v čase a prostoru* [online]. Brno, 2020, 231 s. [cit. 8. 5. 2020]. Disertační práce. Masarykova univerzita, Právnická fakulta. Vedoucí práce Radim Polčák. Dostupné z: https://is.muni.cz/th/wpa9m/

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

[5] POLČÁK, R.; SVANTESSON, D. *Information Sovereignty – Data, Privacy, Sovereign Powers and the Rule of Law.* Chltenham: Edward Elar Publishing, 2017, 262 s., ISBN 978-1-78643-921-5.

[6] SOLOVE, D. J. *Conceptualizing Privacy* [online]. 90 Cal. L. Rev. (2002) 70 s. [cit. 8. 5. 2020]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=313103

[7] ÚOOÚ. *Zabezpečení osobních údajů* [online]. Vytvořeno / změněno: 27. 10. 2017 / 25. 4. 2019 [cit. 8. 5. 2020]. https://www.uoou.cz/8-zabezpeceni-osobnich-udaju/d-27282/p1=3938

[8] WAGNEROVÁ, E., a kol. *Listina základních práv a svobod. Komentář.* Praha: Wolters Kluwer, 2011, 931 s., ISBN 978-80-7357-750-6.

[9] WARREN, D., BRANDEIS, L. The Right to Privacy. *Harvard Law Review* [online]. 1890, roč. IV, č. 5, 29 s. [cit. 8. 5. 2020]. Dostupné z: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

7.2 PRÁVNÍ PŘEDPISY:

[10] Britský Data Protection Act z roku 1998

[11] Listina základních práv a svobod

[12] 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)

[13] 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

[14] Zákon č. 110/2019, o zpracování osobních údajů

7.3 SOUDNÍ ROZHODNUTÍ:

[15] Rozhodnutí Royal Courts of Justice, Court of Appeal, HQ17M01913, ref. A2/2018/2769, ze dne 2. 10. 2019

[16] Nález Ústavního soudu ze dne 22. 3. 2013, Pl. ÚS 24/10

[17] Rozsudek Krajského soudu v Brně ze dne 7. 11. 2018, č.j. 31 A 68/2018-177

---

https://doi.org/10.5817/RPT2020-2-7

PŘEHLED AKTUÁLNÍ JUDIKATURY II/2020

FRANTIŠEK KASL, JAKUB KLODWIG, IVANA KUDLÁČKOVÁ, PAVEL LOUTOCKÝ, JAKUB MÍŠEK, TEREZA NOVOTNÁ, JURAJ VIVODA, JAKUB VOSTOUPAL, VERONIKA ŽOLNERČÍKOVÁ

1. PRÁVO DUŠEVNÍHO VLASTNICTVÍ

AUTORÁDIO JAKO SDĚLOVÁNÍ DÍLA VEŘEJNOSTI

Soud: Soudní dvůr Evropské unie
Věc: C-753/18 (Stim a SAMI)
Datum: 2. 4. 2020
Dostupnost: curia.europa.eu

V původním sporu rozhodovaly švédské soudy ve dvou případech, které byly poté před Soudním dvorem spojeny v jeden. V prvním případě se organizace Stim (švédská organizace pro správu autorských práv hudebních skladatelů a jejich vydavatelů) domáhala u soudu zaplacení náhrady škody za porušení autorských práv od společnosti Fleetmanager, která zprostředkovává krátkodobý pronájem vozidel vybavených radiopřijímačem. V druhém případě se společnost NB domáhala u soudu navrácení poplatků za užívání zvukových záznamů, které platila organizaci SAMI (švédská organizace pro správu práv souvisejících s autorským právem výkonných umělců) taktéž za zprostředkování krátkodobého pronájmu vozidel vybavených radiopřijímači.[1]

Oba případy byly řešeny před švédskými obecnými soudy. V obou případech odvolací soudy nevyhověly organizaci Stim jako žalobkyni v prvním

[1] Body 13, 14 a 16 anotovaného rozhodnutí.

případě a organizaci SAMI jako žalované v druhém případě a organizace tedy podaly kasační stížnosti ke švédskému Nejvyššímu soudu.[2]

Nejvyšší soud ve Švédsku tedy předložil Soudnímu dvoru dvě předběžné otázky: 1) zda se jedná o sdělování veřejnosti v případě krátkodobého pronájmu vozidel s radiopřijímači a 2) jaký je v takovém případě význam objemu činnosti pronajímání vozidel a zejména doby trvání pronájmu.[3]

Sdělování autorského díla veřejnosti je v unijním právu upraveno zejména bodem 27 odůvodnění a čl. 3 odst. 1 směrnice 2001/29 a čl. 8 směrnice 2006/115 týkajících se sdělování veřejnosti, které Soudní dvůr v tomto případě aplikoval.

Soudní dvůr se zabýval nejprve první otázkou a tedy tím, zda krátkodobý pronájem vozidel s radiopřijímači představuje sdělování díla veřejnosti. Z ustálené judikatury Soudního dvora vyplývá, že pojem sdělování veřejnosti představuje dva prvky - „*sdělování*“ a „*veřejnosti*“ – které musí být splněny kumulativně.[4] Sdělování je upřesněno v bodu 27 odůvodnění směrnice 2001/29 tak, že „*pouhé poskytnutí fyzického zařízení pro umožnění nebo uskutečnění sdělování není samo o sobě sdělováním ve smyslu této směrnice*“, což je právě případ poskytnutí radiopřijímače v pronajatém autě, kde se jedná spíše o dodání než-li sdělování. Soudní dvůr tedy dospěl k tomu, že první kumulativní podmínka není splněna a o sdělování veřejnosti se tedy nejedná, z tohoto důvodu se již nezabýval druhou otázkou.[5]

Soudní dvůr tedy došel k závěru, že pronájem vozidel opatřených radiopřijímači bez dalšího nepředstavuje sdělování veřejnosti ve smyslu příslušné právní úpravy.

Autorka: TN

[2] Body 15 a 17 anotovaného rozhodnutí.

[3] Bod 18 anotovaného rozhodnutí.

[4] Bod 30 anotovaného rozhodnutí.

[5] Body 33 až 36 anotovaného rozhodnutí.

OCHRANA FUNKČNÉHO TVARU VÝROBKU AUTORSKÝM PRÁVOM

Soud: Súdny dvor Európskej únie
Věc: C-833/18 (Brompton Bicycle)
Datum: 11. 6. 2020
Dostupnost: curia.europa.eu

Spoločnosť Brompton Bicycle Ltd (*Brompton*) založená pánom SI predáva skladací bicykel, ktorého tvar navrhnutý v roku 1987 umožňuje tri rozličné polohy.[6] Doba platnosti patentu už uplynula. Spoločnosť Chedech/Get2Get (*Get2Get*) predáva vizuálne veľmi podobný a rovnako polohovateľný bicykel. Pán SI a Brompton sa obrátili na belgický súd s tvrdením, že bicykle Get2Get porušujú autorské právo Brompton a osobnostné práva pána SI a žiadali, aby prikázal ich stiahnutie z predaja. Get2Get tvrdí, že vonkajšia úprava ich bicykla je podmienená technickým riešením, aby bicykel mohol mať želané polohy. Brompton namieta, že rovnakú polohovateľnosť možno dosiahnuť aj inými tvarmi bicykla, a preto jeho tvar môže byť chránený autorským právom.

Belgický súd uvádza, že v oblasti práva dizajnov Súdny dvor Európskej únie (SDEÚ) už rozhodol, že na posúdenie toho, či sú znaky vonkajšej úpravy výrobku dané výlučne technickou funkciou tohto výrobku, treba určiť, či je táto funkcia jediným faktorom, ktorý určuje tieto znaky, pričom existencia alternatívnych dizajnov nie je v tejto súvislosti rozhodujúca. Belgický súd sa preto prejudiciálnou otázkou SDEÚ pýta, či sa čl. 2 až 5 smernice 2001/29[7] majú vykladať (podobne) v tom zmysle, že autorskoprávna ochrana, ktorú stanovujú, sa uplatňuje na výrobok, ktorého tvar je minimálne sčasti nevyhnutný na dosiahnutie technického výsledku.

[6] Ide o zloženú polohu, rozloženú polohu a prostrednú polohu umožňujúcu udržať bicykel na zemi v rovnováhe.

[7] Smernica Európskeho parlamentu a Rady 2001/29/ES z 22. mája 2001 o zosúladení niektorých aspektov autorských práv a s nimi súvisiacich práv v informačnej spoločnosti. Podľa článkov 2 až 5 smernice 2001/29 sú autori chránení proti rozmnožovaniu, verejnému prenosu a verejnému šíreniu ich diel bez ich súhlasu.

SDEÚ uvádza, že na predmet spĺňajúci podmienku originality sa môže vzťahovať autorskoprávna ochrana, aj keď jeho zhotovenie bolo určené technickými požiadavkami, pokiaľ toto určenie nebránilo autorovi vtisnúť do daného predmetu vlastnú osobnosť ako prejav jeho slobodných a tvorivých rozhodnutí. Pokiaľ vyjadrenie zložiek predmetu je predurčené ich technickou funkciou, jednotlivé spôsoby realizácie danej myšlienky sú natoľko obmedzené, že myšlienka a jej vyjadrenie splývajú.

Podľa SDEÚ sa čl. 2 až 5 smernice 2001/29 majú vykladať v tom zmysle, že v nich stanovená autorskoprávna ochrana sa uplatní na výrobok, ktorého tvar je minimálne sčasti nevyhnutný na dosiahnutie technického výsledku, pokiaľ tento výrobok je originálnym dielom, ktoré je výsledkom duševnej tvorby v rozsahu, v akom výberom tohto tvaru vyjadril jeho autor svoju tvorivú schopnosť originálnym spôsobom vykonaním slobodných a tvorivých rozhodnutí tak, že uvedený tvar odráža jeho osobnosť. Splnenie týchto podmienok prináleží overiť vnútroštátnemu súdu s ohľadom na skutočnosti veci samej.

Autor: JVi

POJEM „ADRESA“ V SMERNICI O VYMOŽITEĽNOSTI PRÁV DUŠEVNÉHO VLASTNÍCTVA SA NEVZŤAHUJE NA E-MAILOVÚ ADRESU, TELEFÓNNE ČÍSLO ANI IP ADRESU OSOBY, KTORÁ NAHRALA CHRÁNENÉ DIELO NA PLATFORMU

Soud: Súdny dvor Európskej únie
Věc: C-264/19 (Constantin Film Verleih)
Datum: 9. 7. 2020
Dostupnost: curia.europa.eu

Spoločnosť Constantin Film Verleih (*Constantin*) má v Nemecku výlučné práva na používanie filmov, ktoré boli neoprávnene nahraté na YouTube. Constantin od YouTube žiadala identifikačné údaje o používateľoch, ktorí filmy nahrali. Keďže na prvom stupni získala len fiktívne mená používateľov, žiadala aby YouTube poskytla aj ich e-mailové adresy, telefónne čísla a IP adresy. Krajinský súd v Nemecku žalobu Constantin

zamietol, avšak Vyšší krajinský súd na základe jej odvolania zaviazal YouTube poskytnúť e-mailové adresy používateľov. Vo zvyšnej časti odvolanie zamietol.

Súdny dvor Európskej únie (SDEÚ) na základe prejudiciálnej otázky Spolkového súdneho dvora v Nemecku, na ktorý podali Constantin aj YouTube mimoriadny opravný prostriedok, posudzoval, či sa má čl. 8 ods. 2 písm. a) smernice 2004/48[8] vykladať v tom zmysle, že pojem „adresa" sa vzťahuje, pokiaľ ide o používateľa, ktorý nahral súbory, aj na jeho e-mailovú adresu, telefónne číslo a IP adresu použitú na ich nahratie alebo pri poslednom prístupe na používateľský účet.

Podľa čl. 8 smernice 2004/48 musia členské štáty zabezpečiť, aby súdy mohli nariadiť online platforme, aby poskytla mená a adresy osoby, ktorá nahrala film bez súhlasu nositeľa práv. Napriek tomu, že ide o minimálnu harmonizáciu, a teda čl. 8 smernice 2004/48 sa obmedzuje len na presne vymedzené informácie, podľa SDEÚ to nebráni členským štátom priznať aj širšie právo na informácie, ak zabezpečia rovnováhu medzi právami nositeľov práv a právami používateľov.

Avšak keďže smernica 2004/48 neodkazuje na právo členských štátov na účely vymedzenia svojho zmyslu a významu, pojem „adresa" predstavuje pojem práva Únie, ktorý sa má vykladať jednotne v celej Únii. Podľa SDEÚ sa v bežnom jazyku tento pojem vzťahuje len na poštovú adresu a prípravné práce k smernici nenaznačujú, že by sa mal vzťahovať na e-mailovú adresu, telefónne číslo alebo IP adresu. Kontext, v ktorom sa tento pojem používa podľa SDEÚ potvrdzuje takýto výklad a je v súlade s cieľmi smernice.

Podľa SDEÚ sa teda pojem „adresa" v čl. 8 ods. 2 písm. a) smernice 2004/48/ES nevzťahuje, pokiaľ ide o používateľa, ktorý nahral súbory porušujúce právo duševného vlastníctva, na jeho e-mailovú adresu, telefónne číslo, ani na IP adresu použitú na nahratie týchto súborov alebo pri poslednom prístupe na používateľský účet.

Autor: JVi

[8] Smernica Európskeho parlamentu a Rady 2004/48/ES z 29. apríla 2004 o vymožiteľnosti práv duševného vlastníctva.

2. SOUKROMÍ A OSOBNÍ ÚDAJE

PŘÍPUSTNOST ČASOVĚ NEOMEZENÉHO UCHOVÁVÁNÍ FOTOGRAFIÍ, OTISKŮ PRSTŮ A DNA PROFILŮ ODSOUZENÝCH

Soud: Evropský soud pro lidská práva
Věc: Žádost 45245/15 (Gaughran proti Velké Británii)
Datum: 13. 6. 2020
Dostupnost: hudoc.echr.coe.int

Fergus Gaughran, občan Velké Británie, byl v roce 2008 zatčen za řízení v opilosti, byly mu odebrány otisky prstů, vzorek DNA (ze kterého byl vytvořen DNA profil) a byl vyfocen do policejní databáze. Jelikož se k činu doznal, soud mu uložil pokutu a zákaz řízení motorových vozidel na 12 měsíců. Dva měsíce po doznání činu se stěžovatel dovolával zničení biometrických údajů s tím, že jejich další uchovávání je nezákonné, policie však jeho žádost s odkazem na účinnou legislativu zamítla.[9]

Vrchní soud Severního Irska, před který se případ následně dostal, shledal, že uchovávání biometrických údajů stěžovatele představuje legitimní a proporcionální zásah do práva na soukromí.[10] Toto následně potvrdil i Nejvyšší soud Velké Británie, který zdůraznil, že fotografie stěžovatele je uchovávána pouze v lokální databázi, která neumožňuje mapování fotografií, a další údaje představují pouze malý zásah do soukromí.[11]

Stěžovatel se tedy obrátil na Evropský soud pro lidská práva s žádostí o určení, zda časově neomezené uchovávání biometrických údajů odsouzených představuje zásah do práva na soukromí podle Evropské úmluvy o lidských právech.[12]

Článek 8 Úmluvy přiznává každému právo na respekt k soukromému a rodinnému životu. Toto právo může být omezeno pouze na základě záko-

[9] Body 6 až 9 anotovaného rozhodnutí.

[10] Body 10 a 11 anotovaného rozhodnutí.

[11] Body 12 až 19 anotovaného rozhodnutí.

[12] Bod 58 anotovaného rozhodnutí.

na a pouze v případech, kdy je to v demokratické společnosti nezbytné pro účely (mimo jiné) předcházení trestné činnosti.[13]

Skutečnost, že uchovávání představuje zásah do práva na soukromí, byla nesporná i mezi stranami.[14] Při hodnocení legitimity zásahu Soud konstatoval, že primární problém není v neomezené době uchování dat,[15] ale v absenci mechanismů, které by zohledňovaly pachatelův čin, věk, potřebu pro uchování údajů, dobu uplynulou od spáchání činu, zahlazení odsouzení, pachatelovu osobnost a chování a které by umožňovaly pachateli dosáhnout výmazu údajů.[16] Čím vyšší doba uchování údajů, tím spíše musí být nastaveny tyto mechanismy.[17] Problém Soud dále spatřoval i v tom, že fotografie stěžovatele se sice nacházela v lokální databázi, ale bylo ji možné nahrát do národní policejní databáze, která již umožňovala využívat technologie rozeznávání obličejů, což byl pokrok, který se udál mezi rozhodnutím Nejvyššího soudu a rozhodováním Evropského soudu pro lidská práva.[18]

Soud dospěl k závěru, že nerozlišující a neomezeně dlouhé uchovávání údajů představuje neospravedlnitelný zásah do práva na soukromí podle Úmluvy.[19] Zajímavým bodem rozhodnutí je mimo jiné i upozornění, že pokud stát přistoupí k využívání neomezené doby uchování údajů, nelze ignorovat (i potenciální/budoucí) rozvoj technologií, které mohou zásah prohloubit.[20]

Autor: JVo

---

[13] Článek 8 Evropské úmluvy o lidských právech.

[14] Soud při posuzování navázal na případ *S. a Marper proti Velké Británii*, kde se řešilo uchovávání údajů osob neodsouzených. Viz body 60 a 63 až 70 anotovaného rozhodnutí.

[15] Patrné zvláště na rozhodnutích *Peruzzo a Martens proti Německu* zde dne 4. 6. 2013 a *Aycaquer proti Francii* ze dne 22. 6. 2017, více viz bod 87 anotovaného rozhodnutí.

[16] Resp. policie měla k výmazu přistupovat v natolik výjimečných případech, že tento postup soud označil až za hypotetický, viz bod 94 anotovaného rozhodnutí.

[17] Bod 94 anotovaného rozhodnutí.

[18] Bod 68 anotovaného rozhodnutí.

[19] A to i navzdory tomu, že Soud přiznal státům širší „pole působnosti" při zásazích do práva na soukromí odsouzených. Viz bod 96 anotovaného rozhodnutí.

[20] V tomto případě šlo o zmíněný značný pokrok v oblasti technologií rozeznávání obličejů, který se udál mezi rozhodnutím Nejvyššího soudu a Evropského soudu pro lidská práva. Viz bod 68 anotovaného rozhodnutí.

ZASÍLÁNÍ OBCHODNÍCH SDĚLENÍ

Soud: Nejvyšší správní soud České republiky
Věc: 1 As 136/2019 - 38
Datum: 16. 6. 2020
Dostupnost: nssoud.cz

V roce 2014 společnost www.scio.cz, s. r. o. (dále jen „Scio“), zajišťovala pro Masarykovu univerzitu přijímací zkoušky na Ekonomicko-správní fakultu. Bez souhlasu uchazečů přitom rozeslala na tři tisíce emailových adres, které uchazeči o studium uvedli do přihlášky ke studiu, nabídku absolvovat Národní srovnávací zkoušky (dále jen „NSZ“), jako alternativní způsob pro přijetí.[21]

Tímto podle Úřadu pro ochranu osobních údajů (dále jen „ÚOOÚ“) Scio spáchalo správní delikt šíření obchodního sdělení bez souhlasu adresáta, za což vyměřil pokutu 450 000,- Kč. Ačkoliv Scio podalo proti tomuto rozhodnutí rozklad, předseda ÚOOÚ jej zamítl a rozhodnutí potvrdil. Scio podalo žalobu k Městskému soudu v Praze, který shledal, že výrok rozhodnutí ÚOOÚ obsahuje dostatečně konkrétní vymezení skutkových okolností deliktu a žalobu zamítl,[22] načež podala Scio kasační stížnost k Nejvyššímu správnímu soudu (dále jen „NSS“).

NSS se kromě jiného zabýval zejména výkladem pojmu obchodní sdělení, a tedy zda lze zaslaný informativní email obsahující informace o NSZ považovat za obchodní sdělení.[23]

Definice obchodních sdělení je obsažena v § 2 písm. f) zákona o některých službách informační společnosti, přičemž pravidla pro zasílání obchodních sdělení upravuje § 7 a případnou sankci § 11 odst. 1 písm. a) tamtéž.

NSS považoval za nesporné, že email byl „sdělením“ a že Scio jej poslalo při výkonu své podnikatelské činnosti, a tudíž jedinou spornou otázkou zů-

[21] Bod 1 anotovaného rozhodnutí.

[22] Bod 4 anotovaného rozhodnutí.

[23] Body 25-37 anotovaného rozhodnutí.

stává, zda byl email určen k „*přímé či nepřímé podpoře zboží či služeb stěžovatelky*“.[24] Scio namítalo, že jejím záměrem nebylo podpořit své služby, nýbrž informovat uchazeče o podmínkách pro přijetí ke studiu dle § 49 odst. 5 zákona o vysokých školách.[25] NSS se však s tímto tvrzením neztotožnil a uvedl, že není povinností vysokých škol informovat o NSK a ani není rozhodné, jaké byly vnitřní pohnutky Scia, jelikož pojem obchodního sdělení je pojmem objektivním.[26] Proto pokud je hlavní podnikatelskou činnosti Scia testování a zpracování NSZ, tak sdělení rozeslané elektronicky na adresy uchazečů o studium na vysoké škole, informující uchazeče o možnosti absolvovat Sciem organizovanou NSK, má nepochybně za cíl mj. ekonomický prospěch Scia[27] a je tedy obchodním sdělením.

Rozhodnutí ve svém důsledku posiluje ochranu osob před zasíláním obchodních sdělení, jelikož definici obchodního sdělení vykládá objektivně.

Autor: JK

PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

Soud:	Soudní dvůr Evropské unie
Věc:	C-311/18 (Schrems II)
Datum:	16. 7. 2020
Dostupnost:	curia.europa.eu

Tento rozsudek navazuje na rozhodnutí SDEU ve věci Schrems,[28] ve kterém SDEU zrušil rozhodnutí Evropské komise Safe Harbour.[29] V přeformulované stížnosti se Schrems opět domáhal zákazu předávání jeho osobních údajů společností Facebook Ireland z EU jeho mateřské společnosti Facebook Inc.

[24] Bod 28 anotovaného rozhodnutí.

[25] Bod 32 anotovaného rozhodnutí.

[26] Bod 33 anotovaného rozhodnutí.

[27] Bod 36 anotovaného rozhodnutí.

[28] Rozsudek SDEU ze dne 6. října 2015, Schrems I (C-362/14, EU:C:2015:650).

[29] Rozhodnutí Komise ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“ a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států (Úř. věst. 2000, L 215, s. 7; Zvl. vyd. 16/01, s. 119),

sídlící v USA z důvodu příliš širokých pravomocí amerických zpravodajských služeb.[30]

V reakci na novou stížnost Schremse zveřejnila komisařka[31] v květnu 2016 své předběžné závěry a navrhla Vrchnímu soudu,[32] aby předložil SDEU předběžnou otázku. Vrchní soud návrhu vyhověl a předložil SDEU jedenáct předběžných otázek.[33]

Předmětem předběžných otázek byly různé dílčí aspekty oprávněnosti předávání osobních údajů z EU do USA na základě rozhodnutí komise Privacy Shield[34] a na základě standardních smluvních doložek dle rozhodnutí SSD[35]. Středobodem úvah bylo, zda jsou americké zpravodajské služby oprávněny zpracovávat osobní údaje občanů EU předávané do USA a zda to případně způsobuje nedostatečnou úroveň ochrany osobních údajů v USA.

Předmětem zkoumání se stal zejména americký výkonný dekret 12333,[36] prezidentská politická směrnice 28[37] a § 702 FISA,[38] povolující některé sledovací programy (např. PRISM, UPSTREAM)[39]. Z evropské legislativy je dů-

[30] Bod 55 anotovaného rozhodnutí.

[31] Data Protection Commissioner, neboli komisař pro ochranu údajů, Irsko.

[32] High Court, Irsko.

[33] Bod 68 anotovaného rozhodnutí.

[34] Prováděcí rozhodnutí Komise (EU) 2016/1250 ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46 o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí (Úř. věst. 2016, L 207, s. 1).

[35] Rozhodnutí Komise 2010/87/EU ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46 (Úř. věst. 2010, L 39, s. 5), ve znění prováděcího rozhodnutí Komise (EU) 2016/2297 ze dne 16. prosince 2016 (Úř. věst. 2016, L 344, s. 100).

[36] Executive Order 12333 ze dne 4. 12. 1981.

[37] Presidential Political Directive ze dne 17. ledna 2014.

[38] Foreign Intelligence Surveillance Act (zákon o zabezpečování informací o činnostech cizí moci).

[39] Bod 109 anotovaného rozhodnutí.

ležitý zejména čl. 7, 8 a 47 Listiny,[40] čl. 25, 26 a 28 směrnice,[41] čl. 45 GDPR,[42] rozhodnutí SSD a rozhodnutí Privacy Shield.[43]

V projednávaném rozsudku bylo zpochybněno tvrzení, které Komise uvedla v rozhodnutí Privacy Shield a sice, že zřízení mechanismu ombudsmana může zhojit nedostatky zjištěné ve sledovacích programech, jejichž základem je § 702 FISA, PPD-28 a EO 12333, které nepřiznávají subjektům údajů práva vymahatelná vůči orgánům USA před soudy, takže subjekty údajů postrádají právo na účinný prostředek nápravy.[44] Takový nedostatek v soudní ochraně proti zásahům spojeným se zpracováním osobních údajů zpravodajskými programy, způsobuje že rozhodnutí Privacy Shield je neslučitelné s čl. 45 odst. 1 GDPR ve spojení s články 7, 8 a 47 Listiny, a z toho důvodu je neplatné. Současně však SDEU neodhalil žádnou skutečnost, která by mohla mít dopad na platnost rozhodnutí SSD, a tudíž je možné předávat osobní údaje do třetích států včetně USA na základě standardních smluvních doložek,[45] pokud existují vhodné záruky, vymahatelná práva a účinná právní ochrana, zajišťující subjektům údajů rovnocennou úroveň ochrany jako v EU.

Tento velice významný rozsudek zneplatnil rozhodnutí Privacy Shield, na jehož základě bylo možné předávat osobní údaje z EU certifikovaným společnostem sídlícím v USA, a současně ponechal možnost předávat osobní údaje do USA na základě standardních smluvních doložek.

Autor: JK

---

[40] Listiny základních práv Evropské unie

[41] 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.

[42] 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).

[43] Rozhodnutí Komise (EU) 2016/1250 ze dne 12. července 2016 podle směrnice Evropského parlamentu a Rady 95/46 o odpovídající úrovni ochrany poskytované štítem EU-USA na ochranu soukromí (Úř. věst. 2016, L 207, s. 1).

[44] Bod 192 anotovaného rozhodnutí.

[45] Bod 149 anotovaného rozhodnutí.

SPZ JE OSOBNÍ ÚDAJ

Soud: Nejvyšší správní soud
Věc: 1 As 387/2019 - 56
Datum: 13. 8 2020
Dostupnost: nssoud.cz

Městský soud Hořovice poskytl třetí osobě informace ze správního spisu žalobce k řízení o přestupku. Žalobce se u Krajského soudu v Praze domáhal žalobou určení nezákonného zásahu vzniklého předmětným jednáním, kterým bylo poskytnutí jeho jména a příjmení, registrační značky vozidla, fotografie vozidla, popisu jeho jednání a údaji o jeho zmocněnci třetí osobě. Krajský soud uvedl, že registrační značku vozidla lze k majiteli či provozovateli přiřadit pouze na základě údajů z registru silničních vozidel, který není veřejným seznamem a z pouhé informace o registrační značce není možné žalobce jednoznačně určit.[46] Žalobce podal kasační stížnost s argumentem, že registrační značka je osobním údajem v případě, že vlastníkem a provozovatelem motorového vozidla je fyzická osoba.

Nejvyšší správní soud tedy posuzoval, zda poskytnuté informace (především registrační značka) jsou osobním údajem, které podle § 8a zákona o svobodném přístupu k informacím lze poskytnout jen v souladu s právními předpisy upravujícími jejich ochranu a zda poskytnutím těchto údajů došlo v projednávaném případě k nezákonnému zásahu či nikoli.[47]

Nejvyšší správní soud při posuzování povahy registrační značky vycházel z tzv. objektivního pojetí osobních údajů. Uvedl, že informace je osobním údajem, existují-li jakékoliv osoby nebo orgány, které by daný subjekt údajů dokázaly na základě předmětné informace (ve spojení s jimi dostupnými doplňujícími údaji) identifikovat.[48] S odkazem na judikaturu členských států Evropské unie i svoji vlastní Nejvyšší správní soud uvedl, že pokud je vlastník nebo provozovatel vozidla fyzickou osobou, tak je iden-

[46] Srov. bod 4 anotovaného rozhodnutí.

[47] Srov. bod 23 anotovaného rozhodnutí.

[48] Viz bod 25 anotovaného rozhodnutí.

tifikovatelný pouze na základě registrační značky z důvodu jejího zápisu do registru vozidel a takováto značka je pak osobním údajem.[49] Vlastník vozidla a provozovatel je nepřímo identifikovatelný prostřednictvím vozidla, neboť to je v daný okamžik spjato právě s konkrétním vlastníkem a provozovatelem.[50] Je nezbytné ale vzít v potaz fakt, že registrační značka je osobním údajem pouze v případě, kdy se vztahuje k určité fyzické osobě jako provozovateli nebo vlastníka vozidla.[51]

Přestože byl právní závěr krajského soudu korigován, tak Nejvyšší správní soud konstatoval, že v tomto případě nedošlo k přímému zasažení do práv žalobce, neboť zásah nebyl dostatečně individualizován. Pouhá znalost registrační značky není kvalifikovaným zájmem, který by odůvodnil žádost o další údaje z registru vozidel, pomocí kterých by došlo k ztotožnění stěžovatele.[52] Nejvyšší správní soud tedy dospěl k závěru, že kasační stížnost není důvodná a zamítnul ji.

Autorka: IK

PŘÍPUSTNOST PŘEDÁVÁNÍ PROVOZNÍCH A LOKALIZAČNÍCH ÚDAJŮ ZPRAVODAJSKÝM SLUŽBÁM

Soud: Soudní dvůr Evropské unie
Věc: C-623/17 (Privacy International)
Datum: 6. 10. 2020
Dostupnost: curia.europa.eu

Spor mezi nevládní organizací *Privacy International* a zpravodajskými službami Spojeného království (*GCHQ*,[53] *MI5*[54] a *MI6*[55]), se týkal zákonnosti ná-

[49] Viz bod 30 anotovaného rozhodnutí.

[50] Srov. bod 31 anotovaného rozhodnutí.

[51] Srov. bod 33 anotovaného rozhodnutí.

[52] Srov. bod 39 anotovaného rozhodnutí.

[53] Tzn. *Government Communications Headquarters*.

[54] Tzn. *Security Service*.

[55] Tzn. *Secret Intelligence Service*.

rodní právní úpravy umožňující hromadné získávání dat o komunikaci těmito složkami státu.

Žaloba na nezákonnost těchto postupů byla podána v roce 2015 a národní soud se jí zabýval jak z hlediska anglického práva, tak z hlediska EÚLP[56] a unijního práva.[57] Shledal přitom dané postupy v souladu s národním právem a zajištěné přiměřenými opatřeními (opatření pro přístup k datům jinými subjekty, způsoby získávání dat a zajištění nezávislého dohledu) pro soulad s čl. 8 EÚLP.[58]

Na Soudní dvůr se však obrátil v otázce dopadu unijního práva a použitelnosti závěrů z rozhodnutí C-203/15 a C-698/15, *Tele2 Sverige*,[59] na tyto postupy zpravodajských služeb.[60] Předmětem rozhodnutí tak byl výklad čl. 1 odst. 3 a čl. 15 odst. 1 směrnice 2002/58/ES[61] ve znění směrnice 2009/136/ES s přihlédnutím k čl. 4 odst. 2 SEU[62] a čl. 7, 8 a 52 odst. 1 LZPEU.[63,64]

Ohledně dopadu unijního práva na tuto problematiku Soudní dvůr po podrobné analýze[65] dospěl k závěru, že pro výklad nelze aplikovat předchozí judikaturu vztahující se ke směrnici 95/46/ES[66] a že veškeré zpracování osobních údajů ze strany poskytovatelů služeb elektronických komunikací spadá pod rámec směrnice 2002/58/ES, včetně zpracování v důsledku po-

[56] Evropská úmluva o ochraně lidských práv.

[57] Srov. bod 20 anotovaného rozhodnutí.

[58] Bod 21 anotovaného rozhodnutí.

[59] Rozsudek SDEU ze dne 21.12.2016, Tele2 Sverige, C-203/15 a C-698/15, ECLI:EU:C:2016:970.

[60] Body 22 a 29 anotovaného rozhodnutí.

[61] 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).

[62] Smlouva o Evropské unii.

[63] Listina základních práv Evropské unie.

[64] Bod 1 anotovaného rozhodnutí.

[65] Body 37-39 a 42 anotovaného rozhodnutí.

[66] 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 (již není platná).

vinností uložených orgány veřejné moci.[67] I na národní právní předpis umožňující požadovat od těchto poskytovatelů sdílení provozních a lokalizačních údajů se zpravodajskými službami za účelem zajištění národní bezpečnosti tak v tomto směru dopadá unijní právo.[68] V návaznosti na tento závěr se Soudní dvůr zabýval druhou předběžnou otázkou, která se týkala použitelnosti závěrů výše zmíněného rozhodnutí, které předně brání národnímu zákonodárci ukládat poskytovatelům služeb elektronických komunikací obecné a neselektivní předávání provozních a lokalizačních údajů zpravodajským službám.[69] Po podrobné analýze aplikovatelnosti svých dřívějších úvah Soudní dvůr dospěl k závěru o nepřípustnosti výjimky v tomto směru narušující princip zajištění důvěrnosti elektronické komunikace a tedy potvrzení aplikovatelnosti závěrů své výše zmíněné judikatury.

Rozhodnutí je zvláště zajímavé ve dvou směrech. Zaprvé utvrzuje striktní pozici Soudního dvora proti plošným nástrojům sledování elektronické komunikace (data retention) bez ohledu na příjemce (zpravodajské služby) a účel (národní bezpečnost). Zadruhé vytváří směrodatné pravidlo pro ostatní členské státy, byť pro strany daného sporu má vzhledem k vývoji Brexitu závěr Soudního dvora značně nejistou váhu.

Autor: FK

POŘÍZENÍ SKRYTÉHO ZÁZNAMU NA PRACOVIŠTI NEMUSÍ PORUŠIT PRÁVO NA SOUKROMÍ

Soud:	Evropský soud pro lidská práva
Datum:	17. 10. 2019
Věc:	Spojené žádosti 1874/13 a 8567/13 (López Ribalda a další proti Španělsku)
Dostupnost:	hudoc.echr.coe.int

[67] Bod 46 anotovaného rozhodnutí.

[68] Bod 49 anotovaného rozhodnutí.

[69] Bod 50 anotovaného rozhodnutí.

Stěžovatelé, López Ribalda a ostatní, byli ve Španělsku propuštěni ze supermarketu.[70] Kvůli krádežím nainstaloval zaměstnavatel bezpečnostní kamery, veřejné, které byly označeny, a skryté, zabírající i prostory za pokladnou[71] Na základě videozáznamu došlo k propouštění 14 zaměstnanců, včetně stěžovatelů, někteří podepsali dohodu o vyrovnání.[72]

Stěžovatelé zahájili řízení pro neoprávněné propuštění u pracovního tribunálu.[73] U stěžovatelů 1 a 2 zkoumal tribunál přípustnost důkazu pomocí videozáznamu, neshledal porušení práva na soukromí podle čl. 24 španělské ústavy,[74] protože zásah byl proporční k ochraně zaměstnavatelových zájmů.[75] U stěžovatelů 3, 4 a 5 soud posoudil pouze legalitu dohody o vyrovnání.[76] Stěžovatelé podali odvolání ke španělskému Nejvyššímu soudu pro absenci předchozího oznámení o sledování. Soud uvedl, že zaměstnavatel postupoval podle španělského zákoníku práce a ten takové oznámení nevyžaduje.[77] Stěžovatelé se dále obrátili opět na Nejvyšší soud a následně i na španělský Ústavní soud, u obou bylo podání odmítnuto.[78]

Stěžovatelé rozporovali soulad s právem na soukromí podle čl. 8 Úmluvy o ochraně lidských práv. ESLP zkoumal legislativu a judikaturu ve Španělsku. Španělský ústavní soud stanovil ve věci sledování na pracovišti třístupňový test.[79,80] Později rozhodl, že permanentnímu sledování už musí předcházet notifikace[81] a informace o přibližném rámci záběru kamery.[82]

ESLP rozhodoval, zda došlo k porušení práva na spravedlivý proces (čl. 6 Úmluvy) a práva na soukromí (čl. 8 Úmluvy). ESLP neshledal poru-

[70] Bod 3 a 10 anotovaného rozhodnutí.

[71] Bod 11 a 12 anotovaného rozhodnutí.

[72] Bod 17 anotovaného rozhodnutí.

[73] Tzn. *Granollers Employment Tribunal no. 1*.

[74] Bod 25 anotovaného rozhodnutí.

[75] Body 25 až 28 anotovaného rozhodnutí.

[76] Body 29 až 30 anotovaného rozhodnutí.

[77] Bod 33 anotovaného rozhodnutí.

[78] Bod 39 anotovaného rozhodnutí.

[79] Tzn. *Oprávněný zájem, nezbytnost a proporcionalita.*

[80] Bod 54 anotovaného rozhodnutí.

[81] Bod 57 anotovaného rozhodnutí.

[82] Bod 59 anotovaného rozhodnutí.

šení v řízení jako celku.[83] Při posuzování otázky soukromí podle ustálených kritérií[84] shledal, že v předmětné době mělo španělské právo podrobná pravidla pro ochranu soukromí a ta nebyla porušena.[85] Během řízení před španělskými soudy byl důsledně vyhodnocen konflikt zájmů.[86] Nedostatečná informovanost stěžovatelů o sledování je relevantním faktorem, avšak záznam byl použit jenom k jednomu účelu – odhalení krádeží – a toho nešlo dosáhnout jinak.[87] Užití videozáznamu bylo v souladu s principem proporcionality.[88]

ESLP tak zamítl žádost stěžovatelů a neshledal porušení lidských práv ze strany Španělska.[89] Rozhodnutí je zajímavé z hlediska nastavení limitů práva na ochranu soukromí.

Autorka: VŽ

3. PRÁVO NA INFORMACE

APLIKAČNÍ RÁMEC PSI SMĚRNICE

Soud: Soudní dvůr Evropské unie
Věc: C-215/17 (NKBM)
Datum: 14. 11. 2018
Dostupnost: curia.europa.eu

Slovinská novinářka požádala tamní banku NKBM o informace o smlouvách, které tato banka uzavřela mezi roky 2012 a 2014 s poradenskými společnostmi a advokátními kancelářemi. V této době, stejně jako v době žádosti, byla NKBM pod dominantním vlivem subjektu veřejného práva, protože Slovinská republika vlastnila většinu jejího kapitálu.[90] NKBM od-

[83] Body 153 až 161 anotovaného rozhodnutí.
[84] Bod 116 anotovaného rozhodnutí.
[85] Bod 119 anotovaného rozhodnutí.
[86] Body 121 až 124 anotovaného rozhodnutí.
[87] Body 128 až 131 anotovaného rozhodnutí.
[88] Body 132 až 134 anotovaného rozhodnutí.
[89] Bod 137 a 161 anotovaného rozhodnutí.
[90] Bod 18 anotovaného rozhodnutí.

mítla informace poskytnout z důvodu ochrany obchodního tajemství a postupně se bránila soudně, až na úroveň slovinského Nejvyššího soudu, který předložil předběžnou otázku SDEU.

Slovinský zákon zakládal povinnost poskytnout informace, které byly věcně byly předmětem původního sporu, i v případech, kdy veřejný zájem na jejich poskytnutí nepřevažuje nad zájmem povinných subjektů na jejich nezveřejnění.[91] NKBM argumentovala tím, že v důsledku aplikace evropského práva, zejména čl. 1 odst. 2 písm. c) třetí odrážka směrnice 2003/98/ES (ve znění směrnice 2013/37/EU; dále PSI směrnice) a čl. 432 odst. 2 nařízení EU č. 575/2013, není možné informace poskytnout. Prvně jmenované ustanovení totiž zakládá výjimku z aplikace směrnice, když uvádí, že *„směrnice se nepoužije na dokumenty, které nejsou přístupné podle režimů přístupu v členských státech, včetně z důvodů obchodní důvěrnosti (např. obchodního, profesního nebo firemního tajemství)“*. Druhé ustanovení zakládá obdobnou výjimku z poskytování informací v kontextu nařízení č. 575/2013. Předkládací soud proto se proto ve své předběžné otázce ptal, zda uvedená evropská úprava brání členskému státu v zavedení širší informační povinnosti, jako tomu bylo v hodnoceném případě.

SDEU zkraje své argumentace konstatoval, že PSI směrnice stanoví minimální soubor pravidel pro opakované užití informací veřejného sektoru.[92] SDEU pak po aplikaci čl. 2 bod. 2 písm. a) až c) PSI směrnice dospěl k závěru, že NKBM není veřejnoprávním subjektem, a proto se na ni aplikace směrnice nevztahuje.[93] Obdobně pak v případě aplikace nařízení č. 575/2013 dospěl SDEU k závěru, že předmětná právní úprava reguluje povinnost jednou ročně poskytovat určité informace, tedy jinou situaci, než která byla předmětem sporu, kde šlo o žádost.[94] V důsledku toho evropská právní úprava nikterak neovlivňuje hodnocenou úpravu národní.

Z hlediska problematiky PSI jde o připomenutí, že PSI směrnice nezakotvuje právo na přístup k informacím veřejného sektoru, ale *„počítá s existen-*

[91] Bod 21 anotovaného rozhodnutí.

[92] Bod 26 anotovaného rozhodnutí.

[93] Body 27 a 28 anotovaného rozhodnutí.

[94] Body 38 a 39 anotovaného rozhodnutí.

cí takového práva v platných právních předpisech členských států, takže pravidla a postupy týkající se přístupu k těmto informacím nespadají do její působnosti.“[95]

Autor: JM

NEOPRÁVNENÉ BLOKOVANIE WEBOVEJ STRÁNKY PROSTREDNÍCTVOM IP ADRESY

Soud: Európsky súd pre ľudské práva
Věc: Žiadosť 10795/14 (Vladimir Kharitonov proti Rusku)
Datum: 23. 6. 2020
Dostupnost: hudoc.echr.int

Pán Kharitonov prevádzkuje webovú stránku (*digital-books.ru*), na ktorej uverejňuje správy o distribúcií elektronických kníh. Na prevádzku využíva služby zdieľaného úložiska DreamHost. Iná webová stránka (*rastaman.tales.ru*), obsahuje ľudové príbehy o kanabise a je uložená na rovnakom úložisku. Osobitosťou úložiska je, že uložené stránky síce používajú unikátne doménové mená, avšak zdieľajú rovnakú IP adresu. Ruské úrady vyhodnotili, že obsah stránky o kanabise porušuje zákon a operátor Roskomnadzor zablokoval jej IP adresu. V dôsledku blokovania prostredníctvom IP adresy však došlo aj k zablokovaniu stránky pána Kharitonova. Moskovský súd jeho sťažnosť zamietol, pričom len uviedol, že operátor Roskomnadzor pri výkone príkazu konal v rámci svojich kompetencií a v súlade so zákonom.[96] Dopady príkazu na webovú stránku pána Kharitonova neposudzoval.

Po vyčerpaní opravných prostriedkov sa pán Kharitonov obrátil na Európsky súd pre ľudské práva (ESĽP) aby určil, že blokovanie IP adresy malo na neho neprimeraný vedľajší účinok[97] a viedlo porušeniu jeho práva

[95] Bod 32 anotovaného rozhodnutí.

[96] Bod 8 anotovaného rozhodnutia. Blokovanie malo údajne byť odôvodnené zamedzením prístupu k informáciám o výrobe a užívaní drog.

[97] Z angl. „*disproportionate collateral effect*“.

na slobodu prejavu (čl. 10 Dohovoru)[98] a práva na účinný ochranný prostriedok (čl. 13 Dohovoru).

Vnútroštátny predpis nevyžadoval, aby operátor Roskomnadzor pred vykonaním príkazu skúmal, či IP adresu využíva viacero webových stránok[99] ani či účinky blokovania sú proporcionálne, teda či je blokovaný len nelegálny obsah. Zákon neumožňoval sťažovateľovi oboznámiť sa s obsahom príkazu a súdy sa obmedzili len na posúdenie kompetencie operátora príkaz vykonať. ESĽP s odkazom na čl. 10 ods. 2 Dohovoru uviedol, že zásah predstavuje porušenie Dohovoru nie je „stanovený zákonom" a nesleduje niektorý z legitímnych cieľov, ktorých dosiahnutie je „nevyhnutné v demokratickej spoločnosti".

Podľa ESĽP sťažovateľ nemal žiaden vzťah k blokovanej stránke ani nezodpovedal za jej obsahu a preto blokovanie nemohlo byť založené na ustanovení zákona, ktoré malo byť jeho právnym základom.[100] Sťažovateľ podľa ESĽP znášal nežiadúce následky blokovania výlučne z dôvodu totožnosti IP adresy s webovou stránkou obsahujúcou nelegálny obsah.[101] Keďže zákon neposkytoval sťažovateľovi dostatočné právne záruky ochrany pred excesívnymi a arbitrárnymi účinkami príkazu, podľa ESĽP nespĺňal Dohovorom predpokladanú podmienku predvídateľnosti účinkov, teda neumožnil sťažovateľovi regulovať svoje správanie a zásah vo forme blokovania preto nebol „stanovený zákonom"[102] ako to vyžaduje čl. 10 Dohovoru.[103]

Na tomto základe následne ESĽP konštatoval porušenie čl. 10 aj 13 Dohovoru.[104]

Autor: JVi

---

[98] Európsky dohovor o ochrane ľudských práv a základných slobôd. Uvedené právo podľa Dohovoru zahŕňa aj právo „zastavať názory a prijímať a rozširovať informácie alebo myšlienky bez zasahovania štátnych orgánov".

[99] Napríklad prostredníctvom bežne dostupných nástrojov akým je tzv. reverzné prehľadanie IP adresy („*reverse IP lookup*"), ktoré umožňuje zistiť zoznam webových stránok uložených na rovnakom serveri.

[100] Bod 39 anotovaného rozhodnutia.

[101] Bod 42 anotovaného rozhodnutia.

[102] Z angl. „*prescribed by law*".

[103] Bod 46 anotovaného rozhodnutia.

4. OSTATNÍ

PROSTOROVÉ ODPOSLECHY JE MOŽNO VYUŽÍT I V JINÝCH PŘÍPADECH, NEŽ PRO KTERÉ BYLY NAŘÍZENY

Soud: Nejvyšší soud
Věc: 7 Tdo 865/2020
Datum: 1. 9. 2020
Dostupnost: nsoud.cz

České soudy se postupně zabývaly případem, kdy se dva příslušníci Policie České republiky při objasňování a prověřování trestné činnosti podezřelého ve vzájemné součinnosti od tohoto podezřelého snažili vymámit doznání ke spáchání dalšího trestného činu a opatřit tak důkazní materiál k zahájení trestního stíhání i pro trestnou činnost, za kterou nebyl podezřelý usvědčován jinými důkazy.[105] V rámci výslechu byly využity prostorové odposlechy (na základě § 158d trestního řádu – sledování osob a věcí). Ty ale nebyly schváleny soudem pro prokázání spáchání trestné činnosti policistů.

Daným případem se postupně zabývaly nižší soudy. Řešily, jestli došlo k naplnění skutkové podstaty zneužití pravomoci úřední osoby, zneužití bezbrannosti a tísně podezřelého atd. ze strany zmíněných policistů. Zabývaly se ale rovněž důkazní použitelností prostorových odposlechů, které v dané věci tvořily významnou část provedeného dokazování.[106] Na ty se dále primárně zaměříme.

[104] Porušenie čl. 10 aj 13 Dohovoru bolo jednohlasne konštatované, avšak rozhodnutie obsahuje spoločné odlišné stanovisko troch sudcov komory. Aj títo sudcovia zastávajú názor, že zásah nebol „stanovený zákonom“, avšak nie z dôvodu, že zákonná úprava nespĺňala kritérium predvídateľnosti, ale z dôvodu, že zásah nemal vo vnútroštátnom predpise právny základ („*But unlike our colleagues, we believe that this is so because the interference had no basis in domestic law, not because the law did not satisfy the foreseeability requirement.*“). Táto časť sudcov si teda nemyslí, že vnútroštátny predpis je nekompatibilný s Dohovorom a bude potrebná jeho zmena, ale tvrdí že na nápravu by postačovala zmena administratívnej praxe (na úrovni operátora Roskomnadzor) a súdnej praxe (na úrovni domácich súdov), teda bez legislatívnej intervencie.

[105] Bod 2 anotovaného rozhodnutí.

[106] Bod 28 anotovaného rozhodnutí.

Právě procesní použitelnost záznamů o sledování osob a věcí se stala klíčovou otázkou pro Nejvyšší soud, který řešil, jestli nařízené odposlechy lze použít i v jiné trestní věci, než je ta, v níž bylo sledování provedeno. Nejvyšší soud tak zkoumal zejména vzájemné postavení jednotlivých odstavců § 158d trestního řádu, kdy se část odborné veřejnosti kloní k tomu, že daným způsobem pořízený důkaz nelze použít v jiné trestní věci. Soud nicméně zdůraznil, že takový výklad „*by představoval nelogický anachronismus, pokud by jakékoli záznamy ze sledování povoleného soudcem v jiné věci byly důkazně vyloučeny, i když by poskytovaly zásadní důkazní materiál o těch nejzávažnějších zločinech.*“[107] Dále soud uvedl, že by protichůdný výklad byl v logickém rozporu s § 88 odst. 6 trestního řádu, který explicitně (ale za stanovení konkrétních podmínek) s užitím odposlechu v jiné trestní věci počítá.

Nejvyšší soud tak rozhodl (a zrušil předchozí rozhodnutí nižších soudů), že záznamy o sledování osob a věcí dle § 158d lze použít jako důkaz i v jiné trestní věci, než je ta, v níž bylo sledování povoleno, *„je-li i v této věci vedeno řízení o úmyslném trestném činu nebo souhlasí-li s tím osoba, do jejíž práv a svobod bylo sledováním zasahováno.*“[108] Přípustnost takového důkazu je nutno posuzovat zejména v souvislosti s respektem na ochranu soukromí dané osoby, vzhledem k dané situaci (tedy že se jednalo o policisty ve výkonu služby) však nebyla využitelnost důkazu v rozporu s ochranou soukromí.

Soud tak v dané věci vymezil, jakým způsobem lze využít důkazů získaných na základě prostorových odposlechů i v jiné trestní věci. Upozorňujeme však, že neinterpretoval použitelnost odposlechů telekomunikačního provozu (dle § 88 trestního řádu), což bylo mnohdy mylně pochopeno médii.

Autor: PL

[107] Bod 60 anotovaného rozhodnutí.

[108] Bod 54 anotovaného rozhodnutí.

K POSOUZENÍ NARUŠENÍ INTERNETOVÉ NEUTRALITY POSKYTOVATELEM SLUŽEB INTERNETU

Soud: Soudní dvůr Evropské unie
Datum: 15. 9. 2020
Věc: Spojené věci C-807/18 a C-39/19 (Telenor Magyarország)
Dostupnost: curia.europa.eu

Maďarský soud[109] podal předběžnou otázku týkající se tzv. nulového tarifu,[110] kdy je v rámci objemu dat zvýhodňována určitá aplikace nebo služba. Vzešla z řízení Telenor[111] proti maďarskému úřadu pro komunikace a média (NÚKM).[112] Telenor poskytuje služby přístupu k internetu a dva balíčky služeb nazvané MyChat a MyMusic,[113] u kterých NÚKM konstatoval, že porušují neutralitu internetu.[114] SDEU posuzoval soulad opatření NÚKM s nařízením 2015/2020 o přístupu k otevřenému internetu.[115,116]

NÚKM rozhodl, že služby Telenoru odporují čl. 3 odst. 3 nařízení 2015/2020.[117] Telenor rozhodnutí napadl s odvoláním na to, že ke zvýhodnění nedochází jednostranně, ale na základě dohody s koncovými uživateli.[118]

[109] Tzn. Fővárosi Törvényszék – soud hlavního města Budapešti, Maďarsko.

[110] Tzv. *zero rating*

[111] Tzn. *Telenor Magyarország Zrt*.

[112] Tzn. *Nemzeti Média- és Hírközlési Hatóság Elnöke*.

[113] Bod 9 anotovaného rozhodnutí.

[114] Bod 12 anotovaného rozhodnutí.

[115] Nařízení Evropského parlamentu a Rady (EU) 2015/2120 ze dne 25. listopadu 2015, kterým se stanoví opatření týkající se přístupu k otevřenému internetu a mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací a nařízení (EU) 531/2012 o roamingu ve veřejných mobilních komunikačních

[116] Bod 1 a 2 anotovaného rozhodnutí.

[117] Bod 13 anotovaného rozhodnutí.

[118] Bod 15 anotovaného rozhodnutí.

Předkládající soud se ptal, zda musí být na dohodu nahlíženo z hlediska čl. 3 odst. 2 nebo odst. 3 nařízení 2015/2020 a zda má vliv dopad na trh.[119] Soud postrádal v nařízení metodiku.[120]

Nařízení 2015/2020 stanovuje princip internetové neutrality,[121] pro řízení jsou relevantní pravidla v čl. 3, že uživatelé mají přístup k obsahu bez ohledu na jejich polohu, poskytovatele či původ apod. (odst. 1) a tato práva nelze omezit obchodní praktikou či dohodou (odst. 2).[122] Odst. 3 stanovuje zákaz diskriminace při poskytování služeb a přípustné výjimky pro opatření řízení provozu.[123]

Slučitelnost dohody podle čl. 3 odst. 2 s odst. 1 je potřeba vždy posoudit individuálně podle dopadu.[124] Kumulace uzavřených dohod o zvýhodnění v rámci objemu dat ovlivňuje využívání konkrétních aplikací a služeb na trhu.[125] Pokud se tak děje na podstatné části trhu, dohody mohou omezit právo dle odst. 1.[126] Oproti tomu pro aplikaci odst. 3 není dle SDEU třeba posoudit dopad na trh[127] a v případě tarifních balíčků Telenoru je diskriminace dána obchodním cílem opatření a není uplatnitelná žádná z výjimek.[128]

Rozsudek stanovil neslučitelnost této obchodní praktiky s čl. 3 odst. 2 i odst. 3 nařízení 2015/2020. Rozsudek poskytuje cenná vodítka pro posouzení srovnatelných situací v budoucnu.

Autorka: VŽ

[119] Bod 20 anotovaného rozhodnutí.

[120] Bod 19 anotovaného rozhodnutí.

[121] Bod 3 anotovaného rozhodnutí.

[122] Bod 6 anotovaného rozhodnutí.

[123] Tamtéž.

[124] Bod 43 anotovaného rozhodnutí.

[125] Bod 44 anotovaného rozhodnutí.

[126] Bod 45 a 46 anotovaného rozhodnutí.

[127] Body 49 až 51 anotovaného rozhodnutí.

[128] Body 52 a 53 anotovaného rozhodnutí.

POKORNÁ, ANDREA; DVOŘÁKOVÁ HELENA. OCHRANA OSOBNÍCH ÚDAJŮ V KONTEXTU JUDIKATURY SOUDNÍHO DVORA EU, VÝKLADOVÝCH POKYNŮ A STANOVISEK

JAKUB KLODWIG[1]

POKORNÁ, Andrea; DVOŘÁKOVÁ, Helena. Ochrana osobních údajů v kontextu judikatury Soudního dvora EU, výkladových pokynů a stanovisek. Praha: Wolters Kluwer ČR, 2020, 352 s. ISBN 978-80-7598-309-1.

Na přebalu a v úvodu[2] autorky avizují, že je kniha určena zejména pro soudce, justiční čekatele a asistenty soudců a jejím účelem je *„poskytnout rukověť pro výklad čerpající z dostupných odborných zdrojů a zejména judikatury Soudního dvora Evropské unie a Evropského soudu pro lidská práva“*. Po detailním prostudování knihy, lze konstatovat, že tento cíl se autorkám naplnit podařilo, jelikož kniha skutečně podává celkový přehled problematiky ochrany osobních údajů. Stručný výklad předmětných článků autorky obohacují o rozhodovací praxi výše zmíněných soudů, stanovisek WP 29,[3] a také souvisejících ustanovení Hlavy II. Zákona o zpracování osobních

[1] Mgr. Jakub Klodwig, doktorand na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity, e-mail: 434044@mail.muni.cz.

[2] Viz str. XVIII knihy.

[3] Pracovní skupina zřízená podle čl. 29 směrnice 95/46/EC byl nezávislý subjekt, zřízený za účelem výkladu předmětné směrnice a koordinace spolupráce mezi jednotlivými členskými dozorovými úřady pro ochranu osobních údajů. Od účinnosti Obecného nařízení byla tato skupina nahrazena Evropským sborem pro ochranu osobních údajů (EDPB).

údajů[4], což čtenářům umožňuje propojit jednotlivé poznatky a porozumět tak problematice v souvislostech. Obsah knihy chronologicky následuje posloupnost Obecného nařízení[5], ačkoliv její struktura přímo nekopíruje systematiku Obecného nařízení, ale člení se samostatně na sedm částí, desítky kapitol a řadu dalších dílčích celků.

Kniha začíná krátkým úvodním slovem, ve kterém autorky shrnují svoji motivaci k jejímu napsání a děkují svým podporovatelům. První dojem ovšem částečně kazí nesprávné použití pojmů „*data*“ a „*informace*“,[6] hned na druhé straně úvodního textu.[7] Samotný výklad je psán čtivě, kdy jsou kapitoly zahajovány obecným výkladem dané problematiky, a následně je čtenáři vysvětlen význam pojednávané regulace v daných paragrafech či jednotlivých odstavcích. Kniha je tedy vhodná spíše pro začátečníky a právníky, kteří mají pouze základní znalost práva ochrany osobních údajů, nebo kteří potřebují konkrétní ustanovení vysvětlit. Avšak pro svoji spíše obecnou povahu a občasnou absenci detailů či hlubších souvislostí bude kniha méně užitečná pro čtenáře, kteří se na právo ochrany osobních údajů specializují. Tyto drobné výkladové neúplnosti, lze demonstrovat například na výkladu přímého marketingu na str. 87, kde je pouze stručně deklarováno, že mezi zpracování nezbytné pro provedení opatření přijatých před uzavřením smlouvy nepatří přímý marketing, aniž by bylo odkázáno na zásadní úpravu této problematiky v § 89 odst. 3 Zákona o elektronických komunikacích[8], nebo na str. 56, kde text opisuje charakter performativní normy, aniž by byl pojem „*performativní norma*“ jedinkrát v textu použit. Autorky tak pravděpodobně upřednostnily dynamický a stručný výklad, před jeho komplexností. V těchto případech by však bylo doporučitelné použít doplňující výklad formou poznámky pod čarou, nebo alespoň

[4] Zákon č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů.

[5] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

[6] Srov. POLČÁK, Radim. Informace a data v právu. *Revue pro právo a technologie*. [Online]. 2016, č. 13, s. 77 a násl. Dostupné z: https://journals.muni.cz/revue/article/view/4946

[7] Viz str. XVIII knihy.

[8] Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

odkázat na část knihy, která danou problematiku více rozvíjí. Proto je škoda, pokud je na například str. 90, zabývající se výjimkami uvedeno, že: *„Nařízení v případě těchto dvou právních titulů umožňuje členským státům, aby v právním základu stanovily konkrétní ustanovení pro přizpůsobení uplatňování pravidel tohoto nařízení“,* ale již absentuje odkaz nebo alespoň zmínka o § 5 Zákona o zpracování osobních údajů, který takové přizpůsobení (výjimku pro český právní řád) obsahuje.

Je ovšem nutné vyzdvihnout práci autorek s judikaturou, jejíž souhrn se objevuje zpravidla v závěru kapitol, nebo také jako samostatná kapitola v případě, že je judikatura k určitému tématu rozsáhlá. V takovém případě je kapitola dále podrobněji rozčleněna v závislosti na zpracované problematice.[9] Jednotlivé rozsudky jsou vždy věcně popsány, následně je shrnuta i jejich právní kvalifikace a závěry soudu. Autorky tímto způsobem přehledně zpracovávají nejdůležitější rozsudky, které ovlivnily výklad právní úpravy, a jejichž dohledávání a interpretace by byla pro čtenáře nesnadná a časově náročná. Ocenit lze, že pokud jsou některá rozhodnutí významná pro více právních otázek, a tedy se rozhodnutí objevují opakovaně, pak jsou vždy akcentovány jiné pasáže a pouze skutečnosti, které jsou relevantní v dané záležitosti. Nejinak je tomu v první části knihy, zabývající se základním vymezením zpracování osobních údajů. Zde je judikatura Soudního dvora EU zpracována do samostatné kapitoly, v níž jsou rozebrány rozsudky zabývající se pojmem zpracování osobních údajů, věcné nebo také místní příslušnosti, což jsou témata, o nichž pojednávaly první dvě kapitoly.

Druhá část knihy pojednává o zásadách zpracování osobních údajů, kdy je každé zásadě věnována jedna nedlouhá kapitola. Vzhledem k rozebírané matérii se pochopitelně jedná spíše o obecnější část výkladu, který by místy bylo vhodné obohatit o konkrétní příklady, které by čtenáři lépe demonstrovaly užití zásad v praxi. Třetí část knihy, nazvaná *„Právní tituly zpracování jako projev zásady zákonnosti“* je naopak zpracovaná poměrně podrobně, a to zejména kapitoly dvě a pět, zabývající se souhlasem a plněním právní povinnosti nebo úkolu prováděného ve veřejném zájmu nebo při vý-

[9] Viz např. část první, kapitola III., nebo část čtvrtá, kapitola X. knihy.

konu veřejné moci. V tomto kontextu je tak pouze škoda, že se autorky spokojily pouze se stanovisky WP 29 a ve větší míře nezohlednily odbornou literaturu.[10] Větší rozsah kapitol však odhalil dílčí nekonzistentnost, když například na str. 122 je pouze konstatováno, že existuje dvojí výklad čl. 6 odst. 1 písm. f)[11], aniž by autorky vyjádřily vlastní argumentaci nebo alespoň názor, ke kterému výkladu se přiklánějí, zatímco na str. 150 se autorky danou problematikou znovu zabývají a tentokrát své stanovisko vyjadřují. Pokud se tedy autorky zabývají jedním problémem na více místech, bylo by vhodné jasně uvádět v obou případech stejné stanovisko, nebo alespoň odkazovat na pasáž, kde je problematika rozebírána podrobněji.

Čtvrtá část, zabývající se právy subjektů údajů, je hned po předchozí části druhou nejrozsáhlejší. Zejména v této části lze pozitivně hodnotit, že autorky nezapomínají současnou právní úpravu porovnávat s předcházející právní úpravou obsaženou ve Směrnici o ochraně osobních údajů[12] a Zákoně o ochraně osobních údajů[13]. Zajímavé a bezesporu přínosné je také mezinárodní srovnání právní úpravy, jaké lze nalézt na str. 137, kde je komparována právní úprava zpracování osobních údajů orgány veřejné správy v irském, britském a německém právním řádu. Na část zabývající se právy subjektů údajů navazuje, shodně jako je tomu v Obecném nařízení, část zabývající se povinnostmi správce a zpracovatele. Ta kromě obecných povinností[14], které jsou shrnuty v první kapitole rozebírá samostatně povinnost posouzení vlivu na ochranu osobních údajů a předchozí konzultace, povinnosti související se zabezpečením zpracování, problematiku kodexů

[10] Např. POLČÁK, Radim, Matěj MYŠKA, Petr HOSTAŠ, František KASL, Tereza KYSELOVSKÁ, Tomáš LECHNER, Pavel LOUTOCKÝ, Jakub MÍŠEK, Jan TOMÍŠEK, Václav STUPKA a Miroslav UŘIČAŘ. *Právo informačních technologií*. Praha: Wolters Kluwer, 2018. 656 s. Právní monografie. ISBN 978-80-7598-045-8; BORGERIUS, Frederik Zuiderveen. *Consent to Behavioural Targeting in European Law - What are the Policy Implications of Insights from Behavioural Economics?* 27. července 2013. NY: Social Science research Network; MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie*. 2014, roč. 5, č. 9, s. 3–74. ISSN 1805-2797.

[11] Výkladová nejasnost se týká možnosti užití oprávněného zájmu orgány veřejné moci.

[12] 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.

[13] Zákon č. 101/2000 Sb., Zákon o ochraně osobních údajů a o změně některých zákonů.

[14] V souladu s členěním Obecného nařízení se jedná o povinnosti stanovené v čl. 24 až 31.

chování a osvědčení, a také roli pověřence pro ochranu osobních údajů. Právě posledně zmíněná kapitola se však jeví jako příliš stručná, když se autorky pouze povrchně na pěti stranách rozepisují o právech a povinnostech pověřence pro ochranu osobních údajů, aniž by věnovaly pozornost například rozdílům v postavení interních a externích pověřenců pro ochranu osobních údajů nebo problematice ukončení pracovního poměru interního pověřence.

V šesté části knihy se autorky zabývají zvláštními režimy, poskytujícími vyšší úroveň ochrany, mezi které patří zvláštní podmínky pro udělení souhlasu dítěte a zpracování zvláštních kategorií osobních údajů podle čl. 9 Obecného nařízení. Zde jsou rozebrány zejména specifika těchto režimů zpracování osobních údajů, výjimky vyplývající ze samotného Obecného nařízení, a také výjimky, které do českého právního řádu přidal Zákon o zpracování osobních údajů. Knihu pak uzavírá část sedmá, která pojednává o specifických režimech ochrany osobních údajů, které jsou vyjmenovány v kapitole IX. Obecného nařízení, mezi které patří například zpracování osobních údajů formou zveřejnění v úředních dokumentech, zpracování osobních údajů v souvislosti se zaměstnáním, zpracování identifikačních čísel nebo zpracování osobních údajů církvemi a náboženskými sdruženími. Zvláštní prostor zde dostává také zpracování osobních údajů pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu nebo pro statistické účely dle čl. 89 Obecného nařízení.

Kniha tedy kromě problematiky předávání osobních údajů do třetích zemí nebo mezinárodním organizacím, institucionálního nastavení a sankciování pokrývá téměř celý rozsah Obecného nařízení, a podává tak přehledný a ucelený výklad velké části právní úpravy ochrany osobních údajů v českém právním řádu. K přednostem této publikace patří bezesporu přehledná struktura, která z velké části kopíruje systematiku Obecného nařízení, srozumitelná forma výkladu a také kvalitně zpracovaná judikatura, která výklad vhodně doplňuje. Vytknout je však třeba absenci některých odkazů na související právní úpravu a přílišnou strohost výkladu, který se tak hodí spíše pro méně zkušené čtenáře. Obecně se však jedná o poměrně

kvalitní publikaci, která poskytuje dobrý vhled do práva ochrany osobních údajů v českém právním prostředí.

---

https://doi.org/10.5817/RPT2020-2-8

SROVNÁVACÍ STUDIE PRÁVNÍCH INFORMAČNÍCH SYSTÉMŮ: ROZDÍLY MEZI SYSTÉMY PŘI VYUŽITÍ RŮZNÝCH VYHLEDÁVACÍCH STRATEGIÍ[1]

JAKUB HARAŠTA[2]

ABSTRAKT

Vyhledávání právních informací v právních informačních systémech je běžnou součástí života právníka. V zásadě je možné ve dvou modech: jako vyhledávání zprostředkované a nezprostředkované. V rámci zprostředkovaného vyhledávání se spoléháme na souvislosti připravené tvůrcem systému. Jedná se například o přiřazení dokumentu do oblasti úpravy nebo, na specifičtější úrovni, o označení soudních rozhodnutí jako souvisejících s určitým předpisem nebo ustanovením. Při nezprostředkovaném vyhledávání se uživatel naopak spoléhá sám na sebe. Sám formuluje plnotextové dotazy a vyhledává výrazy, které pro něj symbolizují rešeršovaný problém.

V tomto textu se zaměřuji na porovnání výsledků poskytnutých právními informačními systémy ASPI, Beck-online a Codexis v odpovědi na srovnatelné dotazy využívající zprostředkovaných i nezprostředkovaných právních informací.

Po úvodu a přehledu literatury následuje představení výzkumných otázek. Čtvrtá část pak popisuje metodu použitou pro srovnání systémů a data k tomuto srovnání využitá. Pátá část popisuje výsledky srovnání napříč právními infor-

[1] Část tohoto textu v rozsahu podobnosti výsledků jednotlivých právních informačních systémů v odpovědi na metadatové vyhledávání (zejména metoda v části IV.A a výsledky v části V.A) byla publikována jako konferenční příspěvek z Internationalen Rechtsinformatik Symposion IRIS 2019 v Salzburku.

[2] JUDr. Mgr. Jakub Harašta, Ph.D., Odborný asistent, Ústav práva a technologií, Právnická fakulta MU. Kontakt: jakub.harasta@law.muni.cz.

mačními systémy ASPI, Beck-online a Codexis. Šestá část se věnuje diskuzi těchto výsledků a jejich zasazení do kontextu. V poslední části pak předkládám závěr a formuluji doporučení ohledně volby vyhledávacích strategií při sběru právních informací (dokumentů) pro akademickou i praktickou činnost.

Závěrem tohoto textu je, že při využití různých systémů pro zprostředkované vyhledávání (identifikaci soudních rozhodnutí souvisejících s konkrétním ustanovením) pozorujeme výrazné rozdíly. Naopak při zařazení metod nezprostředkovaného vyhledávání (plnotextový dotaz) jsou si výsledky poskytnuté jednotlivými systémy podobnější, byť jsou celkově horší oproti vyhledávání zprostředkovanému.

KLÍČOVÁ SLOVA

vyhledávání právních informací, vyhledávací strategie, srovnání

ABSTRACT

Use of legal information retrieval systems is a common part of every lawyer's life. In principle, it is possible to use two approaches to searching: mediated and non-mediated. As a part of the mediated search, we rely on the context provided by the provider of the information system. This might entail assignment of document with particular topic or labelling court decision as related to particular provision. As a part of the non-mediated search, user relies on herself. She formulates full-text queries to search expressions representing the issue at hand.

In this text, I focus on comparison of results provided by legal information systems ASPI, Beck-online and Codexis in response to comparable search queries employing both mediated and non-mediated search.

The introduction and the literature review is followed by part dedicated to research questions. The fourth part described the method used to compare the systems and the data used for the comparison. In the fifth part, I describe the results and the sixth part is devoted to discussion of these results in wider context. The last part presents a conclusion and contains recommendations regarding the selection of search strategies.

In conclusion, use of different systems for mediated search leads to significant differences between systems. On the contrary, when including non-mediated

search (full-text queries), results provided by individual systems are more similar to each other, but generally less precise compared to mediated search.

KEYWORDS

legal information retrieval, search strategies, comparison

1. ÚVOD

Právníci byli brzkými uživateli systémů pro získávání informací (IR, *information retrieval*). V důsledku toho se problematika vyhledávání právních informací v rámci elektronických systémů stala předmětem diskuze na stránkách (zejména anglickojazyčných) odborných i profesních periodik,[3] ale také předmětem výuky mladých právníků v průběhu studia i na počátku profesní kariéry. Otázky rozvoje strategií pro vyhledávání dokumentů, strategií pro zajištění a udržení uživatelských kompetencí[4] nebo evaluace úspěšnosti vyhledávacích úkonů prováděných uživateli[5] doprovázely rozvoj těchto systémů i jejich rozšiřování v praxi. Proces efektivní identifikace relevantních dokumentů a jejich získávání není, pochopitelně, pouze předmětem akademického zájmu. Má i nezpochybnitelný praktický rozměr. Svědomité vyhledání zdrojů je základem pro kompetentní odpověď klientovi nebo pro náležitou obranu jeho zájmů. Praktici jsou odpovědní za nesprávnou právní radu a její nesprávnost může být způsobena nedokonalostmi v prováděném sběru podkladů (rešerše). Znalost limitů konkrétních právních informačních systémů a obsahu, který se v nich nachází (nebo naopak nenachází), je důležitá. Stejně důležitá je i schopnost právníka pochopit rozdíly mezi systémy a praktické dopady, které tyto rozdíly mají na

[3] Srov. GERSON, Kevin. Evaluating Legal Information Retrieval Systems: How Do the Ranked-Retrieval Methods of WESTLAW and LEXIS Measure Up? *Legal Reference Services Quarterly*, 1999, roč. 17, č. 4, s. 53-67. Viz také KNAPP, Melanie a Rob WILLEY. Comparison of Research Speed and Accuracy Using Westlaw Classic and WestlawNext. *Legal Reference Services Quarterly*, 2013, roč. 32, č. 1-2, s. 126-141. Viz také MART, Susan Nevelow. The Case for Curation: The Relevance of Digest and Citator Results in Westlaw and Lexis. *Legal Reference Services Quarterly*, 2013, roč. 32, č. 1-2, s. 13-53.

[4] Viz BING, Jon. Legal Information Retrieval Systems: The Need for and the Design of Extremely Simple Retrieval Strategies. *Computer/Law Journal*, 1978, roč. 1, č. 1, s. 379-400.

[5] Viz BLAIR, David a M. E. MARON. An Evaluation of Retrieval Effectiveness for a Full-Text Document-Retrieval System. *Communications of the ACM,* 1985, roč. 28, č. 3, s. 289-299.

vyhledávání. Do třetice je pak nutné být si vědom různých vyhledávacích strategií a rozdílů mezi nimi, ať už s cílem dosáhnout větší kvality výsledků nebo nižší časové náročnosti vyhledávání.

Naneštěstí není literatura, která by se kriticky věnovala právním informačním systémům v České republice, respektive některým aspektům uživatelské práce s nimi, v podstatě vůbec k dispozici. Omezujeme se na výuku práce s nimi a rozvoj praktických dovedností vyhledávání v informačních systémech. Porovnání jednotlivých systémů nebo třeba diskuze limitů některých vyhledávacích postupů však v literatuře absentuje.

V České republice mají tradičně dominantní postavení tři právní informační systémy – ASPI (Wolters Kluwer), Beck-online (Nakladatelství C.H. Beck) a Codexis (Atlas Consulting). Součástí kánonu české praxe, který stále přetrvává, je přistupovat k těmto systémům jako k plně zaměnitelným, protože obsahují totožné právní předpisy a z velké části totožné kolekce judikatury. Skutečné rozdíly můžeme najít, jak se často uvádí (a jak i já sám při různých příležitostech studentům opakuji) až na úrovni dalšího obsahu – typicky komentářové literatury zařazené do jednotlivých systémů. Dle mých zjištění nebyla zatím žádná pozornost věnována kritické analýze výsledků poskytovaných těmito systémy v odpovědi na srovnatelné vyhledávací dotazy. Systémy nebyly v České republice podrobeny podobnému srovnání, jako je například možné vidět v některých jiných zemích.[6] Podobným způsobem absentuje i diskuze na téma efektivity vyhledávacích strategií pro práci s právními informačními systémy. Pokud se například zamyslíme nad tím, jak vzniká kresba, jedná se o sled využití jednotlivých technik, které jsou různě časově náročné. Pokud poskytneme k vytvoření

[6] Srov. GERSON, Kevin. Evaluating Legal Information Retrieval Systems: How Do the Ranked-Retrieval Methods of WESTLAW and LEXIS Measure Up? *Legal Reference Services Quarterly*, 1999, roč. 17, č. 4, s. 53-67. Také viz TAYLOR, William L. Comparing KeyCite and Shepard's for Completeness, Currency, and Accuracy. *Law Library Journal*, 2000, roč. 92, č. 2, s. 127-142. Dále KNAPP, Melanie a Rob WILLEY. Comparison of Research Speed and Accuracy Using Westlaw Classic and WestlawNext. *Legal Reference Services Quarterly*, 2013, roč. 32, č. 1-2, s. 126-141. Dále MART, Susan Nevelow. The Case for Curation: The Relevance of Digest and Citator Results in Westlaw and Lexis. *Legal Reference Services Quarterly*, 2013, roč. 32, č. 1-2, s. 13-53. Také viz HELLYER, Paul. Evaluating Shepard's, KeyCite, and BCite for Case Validation Accuracy. *Law Library Journal*, 2018, roč. 110, č. 4, s. 449-476.

kresby časovou dotaci deseti hodin, výsledek bude diametrálně odlišný od situace, kdy poskytneme pouze deset minut. Zkušený profesionál si podle dotace rozvrhne práci a při zpracování s nižší časovou dotací nebude takovou pozornost věnovat jednotlivým detailům. Rozdíl ve výsledku pak bude na první pohled patrný. Bude ale rozdíl na první pohled patrný, pokud se nebude jednat o kresbu, ale o vyhledávání právních informací? Bude si právník schopný poradit s odlišnou časovou dotací a zvolit pro vyhledání informací různé postupy tak, aby jeho vyhledávání nebylo perfektní, ale bylo kompetentní? Z mých (spíše anekdotických) zjištění formou neformálních dotazů plyne, že tomuto věnují právníci jen velmi málo pozornosti. Často mají pocit, že vyhledávání právních informací, jako jakési „pomocné vědy právnické", je pod jejich úroveň a má na jejich práci je relativně malý vliv.

Série metodologických článků uveřejněných v časopise *Jurisprudence* mne přivedla k mnoha otázkám směřujícím právě tímto směrem. Pokud například Kosař s Petrovem uvádí, že *„[p]odstatou případové studie je podrobná analýza jednoho anebo několika málo případů určitého fenoménu či kategorie"*[7], jak se vůbec dozvím o existenci konkrétních případů vhodných k analýze, pokud zpracovávám rozhodovací praxi? Je nějaký rozdíl mezi vyhledáváním vhodných případů formou plnotextových dotazů nebo formou metadatových vazeb mezi ustanovením předpisu a rozhodnutími? Pokud Bobek v poznámce pod čarou poznamenává, že *„[d]obrý komentář totiž zasadí dané ustanovení do širšího kontextu, osvětlí smysl a původ, kriticky analyzuje problémy a navrhne řešení, vtáhne do sebe a kriticky zhodnotí existující judikaturu"*[8], jakým způsobem autor komentáře zajistí, že identifikoval existující judikaturu dostatečným způsobem? A konečně, pokud Urbániková a Smékal uvádí, že při nepopsání použité metody *„jde o tzv. black-box výzkum, kdy závěry padají shůry, nevíme, jak k nim autor došel, a tím pádem*

[7] Viz KOSAŘ, David a Jan PETROV. Jak vybrat „případy" do případové studie a pracovat s nimi v právu: poznatky z výzkumu na pomezí práva a politologie. *Jurisprudence*, 2016, roč. 25, č. 6, s. 24.

[8] Viz BOBEK, Michal. Výzkum v právu: reklama na Nike anebo kvantová fyzika? *Jurisprudence*, 2016, roč. 25, č. 6, s. 5 (poznámka pod čarou 8).

jsme odkázáni jen na slepou důvěru“[9], nedlužíme čtenářům akademických článků vysvětlení, proč jsme do právní analýzy konkrétního ustanovení zařadili tři konkrétní rozhodnutí? Nemůže být fakt, že nám tři konkrétní rozhodnutí nabídne jako související s konkrétním ustanovením ASPI, ale Beck-online nebo Codexis nabídne jako relevantní jiná rozhodnutí, pro výzkumníka, čtenáře nebo praktikujícího právníka důležitý? Poskytuje srovnatelný dotaz do různých systémů stejné výsledky? Pokud ne, jak moc se liší a proč? Pokud se celou tuto záležitost pokusím převést do vyloženě praktických dimenzí: pokud jsem v pozici advokáta připravujícího dovolání k Nejvyššímu soudu a nezohledním v argumentaci relevantní rozhodnutí, mohu poškodit klienta. Ale jak – jakými metodami, jakými postupy a jakým způsobem – zajistím, že při rešerši budu schopen identifikovat všechna relevantní rozhodnutí?

V tomto textu představuji experiment, kterým (i) porovnávám výsledky poskytnuté právními informačními systémy ASPI, Beck-online a Codexis, v odpovědi na srovnatelné dotazy a (ii) porovnávám výsledky poskytnuté právními informačními systémy ASPI, Beck-online a Codexis při změně vyhledávací strategie. Po úvodu, kterým mimo jiné vysvětluji i motivaci pro přípravu tohoto textu, následuje přehled literatury věnované některým otázkám získávání relevantních informací a evaluace úspěšnosti těchto úkonů. Ve třetí části popisuji idealizovaný model, pomocí kterého s kolegy vyučujeme práci s právními informačními systémy mimo jiné i na Právnické fakultě MU a na Justiční akademii, a který poslouží jako základní struktura pro představení tohoto experimentu. Model totiž stojí na některých předpokladech, které v tomto textu ve velmi zjednodušené formě ověřuji a přímo z něj tak vycházejí konkrétní výzkumné otázky, které se tímto textem snažím zodpovědět. Čtvrtá část popisuje metodu a využitá data, pátá prezentuje výsledky. V šesté části výsledky diskutuji a upozorňuji na některé (nezanedbatelné) limity tohoto textu. Poslední část je závěrečná – shrnuje tento text a také obsahuje základní úvahy o možném dalším postupu v této oblasti.

[9] Viz URBÁNIKOVÁ, Marína a Hubert SMEKAL. Právní věda a právní psaní: postačí vždy jako výzkumná metoda "číst, přemýšlet a psát"? *Jurisprudence*, 2017, roč. 26, č. 4, s. 40.

2. LITERATURA

Pokud do jakéhokoli informačního systému zadáme konkrétní dotaz a v odpovědi na něj získáme seznam výsledků, ideálně bychom chtěli dokumenty v databázi rozdělit do 2 kategorií. První kategorií jsou tzv. pravá pozitiva (TP, *true positives*). Jedná se o dokumenty, které jsou pro nás relevantní a jsou obsaženy v seznamu výsledků, který jsme dostali v odpovědi na dotaz. Druhou kategorií jsou tzv. pravá negativa (TN, *true negatives*), což jsou dokumenty, které pro nás nejsou relevantní a v seznamu výsledků, který jsme dostali v odpovědi na dotaz, nejsou obsaženy. Takto jednoduchá však situace není, protože v reálném světě se nám objevují další kategorie dokumentů. Třetí kategorií tak jsou tzv. falešná pozitiva (FP, *false positives*). Jedná se o dokumenty, které pro nás nejsou relevantní, ale z nějakého důvodu došlo k jejich zařazení na seznam výsledků. Poslední kategorií jsou tzv. falešná negativa (FN, *false negatives*), které jsme sice chtěli získat (jsou pro naše vyhledávání relevantní), ale nedošlo k jejich zařazení na seznam výsledků. Nedostatky (tedy zařazení falešně pozitivních dokumentů nebo nezařazení falešně negativních) může být způsobené nedostatky na straně informačního systému nebo databáze (nízká kvalita dat a metadat, nízká uživatelská přívětivost při formulování dotazu) nebo na straně uživatele (nedostatečná kompetence při formulaci dotazů).

Obecně se úspěšnost získávání informací v právních informačních systémech měří pomocí přesnosti (P, *precision*), úplnosti (R, *recall*) a míry F1 (F1, *F1 measure*).[10] Přesnost je poměr počtu relevantních dokumentů získaných v odpovědi na konkrétní dotaz vůči celkovému počtu dokumentů získaných v odpovědi. Úplnost je poměr mezi počtem relevantních dokumentů získaných v odpovědi na dotaz a všech relevantních dokumentů v databázi. Míra F1 je pak harmonickým průměrem přesnosti a úplnosti.[11] Tyto veličiny při evaluaci nabývají hodnoty mezi 0 a 1, kde hodnota 0 indikuje nejméně přesný (resp. úplný nebo správný) výsledek vyhledávání a hodnota 1 indikuje nejvíce přesný (resp. úplný nebo správný) výsledek

[10] Podrobněji ASHLEY, Kevin. *Artificial Intelligence and Legal Analytics*: *New Tools for Law Practice in the Digital Age.* Cambridge: Cambridge University Press, 2017. S. 222.

[11] Tamtéž.

vyhledávání. Dosáhnout v rámci jednoho vyhledávání perfektní přesnosti i perfektní úplnosti (a tím perfektní míry F1) je v podstatě nemožné.[12]

Maximální přesnost (P = 1) je možné představit si tak, že každý dokument zařazený na seznam výsledků je pravé pozitivum (TP) bez ohledu na jejich celkový počet. Pokud mám v databázi sto relevantních dokumentů a v odpovědi na můj dotaz je jich do seznamu výsledků zařazeno pouze pět a seznam výsledků neobsahuje žádný falešně pozitivní dokument, dosáhl jsem maximální přesnosti. Celkový počet falešně negativních dokumentů (FN), tedy relevantních dokumentů, které nebyly zařazeny do seznamu výsledků, při výpočtu přesnosti nehraje roli. Maximální úplnost (R = 1) je možné představit si tak, že na seznam výsledků se musí dostat všechny relevantní výsledky bez ohledu na celkový počet informačního šumu tvořeného falešně pozitivními (FP) výsledky. Pokud tedy mám v databázi sto relevantních dokumentů a do seznamu výsledků jich zařadím pět set, přičemž nezůstane žádný falešně negativní dokument (FN), který bych vyhledáváním nezískal, dosáhnu maximální úplnosti vyhledávání.

Stoprocentně přesné je vyhledávání, které identifikuje právě jeden relevantní dokument – takové vyhledávání je ale mimořádně neúplné. Tento vztah ale platí i opačně. Pokud na seznam výsledků zařadím všechny dokumenty z právního informačního systému, určitě jsem zachytil všechny relevantní dokumenty a dosáhl jsem tak stoprocentní úplnosti. Takové vyhledávání je ale mimořádně nepřesné. Jakýkoli proces získávání informací je tak balancováním mezi přesností a úplností tak, abych si akcentem na jednu metriku nepotlačil metriku druhou. Právě z toho důvodu existuje míra F1, která je, jak bylo uvedeno výše, harmonickým průměrem přesnosti *P* a úplnosti *R*.

Výpočet přesnosti *P*:[13] $P = (TP)/(TP + FP)$

Výpočet úplnosti *R*:[14] $R = (TP)/(TP + FN)$

[12] Viz BING, Jon. Performance of Legal Text Retrieval Systems: The Curse of Boole. *Law Library Journal*, 1987, roč. 79, č. 2, s. 196.

[13] Převzato z Ashley 2017 op. cit. s. 222.

[14] Převzato tamtéž.

$$\text{Výpočet míry } F1\text{:}^{15}\ \mathrm{F1} = \frac{2*TP}{2*TP+FN+FP}$$

Jednou ze slavných studií věnovaných evaluaci procesu získávání právních informací je studie STAIRS publikovaná v roce 1985.[16] Studie poukazovala na velmi nízkou schopnost právníků formulovat relevantní plnotextové vyhledávací dotazy do databáze právních informací. Blair a Maron požádali v rámci této studie právníky o vyhledávání v databázi s tím, že jakmile získají alespoň 75 % všech relevantních dokumentů (tedy dosáhnou $R > 0{,}75$), mají vyhledávání ukončit a požádat výzkumníky o evaluaci tohoto vyhledávání. Po evaluaci výzkumníci zjistili, že ač měli právníci za to, že dosáhli slušné úplnosti vyhledávání, ve skutečnosti byly jejich výsledky velmi špatné ($R < 0{,}2$). Jakkoli se tato studie soustředila zejména na proces identifikace skutkově relevantních dokumentů a nikoli dokumentů právně relevantních, naznačila, že vyhledávání založené na plnotextových dotazech je mimořádně náročné[17] a nevede k optimálním výsledkům. Následné studie pak demonstrovaly, že tento problém se projevuje i v jiných právních informačních systémech[18] a že je typický pro vyhledávání, při kterých uživatelé usilují o vysokou úplnost.[19]

Plnotextové vyhledávání není jediným způsobem, jak získat z informačních systémů relevantní dokumenty. V současné době získáváme právní informace ze systémů využívajících plnotextové vyhledávání, znalostní inženýrství nebo můžeme využít získávání informací založené na zpracování přirozeného jazyka.[20] Všechny tyto postupy mají své výhody a nevý-

---

[15] Převzato tamtéž.

[16] Viz Blair a Maron 1985 op. cit.

[17] Dabney označuje kolekce psaných záznamů s odkazem na Platóna za nevyléčitelně obskurní reprezentace idejí. Viz DABNEY, Daniel. The Curse of Thamus: An Analysis of Full-Text Legal Document Retrieval, *Law Library Journal,* 1986, roč. 78, č. 5, s. 40

[18] Tamtéž.

[19] Viz SORMUNEN, Eero. Extensions to the STAIRS Study – Empirical Evidence for the Hypothesised Ineffectiveness of Boolean Queries in Large Full-Text Databases. *Information Retrieval*, 2001, roč. 4, č. 3-4, s. 257-273.

[20] Viz MAXWELL, Tamsin a Burkhard SCHAFER. Concept and Context in Legal Information Retrieval. *Proceedings of Jurix 2008*. S. 64.

hody, protože perfektní míra F1 (tedy kombinace perfektní přesnosti P a úplnosti R) zůstává nedosažitelná. Systémy založené na znalostním inženýrství se pokouší vystihnout způsob, jakým si právníci pamatují případy, a toto zachytit v rámci počítačových algoritmů a datových struktur.[21] Hlavním problémem těchto systémů je jejich obtížné využití v praxi. Jak uvádí Maxwell a Schafer, systémy využívající znalostního inženýrství jsou často velmi specificky zaměřené a umožňují využívat pouze velmi malé a vysoce strukturované kolekce dokumentů.[22] Získávání informací založené na zpracování přirozeného jazyka pak má značnou výhodu ve škálovatelnosti a také vykazuje od počátku lepší výsledky.[23] Zpracování přirozeného jazyka získává v procesu získávání informací stále prominentnější pozici. Konečným cílem se zdá být snaha zajistit vyhledávání informací prostřednictvím odpovědí na otázky[24] nebo prostřednictvím konceptuálního vyhledávání.[25]

Vyhledávání relevantních právních informací je tak velkou výzvou z pohledu použitých technologií a postupů. Nemenší výzvou je ale i samotný termín relevance – nikoli tedy samotný proces vyhledávání, ale vůbec způsob, jakým rozlišujeme mezi relevantními a nerelevantními dokumenty. Termín *relevance* je totiž velmi často chápán intuitivně. Konceptualizace termínu *relevance* specificky pro právní prostředí se objevila až v roce 2017, kdy Opijnen a Santos přišli s následujícími kategoriemi relevance: algoritmická, bibliografická, tematická, kognitivní, situační a doménová.[26] Tato kategorizace je dle mého názoru zcela zásadní pro pochopení procesu vyhledávání. Některé kategorie mají projevy, které jsou v rámci práva téměř

[21] Viz HAFNER, Carole. Conceptual Organization of Case Law Knowledge Bases. *Proceedings of ICAIL* 1987. S. 35.

[22] Viz Maxwell a Schafer 2008 op. cit., s. 66.

[23] Srov. TURTLE, Howard. Natural Language vs. Boolean Query Evaluation: A Comparison of Retrieval Performance. *Proceedings of SIGIR 1994. S*. 212-220.

[24] Viz Maxwell a Schafer 2008 op. cit., s. 68.

[25] Viz GRABMAIR, Matthias, Kevin ASHLEY, Ran CHEN, Preethi SURESHKUMAR, Chen WANG, Eric NYBERG a Vern WALKER. Introducing LUIMA: an Experiment in Legal Conceptual Retrieval of Vaccine Injury Decisions Using a UIMA Type System and TOOLS. *Proceedings of ICAIL 2015*. S. 69-78.

[26] Viz VAN OPIJNEN, Marc a Cristiana SANTOS. On the Concept of Relevance in Legal Information Retrieval. *Artificial Intelligence and* Law, 2017, roč. 25, č. 1, s. 73.

univerzální – z hlediska práva jako domény je relevantní judikatura publikovaná ve sbírkách, například ve Sbírce soudních rozhodnutí a stanovisek Nejvyššího soudu. V tomto případě se jedná o doménovou relevanci, kde jsou individuální dokumenty vnímány jako relevantní na základě příslušnosti ke třídě dokumentů, která je vnímána jako relevantní. Jiné kategorie jsou však velmi subjektivní a přímo závislé na osobě, která se systémem pracuje. Zkušenému uživateli s dvacetiletou praxí přinese pouze malé množství dokumentů nové informace, zatímco čerstvému absolventovi může novou informaci přinést každý druhý dokument, který nalezne. V tomto případě se jedná o kognitivní relevanci.

Dvě z kategorií, které definovali Opijnen a Santos, jsou využity v experimentu popisovaném v tomto textu. Je to zejména z důvodu, že pokud nezohledníme žádnou konkrétní formu relevance, ale budeme se spoléhat na intuitivní chápání termínu, bude to jako porovnávání jablek s hruškami. První je tzv. tematická relevance, což je vztah mezi tématem formulovaným v uživatelském vyhledávání a tématem dokumentů. Vytvoření vztahu mezi dokumentem a tématem může být explicitní nebo implicitní prostřednictvím automatického indexování slov, manuálního indexování dokumentů nebo poloautomatizované klasifikace.[27] Druhou je tzv. kognitivní relevance, která vystihuje, zda je dokument relevantní pro konkrétního uživatele. Tento typ relevance je, jako takový, subjektivní a silně závislý například na uživatelově apriorní znalosti tématu.[28]

3. MODEL A VÝZKUMNÉ OTÁZKY

Právní informace, ať jsou obsažené v právních předpisech, soudních rozhodnutích nebo jakýchkoli jiných dokumentech, musí být možné v právních informačních systémech vyhledávat. Z toho důvodu musí být dokumenty, které tyto informace obsahují, nějakým způsobem organizovány. Možnost uživatele vyhledat konkrétní dokument vyžaduje určitou organizaci, kterou uživatel musí poznat a na kterou se při vyhledávání může spolehnout.

[27] Tamtéž, s. 74.

[28] Tamtéž, s. 81.

Aby bylo možné od sebe odlišit jednotlivé způsoby vyhledávání – vyhledávací strategie, chceme-li – a dostatečně je studentům vysvětlit, vytvořili jsme si s kolegy Jakubem Míškem a Matějem Myškou zjednodušený model, který jsme před několika lety začali využívat při výuce na PrF MU. Pomocí tohoto zjednodušeného modelu studentům popisujeme a vysvětlujeme některé situace, se kterými se mohou při vyhledávání setkat. Právní informační systémy totiž, jak si nejspíše všiml každý, kdo je při své činnosti intenzivně využívá, neposkytují při srovnatelných dotazech totožné výsledky. V některých situacích mohou být dokonce rozdíly mezi systémy při využití srovnatelného dotazu větší než shody. Ve výuce používaný model, se kterým budu dále pracovat i v tomto textu, umožňuje tyto odlišnosti, když ne přímo vysvětlit, tak alespoň ukázat, jak vznikají.

Zmíněný model, který využíváme ve výuce, má dvě základní složky: data a metadata. V případě metadat pak rozlišujeme mezi objektivními a subjektivními metadaty.

Uživatele v právních informačních systémech zajímají primárně data – tedy texty právních předpisů, soudních rozhodnutí, komentářů nebo jakýchkoli jiných zdrojů právních informací. Textem ustanovení jsme informováni o existenci určitého pravidla, které je textem tohoto ustanovení přímo konstituováno. Často si však nevystačíme pouze s textem ustanovení, ale při snaze toto ustanovení pochopit nám může významně pomoci například jeho zařazení do systematiky předpisu (například do konkrétní hlavy, části a podobně). Data samotná nepřináší v rámci českých právních informačních systémů výrazné problémy. Je zcela legitimní očekávat, že § 12 občanského soudního řádu nalezneme v právním informačním systému ASPI, Beck-online i Codexis, případně i v jakémkoli jiném. Stejně tak je zcela legitimní očekávat, že text tohoto ustanovení bude ve všech právních informačních systémech totožný. V případě soudních rozhodnutí, které se v systémech vyskytují, je situace poněkud komplikovanější. Editorské zásahy nebo přejímání rozhodnutí z různých zdrojů (zákonem předepsané sbírky jednotlivých vrcholných soudů, anotace v časopisech, webové databáze vrcholných soudů a podobně) mohou vést k rozdílům v textech těchto

rozhodnutí.[29] Obecně ale platí, že i v případě soudních rozhodnutí Ústavního soudu, Nejvyššího soudu a Nejvyššího správního soudu tak nějak očekáváme, že texty – tedy data – budou stejné (nebo aspoň velmi podobné) napříč systémy.

Organizace dokumentů výhradně v datové podobě by však znamenala, že se jako uživatelé musíme při jejich vyhledávání spolehnout na plnotextové dotazy. Plnotextové vyhledávání v právních informačních systémech nám umožňuje pomocí různých operátorů specifikovat, zda nás zajímá slovní spojení, zda se mají v textu vyskytovat všechna zadaná slova nebo stačí pouze jedno z nich, případně zda se zadávaná slova mají vyhledat v určité vzdálenosti.[30] Plnotextové vyhledávání s sebou ale nese nevýhody – uživatel sám musí definovat, jaké výrazy vyskytující se v textu dokumentu signalizují, že je pro něj dokument relevantní. Jakkoli přímočaře tento požadavek zní, rozhodně se nejedná o triviální záležitost. Abychom totiž dokázali konkrétní dokument nebo ustanovení nalézt plnotextovým dotazem, musíme do určitě míry tušit, co je v tomto dokumentu napsáno. Alespoň do určité míry tedy musíme vědět, jak je například dané ustanovení naformulováno, jaké obsahuje výrazy, slovní spojení a podobně. U relativně strukturovaných a terminologicky pevně vymezených zdrojů je to často otázka cviku a zkušenosti – právník, který si více pamatuje a „více toho viděl“, má zjednodušenou pozici. U soudních rozhodnutí však takové vyhledávání může být náročné i pro velmi zkušeného uživatele. Při vyhledávání rozsáhlých databází například důkazního materiálu, které budou relativně nestrukturované, je to pak ještě horší, jak ostatně ukázala i shora citovaná STAIRS studie z 80. let minulého století.[31] V rámci plnotextového vyhledávání hraje roli také to, jak daný uživatel umí využívat různé možnosti nabízené informačním systémem. Schopnost práce se systémem se relativně jednoduše nabývá, ale udržet uživatelskou kompetenci (tedy schopnost aktivně používat všechny nebo většinu dostupných funkcí

[29] Srov. HARAŠTA, Jakub. Nejednoznačnost odkazů k soudním rozhodnutím a možnosti řešení. *Revue pro právo a technologie*, roč. 6, č. 11, s. 15-28.

[30] Ne každý právní informační systém nabízí všechny tyto možnosti. Jaké operátory zařadit je i otázkou rozhodnutí tvůrců systému na základě třeba výzkumu uživatelských preferencí.

[31] Viz Blair a Maron 1985 op. cit.

v podobě jednotlivých plnotextových operátorů) je poměrně náročné.[32] I z těchto důvodu hrají při vyhledávání značnou roli metadata, tedy data o datech.

Metadata nám umožňují vyhledat data (ustanovení, soudní rozhodnutí atd.) nikoli nutně pomocí jejich obsahu, ale podle nějaké vlastnosti. Je tak možné omezit vyhledávání soudních rozhodnutí na rozhodnutí vydaná například Nejvyšším soudem v období od 1. ledna 2010 do 31. prosince 2011. Uživatel sám musí přijít s kritérii, která mu pomohou vyhledat relevantní informace. Část kritérií plyne z možností konkrétního informačního systému (co nabízí a co naopak nenabízí), část pak plyne z vědomostí o právním řádu, v jehož rámci uživatel relevantní dokumenty vyhledává. Jak bylo uvedeno výše, v našem modelu rozeznáváme metadata dvojího typu – objektivní metadata a subjektivní metadata. Objektivní metadata jsou specifická pro daný dokumenty a vyskytují se napříč všemi systémy, zatímco subjektivní metadata jsou často specifická pro konkrétní systém. Mohou se tak u jednotlivých iterací dokumentu zařazených v různých informačních systémech lišit. Příkladem objektivního metadatového záznamu je například spisová značka rozhodnutí, datum jeho vydání nebo soud původu. Pomocí těchto kritérií jsme schopni omezit vyhledávání a zároveň jako uživatelé legitimně očekáváme, že dokument bude pomocí těchto metadatových záznamů popsán ve všech systémech. Se subjektivními metadaty je situace opět o něco složitější, ale pro tento text zcela zásadní.

Subjektivní metadatové záznamy se mohou mezi systémy lišit. Mohou se lišit například přítomností příslušného metadatového záznamu. Například ASPI využívá metadatovou kategorii „Oblasti úpravy“ pro popis dokumentů, kterou ale Codexis nemá ekvivalentním způsobem zařazenou. Z mého pohledu jsou ale mnohem zajímavější odlišnosti v metadatových kategoriích, které jsou jako kritérium zařazené do více informačních systémů. Příkladem tohoto stavu může být metadatová kategorie identifikující rozhodnutí jako vztahující se k určitému ustanovení. Tato kategorie je nejen

[32] Příkladem může být vyhledávací funkce umožňující nastavování vzdáleností mezi zadanými výrazy při plnotextovém v právním informačním systému ASPI. Tato funkce je z mých zkušeností uživateli hodnocena velmi pozitivně, ale zároveň na ni uživatelé často zapomínají a často si musejí její existenci připomínat.

přítomná v určité podobě v systémech ASPI, Beck-online i Codexis, ale je také mimořádně často využívána k vyhledávání relevantních dokumentů (a to nejen v České republice[33]). V českém právu neexistuje žádný centrální seznam rozhodnutí, která by se vztahovala k nějakému ustanovení a byla tedy relevantní pro jeho výklad. Než si však povzdechneme nad tím, jak je to české právo zpátečnické, musím poznamenat, že takovýto seznam nebude s největší pravděpodobností existovat v autoritativní podobě v žádné zemi kontinentální právní tradice. A zatímco spisová značka konkrétního rozhodnutí bude totožná ve všech třech zmíněných systémech (byť chyby a překlepy se samozřejmě mohou objevit), vytvoření vazby mezi ustanovením a rozhodnutím může být, při absenci nějaké centrální autority, vytvořeno s důrazem na různé aspekty.[34] Bude tedy přímo záležet na definici situace, kdy je nutné rozhodnutí a ustanovení provázat metadatovým záznamem. Pokud budeme například vztah definovat na základě zmínky daného ustanovení v soudním rozhodnutí, budeme vytvářet metadatové vazby na jiných místech, než pokud budeme za kritérium k vytvoření vazby považovat nejen zmínku daného ustanovení v soudním rozhodnutí, ale i jeho historických předchůdců. Abych uvedl praktický příklad, seznam výsledků rozhodnutí souvisejících s § 14 zákona č. 89/2012 Sb. může zahrnovat (i) rozhodnutí zmiňující § 14 zákona č. 89/2012 Sb. nebo (ii) rozhodnutí zmiňující § 14 zákona č. 89/2012 Sb. a zároveň § 6 zákona č. 40/1964 Sb., protože se jedná o „ideového" předchůdce rešeršovaného ustanovení. Podobně můžeme zvolit variantu, která bude pro tvůrce právního informačního systému výrazně náročnější, kdy budeme vazbu mezi ustanovením a rozhodnutím vytvářet pouze tehdy, pokud je v soudním rozhodnutí vyhledávané ustanovení nejenom zmíněno, ale substantivně diskutováno (soud například rozebírá limity jeho aplikace). Takovéto výsledky jsou pro uživatele mimořádně přínosné, protože snižují jeho informační zahlcení. Přináší s sebou ale další palčivé otázky. Jednou z nich je například

[33] Viz Van Opijnen a Santos 2017 op. cit., s. 74-75.

[34] Srov. ARREDONDO, Pablo. Shepard for a Day: A Novel Class Exercise for Teaching Citators. *Legal Reference Service Quarterly*, 2015, roč. 34, č. 3, s. 244, kde autor volá po zdravém skepticismu směrem k rozhodnutím označeným v rámci amerických informačních systémů červenými, žlutými nebo zelenými vlaječkami podle jejich vzájemného vztahu.

zajištění kontinuity tvorby těchto záznamů při personální nebo jiné změně na straně tvůrce informačních systému. Mělo by nás zajímat, kdo rozhoduje o tom, že je dané ustanovení v soudním rozhodnutí substantivně diskutováno. Jsou rozhodnutí zpracovávána v roce 2020 se stejnou péčí, s jakou byla zpracovávána v roce 2000? Jsou vazby vytvářeny podle stále stejného standardu?

Zdráhám se tento model nazvat teorií organizace dokumentů v právních informačních systémech. S kolegy jej nicméně používáme ve výuce, kde se nám celkem osvědčil. Rozdělení obsahu systémů na data a metadata a rozdělení metadat v systémech na metadata objektivní a subjektivní není složité a pomáhá ilustrovat některé problémy související s vyhledáváním v systémech. Jedná se samozřejmě o model idealizovaný – data nejsou zcela totožná, protože právní informační systémy neobsahují zcela stejné dokumenty. V důsledku odlišného přístupu při budování konkrétní databáze a tvorbě jejího uživatelského rozhraní nemusí být možné je ani totožným způsobem prohledávat. Drobné rozdíly plynou z odlišného postupu zvoleného pro plnotextovou indexaci při zařazení obsahu do systému[35], mohou se vyskytovat chyby (šotci) a podobně.

Podle toho, na jaké části tohoto modelu se uživatel při vyhledávání spolehne pak můžeme rozlišovat vyhledávací strategie zprostředkované, nezprostředkované a kombinované. Volbou zprostředkované strategie se uživatel spoléhá na tvůrce informačního systému, respektive na subjektivní metadata v systému obsažená. Typickým příkladem je všemi uživateli hojně využívaná funkce hledání judikatury související s konkrétním ustanovením. Volbou nezprostředkované strategie se uživatel spoléhá primárně sám na sebe a formuluje plnotextové dotazy nebo využívá objektivní metadata. Plnotextovým vyhledáváním nebo využitím objektivních metadat se sám snaží nadefinovat relevantní dokumenty, které hledá a které pro svoji práci potřebuje. Každý z těchto postupů má svá pro a proti. Zprostředkovanou strategií budeme, pokud shora uvedený model odpovídá realitě, dostávat výsledky závislé na použití toho kterého konkrétního systému. Na druhou

[35] Více viz ŠAVELKA, Jaromír, Matěj MYŠKA, Adam PTAŠNIK a Danuše SPÁČILOVÁ. *Právní informační systémy*. Brno: Tribun EU, 2011. S. 64-72.

stranu ale bude vyhledávání zřejmě časově i kognitivně méně náročné. Nezprostředkovanou strategií strávíme větší množství času a budeme u jejího použití muset jako uživatelé i více přemýšlet. Na druhou stranu se ale oprostíme od závislosti seznamu výsledků na využití konkrétního systému. Kombinované vyhledávací strategie pak využívají kombinaci jak nezprostředkovaných (data, objektivní metadata), tak zprostředkovaných (subjektivní metadata) informací obsažených v systémech. Například onen shora uvedený příklad s dotazem na judikaturu související s § 14 zákona č. 89/2012 Sb. můžeme doprovodit plnotextovým dotazem ve snaze zajistit si menší množství výsledků k dalšímu zpracování.

Z tohoto modelu pak přímo plynou i výzkumné otázky, na které v tomto textu hledám odpověď.

Za prvé: liší se výsledky vyhledávání podle subjektivních metadat mezi jednotlivými systémy? A pokud ano, jak moc? Pokud přijmeme z představeného modelu vycházející premisu, mezi systémy ASPI, Beck-online a Codexis budou při využití srovnatelné zprostředkované vyhledávací strategie seznamy výsledků odlišné. V rámci této otázky tak vlastně budu ověřovat, (a) zda shora představený model odpovídá realitě a (b) jak velké jsou rozdíly mezi výsledky poskytnutými systémy v odpovědi na srovnatelné dotazy.

Za druhé: povede zařazení plnotextového kritéria do vyhledávání podle subjektivních metadat k dosažení výrazně přesnějších výsledků v rámci jednotlivých právních informačních systémů? Tato otázka přímo navazuje na první výzkumnou otázku, kde dochází k využití zprostředkované vyhledávací strategie. Při odpovědi na druhou otázku dojde k využití kombinované vyhledávací strategie (subjektivní metadata plus plnotextový dotaz) a pokusím se zjistit, zda budou výsledky oproti využití zprostředkované vyhledávací strategie přesnější ve smyslu vyšší dosažené úplnosti R, přesnosti P a tím i míry F1.

Za třetí: povede zařazení plnotextového kritéria do vyhledávání podle subjektivních metadat k dosažení podobnějších výsledků napříč jednotlivými informačními systémy? Tato otázka přímo navazuje na obě předcházející výzkumné otázky. Pokud přijmeme z představeného modelu vycházející

premisu, mezi systémy ASPI, Beck-online a Codexis budou při využití srovnatelné kombinované vyhledávací strategie výsledky sice odlišné, ale budou si navzájem podobnější než při využití zprostředkované vyhledávací strategie.

4. METODA A DATA

4.1 ZPROSTŘEDKOVANÉ ÚDAJE: METADATOVÉ VYHLEDÁVÁNÍ

Pochopitelně zde není možné porovnat výsledky poskytované právními informačními systémy ASPI, Beck-online a Codexis kompletně a komplexně, tedy porovnat všechny v těchto systémech existující vazby. Proto jsem pro tento text zvolil porovnání judikatury související se zákonem č. 121/2000 Sb., autorský zákon (dále jen AutZ), a s dnes již neúčinným zákonem č. 101/2000 Sb., o ochraně osobních údajů (dále jen ZOOÚ). K jednotlivým ustanovením těchto dvou předpisů byla mezi 8. a 10. říjnem 2018 vytěžena související rozhodnutí českých soudů pomocí metadatové vazby označující tzv. související judikaturu. Tuto metadatovou vazbu obsahují pod různými názvy všechny tři právní informační systémy a jedná se tak o dotaz, který je srovnatelný svým významem při vyhledávání.

Soudní rozhodnutí získaná popsaným způsobem jsem zorganizoval do databáze, kde bylo každé z rozhodnutí uspořádáno do páru obsahujícího ustanovení U a rozhodnutí *R* a bylo indikováno, ve kterém systému je možné tento pár zachytit. Tím byla vytvořena databáze získaných rozhodnutí, jejíž výňatek je možné vidět v Tab. 1. Zápis v tabulce na prvním řádku indikuje, že pár *U-R* zahrnující ustanovení § 2 AutZ a rozhodnutí č.j. 10 A 186/2013-49 je možné získat ze systému ASPI, ale nikoli ze systémů Beck-online a Codexis. Uvedené rozhodnutí se sice v těchto databázích nachází, ale nevrací se jako výsledek k vyhledávání judikatury související s § 2 AutZ. Podobně pak druhý řádek ukazuje, že pár *U-R* zahrnující ustanovení § 21 ZOOÚ a rozhodnutí sp. zn. I. ÚS 1783/10 je možné získat z právních informačních systémů ASPI a Codexis, ale nikoli ze systému Beck-online. Opět nám tento záznam neříká nic o tom, zda se dané rozhodnutí v právním informačním systému nachází, ale pouze indikuje, zda je

rozhodnutí metadatově provázáno s konkrétním ustanovením jako související.

Ustanovení *U*	Rozhodnutí *R*	ASPI	Beck-online	Codexis
§ 2 AutZ	10 A 186/2013-49	1	0	0
§ 21 ZOOÚ	I. ÚS 1783/10	1	0	1

Tab. 1 Příklad dvou řádků z databáze párů U-R s indikací systémů, ve kterých je pár možné identifikovat pomocí přítomností metadatové vazby

Tímto způsobem tak vznikla databáze, která obsahuje každý pár *U-R*, který se v systémech ASPI, Beck-online a Codexis vyskytl alespoň jednou – tedy obsahuje rozhodnutí *R*, které bylo při metadatovém vyhledávání judikatury související s ustanovením U zachyceno alespoň v jednom z těchto tří systémů. Do vyhledávání byla zahrnuta všechna ustanovení AutZ a ZOOÚ na úrovni jednotlivých paragrafů. Nižší jednotky, tedy odstavce a písmena, nebyla zohledňována.

Na tomto místě je naprosto zásadní zopakovat, že neexistuje žádný autoritativní nebo centrální seznam rozhodnutí, která by se měla objevit v seznamu výsledků v odpovědi na konkrétní dotaz. Shora uvedená databáze tak nahrazuje tento seznam. Porovnávání výsledků poskytnutých jednotlivými systémy se tak děje srovnáním s jakousi idealizovanou databází, která je představována sjednocením množin výsledků poskytnutých jednotlivými systémy. Tato základní databáze (de facto seznam rozhodnutí uvedených jako související s jednotlivými ustanoveními) bude dále obohacena o zavedení plnotextového vyhledávacího parametru a o zohlednění kognitivní relevance jednotlivých rozhodnutí pro expertního a neexpertního uživatele.

4.2 NEZPROSTŘEDKOVANÉ ÚDAJE: PLNOTEXTOVÉ VYHLEDÁVÁNÍ

Do výše uvedené databáze jsem ve druhém kroku zanesl plnotextový parametr, který jsem využil jako druhé kritérium pro vyhledávání. Použitý plnotextový parametr jsem stanovil jako výskyt tří obecných termínů souvisejících s AutZ a tří obecných pojmů souvisejících se ZOOÚ v textu soudního

rozhodnutí. Tyto pojmy se v textu mohou vyskytovat kdekoli a nemusí tak mezi nimi být žádná vzdálenostní či jiná souvislost. Pro AutZ byl plnotextový parametr zvolen jako současný výskyt tří následujících slov: *autor*, *dílo*, *duševní*. Pro ZOOÚ byl plnotextový parametr zvolen jako současný výskyt tří následujících slov: *údaj*, *zpracování*, *správce*. Takováto vyhledávací strategie je mimořádně jednoduchá a je zvolena s přihlédnutím k předpisu, ale nikoli s přihlédnutím ke konkrétnímu ustanovení.

Do databáze, jejíž dva řádky jsou uvedeny v Tab. 1 tak přibyly další hodnoty. Výňatek databáze se zařazeným plnotextovým parametrem je možné vidět v Tab. 2. První řádek indikuje, že pár *U-R* obsahující ustanovení § 2 AutZ a rozhodnutí č.j. 10 A 186/2013-49 v sobě obsahuje dokument, který splňuje plnotextovou podmínku stanovenou jako související s ustanovením AutZ (tedy současný výskyt slov *autor*, *dílo* a *duševní* v textu rozhodnutí). Druhý řádek pak indikuje, že pár *U-R* obsahující ustanovení § 21 ZOOÚ a rozhodnutí sp. zn. I. ÚS 1783/10 v sobě obsahuje dokument, který splňuje plnotextovou podmínku stanovenou pro rozhodnutí související s ustanovením ZOOÚ (tedy současný výskyt slov *údaj*, *zpracování* a *správce*).

Ustanovení *U*	Rozhodnutí *R*	Plnotextové (AutZ)	Plnotextové (ZOOÚ)
§ 2 AutZ	10 A 186/2013-49	1	-
§ 21 ZOOÚ	I. ÚS 1783/10	-	1

Tab. 2 Příklad dvou řádků z databáze párů U-R s indikací splnění plnotextového parametru pro AutZ/ZOOÚ

4.3 KOGNITIVNÍ RELEVANCE ROZHODNUTÍ

V návaznosti na vytvoření databáze obsahující jak výsledky metadatového vyhledávání, tak výsledky vyhledávání s plnotextovým parametrem, jsem pozval tři osoby s právním vzděláním k dalšímu zpracování výsledků. Jejich úkolem bylo po předložení páru *U-R* rozhodnout, zda dané rozhodnutí *R* přispívá k pochopení ustanovení U či nikoli. Jeden z přizvaných právníků byl odborníkem na problematiku ochrany osobních údajů a dostal

tak za úkol vytvořit expertní anotace pro ZOOÚ. Druhý byl odborníkem na problematiku autorského práva a dostal tak za úkol vytvořit expertní anotace pro AutZ. Třetí přizvaný nebyl odborníkem ani v jedné této oblasti a dostal tak za úkol vytvořit neexpertní anotace pro oba předpisy. Do databáze, jejíž dva řádky jsou v Tab. 1 (metadatové vyhledávání) a následně i v Tab. 2 (plnotextový parametr), tak přibyly další hodnoty. Výňatek je možné vidět v Tab. 3. První řádek této tabulky indikuje, že pár *U-R* tvořený ustanovením § 2 AutZ a rozhodnutím č.j. 10 A 186/2013-49 byl v rámci expertních anotací hodnocen jako relevantní – rozhodnutí tedy přispívá odborníkovi k pochopení daného ustanovení (je kognitivně relevantní) – zatímco v rámci neexpertních anotací byl hodnocen jako nerelevantní. Druhý řádek pak indikuje, že pár *U-R* tvořený ustanovením § 21 ZOOÚ a rozhodnutím sp. zn. I. ÚS 1783/10 byl hodnocen jako kognitivně relevantní (přispívající k pochopení ustanovení) v rámci expertních i neexpertních anotací.

Ustanovení *U*	Rozhodnutí *R*	Expertní anotace	Neexpertní anotace
§ 2 AutZ	10 A 186/2013-49	1	0
§ 21 ZOOÚ	I. ÚS 1783/10	1	1

Tab. 3 Příklad dvou řádků z databáze párů U-R s indikací kognitivní relevance z pohledu expertního a neexpertního anotátora

Považuji za nutné na tomto místě vysvětlit, proč jsem do experimentu zahrnul i kognitivní relevanci. Začnu apelem na uživatelskou zkušenost každého, kdo s nějakým informačním systémem musel pracovat. Je poměrně častým jevem, že informační systém zařadí na seznam výsledků dokument, který nám v konečném důsledku k ničemu není. Splňuje totiž nějaké metriky, pro které ho tvůrce systému považoval za důležitý (tematicky relevantní, doménově relevantní a podobně), ale v situaci konkrétního uživatele (z hlediska kognitivní relevance) nám k ničemu není – nepřináší nám novou informaci. Toto je klasický problém všech informačních systémů a databází.

Pokud nám hypotetický systém X na dotaz vrátí seznam výsledků o 20 rozhodnutích a hypotetický systém Y nám na srovnatelný dotaz vrátí 2 rozhodnutí, na první pohled může být lepší využít systému X, který poskytne větší množství relevantních výsledků (v tomto případě mluvím o tematické relevanci v podobě provázání ustanovení a soudního rozhodnutí). Pokud ale do vyhodnocování zařadíme jinou formu relevance (například právě kognitivní relevanci), můžeme zjistit, že z dvaceti rozhodnutí identifikovaných použitím systému X nám k vyřešení problému, před který jsme postaveni, pomáhají pouze tři. Oproti tomu, ze dvou rozhodnutí identifikovaných jako relevantní systémem Y jsou kognitivně relevantní obě dvě. Na první pohled jednoduché srovnání systémů je najednou náročnější a méně přímočaré. Systém X sice identifikoval více kognitivně relevantních rozhodnutí, ale bylo nutné je odfiltrovat dalším zpracováním (přečtením) rozhodnutí, která jako relevantní (související s ustanovením) identifikoval tvůrce příslušného systému. S použitím systému X se tak váže větší časová náročnost a někteří uživatelé tak budou inklinovat k využití systému Y. Pro různé typy uživatelů pak bude sada kognitivních rozhodnutí vypadat jinak v závislosti na odbornosti v konkrétní oblasti a na zkušenostech.

4.4 METODA POROVNÁNÍ VÝSLEDKŮ

Shora uvedeným postupem jsem vytvořil idealizovanou databázi, která mi poslouží pro porovnání jednotlivých systémů a jednotlivých vyhledávacích strategií a tím k zodpovězení stanovených výzkumných otázek. Na tomto místě je nutné připomenout, že cílem tohoto textu není určit, jestli jsou v systémech ASPI, Beck-online a Codexis správně evidované relevantní dokumenty. Vzhledem k chybějícímu autoritativnímu seznamu rozhodnutí souvisejících s konkrétním ustanovením je takový úkon zcela jistě nemožný. Cílem je zjistit, jaká proporce párů *U-R* získaných ze všech tří systémů se vyskytuje v jednotlivých systémech (první výzkumná otázka), jestli vede zařazení plnotextového parametru do vyhledávání k lepším výsledkům (druhá výzkumná otázka) a konečně, zda jsou si výsledky napříč systémy po zařazení plnotextového parametru vzájemně podobnější (třetí výzkumná otázka). Kde je to vhodné, jsou dále v textu uváděny konkrétní

hodnoty přesnosti *P*, úplnosti *R* a míry *F1*, kterých bylo dosaženo porovnáním jednotlivých právních informačních systémů (ASPI, Beck-online, Codexis) s popsanou idealizovanou databází.

5. VÝSLEDKY

5.1 ZÁKLADNÍ PŘEHLED

Idealizovaná databáze, která byla vytvořená sjednocením množin párů *U-R* získaných z právních informačních systémů ASPI, Beck-online a Codexis obsahuje 403 párů pro AutZ a 262 párů pro ZOOÚ. V případě AutZ je 307 těchto párů možné získat z právního informačního systému ASPI, 135 ze systému Beck-online a 248 ze systému Codexis. V případě ZOOÚ je 176 párů možné získat z právního informačního systému ASPI, 81 z právního informačního systému Beck-online a 140 ze systému Codexis. Rozdíly mezi systémy tedy existují a jsou zcela evidentní již z prosté sumy nalezených párů *U-R*.

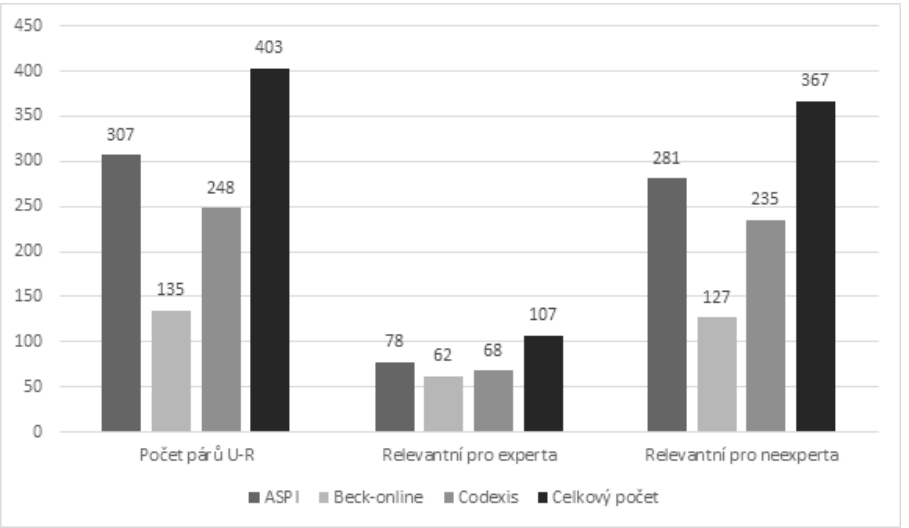
Logickou námitkou je, že právní informační systémy obsahují jiná rozhodnutí. Pokud ale prohlédneme jednotlivé databáze, tak zjistíme, že ze 403 párů *U-R*, které se objevují v idealizované databázi pro AutZ, jich může ASPI obsahovat 380 (94,29 %), Beck-online 368 (91,32 %) a Codexis dokonce 401 (99,51 %). Tato čísla znamenají, že z páru *U-R* se rozhodnutí *R* v dané databázi vyskytuje a vazbu mezi ustanovením a rozhodnutím by tedy bylo možné hypoteticky vytvořit. V případě ZOOÚ je z celkového počtu 262 párů možné v ASPI i v Codexisu možné vytvořit 257 z nich (98,1 %). V případě Beck-online je možné jich vytvořit 247 (94,27 %). Rozdíly mezi systémy co do dokumentů v nich obsažených tedy existují. Tímto ale není možné vysvětlit rozdíly v párech *U-R* (tedy rozhodnutích indexovaných jako souvisejících s určitým ustanovením) objevujících se v jednotlivých databázích. Zjednodušeně řečeno: je jen velmi malý počet rozhodnutí, které by se nenacházely ve všech třech systémech. Konkrétně se jedná o 19 rozhodnutí z celkového počtu 193 pro AutZ (obsah jednotlivých systémů je tedy shodný na 90,16 %) a o 9 rozhodnutí z celkových 154 pro ZOOÚ (obsah jednotlivých systémů je tedy shodný na 94,16 %).

Rozdíly mezi systémy tak primárně nejsou tvořeny tím, jestli se konkrétní rozhodnutí v příslušném systému nachází, ale opravdu tím, zda je dané rozhodnutí indexováno.

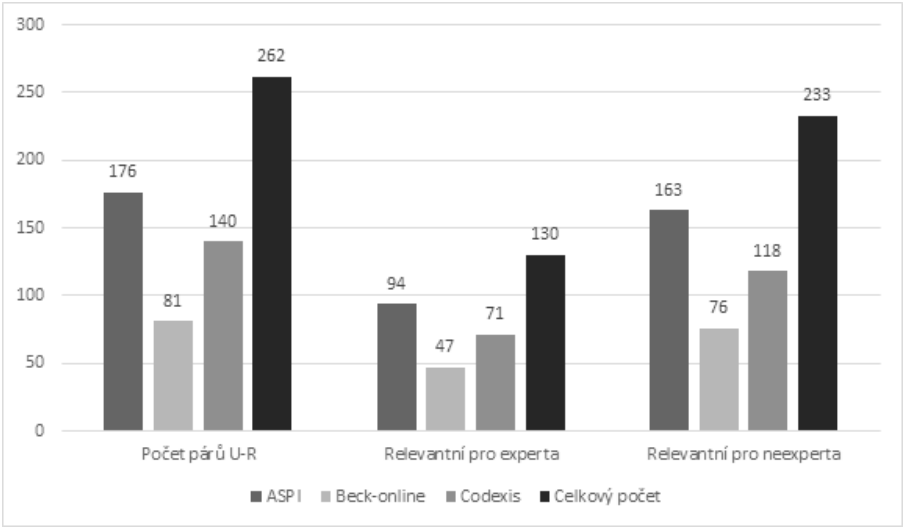
Ze 403 párů *U-R* tematicky relevantních (metadatově provázaných) pro AutZ jich expertní anotátor označil 107 (cca 26 %) jako kognitivně relevantní a neexpertní anotátor pak označil za relevantní 367 párů (cca 91 %). Z počtu 262 párů *U-R* tematicky relevantních pro ZOOÚ jich expertní anotátor označil za kognitivně relevantní 130 (cca 49 %) a neexpertní anotátor pak 233 (cca 90 %).

Společným základem, na kterém se tvůrci všech tří systémů shodli, je přítomnost 74 párů *U-R* v případě AutZ (cca 18 % celkového počtu) a 44 párů v případě ZOOÚ (cca 17 % celkového počtu).

Přehledněji jsou tyto statistiky znázorněné v rámci Obr. 1 a Obr. 2.



Obr. 1 Statistiky párů U-R pro ustanovení AutZ a jejich distribuce napříč systémy s přihlédnutím ke kognitivní relevanci pro expertního a neexpertního uživatele



Obr. 2 Statistiky párů U-R pro ustanovení ZOOÚ a jejich distribuce napříč systémy s přihlédnutím ke kognitivní relevanci pro expertního a neexpertního uživatele

Čísla, tedy počty párů *U-R* vyskytujících se v jednotlivých systémech, jsou tedy odlišná. Základní předpoklad, že při využití subjektivních metadat (tedy vazeb mezi ustanovením a soudním rozhodnutím) pro vyhledávání odlišná budou, se tak potvrdil.

V další části do analýzy zahrnu i kognitivní relevanci, čímž bude možné získat zajímavější vhled do existujících rozdílů mezi jednotlivými systémy. Kromě sumy, tedy prostého konstatování, že konkrétní systém obsahuje více či méně indexovaných párů *U-R* je po zařazení kognitivní relevance možné rozdíly kvantifikovat. Sjednocením množin rozhodnutí získaných z jednotlivých informačních systémů dojde k vytvoření onoho chybějícího autoritativního seznamu souvisejících rozhodnutí, byť pouze pro účely tohoto textu. Tento autoritativní seznam je pak možné porovnat s vyhledáváním v jednotlivých systémech a vypočíst přesnost *P*, úplnost *R* a míru *F1*. Pak můžeme srovnat výsledky poskytnuté jednotlivými systémy a diskutovat vhodnost použití různých vyhledávacích strategií z pozice různých typů uživatelů.

5.2 PODOBNOST VÝSLEDKŮ POSKYTOVANÝCH JEDNOTLIVÝMI SYSTÉMY

V této fázi je možné přikročit ke srovnání systémů. Za tímto účelem z idealizované databáze vzniklé sjednocením množin rozhodnutí získaných z právních informačních systémů ASPI, Beck-online a Codexis získáme výsledky pro jednotlivé právní informační systémy. Cílem je určit, jaká část párů *U-R* z idealizované databáze, se nachází v právním informačním systému ASPI, Beck-online a Codexis a jaká část výsledků v jednotlivých systémech je kognitivně relevantní z pohledu expertního a neexpertního uživatele. V Tab. 4 jsou uvedeny hodnoty přesnosti *P*, úplnosti *R a* míry *F1* vypočtené pro jednotlivé systémy a oba předpisy z pohledu expertního i neexpertního uživatele.

		ASPI			Beck-online			Codexis		
		P	R	F1	P	R	F1	P	R	F1
AutZ	Expertní uživatel	0,254	0,729	0,377	0,459	0,579	0,512	0,274	0,635	0,383
	Neexpertní uživatel	0,915	0,766	0,834	0,941	0,346	0,506	0,948	0,640	0,764
ZOOÚ	Expertní uživatel	0,534	0,723	0,614	0,580	0,362	0,445	0,507	0,546	0,526
	Neexpertní uživatel	0,926	0,700	0,797	0,938	0,326	0,484	0,843	0,506	0,633

Tab. 4 Evaluace výsledků vyhledávání jednotlivými systémy v idealizované databázi judikatury související s AutZ a ZOOÚ z pohledu expertního a neexpertního uživatele

Jakým způsobem tyto výsledky chápat vysvětlíme na příkladu výsledků ASPI. První řádek nám pro právní informační systém ASPI říká, že ze všech párů *U-R* nacházejících se v idealizované databázi, kde expertní anotátor označil rozhodnuti *R* jako relevantní pro pochopení ustanovení *U*, jsme vyhledáváním v ASPI dosáhli přesnosti 25,4 % a úplnosti 72,9 %. Vyhledávání v ASPI nám tedy poskytlo 72,9 % ze všech párů kognitivně relevantních pro expertního uživatele, které se vyskytují ve všech třech informačních systémech zařazených do tohoto textu. Přesnost 25,4 % pak ale znamená, že všechny tyto relevantní páry byly skryty v množství falešně

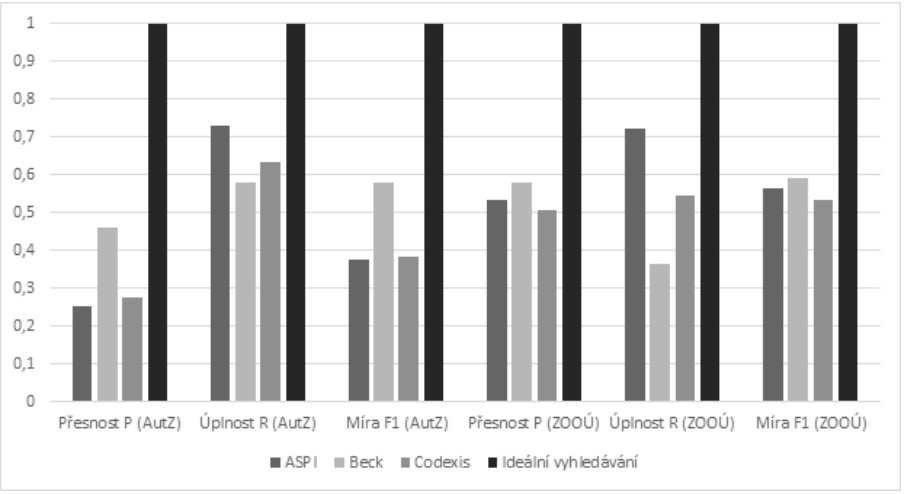
pozitivních výsledků, tedy výsledků, které expertní anotátor nepovažoval za relevantní, ale právní informační systém ASPI je zahrnul do seznamu výsledků.

Poněkud zjednodušeně tedy: pokud si manuálně zpracuji a ohodnotím všechna rozhodnutí, která jsou v právních informačních systémech navázána k AutZ, vykazuje vyhledávání v ASPI pokrytí tří z každé čtveřice relevantních rozhodnutí (to čtvrté bylo expertem posouzeno jako relevantní a zároveň bylo indexováno jiným systémem, než je ASPI). Toto je ale vykoupeno tím, že z každých čtyř rozhodnutí indexovaných v právním informačním systému ASPI vyhodnotil expert jako relevantní jenom jedno. Relativně malé procento relevantních rozhodnutí tedy zůstalo právním informačním systémem ASPI nezachycené (malý počet falešně negativních dokumentů), ale zároveň se jako uživatel budu muset při vyhodnocování výsledků probrat poměrně velkým množstvím dokumentů, které mi pro mé expertní chápání konkrétního ustanovení nepřinesou žádné informace (velký počet falešně pozitivních dokumentů).

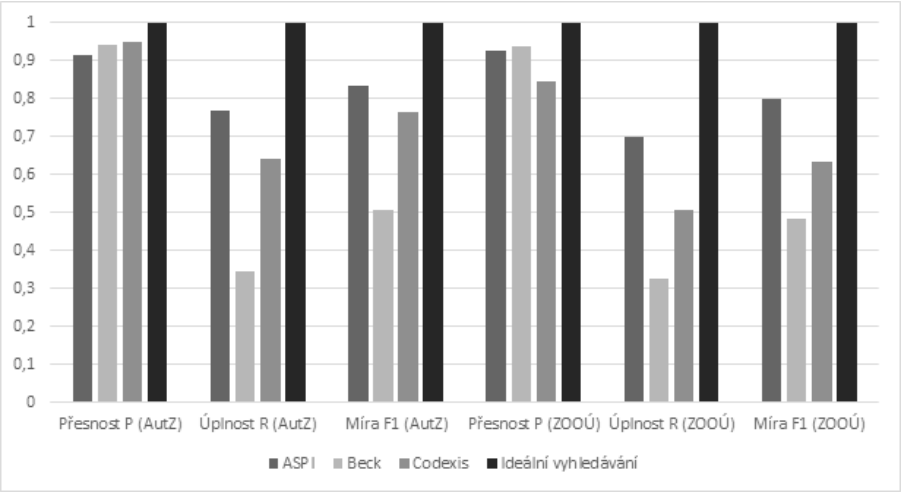
Situace je pak, celkem pochopitelně, odlišná pro neexpertního uživatele. Neexpertní anotátor totiž označil výrazně větší množství soudních rozhodnutí jako kognitivně relevantní. V důsledku nižší znalosti dané domény takovému uživateli přináší více soudních rozhodnutí nové informace. Pro takového uživatele bude mít metadatové vyhledávání v právním informačním systému ASPI, jak je evidentní z Tab. 4, přesnost P 91,5 % a úplnost R 76,6 %. Neexpertní uživatel tedy nedostane všechny dokumenty (zhruba každé čtvrté rozhodnutí označené anotátorem jako důležité mine). Na druhé straně mu ale více než devět z deseti rozhodnutí, které dostane v seznamu výsledků, přinese nové informace.

Srovnání jednotlivých metrik pro právní informační systémy ASPI, Beck-online a Codexis z pozice expertního uživatele je graficky znázorněno na Obr. 3 a z pozice neexpertního uživatele na Obr. 4. Ideálním vyhledáváním (míra $F1 = 1{,}00$), se kterým jsou hodnoty srovnávány, je onen perfektní stav, po kterém všichni při práci s právními informačními systémy toužíme. Tedy stav, kdy na svůj dotaz dostaneme (i) všechna rozhodnutí, která nám pomohou pochopit nebo aplikovat konkrétní ustanovení (úplnost $R = 1{,}00$)

a (ii) všechna rozhodnutí, která dostaneme, jsou pro nás relevantní (přesnost $P = 1{,}00$).



Obr. 3 Porovnání úspěšnosti vyhledávání mezi systémy s ideálním vyhledáváním z pozice expertního uživatele



Obr. 4 Porovnání úspěšnosti vyhledávání mezi systémy s ideálním vyhledáváním z pozice neexpertního uživatele

5.3 ZMĚNA V ÚSPĚŠNOSTI VYHLEDÁVÁNÍ PO ZAVEDENÍ PLNOTEXTOVÉHO PARAMETRU

V této fázi je možné přikročit ke srovnání systémů po zavedení plnotextového parametru. Za tímto účelem z idealizované databáze, vzniklé sjednocením množin rozhodnutí, získaných z právních informačních systémů ASPI, Beck-online a Codexis, získáme výsledky pro jednotlivé právní informační systémy. Cílem je určit, jaká část párů *U-R* z idealizované databáze se nachází v právním informačním systému ASPI, Beck-online a Codexis a jaká část výsledků v jednotlivých systémech je kognitivně relevantní z pohledu expertního a neexpertního uživatele, po zařazení plnotextového parametru nad rámec vyhledávání souvislostí. V Tab. 5 jsou uvedeny hodnoty přesnosti *P*, úplnosti *R* a míry *F1* vypočtené pro jednotlivé systémy a pro oba předpisy z pohledu expertního a neexpertního uživatele. V Tab. 6 je pak znázorněno, jakým způsobem se hodnoty změnily zařazením plnotextového parametru do vyhledávání rozhodnutí souvisejících s konkrétním ustanovením proti vyhledávání bez plnotextového parametru (jedná se tedy o rozdíl hodnot uvedených v Tab. 4 a hodnot uvedených v Tab. 5).

		ASPI			**Beck-online**			**Codexis**		
		P	R	F1	P	R	F1	P	R	F1
AutZ	Expertní uživatel	0,333	0,271	0,299	0,517	0,290	0,371	0,366	0,280	0,318
	Neexpertní uživatel	0,954	0,266	0,366	0,950	0,156	0,267	0,927	0,207	0,339
ZOOÚ	Expertní uživatel	0,602	0,500	0,546	0,612	0,315	0,416	0,606	0,485	0,539
	Neexpertní uživatel	0,963	0,446	0,610	0,955	0,275	0,426	0,913	0,408	0,564

Tab. 5 Evaluace výsledků vyhledávání jednotlivými systémy v idealizované databázi judikatury související s AutZ a ZOOÚ z pohledu expertního a neexpertního uživatele po zařazení plnotextového parametru

		ASPI			Beck-online			Codexis		
		P	R	F1	P	R	F1	P	R	F1
AutZ	Expertní uživatel	0,079 ↑	0,458 ↓	0,077 ↓	0,057 ↑	0,290 ↓	0,141 ↓	0,091 ↑	0,356 ↓	0,066 ↓
	Neexpertní uživatel	0,039 ↑	0,540 ↓	0,469 ↓	0,001 ↑	0,191 ↓	0,239 ↓	0,021 ↓	0,433 ↓	0,426 ↓
ZOOÚ	Expertní uživatel	0,068 ↑	0,223 ↓	0,069 ↓	0,032 ↑	0,046 ↓	0,029 ↓	0,010 ↑	0,061 ↓	0,013 ↑
	Neexpertní uživatel	0,037 ↑	0,253 ↓	0,187 ↓	0,017 ↑	0,051 ↓	0,057 ↓	0,071 ↑	0,099 ↓	0,069 ↓

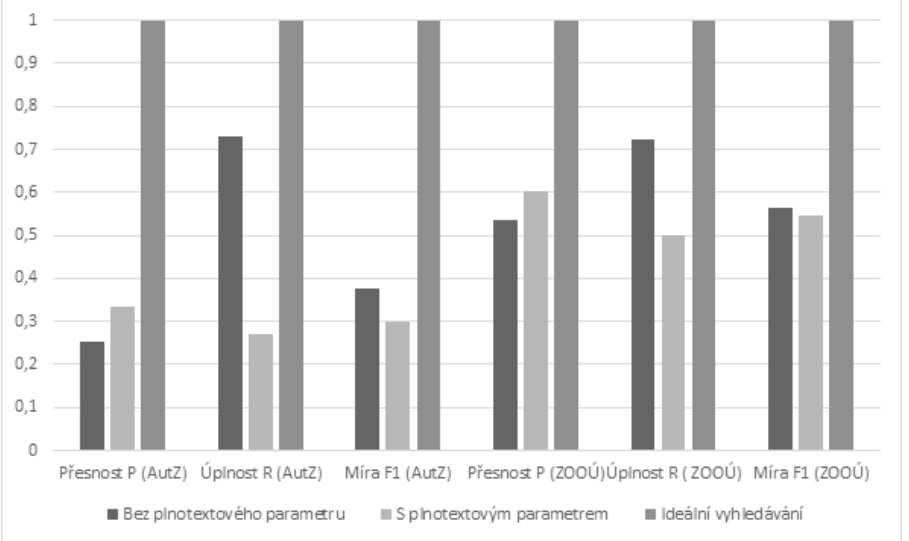
Tab. 6 Změna výsledků vyhledávání po zavedení plnotextového parametru proti vyhledávání bez plnotextového parametru

První řádek Tab. 5 nám (opět na příkladu výsledků ASPI) říká, že ze všech párů *U-R* nacházejících se v idealizované databázi, kde expertní anotátor označil rozhodnuti *R* jako relevantní pro pochopení ustanovení *U*, jsme vyhledáváním v ASPI po zařazení plnotextového parametru dosáhli přesnosti 33,3 % (zlepšení o 7,9 procentního bodu) a úplnosti 27,1 % (zhoršení o 45,8 procentních bodu). Vyhledávání v ASPI nám tedy poskytlo 27,1 % ze všech párů kognitivně relevantních pro expertního uživatele, které se vyskytují ve všech třech informačních systémech zařazených do tohoto textu. Přesnost 33,3 % pak ale znamená, že všechny tyto relevantní páry byly skryty v množství falešně pozitivních výsledků. Tedy výsledků, které expertní anotátor nepovažoval za relevantní, ale právní informační systém ASPI je zahrnul do seznamu výsledků.

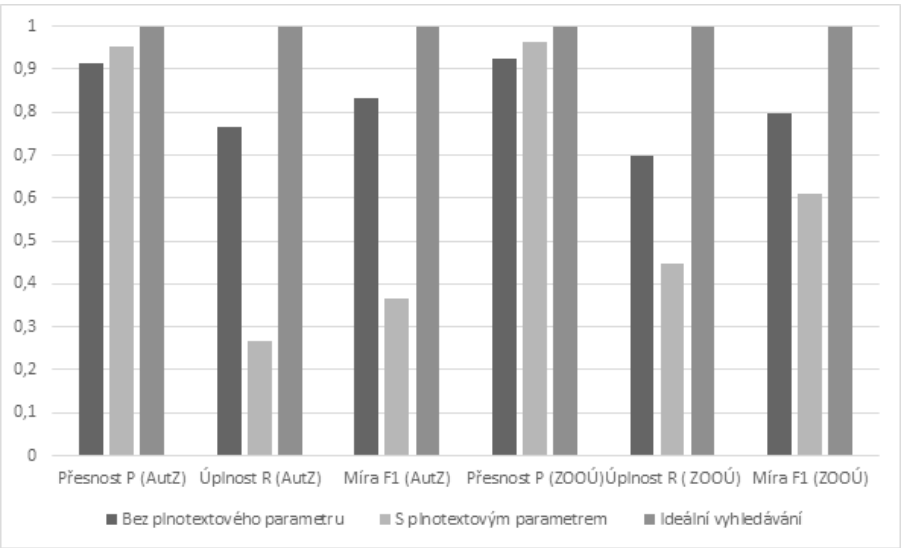
Poněkud zjednodušeně tedy: pokud si manuálně zpracuji a ohodnotím všechna rozhodnutí, která jsou v právních informačních systémech navázána k AutZ, vykazuje vyhledávání v ASPI po zařazení plnotextového parametru pokrytí jednoho z každé čtveřice relevantních rozhodnutí. Toto je pak doprovázeno tím, že z každých čtyř rozhodnutí indexovaných v právním informačním systému ASPI vyhodnotil expert jako relevantní jenom jedno. Část relevantních rozhodnutí tedy zůstala právním informačním systémem ASPI nezachycená (počet falešně negativních dokumentů). Zároveň se jako uživatel budu muset při vyhodnocování výsledků probrat poměrně velkým množstvím dokumentů, které mi pro mé expertní chápání konkrétního ustanovení nepřinesou žádné informace (počet falešně pozitivních dokumentů).

Stejně jako před zařazením plnotextového parametru je situace i v tuto chvíli odlišná pro neexpertního uživatele. Pro takového uživatele bude mít metadatové vyhledávání v právním informačním systému ASPI, jak je evidentní z Tab. 5 a Tab. 6, přesnost 95,4 % (zlepšení o 3,9 procentního bodu) a úplnost 26,6 % (zhoršení o 54 procentního bodu). Neexpertní uživatel tedy ani zdaleka nedostane všechny dokumenty (zhruba tři ze čtyř rozhodnutí označené anotátorem jako důležité mine). Na druhé straně mu ale více než devět z deseti rozhodnutí, které dostane v seznamu výsledků, přinese nové informace.

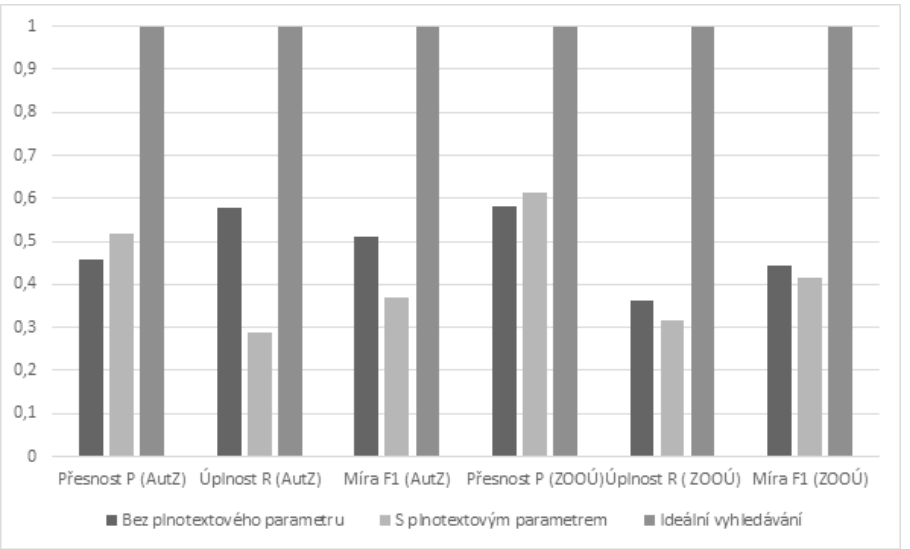
Srovnání jednotlivých metrik je tentokrát rozděleno na samostatné grafy pro jednotlivé právní informační systémy – Obr. 5 a 6 pro ASPI, Obr. 7 a 8 pro Beck-online a Obr. 9 a 10 pro Codexis. Toto zobrazení výsledků umožňuje jednoznačné srovnání úspěšnosti výsledků v jednotlivých systémech po zavedení plnotextového parametru. Dosažené hodnoty jsou opět srovnávány s ideálním vyhledáváním (míra $F1 = 1{,}00$), kdy dostáváme (i) všechna rozhodnutí, která nám pomohou pochopit nebo aplikovat konkrétní ustanovení (úplnost $R = 1{,}00$) a (ii) všechna rozhodnutí, která dostaneme, jsou pro nás relevantní (přesnost $P = 1{,}00$).



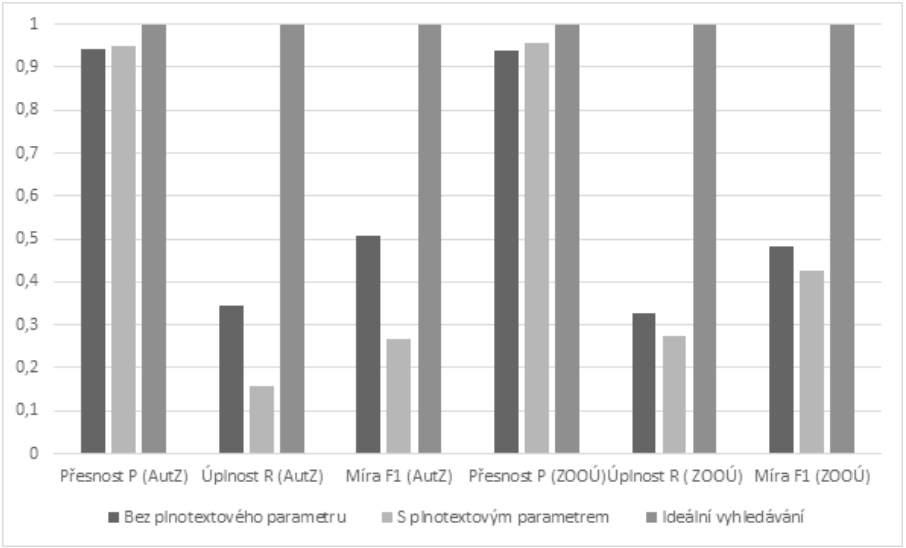
Obr. 5 Porovnání úspěšnosti vyhledávání v ASPI z pozice expertního uživatele před zadáním plnotextového kritéria a po jeho zadání



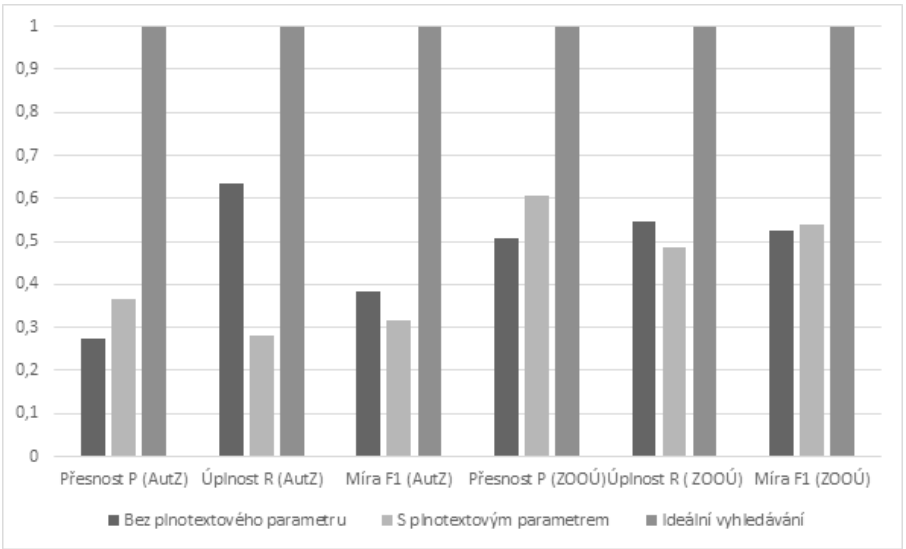
Obr. 6 Porovnání úspěšnosti vyhledávání v ASPI z pozice neexpertního uživatele před zadáním plnotextového kritéria a po jeho zadání



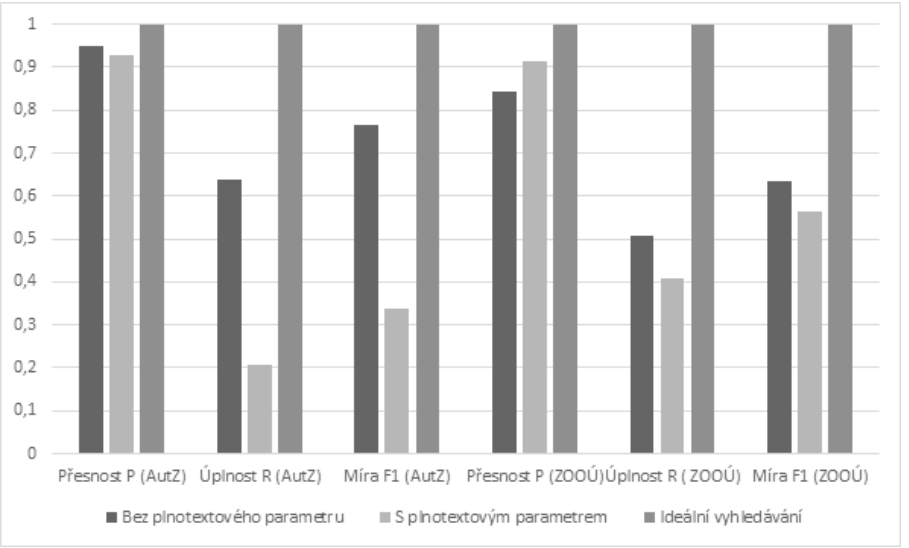
Obr. 7 Porovnání úspěšnosti vyhledávání v Beck-online z pozice expertního uživatele před zadáním plnotextového kritéria a po jeho zadání



Obr. 8 Porovnání úspěšnosti vyhledávání v Beck-online z pozice neexpertního uživatele před zadáním plnotextového kritéria a po jeho zadání



Obr. 9 Porovnání úspěšnosti vyhledávání v Codexis z pozice expertního uživatele před zadáním plnotextového kritéria a po jeho zadání



Obr. 10 Porovnání úspěšnosti vyhledávání v Codexis z pozice neexpertního uživatele před zadáním plnotextového kritéria a po jeho zadání

5.4 PODOBNOST MEZI SYSTÉMY PO ZAVEDENÍ PLNOTEXTOVÉHO PARAMETRU

Nyní je konečně nutné zjistit, zda zavedení plnotextového parametru vedlo k menším rozdílům mezi výsledky poskytnutými jednotlivými právními informačními systémy. Za tímto účelem je nutné zjistit variabilitu mezi hodnotami výsledků jednotlivých systémů při vyhledávání skrze zprostředkované informace (metadatová vazba mezi ustanovením a soudním rozhodnutím) a při vyhledávání skrze kombinaci zprostředkovaných a nezprostředkovaných informací (metadatová vazba mezi ustanovením a soudním rozhodnutím doprovázená plnotextovým parametrem). Jak je vidět z předcházejícího textu, zavedení plnotextového kritéria do vyhledání nevedlo ke zlepšení výsledků – zlepšila se přesnost pro většinu vyhledávání, ale došlo k výraznému snížení úplnosti. Směrodatné odchylky mezi hodnotami jsou v Tab. 7. Na prvním řádku je ve druhém sloupci směrodatná odchylka vypočtená z hodnot přesnosti výsledků poskytnutých právními informačními systémy ASPI, Beck-online a Codexis při vyhledávání expertním uživatelem před zavedením plnotextového parametru. Po zavedení plnotextového para-

metru je hodnota téhož uvedena ve druhém sloupci. Jak je vidět, je nižší – a toto platí pro všechna vyhledávání, ať už expertní či neexpertní a pro AutZ a ZOOÚ. Zavedení plnotextového kritéria jakožto kritéria, které umožňuje nezprostředkované vyhledávání (ve všech systémech je stejné), a jako doplňku ke zprostředkovanému vyhledávání (které je v každém systému jiné), vede ke statisticky podobnějším výsledkům. Ve všech případech je směrodatná odchylka výsledků vyhledávání v systémech bez plnotextového kritéria větší než s plnotextovým kritériem.

		Přesnost *P* (bez pln.)	Přesnost *P* (pln.)	Úplnost *R* (bez pln.)	Úplnost *R* (pln.)	Míra *F1* (bez pln.)	Míra *F1* (pln.)
AutZ	Expertní uživatel	0,092	0,080	0,062	0,008	0,062	0,031
	Neexpertní uživatel	0,014	0,012	0,176	0,030	0,141	0,042
ZOOÚ	Expertní uživatel	0,030	0,004	0,148	0,084	0,069	0,060
	Neexpertní uživatel	0,042	0,022	0,152	0,074	0,128	0,078

Tab. 7 Směrodatné odchylky výsledků dosažených při vyhledávání bez plnotextového parametru (bez pln.) a po zařazení plnotextového parametru (pln.)

6. DISKUZE A LIMITY

V této části se pokusím některé výsledky dále interpretovat a zároveň předestřít limity výzkumu prezentovaného v tomto textu. Těchto limitů je, jak bude za chvíli zřejmé, nemálo a jsou pro pochopení tohoto textu zcela zásadní.

Jakákoli interpretace výsledků je za prvé ovlivněna tím, že srovnání vyhledávání soudních rozhodnutí souvisejících pouze se dvěma předpisy (AutZ, ZOOÚ) poskytlo málo dat na zcela jasné a prokazatelné závěry. Jakkoli bylo manuální zpracování dat ze tří zařazených systémů časově náročné, stejně jako bylo náročné i jejich anotování, jednalo se spíše o práci mravenčí než o práci po stránce dat impozantní svým rozsahem. Tím je některé závěry nutné považovat automaticky za slabší, než by mohly být při zpracování výrazně většího datasetu. Podobně by mohlo být srovnání průkaznější při zpracování rozsáhlejšího předpisu, který má za sebou dlouhou historii (např. zákon č. 141/1961 Sb.) nebo s jehož praktickou aplikací jsou

spojeny těžkosti ohledně kontinuity judikatury (např. zákon č. 89/2012 Sb.).

Výsledky výrazně ovlivňuje i volba plnotextového dotazu, který byl zařazen jako druhý parametr do zprostředkovaného vyhledávání založeného na subjektivních metadatech. Plnotextový dotaz byl zvolen s přihlédnutím ke slovům, která jsou typická pro celý předpis a nikoli pro konkrétní ustanovení. Skrze tento limit je nutné chápat výrazný pokles v úplnosti vyhledávání po zařazení plnotextového parametru. Na první pohled tedy zavedení plnotextového parametru vede k výrazně horším celkovým výsledkům při zcela marginálním zvýšení přesnosti. To je ale způsobeno spíše výběrem konkrétního plnotextového dotazu a výsledek je tak dle mého názoru spíše ilustrativní.

Posledním výrazným limitem tohoto textu je proces vyhodnocování kognitivní důležitosti jednotlivých soudních rozhodnutí z párů *U-R*. Využil jsem jednoho expertního anotátora pro AutZ, jednoho expertního anotátora pro ZOOÚ a jednoho neexpertního anotátora pro oba předpisy. Anotace tímto způsobem je velmi subjektivní. Zvýšení kvality při hodnocení kognitivní relevance jednotlivých rozhodnutí by bylo možné při zařazení většího množství anotátorů v rámci paralelních anotací (kognitivní relevance by pak byla hodnocena pro stejný pár *U-R* více než jedním anotátorem). Při čtení tohoto textu je nutné shora uvedené limity vést v patrnosti.

Co je tedy možné ze shora popsané evaluace vyvozovat? Zjednodušený model, který s kolegy používáme jako názornou pomůcku při výuce, je očividně poměrně přesný. Mezi výsledky poskytovanými jednotlivými právními informačními systémy v rámci dotazu využívajícího subjektivní metadata (rozhodnutí související s konkrétním ustanovením) jsou opravdu poměrně velké rozdíly. Množství párů *U-R*, které byly ze systémů ASPI, Beck-online a Codexis vytěženy, je odlišné. Z toho ale nelze automaticky usuzovat, že by systémy, nabízející více párů (typicky ASPI a Codexis) byly nutně lepší než ty, které jich nabízejí méně (typicky Beck-online). Zde je na místě jistá opatrnost při interpretaci. Mám za to, že tento rozdíl spíše ukazuje na odlišný způsob vytváření vazeb mezi ustanoveními a soudními rozhodnutími. Při vytváření těchto vazeb v systému Beck-online je nejspíše

postupováno konzervativněji, než v případě vytváření vazeb v systémech ASPI a Codexis.

Vyhodnocení výsledků (přesnosti *P*, úplnosti *R* a míry *F1*) po zařazení kognitivní relevance tomuto závěru nasvědčuje. Expertní anotátoři jak v případě AutZ, tak ZOOÚ vyhodnotili některá rozhodnutí jako relevantní pro jejich chápání konkrétního ustanovení a Beck-online v tomto hodnocení vykazuje vyšší hodnotu přesnosti, ale nižší úplnost. Výsledky poskytnuté systémy ASPI a Codexis pak dávají více možností, jak zachytit kognitivně relevantní dokumenty. Tyto rozdíly ale nejsou dle mého nijak zásadní. V případě obou odborníků se nicméně při hodnocení vyhledávání dostal dopředu Beck-online.

Neodborník, celkem pochopitelně, označil jako kognitivně relevantní velkou část všech párů *U-R*, protože jeho doménová znalost je nižší. Tímto se dostaly ve výsledcích dopředu právě systémy, u kterých je možné konstatovat tendenci označovat vazbou mezi ustanovením a rozhodnutím větší množství rozhodnutí (ASPI a Codexis). Pokud uživatel o dané problematice téměř nic neví, bude většina nalezených dokumentů kognitivně relevantní (tedy bude automaticky dosaženo vysoké přesnosti). Takový uživatel pak může těžit z toho, že při použití systému ASPI a Codexis dosáhne větší úplnosti svého vyhledávání.

Při komplexním pohledu na výsledky tak opatrně uzavírám, že při zpracování dat pro Beck-online dochází k vyznačení spíše menšího množství vazeb – hodnocení tématické relevance při tvorbě systému je tedy spíše konzervativnější. Důsledkem je, že je větší šance, že budou takto vyznačené vazby kognitivně relevantní pro expertního uživatele. Naopak v případě systémů ASPI a Codexis to vypadá, že jsou rozhodnutí provazována k jednotlivým ustanovením po překročení nižší hranice. To vede k většímu množství falešných pozitiv při vyhledávání, ale zároveň je oproti Beck-online menší šance, že „něco uteče".

A konečně, zařazení plnotextového parametru do vyhledávání vede k výsledkům, které jsou si napříč systémy statisticky podobnější. Kombinace zprostředkovaného (subjektivní metadata) a nezprostředkovaného (data) vyhledávání sice v tomto konkrétním případě výrazně zhoršilo metriky, po-

mocí kterých jsem vyhledávání hodnotil, ale potvrdilo domněnku, že zařazení dat a objektivních metadat do vyhledávání povede k „objektivnějším“ (napříč systémy podobnějším) výsledkům. Výrazné zhoršení výsledků po zařazení plnotextového parametru není dle mého názoru příliš znepokojivé – hovoří spíše o nevhodné zvoleném parametru v rámci tohoto výzkumu než o negativním vlivu plnotextových parametrů na vyhledávání obecně.

7. ZÁVĚR

V odpovědi na první výzkumnou otázku je tedy nutné uvést, že rozdíly mezi výsledky poskytnutými jednotlivými právními informačními systémy v odpovědi na dotaz obsahující subjektivní metadata opravdu existují. A to poměrně výrazné. Srovnatelné dotazy vyhledávající soudní rozhodnutí související s jednotlivými ustanoveními vedly k identifikaci odlišných dokumentů navázaných na jednotlivá ustanovení AutZ a ZOOÚ. Průnik množin dokumentů provázaných v jednotlivých systémech dosahoval pouze cca 18 % z celkového počtu vazeb u AutZ a pouze cca 17 % z celkového počtu vazeb u ZOOÚ. Po zohlednění kognitivní relevance pro vyhledávání z pohledu expertního a neexpertního uživatele jsou rozdíly mezi systémy značné. Za velmi důležité považuji uvést, že nízký poměr párů *U-R*, které se vyskytují ve všech systémech, má velmi praktický dopad – v podstatě máme čísla, která podporují argument o vhodnosti paralelního využití více právních informačních systémů pro zpracování rešerše. Ideální vyhledávací strategií se jeví využití alespoň dvou informačních systémů. To je sice časově i finančně náročnější, ale jsme pak při vyhledávání schopni identifikovat více relevantních párů a tím dosáhnout větší úplnosti vyhledávání. Jakkoli je přesnost důležitou metrikou, obecně považuji za menší problém získat v seznamu výsledků dokument, který pro mě není relevantní a musím ho vyřadit, než minout relevantní dokument.

V odpovědi na druhou výzkumnou otázku uzavírám, že zavedení plnotextového parametru do vyhledávání obecně zvýšilo přesnost vyhledávání, ale snížilo jeho úplnost. Dosažení vyšší přesnosti a nižší úplnosti přímo vychází z logiky věci. Pokud do vyhledávání doplníme plnotextový parametr,

vyhledávání se pak vlastně skládá ze dvou parametrů. Může tedy dojít k vyřazení některých dokumentů, které byly v seznamu výsledků zařazeny po metadatovém vyhledávání, ale již nemůže dojít k zařazení těch, které první parametr nenaplnily. Logicky tedy dojde ke zvýšení přesnosti (pokud se nám podaří plnotextovým dotazem vyřadit některé původně falešně pozitivní dokumenty), ale ke snížení úplnosti (pokud plnotextovým dotazem vyřadíme dokumenty, které byly původně pravými pozitivy). Podstatné v tomto případě bylo, že téměř vždy došlo k drobnému navýšení přesnosti. Podobně došlo vždy k poklesu úplnosti, často výraznému. To naznačuje, že plnotextový parametr nebyl zvolen zcela optimálně, což je jeden z výrazných limitů tohoto textu.

V odpovědi na třetí výzkumnou otázku je pak nutné uzavřít, že zavedení plnotextového kritéria vedlo k dosažení statisticky podobnějších výsledků napříč jednotlivými informačními systémy. Vyhledávání prostřednictvím zprostředkované strategie (využití subjektivních metadat) přineslo po dodatečném zařazení parametrů z nezprostředkované strategie (využití dat) výsledky, které jsou si napříč systémy podobnější.

Tato oblast – v užším smyslu evaluace výsledků získaných vyhledáváním v právních informačních systémech, v širším smyslu pak kritický přístup k vyhledávání v právních informačních systémech a k volbě vyhledávacích strategií – má dle mého názoru poměrně hodně potenciálu pro další akademický i praktický zájem. Zejména je dle mého názoru nutné ubírat se třemi směry. Za prvé pokusit se o komparaci na rozsáhlejších datech. Jak jsem již uvedl v tomto textu, vhodným se jeví zařazení některého rozsáhlého kodexu, zejména pak zákona č. 89/2012 Sb. Za druhé považuji za zajímavý směr pokusit se určit, zda mnou popsané rozdíly ve vyhledávání mají (a případně jak velký) praktický dopad. Je možné na základě sady dokumentů identifikované v jednom informačním systému dojít k odlišnému závěru než při zohlednění dokumentů získaných vyhledáváním v jiném informačním systému? Zjištění, zda nám sady dokumentů získané z různých systémů přinášejí odlišné informace, by mělo velký praktický význam. Za třetí by pak bylo dle mého názoru zajímavé věnovat se volbě optimální vyhledávací strategie v návaznosti na použité informační systémy a časovou do-

taci. Vyčíslení nákladů na vyhledávání by, opět dle mého názoru, mohlo vést k optimalizaci některých procesů v praxi, ale i ve výuce.[36]

V tomto textu jsem se pokusil představit kritický přístup k právním informačním systémům. Evaluace vyhledávání v jednotlivých systémech s přihlédnutím k využití různých vyhledávacích strategií, jakož i evaluace vyhledávání napříč jednotlivými systémy, by měla být běžnou součástí úvah o práci s právními informačními systémy. Tyto úvahy navíc nejsou pouze teoretické, ale mají velmi silné implikace v rovině zajištění efektivního vyhledávání právních informací. Kritický přístup k vyhledávání v právních informačních systémech může pomoci rozvoji informační gramotnosti právníků.

PODĚKOVÁNÍ

Vznik tohoto textu byl podpořen Grantovou agenturou ČR v rámci projektu GA17-20645S.

Rád bych poděkoval Tereze Novotné, Janu Zibnerovi a Jakubu Míškovi za asistenci se zpracováním dat. Tereza Novotná si zaslouží ještě druhé poděkování, protože její komentáře k první verzi tohoto textu mi jej umožnily výrazně vylepšit.

Dřívější verze tohoto textu a různé části popsaného evaluačního experimentu byly prezentovány na konferencích *Qualitative Research in Law Conference* (název příspěvku *Collecting Case Law for Qualitative Content Analysis: What is the Correct 'Population'?*) v říjnu 2018 v Brně, *Internationales Rechtsinformatik Symposion IRIS* (název příspěvku *Case Law Retrieval: Critical Evaluation of Czech Legal Information Retrieval Systems*) v únoru 2019 v Salzburku a na konferenci *COFOLA* (název příspěvku *Efektivnost vyhledávání v právních informačních systémech: Porovnání strategií využívajících zprostředkované a nezprostředkované údaje k vyhledání relevantních soudních rozhodnutí*) v dubnu 2019 v Telči. Měl jsem také skvělou možnost představit východiska jako na *Work in Progress* semináři na Ústavu práva a tech-

[36] Srov. WILENSKY, Beth. When Should We Teach Our Students to Pay Attention to the Costs of Legal Research? *Perspectives: Teaching Legal Research and Writing*. 2016, roč. 26, č.1-2, s. 41-46.

nologií PrF MU v říjnu 2018. Na všech těchto akcích se mi dostalo cenných kritických připomínek, za které velmi děkuji.

8. LITERATURA

[1] ARREDONDO, Pablo. Shepard for a Day: A Novel Class Exercise for Teaching Citators. *Legal Reference Service Quarterly*, 2015, roč. 34, č. 3, s. 239-244.

[2] ASHLEY, Kevin. *Artificial Intelligence and Legal Analytics*: *New Tools for Law Practice in the Digital Age.* Cambridge: Cambridge University Press, 2017.

[3] BING, Jon. Legal Information Retrieval Systems: The Need for and the Design of Extremely Simple Retrieval Strategies. *Computer/Law Journal*, 1978, roč. 1, č. 1, s. 379-400.

[4] BING, Jon. Performance of Legal Text Retrieval Systems: The Curse of Boole. *Law Library Journal*, 1987, roč. 79, č. 2, s. 187-202.

[5] BLAIR, David a M. E. MARON. An Evaluation of Retrieval Effectiveness for a Full-Text Document-Retrieval System. *Communications of the ACM,* 1985, roč. 28, č. 3, s. 289-299.

[6] BOBEK, Michal. Výzkum v právu: reklama na Nike anebo kvantová fyzika? *Jurisprudence*, 2016, roč. 25, č. 6, s. 3-10.

[7] DABNEY, Daniel. The Curse of Thamus: An Analysis of Full-Text Legal Document Retrieval, *Law Library Journal,* 1986, roč. 78, č. 5, s. 5-40.

[8] GERSON, Kevin. Evaluating Legal Information Retrieval Systems: How Do the Ranked-Retrieval Methods of WESTLAW and LEXIS Measure Up? *Legal Reference Services Quarterly*, 1999, roč. 17, č. 4, s. 53-67.

[9] GRABMAIR, Matthias, Kevin ASHLEY, Ran CHEN, Preethi SURESHKUMAR, Chen WANG, Eric NYBERG a Vern WALKER. Introducing LUIMA: an Experiment in Legal Conceptual Retrieval of Vaccine Injury Decisions Using a UIMA Type System and TOOLS. *Proceedings of ICAIL 2015*. S. 69-78.

[10] HAFNER, Carole. Conceptual Organization of Case Law Knowledge Bases. *Proceedings of ICAIL* 1987. S. 35-42.

[11] HARAŠTA, Jakub. Nejednoznačnost odkazů k soudním rozhodnutím a možnosti řešení. *Revue pro právo a technologie*, roč. 6, č. 11, s. 15-28.

[12] HELLYER, Paul. Evaluating Shepard's, KeyCite, and BCite for Case Validation Accuracy. *Law Library Journal*, 2018, roč. 110, č. 4, s. 449-476.

[13] KNAPP, Melanie a Rob WILLEY. Comparison of Research Speed and Accuracy Using Westlaw Classic and WestlawNext. *Legal Reference Services Quarterly*, 2013, roč. 32, č. 1-2, s. 126-141.

[14] KOSAŘ, David a Jan PETROV. Jak vybrat „případy" do případové studie a pracovat s nimi v právu: poznatky z výzkumu na pomezí práva a politologie. *Jurisprudence*, 2016, roč. 25, č. 6, s. 21-30.

[15] MART, Susan Nevelow. The Case for Curation: The Relevance of Digest and Citator Results in Westlaw and Lexis. *Legal Reference Services Quarterly*, 2013, roč. 32, č. 1-2, s. 13-53.

[16] MAXWELL, Tamsin a Burkhard SCHAFER. Concept and Context in Legal Information Retrieval. *Proceedings of Jurix 2008*. S. 63-72.

[17] SORMUNEN, Eero. Extensions to the STAIRS Study – Empirical Evidence for the Hypothesised Ineffectiveness of Boolean Queries in Large Full-Text Databases. *Information Retrieval*, 2001, roč. 4, č. 3-4, s. 257-273.

[18] ŠAVELKA, Jaromír, Matěj MYŠKA, Adam PTAŠNIK a Danuše SPÁČILOVÁ. *Právní informační systémy*. Brno: Tribun EU, 2011.

[19] TAYLOR, William L. Comparing KeyCite and Shepard's for Completeness, Currency, and Accuracy. *Law Library Journal*, 2000, roč. 92, č. 2, s. 127-142.

[20] TURTLE, Howard. Natural Language vs. Boolean Query Evaluation: A Comparison of Retrieval Performance. *Proceedings of SIGIR 1994. S*. 212-220.

[21] URBÁNIKOVÁ, Marína a Hubert SMEKAL. Právní věda a právní psaní: postačí vždy jako výzkumná metoda "číst, přemýšlet a psát"? *Jurisprudence*, 2017, roč. 26, č. 4, s. 37-41.

[22] VAN OPIJNEN, Marc a Cristiana SANTOS. On the Concept of Relevance in Legal Information Retrieval. *Artificial Intelligence and* Law, 2017, roč. 25, č. 1, s. 65-87.

[23] WILENSKY, Beth. When Should We Teach Our Students to Pay Attention to the Costs of Legal Research? *Perspectives: Teaching Legal Research and Writing*. 2016, roč. 26, č.1-2, s. 41-46.

INSTRUCTIONS FOR AUTHORS

The Review of Law and Technology is a peer-reviewed scientific journal for technological areas of law and jurisprudence.

Since 1st January 2015 the journal is listed in the List of non-impact peer-reviewed journals published in the Czech Republic and since 24th June 2015 in ERIH PLUS database.

Contributions submitted for the Topic and Discussion sections are anonymously peer-reviewed by at least two independent reviewers and the final decision on publication is the in the sole discretion of the editorial board. Review process takes approximately one month. The submissions are not subject to language proofreading.

Contributions shall be submitted through our web-based system available at www.revue.law.muni.cz.

RECOMMENDED EXTENT OF THE CONTRIBUTIONS:

Topic section:	30 – 80 standard pages
Discussion section:	5 – 30 standard pages
Case annotation:	2 – 10 standard pages
Book review:	1 – 5 standard pages

(including spaces, footnotes and bibliography)

CITATIONS FORMAT

Citations shall be in accordance with the ISO 690:2011 citation standard.

Referencing examples are available in interpretations of the aforementioned citation standard (e. g. at www.ezdroje.muni.cz/prehled/zdroj.php?lang=en&id=441).

Individual sources are referenced in the text by upper index. The actual citation of the source is then contained in a footnote.

DEADLINES FOR CONTRIBUTIONS SUBMISSIONS

For the summer issue: 31st March

For the winter issue: 30th September

The Review of Law and Technology is a gold open access journal.

Contributions are included into respective electronic legal information systems operated by Wolters Kluwer ČR, a. s. (ASPI), Nakladatelství C. H. BECK, s. r. o. (beck-online.cz) and ATLAS consulting spol. s r. o. (CODEXIS).

Detailed information about the publication process, structure and format of the contributions, the review process and copyright are available in the “For the authors” section at www.revue.law.muni.cz. Further information is available upon request addressed to editorial staff (contact e-mail revue@law.muni.cz).

REVIEW OF LAW AND TECHNOLOGY

VOLUME 11 | YEAR 2020 | NUMBER 22

DISCUSSION

ANNOTATION

BOOK REVIEW

TOPIC

Review of Law and Technology
Peer-reviewed scientific journal for technological areas of law and jurisprudence, listed in the List of non-impact peer-reviewed journals published in the Czech Republic and ERIH PLUS database.
Only the contributions submitted for the Discussion and Topic sections are peer-reviewed.
Published bi-annually. This issue was published on 31st December 2020.
ISSN 1804-5383 (Print), ISSN 1805-2797 (Online), Ev. nr. MK ČR E 19707
Published by: Masaryk University, Žerotínovo nám. 9, 601 77 Brno, Czech Republic, ID-Nr. 00216224
Editor-in-chief and contact person: JUDr. Matěj Myška, Ph.D., Institute of Law and Technology, Faculty of Law, Masaryk University, Veveří 70, 611 80 Brno, Czech Republic, tel: +420 549494751, fax: +420 541210604, e-mail: revue@law.muni.cz | www.revue.law.muni.cz
Deputy editor-in-chief: Ing. Mgr. František Kasl
Editorial Staff: JUDr. Mgr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek, Ph.D.
Editorial Secretary: Anna Blechová
Editors: Anna Blechová, Martin Erlebach
Editorial Board: doc. JUDr. Radim Polčák, Ph.D. (honorary chairman), JUDr. Zuzana Adamová, Ph.D., prof. JUDr. Michael Bogdan, B.A., LL.M., jur. dr. (Lund), JUDr. Marie Brejchová, LL.M., JUDr. Jiří Čermák, doc. JUDr. Bc. Tomáš Gřivna, Ph.D., doc. JUDr. Josef Kotásek, Ph.D., JUDr. Bc. Zdeněk Kučera, Ph.D., Mgr. Ing. Zbyněk Loebl, LL.M., JUDr. Ján Matejka, Ph.D., prof. RNDr. Václav Matyáš, M.Sc., Ph.D., JUDr. Matěj Myška, Ph.D., Mgr. Antonín Panák, LL.M., Mgr. Bc. Adam Ptašnik, Ph.D., JUDr. Danuše Spáčilová, JUDr. Eduard Szattler, Ph.D., JUDr. Tomáš Ščerba, Ph.D.
Layout: Mgr. Martin Loučka, JUDr. Matěj Myška, Ph.D.
Print: POINT CZ, s.r.o., Milady Horákové 20, 602 00 Brno
The publication of this issue of the Review of Law and Technology was funded by the project „Právo a technologie VIII“, MUNI/A/0989/2019.

MUNI LAW

Ústav práva a technologií

děkuje našim partnerům za podporu v roce 2020

ROWAN LEGAL

vodafone

pwc

PwC Legal

CODEXIS®

Zákony pro lidi.cz

PRÁVNÍ PROSTOR

Diskuze

Anotace

Recenze

Téma

MUNI PRESS