27

REVUE PRO PRÁVO A TECHNOLOGIE

Ústav práva a technologií Právnické fakulty Masarykovy univerzity

Ročník 14 / Rok 2023 / Číslo 27

Revue.law.muni.cz

XV. národní konference | 14. - 15. září 2023, Právnická fakulta, MUNI, Brno

České právo a informační technologie 2023

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

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

Pořadatel konference vyzývá zájemce o aktivní účast, aby hlásili své příspěvky do některé z odborných sekcí. Rozšířený abstrakt v rozsahu 1-2 stran obsahující strukturu příspěvku, výzkumnou otázku a zásadní myšlenky, které budou v prezentaci představeny, posílejte do **31. 7. 2023** na adresu **cpit@law.muni.cz**.
O přijetí příspěvku k prezentaci bude rozhodnuto do 15. 8. 2023.

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

Další informace na webu cpit.law.muni.cz

Předběžný program konference

Čtvrtek 14. září 2023

plenární panelová diskuse

Směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii (NIS 2) a její transpozice

Moderuje: Radim Polčák
Panelisté: TBA

paralelní sekce

Právní informatika

Moderuje: Jakub Harašta
velké jazykové modely; umělá inteligence; strojové učení; získávání právních informací; změny v právním vzdělávání a právní praxi

Aktuální otázky práva duševního vlastnictví

Moderuje: Matěj Myška
upload filtry; uživatelská práva; výjimky a omezení absolutních práv; ochrana software; vymáhání; generativní umělá inteligence; užití ochranných známek online

Právní otázky autonomních systémů

Moderuje: Veronika Příbaň Žolnerčíková
bezpečnost (safety & security); odpovědnost; transparentnost; neosobní data; vytěžování big data

Data governance

Moderuje: Jakub Míšek
nařízení o správě dat; datový altruismus; ochrana prostých dat; harmonizační legislativa; řízený přístup k datům; data veřejného sektoru

Pátek 15. září 2023

paralelní sekce

Ochrana osobních údajů

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

Elektronické důkazy

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

Elektronizace státní správy, online soudnictví

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

Kybernetická bezpečnost a obrana

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

REVUE PRO PRÁVO A TECHNOLOGIE

ROČNÍK 14 | ROK 2023 | ČÍSLO 27

Revue pro právo a technologie
Odborný recenzovaný časopis pro technologické obory práva a právní vědy zařazený na Seznamu recenzovaných neimpaktovaných periodik vydávaných v České republice a v databázi ERIH PLUS.
Recenzovány jsou příspěvky v sekci Diskuze a Téma.
Vychází dvakrát ročně. Toto číslo vyšlo 30. 6. 2023.
ISSN 1804-5383 (Print), ISSN 1805-2797 (Online), Ev. č. MK ČR E 19707
Vydává Masarykova univerzita, Žerotínovo nám. 9, 601 77 Brno, ČR, IČ 00216224
Šéfredaktor a kontaktní osoba: JUDr. Ing. František Kasl, Ph.D., Ústav práva a technologií Právnické fakulty Masarykovy univerzity, Veveří 70, 611 80 Brno, ČR, telefonní kontakt: +420 549 49 5545, kontaktní e-mail: frantisek.kasl@muni.cz | revue@law.muni.cz | https://journals.muni.cz/revue
Zástupkyně šéfredaktora: Mgr. Anna Blechová
Redakce: JUDr. Mgr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek, Ph.D.
Editor: Martin Erlebach
Redakční rada: prof. JUDr. Radim Polčák, Ph.D. (čestný předseda), JUDr. Zuzana Adamová, Ph.D., prof. JUDr. Michael Bogdan, B.A., LL.M., jur. dr. (Lund), JUDr. Marie Brejchová, LL.M., JUDr. Jiří Čermák, prof. JUDr. Bc. Tomáš Gřivna, Ph.D., doc. JUDr. Josef Kotásek, Ph.D., JUDr. Bc. Zdeněk Kučera, Ph.D., Mgr. Ing. Zbyněk Loebl, LL.M., JUDr. Ján Matejka, Ph.D., prof. RNDr. Václav Matyáš, M.Sc., Ph.D., doc. JUDr. Matěj Myška, Ph.D., Mgr. Antonín Panák, LL.M., Mgr. Bc. Adam Ptašnik, Ph.D., JUDr. Danuše Spáčilová, JUDr. Eduard Szattler, Ph.D., JUDr. Tomáš Ščerba, Ph.D.
Grafická úprava: Mgr. Martin Loučka, doc. JUDr. Matěj Myška, Ph.D.
Tisk: POINT CZ, s.r.o., Milady Horákové 20, 602 00 Brno
Vydání tohoto čísla časopisu Revue pro právo a technologie bylo financováno z projektu „Právo a technologie XI", MUNI/A/1293/2022.

POKYNY PRO AUTORY

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

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

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

Příspěvky se podávají prostřednictvím redakčního systému dostupného na adrese https://journals.muni.cz/revue

DOPORUČENÝ ROZSAH PŘÍSPĚVKŮ:

Sekce Diskuze:	15 – 30 normostran
Sekce Anotace:	2 – 10 normostran
Sekce Essays:	5 – 10 normostran
Sekce Recenze závěrečných prací:	2 – 5 normostran
Sekce Recenze:	2 – 5 normostran
Sekce Téma:	30 – 50 normostran

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

CITAČNÍ STANDARD

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

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

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

TERMÍNY PRO DODÁNÍ PŘÍSPĚVKŮ

Do letního čísla: 28. února

Do zimního čísla: 31. srpna

Časopis se hlásí k politice otevřeného přístupu realizovaného zlatou cestou.

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

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

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

https://doi.org/10.5817/RPT2023-1-1

AKT O KYBERNETICKÉ ODOLNOSTI[1]

ZUZANA LIMBERGOVÁ[2]

ABSTRAKT

Článek se věnuje legislativnímu návrhu Evropské Komise na horizontální právní regulaci požadavků na kybernetickou bezpečnost produktů s digitálními prvky, označovanému jako „akt o kybernetické odolnosti“. Po nastínění hlavních principů navrhované regulace a jejích důvodů a cílů je pozornost věnována vztahu k existující unijní legislativě a oblasti působnosti. V další části je pak představeno věcné jádro návrhu, konkrétně vymezení základních pojmů a předmětu právní úpravy, dále požadavky stanovené pro uvádění a dodávání produktů s digitálními prvky na trh a představení principů posuzování shody. Další část je věnována představení hlavních povinností výrobců a ostatních hospodářských subjektů a základním pravidlům dozoru nad trhem a vymáhání. Poslední část se věnuje nastínění některých potenciálně problematických dopadů návrhu nové regulace jako podnětu k diskuzi.

KLÍČOVÁ SLOVA

Akt o kybernetické odolnosti; kybernetická bezpečnost; uvádění produktů na trh; produkty s digitálními prvky; posuzování shody; nový legislativní rámec

---

[1] Tento článek vznikl za podpory projektu "Centrum excelence pro kyberkriminalitu, kyberbezpečnost a ochranu kritických informačních infrastruktur" reg. č.: CZ.02.1.01/0.0/0.0/16_019/0000822 financovaného z EFRR.

[2] JUDr. Zuzana Limbergová, LL.M. je odbornou pracovnicí Ústavu práva a technologií Masarykovy univerzity a advokátkou v Praze, kontaktní e-mail: zuzana.limbergova@aklimbergova.cz.

ABSTRACT

The article focuses on the European Commission's legislative proposal for horizontal regulation of cybersecurity requirements for products with digital elements, referred to as the "Cyber Resilience Act". After outlining the main principles of the proposed regulation and its rationale and objectives, attention is given to its relationship with existing EU legislation and scope. The next section presents the substantive core of the proposal, namely the definition of the basic terms and the subject matter of the legislation, as well as the requirements set out for the making available and placing of products with digital elements on the market and the introduction of the principles of conformity assessment. The next part is devoted to an introduction to the main obligations of manufacturers and other economic operators and the basic rules on market surveillance and enforcement. The last part is devoted to outlining some potentially problematic impacts of the new regulation as the points for discussion.

KEY WORDS

Cyber Resilience Act; Cyber Security; Placing of Products on the Market; Products with Digital Elements; Conformity Assessment; NLF

1. ÚVOD

Legislativní orgány Evropské unie jsou v souladu se strategickými a programovými dokumenty[3] v poslední době velmi činné na poli regulace „digitální oblasti“, ať se jedná o správu a využívání dat, digitální trhy, digitální služby, umělou inteligenci nebo kybernetickou bezpečnost. V září roku 2022 byl Evropskou Komisí předložen legislativní návrh zkráceně ozna-

[3] Např. Společné sdělení Evropskému parlamentu a Radě Strategie kybernetické bezpečnosti EU pro digitální dekádu. JOIN (2020) 18 final. [online]. 2020. [cit. 1. 11. 2022] Dostupné z: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN. Projev předsedkyně Komise von der Leyenové o stavu Unie v roce 2021. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701. nebo Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů. Digitální kompas 2030: Evropské pojetí digitální dekády. COM (2021) 118 final, [online]. 2020. [cit. 1. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.

čovaný jako akt o kybernetické odolnosti[4] plným názvem návrh nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020[5]. Jak samotný název napovídá, nové nařízení cílí na regulatorní zajištění kybernetické bezpečnosti v produktové oblasti a mělo by se jednat o další dílek v evropské legislativní skládačce regulace kybernetické bezpečnosti. Akt o kybernetické odolnosti odpovídá zásadám právních předpisů nového legislativního rámce[6] v oblasti produktové bezpečnosti. Regulatorní přístup návrhu je postaven zejména na následujících principech:

- záměrná a standardní implementace požadavků kybernetické bezpečnosti od počátku a po celý životní cyklus produktu[7];
- zajištění kybernetické bezpečnosti v celém dodavatelském řetězci;
- přístup založený na riziku;
- horizontální (mezioborová) působnost.

Nová regulace má stanovit podmínky pro uvádění na trh všech produktů zahrnujících hardware nebo software a jeho řešení pro zpracování dat na dálku, včetně hardwarových a softwarových komponent uváděných na trh samostatně. Vztahovat se bude jak na software obsažený v hmotných produktech, tak na software nabízený zcela samostatně. Podmínkou je, že zamýšlené nebo důvodně předpokládané použití příslušného produktu zahrnuje přímé nebo nepřímé logické nebo fyzické datové připojení k zařízení nebo síti, což ovšem v dnešní době splní valná většina hardwarových i soft-

[4] V originále „Cyber Resilience Act“ uveřejněný dne 15. 9. 2022, viz European Comision. Shaping Europe’s digital future. Cyber Resilience Act. [online]. 2022. [cit. 1. 11. 2022] Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act..

[5] Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020, COM/2022/454 final. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52022PC0454&qid=1667332176493. Pro zjednodušení bude používán v tomto článku zkrácený název „akt o kybernetické odolnosti“ případně, tam kde je to s ohledem na kontext vhodné a není to na úkor jednoznačnosti významu, bude používáno také označení „návrh“ nebo „nařízení“.

[6] „New Legislative Framework (NLF)“. Podrobněji k vysvětlení NLF viz Sdělení Komise. „Modrá příručka“ k provádění pravidel EU pro výrobky 2022. 2022/C 247/01. s. 9-10. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC.

[7] „Security by default and by design“.

warových produktů. Jak bude dále uvedeno, jsou některé typy produktů nebo jejich modely distribuce z působnosti vyňaty, ne vždy jsou však tyto výjimky formulovány jednoznačně a dostatečně určitě. Osobní působnost je pak vymezena jak vůči výrobcům, tak i dalším článkům distribučního řetězce, jako jsou dovozci a distributoři.

Předmětem tohoto článku je legislativní návrh ve znění předloženém Komisí a uveřejněném dne 15. září 2022. V době psaní tohoto příspěvku byl legislativní proces v raném stadiu, v průběhu projednávání návrhu v Radě a Evropském parlamentu může dojít ještě k řadě změn. Cílem tohoto článku je představit čtenáři hlavní obsah aktu o kybernetické odolnosti a upozornit za účelem vyvolání další diskuze na některé potenciálně problematické souvislosti.

2. DŮVODY A CÍLE NÁVRHU

Hlavním deklarovaným důvodem návrhu nové právní úpravy je nutnost posílení kybernetické odolnosti hardwaru i softwaru proti kybernetickým útokům pro všechny produkty s digitálními prvky, na které se nevztahuje žádná speciální úprava. Posílení kybernetické odolnosti jednotlivých produktů by mělo vést s ohledem na vzájemnou propojenost informačních systémů, sítí a prostředí k posílení kybernetické odolnosti v rámci celého vnitřního trhu Unie. Zajištění vyšší kybernetické odolnosti má vést ke snížení případných majetkových škod a nemajetkové újmy způsobených úspěšnými kybernetickými útoky, nákladů vynakládaných v souvislosti s kybernetickými útoky a jejich prevencí včetně souvisejících nepřímých nákladů např. na pojištění. Zprostředkovaně pak má nová právní úprava přispět k lepší ochraně práv jednotlivců, která mohou být důsledky kybernetických útoků negativně dotčena.

Komise definuje dva hlavní problémy a jim odpovídající dva hlavní cíle, kterých má být přijetím nové právní úpravy dosaženo[8]:

[8] Blíže viz akt o kybernetické odolnosti. Důvodová zpráva. a Commission staff working document. Impact Assessment Report. Part 1/3. SWD (2022) 282 final. [online]. 2022. [cit. 1. 11. 2022] Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

1. Prvním problémem je nízká úroveň kybernetické bezpečnosti produktů s digitálními prvky. Odpovídajícím cílem je tak vytvoření podmínek pro vývoj bezpečných produktů s digitálními prvky zajištěním toho, aby produkty byly uváděny na trh s méně zranitelnostmi a aby výrobci zohledňovali bezpečnost v průběhu celého životního cyklu produktu.
2. Druhým problémem je nízká informovanost a z toho vyplývající nedostatečné porozumění otázce kybernetické bezpečnosti produktů na straně uživatelů. Odpovídajícím cílem k řešení tohoto problému je vytvoření podmínek umožňujících uživatelům zohlednění kybernetické bezpečnosti při výběru a používání produktů s digitálními prvky.

V návaznosti na dva hlavní cíle sleduje akt o kybernetické odolnosti čtyři konkrétní cíle: (i) zajištění zlepšení bezpečnosti produktů s digitálními prvky na straně výrobců od fáze návrhu a vývoje a během celého životního cyklu, (ii) zajištění soudržného rámce kybernetické bezpečnosti na celém vnitřním trhu, který výrobcům usnadní dodržování předpisů, (iii) zvýšení transparentnosti bezpečnostních vlastností produktů s digitálními prvky a (iv) umožnění bezpečného používání produktů s digitálními prvky uživatelům z řad podniků i spotřebitelů.

Základem aktu o kybernetické odolnosti v primárním právu je vcelku nepřekvapivě článek 114 Smlouvy o fungování Evropské unie, tedy přijetí opatření nezbytných pro vytvoření a fungování vnitřního trhu, protože přijímání právních úprav této problematiky na úrovni členských států by vedlo k fragmentaci regulace a vytváření překážek fungování vnitřního trhu.

3. VZTAH K EXISTUJÍCÍ LEGISLATIVĚ A PŮSOBNOST

V případě přijetí bude akt o kybernetické odolnosti třetím unijním normativním aktem věnovaným specificky problematice kybernetické bezpečnosti. Prvním z těchto aktů byla v roce 2016 směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné

úrovně bezpečnosti sítí a informačních systémů v Unii[9], nahrazená v roce 2022 novou směrnicí zkráceně označovanou jako „směrnice NIS2“[10]. V roce 2019 následoval akt o kybernetické bezpečnosti[11].

Zatímco směrnice NIS (a stejně tak nová verze v podobě směrnice NIS2) vyžaduje transpozici vnitrostátním právním aktem a jejím hlavním cílem je zajistit kybernetickou bezpečnost vybraných sítí a služeb s významný společenským dopadem, akt o kybernetické odolnosti bude mít jako nařízení přímou a horizontální působnost, protože by se měl vztahovat na všechny produkty s digitálními prvky dodávané na vnitřním trhu EU bez ohledu na to, jak a kým jsou používány. Akt o kybernetické odolnosti by měl usnadnit dodržování požadavků na bezpečnost dodavatelského řetězce ze strany povinných subjektů podle NIS2 zajištěním bezpečnosti jimi používaných produktů po celou dobu jejich životního cyklu, tedy včetně zajištění bezpečnostních záplat a aktualizací.[12] Naopak akt o kybernetické odolnosti se nevztahuje na poskytování služeb včetně software formou služby (k tomuto tématu podrobněji v dalším textu), což by měla převážně pokrývat právě směrnice NIS2 prostřednictvím regulace poskytovatelů cloudových služeb. Zároveň by ale oba právní předpisy měly být vzájemně v souladu a navzájem se podporovat. Akt o kybernetické odolnosti přejímá ze směrnice NIS2 některé definice a předpokládá zapojení agentury ENISA a národních CSIRT týmů zřizovaných na základě směrnice NIS2 do plnění některých úkolů zejména v oblasti sdílení informací.

Akt o kybernetické bezpečnosti, který má rovněž formu nařízení, využívá obdobné nástroje jako akt o kybernetické odolnosti v podobě posouzení

[9] V souladu s obvyklým územ bude v článku pro tuto směrnici používáno zkrácené označení „směrnice NIS“.

[10] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 („směrnice NIS 2“).

[11] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“).

[12] Viz recitál 11 aktu o kybernetické odolnosti.

shody, ať formou prohlášení o shodě nebo posuzování shody třetí stranou. Významným rozdílem je ale dobrovolnost užití certifikačních schémat přijatých na základě aktu o kybernetické bezpečnosti oproti povinnému posouzení kybernetické bezpečnosti a bezpečnostních rizik na základě aktu o kybernetické odolnosti. Certifikační schémata přijatá na základě aktu o kybernetické bezpečnosti mohou mít širší věcnou působnost, když se kromě produktové kybernetické bezpečnosti mohou vztahovat rovněž na služby a procesy[13]. Zároveň vymezení produktů podle aktu o kybernetické bezpečnosti nezahrnuje všechny produkty s digitálními prvky, jak je definuje akt o kybernetické odolnosti[14]. Subjekty určené k posuzování shody třetí osobou se v obou nařízeních částečně překrývají, stejně tak institucionální zaštítění tvorby příslušných norem posuzování shody. Z níže uvedeného shrnutí vyplývá, že obě nařízení vykazují v oblasti posuzování shody rovněž odlišnosti, nic to však nemění na tom, že se obě úpravy navzájem částečně duplikují.

Tabulka srovnání dílčích parametrů posuzování shody a certifikace.

	Akt o kybernetické bezpečnosti (CSA)	**Akt o kybernetické odolnosti (CRA)**
předmět posouzení/ certifikace	• produkt IKT = prvek nebo skupina prvků sítě nebo informačního systému • služba IKT = služba spočívající plně nebo převážně v přenosu, ukládání, získávání či zpracovávání informací prostřednictvím sítí a informačních systémů • proces IKT = soubor činností prováděných za účelem navrhování, vývoje, poskytování nebo údržby produktů nebo služeb IKT	produkt s digitálními prvky = softwarový nebo hardwarový produkt a jeho řešení pro zpracování dat na dálku, včetně softwarových nebo hardwarových součástí, které mají být uvedeny na trh samostatně

[13] Viz čl. 46 aktu o kybernetické bezpečnosti.

[14] Srov. čl. 3 bod 12 aktu o kybernetické bezpečnosti a čl. 3 bod 1 aktu o kybernetické odolnosti.

povinnost posouzení/ certifikace	certifikace pro uvedení na trh nepovinná, ledaže zvláštní předpis stanoví jinak	posouzení shody pro uvedení na trh povinné
výstup posouzení	evropský certifikát kybernetické bezpečnosti nebo EU prohlášení o shodě	prohlášení o shodě; certifikát EU přezkoušení typu nebo rozhodnutí o posouzení systému kvality při posouzení třetí osobou
norma pro posouzení shody/ certifikaci	evropský systém certifikace kybernetické bezpečnosti (certifikační schéma) - prováděcí akt Komise	příloha č. I CRA; harmonizované normy; obecné specifikace – prováděcí akt Komise
institucionální zajištění tvorby norem pro posouzení shody/ certifikaci	**ENISA** – navrhuje certifikační schéma; **Komise** – schvaluje certifikační schéma formou prováděcího aktu	evropské normalizační organizace na žádost Komise (harmonizované normy); Komise (obecné specifikace); Rada + EP – příloha č. I CRA
Institucionální zajištění posouzení shody třetí osobou	akreditovaný subjekt[15]; nebo vnitrostátní orgán certifikace kybernetické bezpečnosti; nebo akreditovaný veřejný subjekt	oznámený subjekt posuzování shody splňující požadavky CRA, primárně se předpokládá využití akreditovaných subjektů
možnost vlastního posouzení shody výrobcem	ano, pouze pro kategorii certifikace „základní“, a pokud to umožňuje certifikační schéma	ano, pokud nejde o kritický produkt třídy II, nebo třídy I, pro který nebyly použity/neexistují odpovídající normy

[15] Jedná se o akreditaci podle nařízení Evropského parlamentu a Rady (ES) 765/2008 kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93.

Dozor a vymáhání	vnitrostátní orgán certifikace kybernetické bezpečnosti	vnitrostátní orgán dozoru nad trhem – spolupracuje s orgánem certifikace kybernetické bezpečnosti podle CSA
sankce	výši a pravidla ukládání stanoví členský stát	konkrétní výši a pravidla ukládání stanoví členský stát, maximální limity určuje CRA
vzájemná nahraditelnost posouzení/ certifikace	ne (certifikaci nelze nahradit posouzením podle CRA)	ano, pokud tak stanoví Komise aktem v přenesené pravomoci; povinně pro vysoce kritické produkty, pokud tak stanoví Komise

Mezi oběma nařízeními budou existovat styčné plochy a interakce, nařízení by proto měla být vzájemně kompatibilní. Akt o kybernetické odolnosti má svěřit Komisi pravomoc prostřednictvím přijetí aktu v přenesené pravomoci upřesnit kategorie vysoce kritických produktů s digitálními prvky, pro které budou výrobci povinni získat evropský certifikát kybernetické bezpečnosti v rámci evropského systému certifikace, aby prokázali shodu se základními požadavky stanovenými aktem o kybernetické odolnosti[16]. Protože vymezení těchto vysoce kritických produktů je ponecháno na prováděcích předpisech a uvážení Komise, znamená to pro výrobce značnou nejistotu, jakým procesem posuzování shody budou muset vyvíjené produkty projít, kterou ještě posiluje skutečnost, že certifikační schémata podle aktu o kybernetické bezpečnosti stále nebyla schválena.

Komisi je rovněž svěřena pravomoc prostřednictvím prováděcích aktů specifikovat evropské systémy certifikace kybernetické bezpečnosti, které lze použít k prokázání shody se základními požadavky podle aktu o kybernetické odolnosti, a dále případně určit, zda certifikát kybernetické bezpečnosti vydaný v rámci těchto systémů ruší povinnost výrobce nechat

[16] Viz čl. 6 odst. 5 aktu o kybernetické odolnosti.

provést posouzení shody třetí stranou [17]. Zároveň by potřeba nových evropských systémů certifikace kybernetické bezpečnosti pro produkty s digitálními prvky měla být posuzována s ohledem na existenci a obsah aktu o kybernetické odolnosti, zohledňovat základní požadavky v něm stanovené a usnadňovat s ním soulad.[18]Tato ustanovení přímo vyvolávají otázku, z jakého důvodu není přímo aktem o kybernetické odolnosti bez dalšího umožněno nahrazení posouzení shody certifikací podle aktu o kybernetické bezpečnosti a jaký má vůbec paralelní udržování dvou systémů posuzování shody, navíc prováděného často stejnými subjekty, smysl. Na nejasnost vztahu mezi certifikačními orgány ve smyslu aktu o kybernetické odolnosti a orgány oprávněnými k certifikaci kybernetické bezpečnosti podle jiných použitelných předpisů ostatně upozornil ve svém stanovisku i Evropský hospodářský a sociální výbor[19].

Akt o kybernetické odolnosti by měl mít povahu horizontální úpravy vztahující se na všechny produkty s digitálními prvky, jejichž zamýšlené nebo důvodně předpokládané použití zahrnuje přímé nebo nepřímé logické nebo fyzické datové připojení k zařízení nebo síti. S ohledem na existenci speciálních unijních právních předpisů pro některé kategorie produktů návrh stanoví výčtem těchto speciálních předpisů konkrétní výjimky z obecné působnosti aktu o kybernetické odolnosti[20], a dále obecné podmínky, za kterých může být použití aktu o kybernetické odolnosti na produkty s digitálními prvky, na něž se vztahují jiná pravidla Unie, omezeno nebo vyloučeno.[21] Generální výjimka z působnosti by pak měla platit pro produkty s digitálními prvky vyvinuté výlučně pro účely národní bezpečnosti nebo

[17] Viz čl. 18 odst. 4 aktu o kybernetické odolnosti.

[18] Viz recitál 39 aktu o kybernetické odolnosti.

[19] Viz Stanovisko Evropského hospodářského a sociálního výboru k návrhu nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020 (COM(2022) 454 final – 2022/0272 (COD). (2023/C 100/15). [online]. 2022. [cit. 16. 3. 2023] Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:52022AE4103.

[20] Viz čl. 2 odst. 2, 3 aktu o kybernetické odolnosti. Jedná se např. o diagnostické a zdravotnické prostředky nebo motorová vozidla.

[21] Viz čl. 2 odst. 4 aktu o kybernetické odolnosti.

pro vojenské účely a produkty speciálně určené ke zpracování utajovaných informací.

Navrhované nařízení má řešit pouze požadavky na kybernetickou bezpečnost produktů s digitálními prvky, nikoli požadavky na jejich bezpečnost všeobecně. Na ty se budou vztahovat buď speciální unijní předpisy, nebo nařízení o obecné bezpečnosti výrobků, jehož návrh je také v legislativním procesu[22].

Speciální pravidla jsou stanovena pro strojní výrobky a produkty s digitálními prvky, které jsou zároveň vysoce rizikovými systémy umělé inteligence, kdy by v zásadě splnění požadavků podle aktu o kybernetické odolnosti mělo dokládat zároveň soulad s požadavky na kybernetickou bezpečnost stanovenými ve speciálních úpravách[23].

4. PŘEDMĚT PRÁVNÍ ÚPRAVY A ZÁKLADNÍ POJMY

Předmětem aktu o kybernetické odolnosti bude:

1) stanovení pravidel pro uvádění produktů s digitálními prvky na trh;
2) stanovení základních požadavků na navrhování, vývoj a výrobu produktů s digitálními prvky a povinností hospodářských subjektů v souvislosti s těmito produkty;
3) stanovení základních požadavků na procesy řešení zranitelnosti zavedené výrobci a povinností hospodářských subjektů v souvislosti s těmito procesy;

to vše s cílem zajistit kybernetickou bezpečnost produktů s digitálními prvky během celého jejich životního cyklu, a dále

4) stanovení pravidel pro dozor nad trhem a prosazování stanovených pravidel a požadavků.

Ústředním pojmem, ke kterému se vztahují všechny povinnosti a pravidla stanovená aktem o kybernetické odolnosti, je *produkt s digitálními*

[22] Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o obecné bezpečnosti výrobků, o změně nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 a o zrušení směrnice Rady 87/357/EHS a směrnice Evropského parlamentu a Rady 2001/95/ES. COM/2021/346 final. [online]. 2022. [cit. 6. 11. 2022] Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A52021PC0346.

[23] Podrobněji viz čl. 8 a čl. 9 aktu o kybernetické odolnosti.

prvky. Návrh tento pojem definuje jako *„jakýkoli softwarový nebo hardwarový produkt a jeho řešení pro zpracování dat na dálku, včetně softwarových nebo hardwarových součástí, které mají být uvedeny na trh samostatně“*[24]. Definice zahrnuje jak komplexní produkty s digitálními prvky složené z hardwarových i softwarových komponentů, tak hardware nebo software[25] uváděné na trh samostatně, podmínkou ovšem je, aby se jednalo o produkty, jejichž zamýšlené nebo předpokládané použití zahrnuje přímé či nepřímé logické nebo fyzické datové připojení k zařízení nebo síti. Produkty s digitálními prvky, které jsou výhradně off-line, do působnosti navrhovaného nařízení nespadají. Využití produktu koncovým uživatelem je nerozhodné, nezáleží na tom, zda se jedná o software pro řízení průmyslové výroby, server používaný neziskovou organizací nebo chytré hodinky určené pro spotřebitele.

Návrh obsahuje speciální vymezení vůči obchodnímu modelu poskytování software formou služby (SaaS). Recitál 9 stanoví, že *„Toto nařízení zajišťuje vysokou úroveň kybernetické bezpečnosti produktů s digitálními prvky. Neupravuje služby, například Software jako služba (SaaS)…“*[26], což je logické, protože nařízení spadá stejně jako ostatní předpisy NLF do oblasti produktové bezpečnosti, nedává smysl vztahovat je na služby. Text recitálu ale pokračuje: „s *výjimkou řešení pro zpracování dat na dálku týkajících se produktu s digitálními prvky, čímž se rozumí jakékoli zpracování dat na dálku, pro něž je software navržen a vyvinut výrobcem daného produktu nebo za nějž je tento výrobce odpovědný, a pokud by neexistoval, nebylo by možné, aby tento produkt s digitálními prvky plnil některou ze svých funkcí“*[27], což výklad působnosti nařízení komplikuje. Z textace není zcela zřejmé, zda se v případě zpracování dat na dálku, které je nutné pro plné fungování produktu s digitálními prvky a které je vyvíjeno týmž výrobcem nebo pod jeho odpovědností, má akt o kybernetické odolnosti vztahovat na celé toto řešení, i pokud je poskytováno formou služby, nebo zda tímto způsobem je pouze zdůrazněno,

[24] Viz čl. 3 bod 1) aktu o kybernetické odolnosti.

[25] Oba tyto dílčí pojmy aktu o kybernetické odolnosti rovněž samostatně definuje, viz čl. 3 body 6) a 7).

[26] Viz recitál 9 aktu o kybernetické odolnosti.

[27] Viz recitál 9 aktu o kybernetické odolnosti.

že *software* výrobce využívaný pro zpracování dat na dálku, byť by byl nabízen formou poskytování služby, nemá být z působnosti nařízení vyňat. Zpracováním dat na dálku je „*jakékoli zpracování dat na dálku, pro které výrobce navrhuje a vyvíjí software nebo za jehož návrh a vývoj výrobce zodpovídá, přičemž neexistence tohoto softwaru by bránila tomu, aby produkt s digitálními prvky plnil některé ze svých funkcí*“, definice je natolik široká, že spíše zahrnuje i zpracování dat formou služby, je-li k ní využíván software vyvíjený výrobcem či pod jeho odpovědností než pouze tento software. V případech, kdy produkt využívá SaaS třetí strany, za který nenese výrobce odpovědnost, se však působnost nařízení na tuto službu vztahovat nebude.

Účelem nařízení je zajistit, aby na společný trh byly dodávány pouze produkty s digitálními prvky splňující stanovené bezpečnostní požadavky, což by ale nemělo bránit technologickému vývoji a výzkumu. Proto je umožněno uvolnění testovacích nebo předváděcích verzí produktů s digitálními prvky bez toho, aby splňovaly stanovené požadavky, pouze však v omezeném režimu[28]. Z obdobných důvodů se nemá nařízení vztahovat na software s otevřeným zdrojovým kódem (tzv. open source software)[29], je-li nabízen bezplatně a mimo rámec obchodní činnosti, tedy i bez poskytování podpůrných nebo souvisejících služeb (typicky služby typu maintenance) na komerční bázi. Za obchodní činnost je navíc obdobně jako ve směrnici o poskytování digitálního obsahu[30] označováno i použití osobních údajů z jiných důvodů než výlučně zlepšení bezpečnosti, kompatibility nebo interoperability software. Vynětí open source softwaru je však uvedeno pouze v recitálu návrhu, nikoli již dále v normativním textu. Zároveň mohou vznikat nejasnosti, co ještě lze považovat za dodávání *mimo rámec obchodní činnosti*, když uvedení na trh zahrnuje i bezplatné dodání[31].

Akt o kybernetické odolnosti produkty s digitálními prvky dále kategorizuje a vyčleňuje dvě skupiny produktů, které podléhají speciálnímu zpřísněnému režimu. Jedná se o *kritické produkty s digitálními prvky a vysoce*

[28] Blíže viz čl. 4 odst. 2 a 3 a recitál 21 aktu o kybernetické odolnosti.

[29] Viz recitál 10 aktu o kybernetické odolnosti.

[30] Směrnice Evropského parlamentu a Rady (EU) 2019/770 ze dne 20. května 2019 o některých aspektech smluv o poskytování digitálního obsahu a digitálních služeb.

[31] Viz čl. 3 body 22) a 23 aktu o kybernetické odolnosti.

kritické produkty s digitálními prvky. Tyto dvě kategorie mají stanovena přísnější kritéria pro dodávání na trh než ostatní produkty s digitálními prvky.

Kritické produkty s digitálními prvky jsou produkty s digitálními prvky, které představují kybernetické bezpečnostní riziko v souladu se stanovenými kritérii a jejichž základní funkce odpovídá funkcím uvedeným v příloze III aktu o kybernetické odolnosti. Tato kategorie je pak dále dělena do dvou tříd podle výčtu uvedeného v příloze III. Do I. třídy náleží např. samostatné i vestavěné prohlížeče, správci hesel, systémy řízení sítě nebo software pro správu mobilních zařízení, do II. – kritičtější – třídy náleží např. operační systémy pro servery, stolní počítače a mobilní zařízení, čipové karty, čtečky čipových karet a tokeny nebo mikroprocesory[32]. Seznam uvedený v příloze III může být měněn aktem Komise přijatým v přenesené pravomoci, čímž by mělo být zajištěno, že legislativní úprava bude dostatečně flexibilně reagovat na technologický vývoj. Komisi je také svěřena pravomoc přijetím aktu v přenesené pravomoci upřesnit definice kategorií kritických produktů.

Vysoce kritické produkty s digitálními prvky jsou produkty s digitálními prvky, které představující kybernetické riziko s ohledem na speciální kritéria, kterými jsou (i) používání nebo spoléhání se základními subjekty podle přílohy I směrnice NIS2 na takový produkt nebo (ii) relevance pro odolnost celého dodavatelského řetězce produktů s digitálními prvky vůči událostem způsobujícím narušení. Vysoce kritické produkty s digitálními prvky akt o kybernetické odolnosti neurčuje, ale svěřuje tuto pravomoc Komisi[33]. Důsledkem rozdělení produktů s digitálními prvky na vysoce kritické, kritické a „nekritické“ je různá míra náročnosti procesu posuzování shody, kterému podléhají, s ohledem na možná rizika spojená s jejich použitím.

[32] Pro kompletní výčet viz Příloha III aktu o kybernetické odolnosti.

[33] Viz čl. 6 odst. 5 Aktu o kybernetické odolnosti.

5. UVÁDĚNÍ A DODÁVÁNÍ PRODUKTŮ S DIGITÁLNÍMI PRVKY NA TRH

Obdobně jako u ostatních právních předpisů nového legislativního rámce je i v aktu o kybernetické odolnosti důležitým pojmem uvedení produktu s digitálními prvky na trh. Uvedením produktu s digitálními prvky na trh se rozumí „*první dodání produktu s digitálními prvky na trh Unie*“[34]. Dodáním na trh je pak „*jakékoli dodání produktu s digitálními prvky k distribuci nebo použití na trhu Unie v rámci obchodní činnosti, ať už za úplatu, nebo bezplatně*“[35]. Přitom pojmy *dodání* i *uvedení* se vztahují na každý jednotlivý produkt, nikoli na typ produktu, ať už byl vyroben nebo vyvinut individuálně nebo sériově[36]. To mj. znamená, že pravidla aktu o kybernetické odolnosti se budou vztahovat i na produkty s digitálními prvky (jako individuální jednotky), jejichž typ nebo model byl na unijní trh dodáván již přede dnem použitelnosti aktu o kybernetické odolnosti, pokud tyto jednotlivé produkty jako samostatné jednotky byly dodány až poté. K tomu je třeba doplnit, že na základě přechodných ustanovení se povinnosti výrobců informovat o zranitelnostech nebo incidentech podle čl. 11 mají vztahovat i na produkty s digitálními prvky uvedené na trh Unie přede dnem použitelnosti aktu o kybernetické odolnosti.

Dodání i uvedení produktu s digitálními prvky předpokládá nabídku nebo dohodu (písemnou či ústní) mezi dvěma či více právnickými nebo fyzickými osobami za účelem převodu vlastnictví, držby či jakéhokoli jiného práva týkajícího se dotčeného produktu. Může se přitom jednat nejen o převod vlastnického práva, ale např. i výpůjčku, nájem nebo leasing[37].

Povinnosti hospodářských subjektů návrh vztahuje k uvedení produktů s digitálními prvky na trh, nikoli k jejich prostému vyrobení, vývoji

[34] Čl. 3 odst. 22 aktu o kybernetické odolnosti.

[35] Čl. 3 odst. 23 aktu o kybernetické odolnosti.

[36] Viz sdělení Komise. „Modrá příručka“ k provádění pravidel EU pro výrobky 2022. 2022/C 247/01. s. 19-20. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC

[37] Viz sdělení Komise. „Modrá příručka“ k provádění pravidel EU pro výrobky 2022. 2022/C 247/01. s. 19-20. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC

nebo užívání. Na produkty s digitálními prvky, které nejsou výrobcem uváděny na trh, typicky na výsledky interního vývoje software, který je užíván výhradně subjektem, který jej vyvinul pro své vlastní účely, by se povinnosti hospodářských subjektů podle aktu o kybernetické odolnosti vztahoval neměly[38], na rozdíl však od produktů vyrobených výrobcem pro zákazníka na zakázku, u kterých k uvedení a dodání na trh dochází.

Produkty s digitálními prvky bude podle aktu o kybernetické odolnosti možné dodávat na trh pouze v případě, že

- splňují základní požadavky stanovené v oddíle 1 přílohy I aktu o kybernetické odolnosti za podmínky, že jsou řádně instalovány, udržovány a používány k určenému účelu či za podmínek, které lze rozumně předvídat a, je-li to relevantní, aktualizovány a
- výrobcem zavedené postupy jsou v souladu se základními požadavky stanovenými v oddíle 2 přílohy I aktu o kybernetické odolnosti[39].

Oddíl 1 přílohy I aktu o kybernetické odolnosti obsahuje seznam bezpečnostních požadavků týkající se vlastností produktů s digitálními prvky na základě posouzení rizik těchto produktů provedeného výrobcem.

Oddíl 2 přílohy I aktu o kybernetické odolnosti stanoví požadavky na řešení zranitelností, které musí výrobci zavést do svých postupů nejen při designu a výrobě produktu, ale také v poprodejní fázi, kdy jsou zejména povinni sdílet informace o možných zranitelnostech a zajišťovat bezpečnostní opravy nebo aktualizace včetně jejich bezplatného šíření po očekávanou dobu životnosti produktu nebo po dobu pěti let od jeho uvedení na trh (podle toho, která doba je kratší). Zranitelnost je definována shodně jako ve směrnici NIS2, tedy jako slabá stránka, snížená odolnost nebo chyba prostředku, systému, procesu nebo kontroly, která může být využita kybernetickou hrozbou[40].

[38] Viz vysvětlení obsažené ve sdělení Komise. „Modrá příručka“ k provádění pravidel EU pro výrobky 2022. 2022/C 247/01. s. 19-20. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC

[39] Čl. 5 aktu o kybernetické odolnosti.

Soulad produktu s digitálními prvky s požadavky stanovenými v oddíle 1 přílohy I aktu o kybernetické odolnosti a soulad výrobcem zavedených postupů se základními požadavky stanovenými v oddíle 2 přílohy I aktu o kybernetické odolnosti se dokládá prohlášením o shodě a umístěním CE označení[41]. Prohlášení o shodě lze vydat až po provedení posouzení shody v souladu s čl. 24 aktu o kybernetické odolnosti. Výrobce má na výběr ze tří variant postupů posuzování shody s využitím čtyř různých modulů[42]:

1. postup vnitřní kontroly (na základě modulu A)[43], tedy zjednodušeně vlastní posouzení shody výrobcem;
2. EU přezkoušení typu (na základě modulu B), po kterém musí následovat shoda s EU typem založená na interním řízení výroby (na základě modulu C)[44]; tzn. nechat provést posouzení shody typu produktu třetí oprávněnou osobou a zavést kontrolní mechanismy zaručující řízení výroby tak, aby byla zajištěna shoda s typem, který byl předmětem posouzení; nebo
3. posuzování shody založené na komplexním zabezpečení kvality (na základě modulu H)[45]; tj. přezkoumání a posouzení komplexního systému zabezpečení kvality třetí oprávněnou osobou.

---

[40] Čl. 3 bod 38) aktu o kybernetické odolnosti ve spojení s čl. 4 bod 8 návrhu SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148. COM/2020/823 final. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:52020PC0823.

[41] Podrobněji viz čl. 10 odst. 7 a čl. 21 aktu o kybernetické odolnosti, a dále čl. 30 nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93.

[42] Jedná se o moduly ve smyslu přílohy II Rozhodnutí Evropského parlamentu a Rady č. 768/2008/ES ze dne 9. července 2008 o společném rámci pro uvádění výrobků na trh a o zrušení rozhodnutí Rady 93/465/EHS.

[43] Blíže viz příloha VI aktu kybernetické odolnosti ve spojení s přílohou II Rozhodnutí Evropského parlamentu a Rady č. 768/2008/ES..

[44] Blíže viz příloha VI aktu kybernetické odolnosti ve spojení s přílohou II Rozhodnutí Evropského parlamentu a Rady č. 768/2008/ES.

[45] Blíže viz příloha VI aktu kybernetické odolnosti ve spojení s přílohou II Rozhodnutí Evropského parlamentu a Rady č. 768/2008/ES.

Jedná-li se o kritický produkt s digitálními prvky třídy II, musí být shoda se základními požadavky prokázána jedním z postupů uvedených shora pod body 2 nebo 3, vždy tedy s provedením posouzení shody třetí stanou, ledaže Komise určila, že povinnost posouzení třetí stranou lze nahradit certifikátem kybernetické bezpečnosti vydaným v rámci systému certifikace kybernetické bezpečnosti.

Pro kritický produkt s digitálními prvky třídy I je požadováno prokázání shody se základními požadavky rovněž jedním z postupů uvedených shora sub 2 nebo 3, pouze však v případě, kdy výrobce pro posouzení souladu nepoužil harmonizované normy[46], obecné specifikace[47] nebo evropský systém certifikace kybernetické bezpečnosti[48] určený Komisí[49] nebo jestliže použitelné harmonizované normy, obecné specifikace nebo evropský systém certifikace kybernetické bezpečnosti neexistují.

V případě „nekritických" produktů s digitálními prvky je možné využít bez dalších omezení i posouzení shody uvedené výše sub 1, které provádí výrobcem sám bez zapojení třetí osoby. Zároveň jsou-li „nekritické" produkty s digitálními prvky a postupy výrobce ve shodě s harmonizovanými normami nebo obecnými specifikacemi, nebo bylo-li pro ně vydáno prohlášení o shodě nebo certifikát podle evropského systému certifikace kybernetické bezpečnosti určeného Komisí, má se za to, že jsou tyto produkty ve shodě i se základními požadavky uvedenými v příloze I aktu o kybernetické odolnosti.

Pro kategorii vysoce kritických produktů s digitálními prvky, pokud je Komise stanoví, budou výrobci povinni k prokázání shody získat evropský certifikát kybernetické bezpečnosti podle certifikačního schématu na základě aktu o kybernetické bezpečnosti.

---

[46] Harmonizované normy, na něž byl zveřejněn odkaz v Úředním věstníku EU, ve smyslu čl. 2 odst. 1) psím. c) Nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci.

[47] Obecné specifikace ve formě prováděcích aktů je při naplnění podmínek stanovených čl. 19 aktu o kybernetické odolnosti oprávněna vydávat Komise.

[48] Evropský systém certifikace kybernetické bezpečnosti podle aktu o kybernetické bezpečnosti.

[49] Viz čl. 18 odst. 4 aktu o kybernetické odolnosti.

Je-li v rámci posuzování shody požadováno zapojení třetí osoby, bude se jednat o subjekty posuzování shody. Subjekt posuzování shody musí splňovat podmínky stanovené aktem o kybernetické odolnosti, zejména týkající se odbornosti, nezávislosti a nestrannosti, a musí být oznámen Komisi a ostatním členským státům příslušným oznamujícím orgánem členského státu.[50] Subjekty posuzování shody zároveň mohou splnění způsobilosti prokázat osvědčením o akreditaci vydaným na základě nařízení (ES) č. 765/2008[51].

Pokud je produkt s digitálními prvky v souladu s aktem o kybernetické odolnosti, nesmí členské státy bránit jeho dodávání na trh, pouze však pro hlediska, na něž se akt o kybernetické odolnosti vztahuje. Pro jiná hlediska mohou členské státy dodávání konkrétního produktu s digitálními prvky bránit, pouze však v případě, že se tím nedostanou do rozporu s jinou unijní legislativou či judikaturou[52].

6. HLAVNÍ POVINNOSTI HOSPODÁŘSKÝCH SUBJEKTŮ

Akt o kybernetické odolnosti by měl ukládat povinnosti širokému spektru hospodářských subjektů od výrobců a jejich zmocněných zástupců přes dovozce a distributory až po jakékoli osoby, které provedou podstatnou změnu produktu s digitálními prvky.

Největší porce povinností by se měla vztahovat na výrobce, kterým se rozumí „*jakákoli fyzická nebo právnická osoba která vyvíjí nebo vyrábí produkty s digitálními prvky nebo která nechala produkty s digitálními prvky navrhnout, vyvinout nebo vyrobit a uvádí je na trh pod svým jménem nebo ochrannou známkou, ať už za úplatu, nebo bezplatně*“[53]. Pokud však dovozce nebo distributor uvede na trh produkt s digitálními prvky pod svým jménem nebo

[50] Podrobněji viz čl. 29 a násl. aktu o kybernetické odolnosti.

[51] Nařízení Evropského parlamentu a Rady (ES) 765/2008 kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93.

[52] Srov. zejména rozhodnutí Soudního dvora ve věci 120/78 „Cassis de Dijon“ a nařízení (EU) 2019/515 o vzájemném uznávání zboží uvedeného v souladu s právními předpisy na trh v jiném členském státě.

[53] Čl. 3 odst. 18 aktu o kybernetické odolnosti.

ochrannou známkou, vztahují se na něj povinnosti výrobce a je považován pro účely aktu o kybernetické odolnosti za výrobce. Stejný důsledek má i provedení podstatné změny produktu s digitálními prvky již uvedeného na trh dovozcem či distributorem. Podobné důsledky nastávají i pro jakoukoli třetí osobu, která provede podstatnou změnu produktu s digitálními prvky. Taková osoba se považuje za výrobce a vztahují se na ní relevantní povinnosti, pokud jde o část produktu, která je podstatnou změnou ovlivněna, případně dokonce ve vztahu k celému produktu, jestliže byla podstatnou změnou ovlivněna kybernetická bezpečnost produktu s digitálními prvky jako celku[54]. Podstatnou změnou produktu se přitom rozumí „*změna produktu s digitálními prvky po jeho uvedení na trh, která ovlivňuje soulad produktu s digitálními prvky se základními požadavky stanovenými v oddílu 1 přílohy I nebo vede ke změně zamýšleného použití, pro které bylo provedeno posouzení produktu s digitálními prvky*“[55].

Případná změna produktu s digitálními prvky má významný dopad i pokud je provedena přímo výrobcem po uvedení produktu na trh. Výrobce by měl nejprve vyhodnotit, zda taková změna naplňuje definici podstatné změny a v případě kladného výsledku provést ověření shody s požadavky nařízení, případně nové posouzení shody. Pokud „*aktualizace softwaru mění původní zamýšlené funkce, druh nebo výkon produktu a tyto změny nebyly v původním posouzení rizik předvídány nebo se změnila povaha nebezpečí nebo se v důsledku aktualizace softwaru zvýšila úroveň rizika*“[56], měl by být software považován za podstatně změněný. V případě software je provádění změn ve formě aktualizací časté a obvyklé, řada aktualizací směřuje ke zvýšení výkonu, optimalizaci chodu, rozšíření funkcionalit nebo ke zvýšení bezpečnosti produktu. Jestliže každá aktualizace bude na straně výrobců vyvolávat nutnost interního posouzení, zda je podstatnou změnou a případně nutnost nového posouzení shody, může to vést paradoxně ke zhoršení bezpečnosti software nebo nežádoucímu zpomalení jeho vývoje[57].

[54] Čl. 15 a čl. 16 aktu o kybernetické odolnosti.

[55] Čl. 3 bod 31 aktu o kybernetické odolnosti.

[56] Recitál 22 aktu o kybernetické odolnosti.

Kromě již zmíněné povinnosti provést odpovídající postupy posuzování shody jsou výrobci zejména povinni při uvádění produktu s digitálními prvky na trh zajistit návrh, vývoj a výrobu produktu v souladu se základními požadavky stanovenými v oddíle 1 přílohy I včetně provedení posouzení kybernetických bezpečnostní rizik spojených s produktem. Toto posouzení musí být součástí povinně pořizované technické dokumentace produktu s digitálními prvky, jejíž náležitosti stanoví příloha V návrhu. Technickou dokumentaci musí výrobce průběžně aktualizovat po dobu očekávané životnosti produktu nebo po dobu pěti let od uvedení produktu na trh, podle toho, která doba je kratší, a uchovat jí pro potřeby dozorových orgánů po dobu deseti let od uvedení produktu s digitálními prvky na trh. Pro sériově vyráběné produkty (což bude většina) musí výrobci zajistit, že zůstanou ve shodě po celou dobu výroby.

Důležitou skupinu povinností lze zkráceně označit jako due diligence ve vztahu k dodavatelům. Výrobci musí při začleňování součástí od třetích stran do svého produktu s digitálními prvky postupovat s náležitou péčí a zajistit, aby tyto součásti neohrožovaly bezpečnost produktu. Součástí této povinnosti je i pořízení softwarového kusovníku, což je „*formální záznam obsahující podrobnosti o dodavatelském řetězci a vztazích v něm u součástí začleněných do softwarových prvků produktu s digitálními prvky*“[58]. I po uvedení produktu s digitálními prvky na trh musí výrobce systematicky dokumentovat relevantní aspekty kybernetické bezpečnosti vztahující se k produktu, a zejména zajistit odhalování a řešení zranitelností.

Další skupinu tvoří informační povinnosti výrobce vůči uživatelům. Výrobce je jednak povinen k produktu s digitálními prvky umístit označení CE[59], vydat a k produktu přiložit prohlášení o shodě. Tím však jeho informační povinnost nekončí. Výrobce je povinen zajistit, aby k produktům

[57] Srov např. Digitaleurope. Cybersecurity everywhere: deciphering the Cyber Resilience Act. [online]. 23. 1. 2023. [cit. 16. 4. 2023]. Dostupné z: https://www.digitaleurope.org/policies/cybersecurity/ nebo BSA Recommendations on the EU Cyber Resilience Act. [online]. 2022. [cit. 30. 11. 2022]. Dostupné z: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Akt-o-kyberneticke-odolnosti-nova-pravidla-kyberneticke-bezpecnosti-pro-digitalni-produkty-a-podpurne-sluzby_cs.

[58] Čl. 3 bod 37 aktu o kybernetické odolnosti.

byly elektronicky nebo ve fyzické podobě připojeny informace a pokyny, které musí být jasné, srozumitelné, snadno pochopitelné, čitelné a v jazyce snadno srozumitelném uživatelům a jejichž minimální náležitosti stanoví příloha II nařízení. Výrobce je rovněž povinen informovat uživatele o incidentech a souvisejících nápravných opatřeních nebo o ukončení své činnosti.

Poslední skupinou povinností výrobců jsou povinnosti týkající se spolupráce s orgány dozoru. Výrobci jsou povinni poskytnout kterémukoli orgánu dozoru nad trhem na jeho žádost všechny informace nezbytné k prokázání shody produktu s digitálními prvky a výrobcem zavedených postupů se základními požadavky podle přílohy I, a dále s orgánem dozoru spolupracovat na odstranění kybernetických bezpečnostních rizik produktů s digitálními prvky, které uvedli na trh. Pokud výrobce ukončí činnost a není tak schopen plnit své povinnosti, je o tom rovněž povinen předem informovat orgány dozoru nad trhem.

Z hlediska ochrany před kybernetickým nebezpečím je obzvlášť důležitá povinnost výrobce informovat agenturu ENISA o každé aktivně zneužívané zranitelnosti produktu s digitálními prvky a o jakémkoli incidentu s dopadem na bezpečnost produktu, a to bez zbytečného odkladu nejpozději však do 24 hodin poté, co se o těchto skutečnostech dozví.

Povinnosti dovozců a distributorů se pak vztahují zejména k zajištění nebo ověření splnění povinností výrobce, informačních povinností a spolupráce s orgány dozoru nad trhem[60].

7. DOZOR A VYMÁHÁNÍ

Pro dozor nad trhem a kontrolu se použije nařízení Evropského parlamentu a Rady (EU) 2019/1020[61]. Každý členský stát je povinen určit jeden nebo

[59] Podrobnosti ke způsobu připojení CE označení stanoví čl. 22 aktu o kybernetické odolnosti, který zohledňuje i specifika jednotlivých typů produktů s digitálními prvky, kdy v případě softwaru postačuje např. uvedení označení na internetových stránkách.

[60] K povinnostem dovozců a distributorů podrobněji viz čl. 13 a čl. 14 aktu o kybernetické odolnosti.

[61] Nařízení Evropského parlamentu a Rady (EU) 2019/1020 ze dne 20. června 2019 o dozoru nad trhem a souladu výrobků s předpisy a o změně směrnice 204/42/ES a nařízení (ES) č. 765/2008 a (EU) č. 305/2011.

více orgánů dozoru nad trhem pro účely zajištění provádění aktu o kybernetické odolnosti. Může se jednat o orgány nové nebo stávající. Orgány dozoru nad trhem mají povinnost vzájemné spolupráce za účelem jednotného uplatňování nařízení včetně vytvoření specializované skupiny pro správní spolupráci[62] nebo organizování společných kontrolních akcí (tzv. „sweepy")[63]. V případě vzniku podezření, že produkt s digitálními prvky včetně řešení jeho zranitelností představuje významné bezpečnostní riziko, je orgán dozoru povinen provést jeho hodnocení z hlediska souladu se všemi požadavky stanovenými aktem o kybernetické odolnosti. Důsledkem zjištěného nesouladu může být uložení povinnosti přijmout vhodná opatření příslušnému hospodářskému subjektu, v krajním případě až zákaz dodávání produktu na trh příslušného státu nebo povinnost jeho stažení z trhu či oběhu. V případě odůvodněných opatření jsou ostatní členské státy povinny přijmout nezbytná opatření k zajištění stažení nevyhovujícího produktu s digitálními prvky i z jejich trhů.

Zajímavým nástrojem je možnost vyžadovat přijetí dalších dodatečných opatření u produktů s digitálními prvky, které jsou v souladu s aktem o kybernetické odolnosti, přesto však představují významné kybernetické bezpečnostní riziko, a navíc riziko pro zdraví nebo bezpečnost osob, pro dodržování povinností podle unijního nebo vnitrostátního práva, jejichž cílem je ochrana základních práv, pro pravost, důvěryhodnost nebo důvěrnost služeb nabízených prostřednictvím elektronického informačního systému základními subjekty podle směrnice NIS2 nebo pro jiné aspekty ochrany veřejného zájmu. Takto může postupovat dozorový orgán členského státu na základě vlastního provedeného hodnocení nebo z podnětu Komise. Komise má také rozhodující slovo při posouzení důvodnosti přijatých opatření[64].

Stanovení pravidel ukládání a prosazování sankcí za porušení nařízení má být svěřeno členským státům. Sankce musí být přiměřené, účinné a odrazující, návrh nařízení stanoví pouze horní hranici správních pokut a zá-

[62] Čl. 41 odst. 11 aktu o kybernetické odolnosti.

[63] Čl. 49 aktu o kybernetické odolnosti.

[64] Podrobněji viz čl. 46 aktu o kybernetické odolnosti.

kladní pravidla jejich vyměřování stanovením okolností, které musí brát orgán dohledu v úvahu[65].

V návrhu jsou určité činnosti svěřeny rovněž agentuře ENISA, a to zejména v oblasti koordinace a předávání informací o zranitelnostech CSIRT týmům členských států a Evropské síti styčných organizací pro řešení kybernetických krizí (EU-CyCLONe), zpracování zpráv o nových trendech v oblasti kybernetických bezpečnostních rizik produktů s digitálními prvky a spolupráce s Komisí v případě produktů s digitálními prvky představujících významné kybernetické bezpečnostní riziko.

8. POTENCIÁLNĚ PROBLEMATICKÉ SOUVISLOSTI

Tato část článku je věnována některým potenciálně problematickým důsledkům přijetí navrhované úpravy. Nečiní si nárok na úplnost, zajisté lze najít i další problematické konsekvence, ani na nevyvratitelnou správnost. Účelem je spíše podnítit čtenáře k dalšímu přemýšlení nad návrhem a vyvolat diskuzi.

Posuzování shody produktů s digitálními prvky je podle aktu o kybernetické odolnosti vztaženo objektově, tedy k produktu s digitálními prvky. Bezpečnostní požadavky uvedené v oddíle 1 přílohy I aktu o kybernetické odolnosti se týkají vlastností samotného produktu s digitálními prvky. Požadavky na řešení zranitelností v oddíle 2 přílohy I aktu o kybernetické odolnosti se vztahují k procesu řešení zranitelností, ale pouze příslušného produktu s digitálními prvky, nevztahují se k výrobním ani jiným procesům výrobce jako subjektu, nezohledňují další rizikové faktory jako např. ovládání výrobce. Přitom v dnešní době spočívá kybernetické bezpečnostní riziko často nikoli pouze v technickém řešení produktu, jako spíše v jeho výrobci a geopolitických souvislostech zázemí výrobce. Příkladem jsou např. významná varování NÚKIB z roku 2018 před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation[66]

[65] Podrobněji k sankcím viz čl. 53 aktu o kybernetické odolnosti.

[66] Varování NÚKIB ze dne 17. 12. 2018 před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation. [online]. 2018. [cit. 15. 11. 2022]. Dostupné z: https://nukib.cz/cs/uredni-deska/.

a z roku 2022 před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím, kde NÚKIB uvádí: „*Kybernetická bezpečnost nespočívá pouze na posuzování technických aspektů používaných technologií, ale například při výběru dodavatelů je nutné zvážit i netechnické aspekty bezpečnosti daných technologií, tedy posoudit důvěryhodnost dodavatelů a poddodavatelů (výrobců) dané technologie*“[67]. V současnosti v České republice vzniká návrh zákona, který by měl zavést mechanismus prověřování dodavatelů technologických prvků nejvýznamnější (strategické) infrastruktury a v případě jejich vysoké rizikovosti omezit využití takových dodavatelů pro tyto nejkritičtější infrastruktury[68]. Návrh aktu o kybernetické odolnosti takovéto aspekty nereflektuje. Výslovně však zmiňuje možnost členských států zohlednit i netechnické aspekty kybernetické bezpečnosti včetně nežádoucího vlivu třetí země na dodavatele v souvislosti s potřebou zajištění vysoké úrovně odolnosti a koordinovaným posouzením rizik kritických dodavatelských řetězců ve smyslu směrnice NIS2[69]. Dále může členský stát, resp. jeho orgán dozoru nad trhem, postupovat podle čl. 46 aktu o kybernetické odolnosti upravujícího postup v případě vyhovujících produktů představujících významné kybernetické bezpečnostní riziko. Podle čl. 46 však nestačí k tomuto postupu pouhá skutečnost, že produkt představuje významné kybernetické riziko, ale musí vyvolat i další riziko ve vyjmenovaných oblastech jako je např. zdraví nebo bezpečnost osob.

Problematické je vymezení působnosti aktu o kybernetické odolnosti ve vztahu k software poskytovanému formou služby (SaaS) s ohledem na formulaci výjimky pro zpracování dat na dálku. Na problematičnost a nejasnost tohoto vymezení poukazují četní zástupci veřejnosti v rámci veřejné

[67] Varování NÚKIB ze dne 30. 5. 2022 před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím. [online]. 2022. [cit. 15. 11. 2022]. Dostupné z: https://nukib.cz/cs/uredni-deska/.

[68] Viz NÚKIB. Stát vstupuje do závěrečné fáze přípravy návrhu zákona o snižování rizik spojených s dodavateli informačních a komunikačních technologií. [online]. 2022. [cit. 25. 11. 2022]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1911-stat-vstupuje-do-zaverecne-faze-pripravy-navrhu-zakona-o-snizovani-rizik-spojenych-s-dodavateli-informacnich-a-komunikacnich-technologii/

[69] Viz recitál 33 aktu o kybernetické odolnosti.

diskuze k návrhu[70] a organizace expertů nebo výrobců[71]. Samotná skutečnost, že v podstatě všichni komentující považují vymezení dopadu aktu o kybernetické odolnosti na poskytování software nebo platforem formou služby za nejasné, je známkou toho, že by příslušná ustanovení měla být přepracována. Nesrozumitelnost nebo nejasnost právní normy pro její adresáty je třeba považovat za nedostatek významně snižující právní jistotu, která je jedním z účelů práva, proto je žádoucí takový nedostatek v legislativním procesu odstranit. Nařízení se řadí k předpisům produktové bezpečnosti NLF, je logické nevztahovat je na služby, nicméně to neznamená, že by nutně měly být vyňaty produkty s digitálními prvky používané k poskytování těchto služeb. Výklad působnosti norem NLF zahrnuje pod pojem *dodání na trh* rovněž poskytování výrobků formou výpůjčky, leasingu, nájmu[72], obecněji tedy jakékoli dodání za účelem použití v rámci obchodní činnosti. Poskytování software formou služby se s ohledem na jeho nehmotnou podstatu, kdy zákazník software jako takový neužívá, ale čerpá pouze výsledky služby, samozřejmě liší od nájmu nebo výpůjčky hmotného produktu. Pro samotný software užívaný k poskytování služby, nikoli však pro službu jako takovou, by podle mého názoru mělo být splnění požadavků nařízení požadováno. Text nařízení by měl v této otázce být jasný a srozumitelný.

---

[70] Viz např. Evropská komise. Podělte se o svůj názor. Akt o kybernetické odolnosti – nová pravidla kybernetické bezpečnosti pro digitální produkty a podpůrné služby. The Federation of Finnish Enterprises. nebo BSA Recommendations on the EU Cyber Resilience Act. [online]. 2022. [cit. 30. 11. 2022]. Obojí dostupné z: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Akt-o-kyberneticke-odolnosti-nova-pravidla-kyberneticke-bezpecnosti-pro-digitalni-produkty-a-podpurne-sluzby_cs.

[71] Srov. např. Center for Data Innovation. Feedback to the European Commission on the Draft Cyber Resilience Act. [online]. 15. 12. 2022. [cit. 16. 4. 2023]. Dostupné z: https://datainnovation.org/2022/12/feedback-to-the-european-commission-on-the-draft-cyber-resilience-act/ nebo Digitaleurope. Cybersecurity everywhere: deciphering the Cyber Resilience Act. [online]. 23. 1. 2023. [cit. 16. 4. 2023]. Dostupné z: https://www.digitaleurope.org/policies/cybersecurity/

[72] Viz „Modrá příručka“ k provádění pravidel EU pro výrobky 2022. 2022/C 247/01. s. 19 [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC.

K nejasným a veřejností hojně kritizovaným ustanovením patří dále vymezení výjimky pro software s otevřeným zdrojovým kódem[73]. V důsledku požadavku na dodávání mimo rámec obchodní činnosti a zároveň široce pojatý rozsah toho, co vše je uvedením produktu na trh, vznikají otázky, jaké všechny aktivity poskytnutí open source software lze ještě vnímat jako nekomerční a jaké již nikoli. Vzhledem k (nejen) ekonomickému významu, který má open source software celosvětově pro rozvoj celého IT odvětví, je zároveň na místě vymezit vztah aktu o kybernetické odolnosti k regulaci tohoto typu software přímo v normativním textu.

Dalším potenciálně problematickým místem je stanovení povinnosti výrobcům produktů s digitálními prvky po očekávanou dobu životnosti produktu nebo po dobu pěti let od jeho uvedení na trh – podle toho, která doba je kratší – zajistit, že je se zranitelnostmi tohoto produktu nakládáno účinně a v souladu se základními požadavky stanovenými v oddíle 2 přílohy I[74], což mj. zahrnuje poskytování bezpečnostních aktualizací. Návrh ale neobsahuje žádnou definici ani pravidla pro určení *očekávané doby životnosti*. Zejména v případě software je stanovení očekávané doby životnosti problematické. Lze jí chápat tak, že očekávaná doba životnosti končí vydáním nové verze téhož software? To by dávalo logický smysl z pohledu výrobců, kteří by nemuseli podporovat řešení zranitelností u více verzí téhož software najednou. Ovšem z pohledu uživatelů jde, zejména v případě placeného software, o situaci významně nežádoucí, která by je nutila k pořizování dalších verzí. Očekávanou dobu životnosti by mohl uvádět přímo výrobce, nicméně to by si pak výrobce sám stanovil dobu, po kterou je povinen zranitelnosti produktu řešit a regulace této doby v právním aktu by ztrácela význam.

Zavedení nové regulace bude pro výrobce produktů s digitálními prvky představovat nové náklady zejména na zajištění compliance, due diligence dodavatelského řetězce nebo nutné administrativy, ať již v podobě interních (např. nutnost najmout nové zaměstnance) nebo externích (zejm. na posouzení shody subjektem posuzování shody) nákladů. Logika fungování

[73] Viz recitál 10 aktu o kybernetické odolnosti.

[74] Viz čl. 10 odst. 6 aktu o kybernetické odolnosti.

trhu vede k závěru, že tyto náklady se pravděpodobně promítnou do ceny produktů s digitálními prvky jejím navýšením[75]. To by v případě významnějšího navýšení ceny mohlo vést zejména u spotřebitelů k nákupu alternativních produktů s digitálními prvky ze třetích zemí, které podobné regulaci nepodléhají a jsou proto levnější. V takovém případě by se částečně ztrácel Komisí očekávaný efekt jak celkového zvýšení kybernetické bezpečnosti navzájem propojených zařízení, tak ekonomické stimulace výroby produktů s digitálními prvky v Unii a zvýšení poptávky po nich i mimo EU[76]. Publikované výzkumy svědčí spíše o opaku, kdy většina spotřebitelů uvádí ochotu zaplatit vyšší cenu za bezpečnější produkt s digitálními prvky[77], je však namístě zmínit, že tyto výzkumy vycházejí z dotazníkových šetření, nikoli reálného tržního chování, a byly provedeny v ekonomicky silných státech. Jejich závěry tak nemusí platit pro trhy slabších ekonomik východní nebo jižní Evropy. Podíl spotřebitelů na poptávkové straně trhu produktů s digitálními prvky je, přinejmenším v případě softwaru, pravděpodobně významně menší[78] než podíl hospodářských subjektů, toto spotřebitelské chování (pokud k němu dojde) tak zřejmě nebude mít významnější dopad.

Navýšení nákladů přitom nejcitelněji dopadne zejména na malé a střední podniky („SMEs“) včetně start-upů a technologických inovátorů. SMEs tvoří většinu výrobců produktů s digitálními prvky v Unii, ačkoli jejich tržní podíl tomu neodpovídá. Např. na trhu softwarových produktů SMEs představují více než 99 % hospodářských subjektů, většinu (59 %)

[75] Srov. Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. SWD (2022) 282 final. Part 1/3. s. 62. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment

[76] Viz důvodová zpráva aktu o kybernetické odolnosti.

[77] Srov. Blythe, J.M., Johnson, S.D. & Manning, M. What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. Crime Science. 9, 1 (2020). https://doi.org/10.1186/s40163-019-0110-3.

[78] Srov. Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. SWD (2022) 282 final. Part 1/3. s. 25. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment

obratu ale vytváří několik „velkých hráčů“[79]. Navýšení nákladů přitom bude mít jasně závažnější dopad na SMEs než na kapitálově silné velké korporace[80], což může vést v některých případech k další redukci jejich podílu na trhu. Obava ze zatížení dopadajícího na SMEs z řad výrobců se opakovaně objevuje i v rámci veřejné diskuze ze strany jednotlivých podniků i jejich asociací.[81]

Do kategorie SMEs spadají i mikropodniky[82], které tvoří dokonce 94 % SMEs působících na softwarovém trhu Unie[83]. Realita přinejmenším v České republice je taková, že významnou část těchto „mikropodniků“ představují ve skutečnosti vývojáři – jednotlivci zcela bez zaměstnanců působící jako tzv. „freelanceři“, tedy samostatní podnikatelé (v ČR v režimu živnostenského podnikání) pracující na různých softwarových projektech, jak pro zákazníky z řad korporací, tak nezávisle z vlastní iniciativy . Tito vývojáři se budou ocitat v různém právním postavení podle toho, zda software samostatně vyvíjejí a dodávají pod svým jménem, nebo působí pouze jako členové většího vývojářského týmu pro projekt řízený jinou (zpravidla právnickou) osobou, která software uvádí na trh pod svým jménem nebo

---

[79] Viz Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. SWD (2022) 282 final. Part 1/3. s. 24. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment

[80] Podrobněji viz Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. SWD (2022) 282 final. Part 1/3, s. 55-56 [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

[81] Podrobněji srov. Evropská komise. Podělte se o svůj názor. Akt o kybernetické odolnosti – nová pravidla kybernetické bezpečnosti pro digitální produkty a podpůrné služby. The Federation of Finnish Enterprises. [online]. 2022. [cit. 15. 11. 2022]. Dostupné z: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410 Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services/feedback_en?p_id=31490443

[82] Mikropodnikem je podnik s 0-9 zaměstnanci.

[83] Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. SWD (2022) 282 final. Part 2/3, s. 29. [online] 2022. [cit. 8. 11. 2022]. Dostupné z: https://digital-strategy-.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

ochrannou známkou. V případě samostatně vyvíjeného software, který vývojář nabízí nebo dodává svým jménem, se bude dostávat do postavení výrobce a bude muset plnit povinnosti stanovené aktem o kybernetické odolnosti, což bude pro jednotlivce znamenat velkou administrativní zátěž.

Povinnost zaobírat se kybernetickou bezpečností, podstoupit proces posuzování shody a vytvářet povinnou dokumentaci může vést rovněž k prodloužení doby vývoje a výroby produktu s digitálními prvky oproti konkurenci, což může mít za následek ztrátu konkurenční výhody prvního uvedení určitého typu produktu nebo jeho nové verze na globální trh oproti výrobcům ze třetích zemí[84]. Mimoevropští výrobci mohou dát přednost prvotnímu uvedení nového produktu s digitálními prvky nejprve na trzích s méně náročnými legislativními požadavky, a až posléze uvést produkt na trh také v Unii, což by mohlo mít za následek technologické zaostávání unijního trhu za zbytkem světa, zejména asijskými trhy.

Uplatňování aktu o kybernetické odolnosti podstatně zatíží nejen výrobce, ale i subjekty posuzování shody a vnitrostátní orgány dozoru nad trhem. S ohledem na množství běžně používaných produktů s digitálními prvky, které narůstá doslova na denní bázi, a jejich rozdílnost a složitost je jen obtížně představitelné, že orgány dozoru nad trhem budou skutečně schopny provádět efektivní dozor a kontrolu dodržování nové regulace.

9. ZÁVĚR

Akt o kybernetické odolnosti by měl navázat na stávající unijní právní úpravu a doplnit chybějící část v podobě regulace produktové kybernetické bezpečnosti. Legislativně technicky odpovídá ostatním předpisům nového legislativního rámce (NLF), atypický je ale svou horizontální působností, která má zahrnovat širokou škálu navzájem odlišných produktů. Potřebnost přijetí aktu o kybernetické odolnosti lze mít za dostatečně odůvodněnou jednak nutností ochrany práv jednotlivců, která mohou být v době digitálně propojeného internetu věcí (IoT) zranitelností produktů s digitálními prvky

[84] K otázce výhody prvního uvedení na trh srov. Evropská Komise. Commission staff working document. Impact Assessment Report. Part 1/3. SWD (2022) 282 final. s. 11. s. 64. [online]. 2022. [cit. 1. 11. 2022] Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

ohrožena, a zároveň zjevným selháváním trhu v této oblasti. Ze stávající zkušenosti je zřejmé, že motivace výrobců zavést opatření posilující kybernetickou bezpečnost jejich produktů bez existence regulatorního tlaku, je nedostatečná[85].

Nové nařízení bude přínosem pro koncové uživatele produktů s digitálními prvky, ať již z řad spotřebitelů, podnikatelů nebo správců kritických informačních infrastruktur, kteří se budou moci spolehnout na minimální standard kybernetické bezpečnosti všech produktů s digitálními prvky dodávaných na trh v Unii bez nutnosti složitě získávat dnes často nedostupné informace. Skutečnost, že se jedná o jednotnou regulaci pro celý společný trh, by měla být přínosem i pro výrobce, dovozce a distributory produktů s digitálními prvky, kteří se tak budou moci spoléhat na stejná pravidla platná pro celý trh Unie bez nutnosti zajišťovat soulad se standardy stanovenými jednotlivými státy. Uživatelé z řad povinných subjektů podle směrnice NIS2 ale budou muset stejně zvažovat i u produktů uvedených na trh v souladu s tímto nařízením, zda neexistují i jiná (netechnická) rizika kybernetické bezpečnosti spojená s užíváním těchto produktů. Otázkou je, zda by nebylo vhodnější přímo v aktu o kybernetické odolnosti upravit právě i zohlednění těchto typů rizik.

Z hlediska znění textu nařízení by bylo vhodné, aby akt o kybernetické odolnosti jasně definoval, zda nebo kdy se vztahuje na software nabízený formou služby a kdy nikoli. Stejně tak by bylo vhodné doplnit pravidla nebo alespoň výkladová vodítka pro určení očekávané doby životnosti. Rovněž částečné vynětí open source softwaru z působnosti nařízení by bylo vhodné zakotvit přímo v normativním textu nikoli pouze v recitálu a učinit je jasnějším.

Z hlediska faktických dopadů nové regulace lze očekávat u výrobců software a hardware, přinejmenším v počátečním období, navýšení nákladů na

[85] Srov. TOMLINSON, Andrew; PARKIN, Simon; SHAIKH, Siraj Ahmed. Drivers and barriers for secure hardware adoption across ecosystem stakeholders. Journal of Cybersecurity, 2022, roč 8., č. 1, s. 7. nebo Evropská Komise. Commission staff working document. Impact Assessment Report. Part 1/3. SWD (2022) 282 final. s. 17. [online]. 2022. [cit. 1. 11. 2022] Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

vývoj a výrobu produktů s digitálními prvky, které může být pro výrobce z řad SMEs problematické a může vést k posílení tržního postavení kapitálově silných „velkých hráčů“ na úkor inovativních start-upů a jiných menších podniků nebo nezávislých vývojářů. Z pracovních dokumentů Komise je zřejmé, že si je tohoto nebezpečí vědoma. Pro snížení zátěže spojené s adaptací na novou právní úpravu by proto bylo vhodné zavést opatření, například ve formě bezplatného přístupu k odpovídajícím metodickým nástrojům, postupům, šablonám a dalším informacím, která zejména malým a středním podnikům tento proces usnadní.

10. SEZNAM ZDROJŮ

[1] Blythe, J.M., Johnson, S.D. & Manning, M. What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. Crime Science. 2022, č. 9. https://doi.org/10.1186/s40163-019-0110-3.

[2] Chiarra, P. G. The Cyber Resilience Act: the EU Commission’s proposal for a horizontal regulation on cybersecurity for products with digital elements. Int. Cybersecur. Law Rev. 2022, č. 3, s. 255–272. https://doi.org/10.1365/s43439-022-00067-6.

[3] Tomlinson, A. Parkin, S. Shaikh, S.A. Drivers and barriers for secure hardware adoption across ecosystem stakeholders. Journal of Cybersecurity, 2022, roč 8., č. 1, s. 1-14. https://academic.oup.com/cybersecurity/article/8/1/tyac009/6656148?searchresult=1

[4] Evropská Komise. Společné sdělení Evropskému parlamentu a Radě Strategie kybernetické bezpečnosti EU pro digitální dekádu. JOIN (2020) 18 final. [online]. 202. [cit. 1. 11. 2022] Dostupné z: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN.

[5] Evropská Komise. Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů. Digitální kompas 2030: Evropské pojetí digitální dekády. COM (2021) 118 final, [online]. 2020. [cit. 1. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52021DC0118.

[6] Projev předsedkyně Komise von der Leyenové o stavu Unie v roce 2021. [online]. 2021. [cit. 1. 11. 2022]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701.

[7] Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020, COM/2022/454 final. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52022PC0454&qid=1667332176493.

[8] Evropská Komise. Sdělení Komise. „Modrá příručka“ k provádění pravidel EU pro výrobky 2022. 2022/C 247/01. s. 9-10. [online]. 2022. [cit. 8. 11. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2022:247:TOC.

[9] Evropská Komise. Commission staff working document. Impact Assessment Report. Part 1/3. SWD (2022) 282 final. [online]. 2022. [cit. 1. 11. 2022] Dostupné z: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-impact-assessment.

[10] Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o obecné bezpečnosti výrobků, o změně nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 a o zrušení směrnice Rady 87/357/EHS a směrnice Evropského parlamentu a Rady 2001/95/ES. COM/2021/346 final. [online]. 2022. [cit. 6. 11. 2022] Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A52021PC0346

[11] Rozsudek Soudního dvora ze dne 20. února 1979 ve věci 120/78 „Cassis de Dijon". ECLI:EU:C:1979:42. Dostupné z : https://curia.europa.eu/jcms/jcms/Jo1_6308/

[12] Varování NÚKIB ze dne 17. 12. 2018 před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation. [online]. 2018. [cit. 15. 11. 2022]. Dostupné z: https://nukib.cz/cs/uredni-deska/

[13] Varování NÚKIB ze dne 30. 5. 2022 před použitím chytrých elektroměrů ze zemí s nedůvěryhodným právním prostředím. [online]. 2022. [cit. 15. 11. 2022]. Dostupné z: https://nukib.cz/cs/uredni-deska/.

[14] Podělte se o svůj názor. Akt o kybernetické odolnosti – nová pravidla kybernetické bezpečnosti pro digitální produkty a podpůrné služby. [online]. 2022. [cit. 15. 11. 2022]. Dostupné z: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Akt-o-kyberneticke-odolnosti-nova-pravidla-kyberneticke-bezpecnosti-pro-digitalni-produkty-a-podpurne-sluzby_cs.

[15] NÚKIB. Stát vstupuje do závěrečné fáze přípravy návrhu zákona o snižování rizik spojených s dodavateli informačních a komunikačních technologií. [online]. 2022. [cit. 25. 11. 2022]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1911-stat-vstupuje-do-zaverecne-faze-pripravy-navrhu-zakona-o-snizovani-rizik-spojenych-s-dodavateli-informacnich-a-komunikacnich-technologii/

[16] Digitaleurope. Cybersecurity everywhere: deciphering the Cyber Resilience Act. [online] 2023. [cit. 16. 4. 2023]. Dostupné z: https://www.digitaleurope.org/policies/cybersecurity/

[17] Center for Data Innovation. Feedback to the European Commission on the Draft Cyber Resilience Act. [online] 2022. [cit. 16. 4. 2023]. Dostupné z: https://datainnovation.org/2022/12/feedback-to-the-european-commission-on-the-draft-cyber-resilience-act/

https://doi.org/10.5817/RPT2023-1-2

VIRTUÁLNÍ AKTIVA A VIRTUÁLNÍ MĚNY – OBSAH A VÝVOJ POJMU, PRÁVNÍ POVAHA, REGULACE A MOŽNÁ ÚSKALÍ

ANETA SCHWARZOVÁ[1]

ABSTRAKT

Příspěvek je zaměřen na aktuální problematiku virtuálních aktiv, virtuálních měn a jejich vývoj v posledních letech. Autorka blíže specifikuje jednotlivá hlediska, jakými na virtuální aktiva právo nahlíží. Kromě dílčích ustanovení, která se vyskytují v českém právním řádu, stanovisek tuzemských institucí a pohledů z řad odborné veřejnosti, uvádí také příklady zahraničních úprav, které jsou zastoupeny podle různých přístupů v daných státech k této problematice. Ve svém příspěvku upozorňuje na možná úskalí, která se promítají do různých sfér a zamýšlí se nad případnými způsoby, jaká možná řešení tyto situace nabízejí.

KLÍČOVÁ SLOVA

Virtuální aktiva; virtuální měny; kryptoměny; Bitcoin; blockchain; AML zákon; MiCA; balíček digitálních financí

ABSTRACT

The paper focuses on current issues with virtual assets, virtual currencies and their development in recent years. The author provides a detailed examination of the various ways in which the law views virtual assets. In addition to examining

[1] JUDr. Aneta Schwarzová je doktorandkou na Fakultě právnické Západočeské univerzity v Plzni na katedře občanského práva, kontaktní e-maily: *aschwarz@kpo.zcu.cz, schwarzova.aneta@seznam.cz.*

partial provisions in the Czech legal system, the author also considers the opinions of domestic institutions, the views of the professional community, and provides examples of foreign regulations that could be used as inspiration for de lege ferenda considerations. The author draws attention to potential pitfalls in various areas and offers suggestions for addressing these issues.

KEY WORDS

Virtual assets; Virtual Currencies; Cryptocurrencies; Bitcoin; Blockchain; AML Law; MiCA; Digital Finance Package

1. ÚVOD

Nelze přehlédnout, že se v posledních letech problematika virtuálních aktiv dosti radikálně prosazuje a dostává do popředí zájmu širší veřejnosti. Především díky prudkému nárůstu ceny bitcoinu v posledních letech, se zájem o tuto oblast rapidně zvýšil. Stále se rozšiřuje síť míst, kde lze virtuálními aktivy běžně platit.[2] Není tomu tak dávno, kdy by se zdála dnešní realita jen těžko uvěřitelnou. V současné době se v České republice nachází k čtyřem tisícům obchodů, kde virtuální měny přijímají.[3] V roce 2022 se na světě nacházelo už více než 16 500 bitcoinmatů,[4] z toho na našem území přibližně kolem padesáti.[5] Jak už název napovídá, účelem bitcoinmatů je směna státem běžně uznávaných měn za dosud nejrozšířenější kryptoměnu – Bitcoin. Ovšem virtuální aktiva nejsou pouze Bitcoin a kryptoměny, existuje jich celá řada. Na konci roku 2022 existovalo přes 21 800 kryptoměn,[6] zatímco v roce 2018 jich bylo známo pouze 1 400. Dále se současnosti vy-

[2] Kavárny, ubytování, pohonné hmoty aj. více viz: iKrypto.cz. *Kde všude můžeme platit bitcoinem*. [Online] Publikováno 16. 3. 2019 [cit. 31. 1. 2023]. Dostupné z: https://www.ikrypto.cz/kde-vsude-muzeme-platit-bitcoinem/.

[3] Měšec.cz. *V obchodech už zaplatíte kryptoměnou. V Česku jsou jich zatím necelé 4 tisíce.* [Online] Publikováno 23. 10. 2021 [cit. 31. 1. 2023]. Dostupné z: https://www.mesec.cz/clanky/v-obchodech-uz-zaplatite-kryptomenou-v-cesku-je-jich-zatim-necelych-4-tisice/.

[4] E15.cz. *Bitcoinmaty se množí. Hotovost za digitální měnu jde směnit už na 16 500 místech.* [Online] Publikováno 16. 3. 2021. [cit. 31. 1. 2023]. Dostupné z: https://www.e15.cz/kryptomeny/bitcoinmaty-se-mnozi-hotovost-za-digitalni-menu-jde-smenit-uz-na-16-500-mistech-1378796.

[5] Kurzy.cz. *Bitcoinmaty, bitcoin bankomaty v ČR.* [Online] © 2000–2022. [cit. 31. 1. 2023]. Dostupné z: https://www.kurzy.cz/bitcoinmaty/.

víjejí stále nové a nové technologie. Kromě „tradičních" kryptoměn dnes existují virtuální aktiva, jako například NFT, která jsou unikátními originály a nabízejí nová využití.

V souvislosti s pokrokem vždy vyvstává řada nových otázek. Jak na tuto sféru nahlíží v tomto případě právo? Co je tedy virtuální měna? Je virtuální měna vůbec měnou? Toto je jen několik málo otázek, kterými se v článku budeme zabývat. Zvláštní prostor bude také věnován Bitcoinu jakožto doposud nejznámější kryptoměně, která významným způsobem přispěla k popularizaci této oblasti. Z původně zanedbatelného, možná až bezvýznamného množství „čehosi", majícího význam a hodnotu hlavně pro počítačové nadšence a pole technického pokroku, se stal fenomén, jenž někteří směle označují jako možné univerzální platidlo budoucnosti.[7] Kromě sféry finančního a daňového práva postupně zasahují virtuální měny a virtuální aktiva obecně i do jiných oblastí.

Virtuální měny postupně způsobují nové situace i v dalších právních oblastech, jakými jsou rodinné právo, dědické právo, právo sociálního zabezpečení, oblast exekuce. Lze konstatovat, že se rozhodně nejedná o ojedinělé operace a zanedbatelnou problematiku. Do budoucna lze předvídat, že se dokonce nárůst zájmu o virtuální aktiva může zvýšit a s ním vyvstane další řada otázek, na které budeme muset hledat odpovědi, přestože v kontextu práva zatím stojí virtuální měny tak trochu stranou. Kromě toho se v souvislosti s těžbou kryptoměn otevírají otázky technologického pokroku a ochrany životního prostředí. Rozhodně se už nyní jedná o velmi zásadní a komplexní téma, které se postupně dostalo do společenského povědomí a přirozeně si našlo své místo.

Téma je pojato především analyticky od obecného ke zvláštnímu. Široký prostor je věnován vymezení pojmů, které s problematikou souvisí, a také jejich povaze. Práce si neklade za cíl vyčerpat takto široké téma, jakým jsou

---

[6] Exploding topics. *How Many Cryptocurrencies are There In 2023?* [Online] Publikováno 25. 11. 2022 [cit. 31. 1. 2023]. Dostupné z: https://explodingtopics.com/blog/number-of-cryptocurrencies.

[7] Česká televize. 90'ČT24. *Bitcoin – univerzální platidlo budoucnosti?*. [Online] Publikováno 15. 8. 2017 [cit. 31. 1. 2023]. Dostupné z: https://www.ceskatelevize.cz/porady/11412378947-90-ct24/217411058130815-bitcoin-univerzalni-platidlo-budoucnosti.

virtuální měny a aktiva, nýbrž poskytnout čtenáři srozumitelný vhled do dané problematiky a poukázat na některé problémy, které v této souvislosti v posledních letech vyvstaly, případně jak je možné je řešit. Práce poskytuje prostor i příkladům zahraniční úpravy a následně také úvaze *de lege ferenda*. Dále je věnována pozornost aktuálně projednávané jednotné právní úpravě Evropské unie v rámci Balíčku digitálních financí, která má dopadat na trh s virtuálními aktivy.

2. VYMEZENÍ POJMŮ

S problematikou virtuálních měn je provázáno několik souvisejících pojmů, které je nutné si nejprve vymezit.

2.1 POJEM VIRTUÁLNÍ MĚNA A POJMY SOUVISEJÍCÍ

Prvním, a pro nás klíčovým pojmem, kterému je třeba věnovat pozornost, je již zmíněný pojem *virtuální měna*. Obsahově se jedná o pojem odlišný od pojmu kryptoměna, digitální měna či digitální peníze.

Digitální měny jsou elektronicky vytvořené a uložené aktivum. Charakteristickým prvkem je neexistence fyzické podstaty. Jsou nadřazeným pojmem pro kryptoměny i pro elektronické peníze. Mohou být využívány k nákupu zboží, služeb či produktů v rámci online her.[8]

Digitální peníze představují peněžní hodnotu uloženou v digitálním médiu. Příkladem může být hodnota uložená na předplacené kartě. Pro digitální peníze lze také použít pojem e-peníze (*e-money tokens* viz dále). Digitální peníze lze dále dělit na centralizované (např. CBDC) a decentralizované (např. Bitcoin).[9]

Kryptoměny jsou typy virtuálních nebo digitálních měn, které jsou ošetřené proti padělání speciálním druhem šifrování,[10] zvaným kryptografie.

[8] DigiSlovník. *Digitální měna.* [Online] Publikováno © 2020 [cit. 31. 1. 2023]. Dostupné z: https://portaldigi.cz/digislovnik/digitalni-mena/.

[9] Evropská centrální banka. *Co jsou peníze?* [Online] Publikováno 24. 11. 2015, aktualizováno 20. 6. 2017 [cit. 31. 1. 2023]. Dostupné z: https://www.ecb.europa.eu/ecb/educational/explainers/tell-me-more/html/what_is_money.cs.html.

[10] Technopedia.com. *Cryptocurrency.* [Online] Publikováno 2019 [cit. 31. 1. 2023]. Dostupné z: https://www.techopedia.com/definition/27531/cryptocurrency.

Kryptografie je druh šifrovacího formátu, který není možný rozpoznat neautorizovaným uživatelem.[11] K tomuto se užívají složité algoritmy, které je pro počítače obtížné rozšifrovat. V případě Bitcoinu je používána kombinace tzv. *hashovací funkce*[12] a digitálního podpisu.[13] Kryptoměny se dále dělí na měny (*coin*) a tokeny (*tokens*).[14]

Virtuální měna je právním pojmem, jehož definice vychází z AML směrnice, nicméně ji doslovně nekopíruje. Pátá AML směrnice poskytuje vymezení pojmu virtuální měna (*virtual currencies*) jako *„digitální reprezentace hodnoty, která není vydána či garantována centrální bankou ani orgánem veřejné moci, není nutně spojena se zákonně stanovenou měnou a nemá právní status měny či peněz, je však fyzickými nebo právnickými osobami přijímána jako prostředek směny a může být elektronicky převáděna, uchovávána a obchodována“* (čl. 3 písm. d) bod 18) páté AML směrnice).

V rámci českého právního řádu byl pojem virtuální měna definován jako *„elektronicky uchovávaná jednotka bez ohledu na to, zda má nebo nemá emitenta, a která není peněžním prostředkem podle zákona o platebním styku, ale je přijímána jako platba za zboží nebo služby i jinou osobou odlišnou od jejího emitenta“* (§ 2 odst. 1 písm. l) AML zákona ve znění platném do 31. 12. 2020). K zakotvení tohoto pojmu došlo především pro účely trestního a daňového práva, a to z důvodu nutnosti, vzhledem k značné rizikovosti, které mohou tyto měny představovat, a také vzhledem k jejich minimální vysle-

---

[11] TechTerms. *Cryptography*. [Online] Publikováno 2019 [cit. 31. 1. 2023]. Dostupné z: https://techterms.com/definition/cryptography.

[12] Hashovací funkce, nebo také kryptografická hashovaní funkce, představuje algoritmus, kterým se jednosměrně šifrují zprávy. Na vstupu stojí libovolně dlouhá zpráva a na výstupu tzv. hash – otisk o přesně definované délce, který nejsme schopni zpátky rozšifrovat do původní zprávy. Více viz: Krypto-world.info. *Hašovací funkce, principy, příklady a kolize.* [Online] Publikováno 19. 03. 2005 [cit. 31. 1. 2023]. Dostupné z: http://crypto-world.info/klima/2005/cryptofest_2005.htm. Nebo také Clever and smart. *Základy kryptografie pro manažery: hashovací funkce.* [Online] Publikováno 1. 7. 2010 [cit. 31. 1. 2023]. Dostupné z: https://www.cleverandsmart.cz/zaklady-kryptografie-pro-manazery-hashovaci-funkce/.

[13] STROUKAL, Dominik, SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti: Třetí rozšířené vydání. Historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. 3. vyd. Praha: Grada Publishing, 2021. s. 29.

[14] Tradearena.cz. *Co je digitální měna, kryptoměna nebo token*. [Online] Publikováno 29. 7. 2019 [cit. 31. 1. 2023]. Dostupné z: https://www.tradearena.cz/rubriky/aktuality/co-je-digitalni-mena-kryptomena-nebo-token_806.html.

dovatelnosti, s níž souvisí relativní anonymita zúčastněných stran a ruku v ruce také vysoký potenciál pro zneužití těchto měn k financování nelegální činnosti.[15] Pojem anonymita v této souvislosti však není přesný. AML zákon i AML směrnice pracují s tímto pojmem, a to povětšinou obecně bez dalšího. Pojem anonymita se ve vztahu k Bitcoinu vyskytuje i v judikatuře.[16] Míru anonymity je třeba posuzovat vždy ve vztahu ke konkrétnímu příkladu. Na některých místech sice nalezneme obraty, které různou míru anonymity připouštějí (např. rec. 8. preambule páté AML směrnice: *„využíváním určité míry anonymity na těchto platformách“*), jedná se spíše o ojedinělý případ. Jako příklad zcela anonymní kryptoměny je uváděno Monero (*XMR*). V souvislosti s Bitcoinem a kryptoměnami s veřejným blockchainem je odpovídající použití pojmu *pseudonymita*. Jednotlivé transakce jsou totiž u těchto měn zaznamenávány do blockchainu, který je veřejně přístupný a je tedy možné v něm dohledat detailní transakční historii bitcoinové adresy.[17] Bitcoinová adresa[18] představuje jakýsi pseudonym uživatele. Mezi veřejně přístupné informace patří jednotlivé transakce mezi bitcoinovými adresami. Propojení bitcoinových adres s konkrétní identitou je náročný a nákladný, nikoliv však nemožný, proces. Zvýšení míry anonymity je možné docílit prostřednictvím VPN nebo učiněním některého mezikroku, jako například převodem na ryze anonymní kryptoměnu a zpět.[19]

Novela AML zákona přinesla také terminologické změny. Od 1. 1. 2021 je pojem virtuální měna nahrazen pojmem *virtuální aktivum*. Oproti pojmu virtuální měna je pojem virtuální aktivum širší a lze pod něj zahrnout celou

---

[15] TVRDÝ, Jiří, VAVRUŠKOVÁ, Adriana. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.* 2. vyd. Praha: C. H. Beck, 2018. s. 10. Srovnej: Důvodová zpráva AML zákona.

[16] Rozsudek Soudního dvora (pátého senátu) ze dne 22. října 2015. Skatteverket v. David Hedqvist, ve věci C-264/14, bod 11.

[17] Finex.cz. *Anonymní kryptoměny: jak privátní transakce fungují a nakolik jsou spolehlivé?* [Online] Publikováno 28. 11. 2020 [cit. 31. 1. 2023]. Dostupné z: https://finex.cz/anonymni-kryptomeny-jak-privatni-transakce-funguji-a-nakolik-jsou-spolehlive/.

[18] Rozsudek Soudního dvora (pátého senátu) ze dne 22. října 2015. Skatteverket v. David Hedqvist, ve věci C-264/14, bod 11.

[19] CryptoKingdom. *Co je to pseudonymita?* [Online] Publikováno 15. 10. 2019 [cit. 31. 1. 2023]. Dostupné z: https://cryptokingdom.tech/cs/magazin/zacatecnik/co-je-to-pseudonymita.

řadu dalších tokenů, jejichž platební funkce je potlačena a naopak je zdůrazněna funkce investiční.[20] K terminologickému posunu došlo na doporučení č. 15 Výboru expertů pro hodnocení opatření proti praní špinavých peněz a financování terorismu Rady Evropy (*MONEYVAL*), který je jedním z přidružených členských uskupení Finančního akčního výboru (*FATF*)[21].

Virtuální aktivum je dle českého právního řádu *„elektronicky uchovatelná nebo převoditelná jednotka, která je způsobilá plnit platební, směnnou nebo investiční funkci bez ohledu na to, zda má nebo nemá emitenta, pokud se nejedná o cenný papír, investiční nástroj, nebo peněžní prostředek podle zákona o platebním styku[22], nebo jednotku podle § 3 odst. 3 písm. c) bodů 4 až 7 zákona o platebním styku, nebo jednotku, kterou je prováděna platba podle § 3 odst. 3 písm. e) zákona o platebním styku, nebo jednotkou podle písmene a) bodu 2 a kterou lze v konečném důsledku zaplatit pouze za úzce vymezený okruh zboží nebo služeb, který zahrnuje elektronicky uchovatelnou nebo převoditelnou jednotku podle písmene a)“* (§ 4 odst. 9 AML zákona v platném znění od 1. 1. 2021). Důvodová zpráva k AML zákonu uvádí, že v souvislosti s § 4 odst. 9 písm. b) AML zákona[23] půjde typicky o elektronicky uchovávané jednotky, za které lze pořídit pouze jiné elektronicky uchovávané jednotky, přičemž jsou tyto elektronicky uchovávané jednotky způsobilé plnit platební funkci třeba prostřednictvím *smart contractu*.[24] Komentář k tomuto ustanovení vy-

[20] Důvodová zpráva k zákonu č. 527/2020 Sb., kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, a další související zákony, zákony související s přijetím zákona o evidenci skutečných majitelů a zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů.

[21] Finanční analytický úřad. *MONEYVAL*. [Online] Publikováno © 2022 [cit. 31. 1. 2023]. Dostupné z: https://www.financnianalytickyurad.cz/moneyval.

[22] Např. elektronické stravenky nebo elektronické vstupenky. Tyto jsou vyloučeny z důvodu minimálního rizika z hlediska legalizace výnosů z trestné činnosti a financování terorismu.

[23] § 4 odst. 9 písm. a) AML zákona*: „jednotkou podle písmene a) bodu 2 a kterou lze v konečném důsledku zaplatit pouze za úzce vymezený okruh zboží nebo služeb, který zahrnuje elektronicky uchovatelnou nebo převoditelnou jednotku podle písmene a)“*.

[24] Důvodová zpráva k zákonu č. 527/2020 Sb., kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, a další související zákony, zákony související s přijetím zákona o evidenci skutečných majitelů a zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů.

světluje, že zde zákonodárce vytvořil pravidlo dopadající i na velmi specifické situace, které by představovaly výjimku ve vztahu k písm. a) bodu 2. tohoto ustanovení. Konkrétně uvádí příklad, kdy na platformě Ethereum lze vytvořit vlastní virtuální měnu, kterou lze použít pouze k platbám za úzce vymezený okruh zboží, které zahrnuje jiné další virtuální aktivum. Na tyto obchody by se vztahovala výjimka podle písm. a) bodu 2. výše citovaného ustanovení a nebylo by tedy možné onu virtuální měnu sloužící k výše uvedeným platbám považovat za virtuální aktivum. Současně by byla tato jednotka snadno směnitelná za jiné univerzální virtuální aktivum. Tato virtuální měna by s sebou nesla také výrazná rizika z hlediska legalizace výnosů z trestné činnosti. Zákonodárce prostřednictvím tohoto ustanovení uzavřel mezeru, která by pro virtuální měny spadající do účelového řetězce takto vznikla.[25]

Dále je třeba se zamyslet nad, do jisté míry až návodným, používáním slova *„měna“* ve výše zmiňovaných pojmech. Pojmy – virtuální, digitální, krypto- – se slovem měna operují. Pojem měna je však jasně a striktně vymezen. Jedná se o pojem právní, konkrétně o právní kategorii. Měna je definována jako *„peněžní soustava, která je používána a zákonem upravena na území určitého státu.“*[26] Z této definice vyplývá, že v případě virtuální měny, digitální měny nebo kryptoměny o měnách nehovoříme, a tudíž se jedná o název čistě formální. Virtuální měny ze své podstaty nepůsobí na území určitého státu, nýbrž ve virtuálním prostoru napříč státy. Jedná se spíše o univerzální jednotku, která působí ve všech státech bez rozdílu, v celém digitálním prostoru, na základě určitého společenského zájmu, je závislá na výpočetní technologii a její hodnotu lze převést odpovídajícím kurzem na fiat měny nebo virtuální aktiva.

Komplexní úprava virtuálních měn, nebo v širším pojetí virtuálních aktiv, se vyskytuje spíše výjimečně. Některé státy se na tento pokrok snaží reagovat a postupně přijímají dílčí ustanovení, která definují pojem pro potřeby trestního práva. Stanoviska, jakým způsobem obecně k právní úpravě

[25] HLAVINOVÁ, Markéta, KABEŠ, Viktor In.: HLAVINOVÁ, Markéta, KABEŠ, Viktor; PILÍKOVÁ, Jaroslava. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu*. 3. vyd. Praha: C. H. Beck, 2022. s. 29-47.

[26] JÁNOŠÍKOVÁ, Petra a kol. *Finanční a daňové právo*. 2. vyd. Plzeň: Aleš Čeněk, 2016. s. 38.

přistoupit, však nejsou jednotná. Odborníci z jednotlivých států se samozřejmě individuálně vyjadřují k dílčím problémům, které s touto problematikou korelují, avšak komplexních úprav je pomálu. Ve světovém měřítku můžeme hovořit konkrétně o japonské právní úpravě, v evropském o úpravě maltské.

Obecně lze shrnout, že virtuální měny nejsou měnami v právním slova smyslu. Ovšem našli bychom i výjimku z tohoto tvrzení. Dne 7. 9. 2021 se stal Salvador první zemí na světě, která oficiálně přijala jako zákonné platidlo kryptoměnu Bitcoin.[27] Jedná se o velice progresivní a zároveň kontroverzní krok, na který se snesla vlna kritiky. Své obavy v této souvislosti vyjádřil také Mezinárodní měnový fond (dále také jako *„MMF"*). MMF se obává nebezpečí se zřetelem na finanční ochranu spotřebitelů a finanční stabilitu státu. Důvodem je vysoká volatilita bitcoinu, která může pro Salvador znamenat ekonomická rizika.[28]

Zbývá posoudit, zda virtuální měna naplňuje definiční znaky pro pojem *peníze*. Peníze představují pojem historicko-ekonomický,[29] jejichž definice je následující: *„Penězi rozumíme cokoliv, co slouží jako běžně přijímaný prostředek směny či placení. Peníze musí být přijímány jako platidlo ke kupování statků a služeb."*[30] Z toho lze dovozovat, že virtuální měnu nelze obecně a bez dalšího považovat ani za peníze v pravém slova smyslu. Samozřejmě se jedná o jednotku, která slouží ve společnosti také ke směně či placení. Problém lze však spatřit ve výkladu neurčitého právního pojmu *„běžně přijímaný prostředek"*. Přestože se v posledních letech zájem o užívání virtuálních měn rapidně zvýšil, lze jich jen málo považovat za takové, které by význam tohoto pojmu pro svou rozšířenost byly schopny naplnit. Ve vztahu

---

[27] ČTK. České noviny. *Salvador je ode dneška první zemí na světě, kde lze platit bitcoinem.* [Online] Publikováno 7. 09. 2021 [cit. 31. 1. 2023]. Dostupné z: https://www.ceskenoviny.cz/zpravy/salvador-ktery-zavadi-bitcoin-jako-platidlo-jich-nyni-drzi-400/2086277.

[28] Novinky.cz. *Salvador by neměl používat bitcoin jako zákonné platidlo, burcoval MMF.* [Online] Publikováno 25. 11. 2021 [cit. 31. 1. 2023]. Dostupné z: https://www.novinky.cz/internet-a-pc/clanek/salvador-by-nemel-pouzivat-bitcoin-jako-zakonne-platidlo-burcoval-mmf-40379097.

[29] JÁNOŠÍKOVÁ, Petra a kol. *Finanční a daňové právo*. 2. vyd. Plzeň: Aleš Čeněk, 2016. s. 38.

[30] Ibidem.

k pojmu virtuální aktivum je situace ještě komplikovanější, neboť pod tento pojem lze podřadit i virtuální aktiva, která platební funkci neplní.

V této souvislosti je významným rozhodnutím Rozsudek Soudního dvora (pátého senátu) ze dne 22. října 2015, Skatteverket v. David Hedqvist, věc C-264/14. V této věci se jednalo o řízení o předběžné otázce, kterou vznesl Švédský Nejvyšší správní soud (dále také jako *„ŠNSS“*). ŠNSS řešil spor mezi Davidem Hedqvistem a švédskou daňovou správou. Hedqvist si chtěl zřídit obchodní společnost, jejíž činnost by spočívala ve směně fiat měny za bitcoin a zpět.[31] Zisk společnosti by představoval pouze rozdíl mezi nákupní a prodejní cenou, přičemž si společnost nebude účtovat žádné další poplatky.[32] Hedqvist se před zahájením této činnosti obrátil na komisi pro daňové právo, aby mu vyjádřila předběžné stanovisko k otázce, zda z nákupu a prodeje jednotek virtuální měny bitcoin musí být odváděna DPH. Komise pro daňové právo posoudila toto jednání jako směnárenskou službu za úplatu a zároveň uvedla, že se na tuto směnárenskou službu vztahuje osvobození od DPH. Dále Komise pro daňové právo uvádí, že *virtuální měna „bitcoin“ je platebním prostředkem, který je používán obdobným způsobem jako zákonné platební prostředky*.[33] Proti rozhodnutí podala Skatteverket (v *překladu Švédská daňová správa*) žalobu k ŠNSS, v níž vyjádřila své opačné stanovisko. ŠNSS vyjádřil své pochybnosti a obrátil se na Evropský soudní dvůr (dále také jako *„ESD“*) ve věci předběžné otázky. ŠNSS položil ESD následující otázky, a to, zda se v tomto případě jedná o poskytování služeb za úplatu, a jestliže ano, zda jsou tyto operace osvobozeny od daně. ESD uvádí, že virtuální měna s obousměrným tokem, v tomto případě Bitcoin, která je směňována za fiat měny, nemůže být považována za hmotný majetek ve smyslu článku 14 směrnice o DPH, neboť tato měna nemá jiný účel, než účel platidla.[34] Tato plnění považuje za poskytnutí služby ve smyslu článku 24 směrnice o DPH. V případě směny fiat měn za virtuální měny (v tomto případě Bitcoin) oproti zaplacení částky, která odpovídá marži, již před-

[31] Rozsudek Soudního dvora (pátého senátu) ze dne 22. října 2015. Skatteverket v. David Hedqvist, ve věci C-264/14, bod 10.

[32] Ibidem, bod 13.

[33] Ibidem, bod 17.

[34] Ibidem, bod 24.

stavuje rozdíl mezi cenou nákupní a prodejní cenou zákazníkům, považuje ESD takové jednání za poskytnutí služby za úplatu.[35]

Osobně se domnívám, že stanovisko ESD týkající se toho, že virtuální měna Bitcoin je výhradně platebním prostředkem je do jisté míry již zastaralé. Toto tvrzení by bylo možné vztáhnout na virtuální aktiva, jejichž funkcí je skutečně převážně nebo výhradně funkce platební (viz dále). V tomto ohledu se funkce Bitcoinu v průběhu let od zamýšleného záměru změnila, podobně jako u dalších virtuálních měn, a rozšířila. K původní platební funkci přibyly i další a tím jí i částečně utlumily. Na jedné straně lze argumentovat, že se počet míst, kde je možné platit virtuálními měnami za zboží či služby, v posledních letech rapidně zvýšil. Naproti tomu, ale někteří kupující virtuálních měn této možnosti nevyužívají a za tímto účelem si je nepořizují. Majitelé těchto jednotek s nimi v takovém případě tedy neplatí, naopak s nimi spekulují, dlouhodobě je drží a vnímají je jako investici. Dlouhodobé investování do některých virtuálních měn se pro některé stalo novým trendem.[36] Využití virtuálních aktiv nelze snadno zobecnit, neboť je velmi různorodé. V současné době bych závěr ESD spíše vztáhla k virtuálním aktivům, která jsou charakteristická právě pro svou platební funkci, a to stablecoinům.

S výkladem druhé části definice nastává obdobný problém. Přijímání virtuálních měn je zatím založeno na dobrovolnosti a jakémsi kolektivním zájmu je jako platidlo používat. Vzhledem k tomu tak není naplněna podmínka povinnosti je jako platidlo přijímat.

Jiná definice říká, že peníze jsou *„zvláštní druh univerzálního zboží používaného k vyjadřování cen ostatního zboží, ke zprostředkování jeho koupě a prodeje a k provádění různých druhů plateb.“*[37] Tuto definici nelze vztáhnout na virtuální aktiva obecně, neboť v současné době existují i taková,

---

[35] Rozsudek Soudního dvora (pátého senátu) ze dne 22. října 2015. Skatteverket v. David Hedqvist, ve věci C-264/14, bod 26-31

[36] Kriptomat. *Jak investovat do kryptoměn pro dlouhodobý zisk.* [Online] Publikováno © 2023 [cit. 31. 1. 2023]. Dostupné z: https://kriptomat.io/cs/kryptomeny/jak-investovat-do-kryptomen/.

[37] KOTÁB, Petr In.: BAKEŠ, Milan a kol. *Finanční právo*. 6. vyd. Praha: C. H. Beck, 2012. s. 335–341.

která platební funkci vůbec nenaplňují. Tedy virtuální aktiva s výhradně investiční funkcí by této definici nevyhovovala, naopak ta se zcela nebo alespoň částečnou platební funkcí ano.

Z hlediska praktičnosti využití virtuálních měn jako platidla je nutné poukázat na vysokou volatilitu, která jim sice nebrání být platidlem, ale činí je do jisté míry nevhodnými pro toto použití. Uvedu příklad nákupu nemovité věci v souvislosti s volatilitou bitcoinu a fiat měnou podléhající inflaci. V souvislosti s pandemií covid-19 bylo možné dne 12. března 2020 zaznamenat prudký propad z hodnoty 7 200 USD na 5 678 USD během 15 minut. Hodnota bitcoinu dále klesala a spadla až pod 3 900 USD za jediný den.[38] Koncem května 2020 opět kurz vystoupal nad 9000 USD. Dalším příkladem je situace v průběhu konce roku 2021 a první poloviny roku 2022. Bitcoin od listopadu 2021 do první poloviny května 2022 klesl z necelých 67 000 USD pod 29 000 USD. V případě, že bychom v uvedených časových obdobích (v prvním případě i dnech a hodinách) za bitcoiny nakupovali, velice by také záleželo na tom, kdy bychom transakci učinili. Prodávali bychom nemovitost dne 12. 3. 2020 za 10 BTC, získali bychom v přepočtu na začátku dne 72 000 USD a na konci dne už jen 39 000 USD, což je poměrně markantní rozdíl. V případě, že by chtěl prodávající s bitcoiny dál nakládat a realizoval by jejich hodnotu (převedl je na fiat měnu), došlo by k realizované ztrátě, naopak pokud by je držel, a to až do listopadu 2021, vydělal by na tom. Naproti tomu kurz dolaru, eura, české koruny byl méně volatilní a mohl tak na první pohled pro laika působit praktičtěji a možná i důvěryhodněji pro provedení transakce, například právě pro realizaci koupě nemovité věci. Tyto fiat měny (respektive cenové páry měn USD/EUR, EUR/CZK) sice nejsou tolik volatilní jako virtuální měny, ale i tak kolísají. Kromě toho je nutno zmínit, že se v současné době řada států potýká s vysokou inflací, která má na výslednou cenu vliv. V lednu 2023 dosahovala v České republice inflace 17,6 %,[39] přičemž průměrná míra

[38] Forbes. *Brutální propad bitcoinu. Kryptoměna je prvním poraženým ekonomické krize*. [Online] Publikováno 16. 3. 2020 [cit. 31. 1. 2023]. Dostupné z: https://www.forbes.cz/brutalni-propad-bitcoinu-kryptomena-je-prvnim-porazenym-ekonomicke-krize/.

[39] Česká národní banka. *Prognóza ČNB – zima 2023*. [Online] Publikováno 2. 2. 2023 [cit. 31. 1. 2023]. Dostupné z: https://www.cnb.cz/cs/menova-politika/prognoza/.

inflace za rok 2022 dosahovala 15,1 %.[40] V Turecku byla v listopadu 2022 míra inflace 84,4 % a v prosinci 2022 64,3 %.[41] S inflací se dlouhodobě potýká také Venezuela, která má velké ekonomické problémy. Průměrná míra inflace za rok 2022 ve Venezuele dosáhla 234 %, což zde představovalo zpomalení oproti předchozímu roku.[42] V případě již výše zmíněného prodeje nemovité věci bychom zde dostali od kupujícího zaplacenou částku například 2 miliony korun českých. V případě ponechání peněz na účtu by se však znehodnocovaly, jejich hodnota by se snižovala a postupem času bychom za ně koupili stále méně. To znamená, že porostou-li ceny v daném státě, za konkrétní zboží nebo službu zaplatíte více, tedy stejná nemovitá věc by byla dražší.

Zde je nutné rozlišovat pojmy inflace a volatilita, neboť jsou to dva odlišné pojmy. Inflace je míra, jakou ceny v ekonomice stoupají v průběhu času. Inflace je důsledkem nadměrného tisku peněz, stoupajících nákladů na výrobu a dalších jiných faktorů. Cílem centrálních bank je udržet inflaci na přijatelné úrovni, aby bylo zajištěno stabilní ekonomické prostředí.[43] Volatilita naproti tomu představuje míru, jakou se cena za jednotku mění v krátkém časovém období.[44] Bitcoin je známý svou vysokou volatilitou, což znamená, že jeho cena se může rychle a výrazně měnit. To má za následek, že je pro investory náročné předvídat jeho budoucí vývoj. Jeho volati-

[40] Česká národní banka. *Inflace v prosinci 2022 zpomalila.* [Online] Publikováno 11. 1. 2023 [cit. 31. 1. 2023]. Dostupné z: https://www.cnb.cz/cs/verejnost/servis-pro-media/komentare-cnb-ke-zverejnenym-statistickym-udajum-o-inflaci-a-hdp/Inflace-v-prosinci-2022-zpomalila/.

[41] FXstreet.cz. *Inflace v Turecku v prosinci klesla na 64,3 procenta, nejvíce od roku 1995.* [Online] Publikováno 3. 1. 2023 [cit. 31. 1. 2023]. Dostupné z: https://www.fxstreet.cz/inflace-v-turecku-v-prosinci-klesla-na-643-procenta-nejvice-od-roku-1995.html.

[42] Euro.cz. *Inflace ve Venezuele zpomalila, přesto loni dosáhla 234 procent. Velké problémy má stále i Turecko.* [Online] Publikováno 25. 1. 2023 [cit. 31. 1. 2023]. Dostupné z: https://www.euro.cz/clanky/inflace-ve-venezuele-zpomalila-presto-loni-dosahla-234-procent-velke-problemy-ma-stale-i-turecko/.

[43] Finex.cz. *Inflace: Co je to inflace? Jaké jsou její příčiny a jaké může mít dopady?.* [Online] Aktualizováno 1. 11. 2022 [cit. 31. 1. 2023]. Dostupné z: https://finex.cz/inflace/.

[44] Finex.cz. *36. díl Seriálu technické analýzy – Co je to volatilita.* [Online] Publikováno 7. 9. 2019 [cit. 31. 1. 2023]. Dostupné z: https://finex.cz/technicka-analyza-volatilita/.

lita může být naopak pro některé investory atraktivní, neboť s ním mohou spekulovat a snažit se na kurzu krátkodobě vydělat.[45]

To, že je bitcoin volatilní ještě neznamená, že jsou fiat měny lepším uchovatelem hodnoty. Rozhodně ne v dlouhodobém horizontu. Jak již bylo uvedeno výše, fiat měny podléhají inflaci například právě z důvodu tisku peněz. Naopak Bitcoin je z dlouhodobého hlediska deflační kryptoměnou. Sice se nyní ještě uvolňují další jednotky bitcoinu do oběhu, ale počet bitcoinů je konečný a od určitého okamžiku se začne snižovat (důvodem jsou ztráty přístupových hesel k peněženkám, nebo nemožnost zjištění přístupových hesel v případě úmrtí držitele). Domnívám se, že je třeba se vždy konkrétně zamýšlet nad otázkami praktičnosti, uchovatelností hodnoty a možnými riziky a posuzovat je navzájem. Zatímco inflace je ukazatelem stability měny, volatilita ukazuje na míru rizika, kterému jsou investoři vystaveni při investování či dalších operacích s tímto aktivem. Osobně v tomto kontextu spatřuji ve virtuálních měnách řešení pro země trpící vysokou inflací a špatnou životní úrovní.

Lze postupně dovodit, že by virtuální měna mohla být komoditou. Definic tohoto pojmu je řada, nicméně se v některých aspektech podobají. Komoditou by předně mělo být zastupitelné zboží, dodávané od různých dodavatelů, bez rozdílu kvality tohoto zboží.[46] Zde dovozuji závěr, že lze tyto podmínky naplnit. *Kvalitu* konkrétního virtuálního aktiva ovlivnit nelze, to znamená, že každý bitcoin si bude v tomto slova smyslu roven a nebude více kvalitnější jednotka a méně kvalitnější jednotka.

V některých případech bude i podmínka *zastupitelnosti* splněna. Lze samozřejmě namítat, že každý bitcoin je unikátní, protože má vlastní jedinečný kód a tudíž nezastupitelný. Toto tvrzení by se však mohlo vztahovat i na papírové bankovky, které jsou označeny sériovými čísly. V souvislosti s kryptoměnou Bitcoin je vhodnější použití pojmu *nezaměnitelný*. Každý bitcoin je v tomto směru originál (důvodem je jeho unikátní kód). Toto ovšem

[45] E15. *Investice do bitcoinu jako riziko i šance. Volatilita vytváří obchodní příležitosti.* [Online] Publikováno 31. 3. 2021 [cit. 31. 5. 2022]. Dostupné z: https://www.e15.cz/kryptomeny-investice.

[46] ITBIZ. *Komodita.* [Online] Publikováno 13. 09. 2011 [cit. 31. 1. 2023]. Dostupné z: https://www.itbiz.cz/slovnik/ekonomie/komodita.

neplatí pro všechny kryptoměny bez dalšího. Mezi částečně zaměnitelné kryptoměny se řadí např. Dash a Zcash, jako spíše zaměnitelné se uvádí příklady kryptoměn Bytecoin a Monero.[47] Stejně tak vnímám tento pojem jako vhodnější i ve vztahu k bankovkám, pokud nepůjde o sběratelské kusy bankovek nebo mincí, budou vůči sobě zaměnitelné. Pojem *nezastupitelný* se v oblasti virtuálních aktiv používá v souvislosti s tzv. NFT (*non-fungible token*). NFT jsou ze své podstaty nezaměnitelné tokeny, které představují důkaz o vlastnictví určitého souboru dat. V případě unikátního digitálního díla hovoříme například o virtuálním obrazu nebo URL adresách. NFT mohou sloužit také jako certifikáty k dílům (věcem), které jsou uloženy mimo digitální sféru. V takovém případě jde například o unikátní spojení NFT s hodinkami ROLEX, které fyzicky vlastníte, přičemž NFT funguje jako jakýsi list vlastnictví. Dalším příkladem je vygenerování určitého množství NFT, která mohou sloužit jako vstupenka nebo přístup k výtisku knihy.[48]

Dalším bodem je podmínka dodávání od různých dodavatelů. Pomineme-li prvotní vytvoření této technologie, je v současné době bitcoin tzv. těžen (*mining*), a to různými osobami (těžaři, *miners*) po celém světě. Samozřejmě otázkou zůstává, nakolik je i toto tvrzení reálné, vzhledem k dominantním *těžařským farmám*, které se nyní vyskytují především ve Spojených státech amerických a v Kazachstánu.[49] Pomineme-li však těžařská centra, dalo by se toto těžení označit za emitování, tudíž nám zde vzniká jakýsi primární trh. Na sekundárním trhu je obchodován a nabízen mezi osobami, které ho od „těžařů" odkoupily. Některé definice operují jen se slovem dodavatel, nikoliv výrobce, tudíž na to nebude mít vliv konečné množství tohoto produktu. V případě, že by některá z definic pracovala s pojmem výrobce, mohl by nastat problém. Celkový počet bitcoinů je konečný, což ne-

[47] Finex.cz. *Anonymní kryptoměny: jak privátní transakce fungují a nakolik jsou spolehlivé?* [Online] Publikováno 28. 11. 2020 [cit. 31. 1. 2023]. Dostupné z: https://finex.cz/anonymni-kryptomeny-jak-privatni-transakce-funguji-a-nakolik-jsou-spolehlive/.

[48] Finex.cz. *Non-fungible tokeny (NFT): Co to je, jak fungují a vyplatí se do nich investovat?* [Online] Publikováno © 2014-2023 [cit. 31. 1. 2023]. Dostupné z: https://finex.cz/rubrika/nft/.

[49] ČT24. *Kazachstán se stal druhým největším těžařem bitcoinu. Farmy spotřebují osm procent energie v zemi.* [Online] Publikováno 13. 11. 2021 [cit. 31. 1. 2023]. Dostupné z: https://ct24.ceskatelevize.cz/svet/3399608-kazachstan-se-stal-druhym-nejvetsim-tezarem-bitcoinu-farmy-spotrebuji-osm-procent.

platí obecně pro virtuální aktiva. Do oběhu jsou bitcoiny postupně uvolňovány v rámci procesu, při kterém jsou potvrzovány a zpracovávány transakce. Jedná se o propůjčení výpočetní techniky k řešení matematických operací a ověřování transakcí v síti. Jednotlivé bitcoiny představují odměnu za tento proces. Tato odměna je nastavena na pevně danou hodnotu. Po konkrétním počtu ověřených bloků dochází k tzv. půlení (*halving*), kdy se uvedená odměna sníží o polovinu. Uvedený proces slouží k omezení celkového počtu bitcoinů, které mohou být vytvořeny.[50] Bitcoiny lze dále dělit a nabízet, ale všichni prodejci se v určitý moment stanou skutečně jen dodavateli a budou přeprodávat z konečného množství již vytěžených bitcoinů. Pokud bychom výše uvedenou definici vztáhli na virtuální aktiva obecně, jejich počet se naopak zvyšuje a stále jsou vytvářena nová. V listopadu 2022 existovalo přes 21 800 kryptoměn,[51] přičemž ještě v květnu 2022 jich existovalo přibližně 19 500.[52] Pro zajímavost v roce 2018 existovalo pouze kolem 1 400 kryptoměn.[53] Množství kryptoměn se od března 2022 zvýšilo z přibližně 10 300 kryptoměn na zmíněných 21 800.[54] Je nutné však dodat, že se odhaduje, že po odečtení „mrtvých" kryptoměn jich zbývá kolem 9 300 aktivních.[55]

[50] K poslednímu půlení došlo 11. května 2020. Další půlení se očekává přibližně v roce 2024.

[51] Exploding topics. *How Many Cryptocurrencies are There In 2023?* [Online] Publikováno 25. 11. 2022 [cit. 31. 1. 2023]. Dostupné z: https://explodingtopics.com/blog/number-of-cryptocurrencies.

[52] CoinMarketCap. *Today´s Cryptocurrency Prices by Market Cap.* [Online] Publikováno © 2022 [cit. 31. 1. 2023]. Dostupné z: https://coinmarketcap.com/.

[53] FXstreet.cz. *První fond v Česku umožňuje investici do kryptoměn.* [Online] Publikováno 31. 1. 2018 [cit. 31. 1. 2023]. Dostupné z: https://www.fxstreet.cz/prvni-fond-v-cesku-umoznuje-investici-do-kryptomen.html.

[54] Exploding topics. *How Many Cryptocurrencies are There In 2022?* [Online] Publikováno 25. 3. 2022 [cit. 31. 1. 2023]. Dostupné z: https://explodingtopics.com/blog/number-of-cryptocurrencies.

[55] Exploding topics. *How Many Cryptocurrencies are There In 2023?* [Online] Publikováno 25. 11. 2022 [cit. 31. 1. 2023]. Dostupné z: https://explodingtopics.com/blog/number-of-cryptocurrencies.

Další z definic říká, že komodita je produkt odlišný od služby, s čímž můžeme souhlasit.[56] Podmínku obchodovatelnosti[57] můžeme také víceméně považovat za splněnou vzhledem k současné síti míst, kde je možné virtuální aktiva koupit, prodat či provádět jiné operace. Zájem o konkrétní virtuální aktiva, bychom museli sledovat individuálně. V případě podmínění komodity hodnotou lze hovořit opět o sporné otázce. Virtuální aktiva sama o sobě vnitřní hodnotu nemají. Hodnota představuje proměnnou, jež je závislá na nabídce a poptávce. Takto by však bylo možné přistupovat i k jiným, řekněme tradičnějším komoditám, například zlatu. Z hlediska zájmu o držení těchto komodit pandemie covid-19 poukázala na nedůvěru některých držitelů virtuálních měn, neboť se v době pandemické krize stalo na okamžik zlato více vyhledávanou komoditou, situace se však brzy změnila a zájem o virtuální aktiva roste.[58]

Z výše uvedeného vyplývá, že pravděpodobně nejblíže má virtuální měna svou povahou ke komoditě. V každém případě nelze do budoucna vyloučit přehodnocení některých pojmů a jejich významů, jak je chápeme dnes. Toto se ostatně již stalo, kdy byl v rámci právní terminologie rozšířen pojem virtuální měna na pojem virtuální aktivum, respektující vývoj a zahrnující celou řadu dalších různorodých operací. K vnímání virtuálních měn jako komodit je záhodno zmínit, že v současné době je pouze Bitcoin oficiálně považován za obchodovatelnou komoditu. V roce 2015 byl Komisí pro komoditní obchody (*Commodity Futures Trading Commission, CFTC*) za komoditu oficiálně označen.[59]

---

[56] Dictonary.com. *Commodity*. [Online] Publikováno 2019 [cit. 31. 1. 2023]. Dostupné z: https://www.dictionary.com/browse/commodity.

[57] Cambridge Dictonary. *Commodity*. [Online] Publikováno 2019 [cit. 31. 1. 2023]. Dostupné z: https://dictionary.cambridge.org/dictionary/english/commodity.

[58] iDNES.cz. *Cena zlata v korunách zlomila dosavadní rekordy. Může růst i nadále*. [Online] Publikováno 19. 5. 2020 [cit. 31. 1. 2023]. Dostupné z: https://www.idnes.cz/ekonomika/zahranicni/zlato-cena-rekord-krize-investice-pandemie-covid-19-koruna-dolar.A200519_153409_eko-zahranicni_mato.

[59] Investiční web. *Bitcoin byl oficiálně označen za komoditu. Vrátí se jeho dřívější sláva?* [Online] Publikováno 21. 09. 2015 [cit. 31. 1. 2023]. Dostupné z: https://www.investicniweb.cz/ekonomika-politika/bitcoin-byl-oficialne-oznacen-za-komoditu-vrati-se-jeho-drivejsi-slava.

2.2 BITCOIN

Bitcoin je digitální nekrytá kryptoměna, jež vznikla v roce 2009, pracující na principu *peer-to-peer (P2P)*, neboli *klient-klient*.[60] Jedná se tedy o měnu čistě virtuální, která není žádným způsobem centrálně řízena přes konkrétní server. Jejím zakladatelem je údajně osoba nebo skupina osob pod pseudonymem Satoshi Nakamoto. Vše je však zahaleno rouškou nevědomosti a kolem pravé identity zakladatelů se vedou jen spekulace.[61] Některé zdroje dokonce tvrdí, že autor této technologie již nežije.[62] Tyto spekulace však nehrají významnou roli, neboť ať už tvůrci žijí či ne, nemají již na měnu žádný vliv.

Bitcoin nebyl prvním pokusem o univerzální digitální platidlo. S technickým pokrokem se samozřejmě postupně čím dál častěji objevovaly snahy vytvořit univerzální digitální měnu v počítačovém světě. Každý z nápadů však trpěl svou nedokonalostí, a to především z hlediska zabezpečení měn. Největší hrozbou byla tzv. *dvojitá útrata*. Tento pojem si lze představit následovně. Pro určitou hodnotu je vydána konkrétní informace – kód, kterým lze zaplatit. V případě dvojí útraty by jeden subjekt tuto informaci duplikoval a zaplatil by tímto kódem dvakrát. Aby tomu bylo možné předcházet a zamezit, je v případě kryptoměny Bitcoin vytvořen tzv. *blockchain*. Blockchain si lze představit jako decentralizovanou účetní knihu, v níž jsou všechny transakce zaznamenávány a sdíleny, čímž je zamezeno možnosti transakci duplikovat.[63]

S jistotou lze v současnosti říci, že Bitcoin aktuálně představuje nejznámější a nejrozšířenější virtuální měnu na světě. V každém případě, jak bylo řečeno, pojem měna může být značně zavádějící. Bitcoin bychom mohli po-

[60] STROUKAL, Dominik, SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti: Třetí rozšířené vydání. Historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. 3. vyd. Praha: Grada Publishing, 2021. s. 28.

[61] Ibidem, s. 28–32.

[62] CCN. *Bitcoin Creator Satoshi is 'Already Dead', Claims BitMEX CEO.* [Online] Publikováno 23. 09. 2019 [cit. 31. 1. 2023]. Dostupné z: https://www.ccn.com/bitcoin-creator-satoshi-dead/.

[63] STROUKAL, Dominik, SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti: Třetí rozšířené vydání. Historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. 3. vyd. Praha: Grada Publishing, 2021. s. 28–32.

važovat za formu platebního systému, druh zboží, nebo jak je již uvedeno výše, komoditu.[64] V roce 2014 bylo, kvůli rostoucímu zájmu o kryptoměny a množství transakcí, vydáno stanovisko odborných pracovníků ČNB.[65] Toto stanovisko ČNB nabízí dílčí nezávazné negativní vymezení Bitcoinu, resp. kryptoměn. O rok později jej ČNB na své konferenci potvrdila. Podle těchto výstupů bitcoiny nejsou bezhotovostními peněžními prostředky, ani elektronickými penězi (§ 4 ZoPS[66]), ani peněžními prostředky (§ 2 odst. 1 písm. c) ZoPS). Dále se nejedná ani o bezhotovostní obchod s cizí měnou (§ 2 odst. 1 písm. e) ZoPS) ani o žádnou jinou platební službu. Zaměstnanci ČNB uvádí, že pro jejich obchodování není třeba žádného povolení ČNB, především z důvodu, že kryptoměna nepodléhá jejímu dohledu, a tudíž ČNB logicky ani nemůže žádné povolení udělit, a to ani k přijímání úhrad zboží a služeb. Výjimku ovšem tvoří povolení ČNB pro finanční instituce, které smí s bitcoiny obchodovat pouze v rámci správy vlastního majetku. Dále je ve světle zákona o směnárenské činnosti řečeno, že bitcoiny nenaplňují *„hmotné znaky předmětu směny ani znak „znějící na určitou měnu““*.[67]

Je také důrazně upozorňováno na fakt, že zatím není možné založit podnik, kde by bylo možné platit za zboží a služby pouze virtuálními měnami, bez toho aniž by byla přijímána oficiálně uznaná tuzemská měna. Stanovisko ČNB sice nevylučuje platbu bitcoinem, upozorňuje ale potenciální obchodníky, aby věnovali pozornost skutkové podstatě trestného činu ohrožování oběhu tuzemských peněz (§ 239 odst. 2 písm. a) TZ[68]) a vyvarovali se jejího naplnění.

---

[64] CFO world. *Bitcoin a jiné virtuální měny z pohledu práva.* [Online] Publikováno 16. 01. 2017 [cit. 31. 1. 2023]. Dostupné z: https://cfoworld.cz/legislativa/bitcoin-z-pohledu-prava-4199.

[65] ČNB. *Obchodování s bitcoiny.* [Online] Publikováno 10. 02. 2014 [cit. 31. 1. 2023]. Dostupné z: https://www.cnb.cz/export/sites/cnb/.galleries/documents/FAQ_download-gallery/obchodovani_s_bitcoiny.pdf.

[66] Zákon č. 370/2017 Sb., o platebním styku.

[67] ČNB. *Obchodování s bitcoiny.* [Online] Publikováno 10. 02. 2014 [cit. 31. 1. 2023]. Dostupné z: https://www.cnb.cz/export/sites/cnb/.galleries/documents/FAQ_download-gallery/obchodovani_s_bitcoiny.pdf.

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

Bitcoin rozhodně oficiálně započal novou éru a má velký podíl na popularizaci a zájmu širší veřejnosti o oblast dnes již virtuálních aktiv.[69] Je proto nanejvýš nezbytné vyřešit celou řadu otázek souvisejících s virtuálními měnami a dalšími virtuálními aktivy, protože už nyní ovlivňují pole ekonomické a finanční. Globální význam Bitcoinu lze také dovodit z nominace na Nobelovu cenu.[70] Ač byla tato nominace neúspěšná z důvodu neznámé totožnosti autora Bitcoinu, už jen diskuze a navržení nominace dokazuje, o jak zásadní jev se jedná. Některé osobnosti dokonce označují Bitcoin za revoluční vynález nebo tzv. *digitální zlato*.[71] Jiní ho naopak označují za největší šílenství od 16. století, kdy došlo k tzv. „Tulipánovému šílenství".[72] Samozřejmě, že před Bitcoinem byly pokusy o univerzální virtuální měny, nicméně žádný z těchto pokusů nebyl tak úspěšný. Vyskytují se názory, zda je správné navrhovat právě Satoshiho Nakamotu na získání Nobelovy ceny za inovaci a nápad, který je vlastně na světě již od devadesátých let. V každém případě se v konečném důsledku vzhledem k nominaci zatím stejně nic nezmění.

3. POSOUZENÍ PRÁVNÍ POVAHY VIRTUÁLNÍ MĚNY V ČESKÉ REPUBLICE

Názory na právní povahu virtuálních měn se různí. Vzhledem k tomu, že se jedná o stále poměrně novou problematiku, kterou je možné se seriózněji zabývat až v poslední dekádě, teprve krystalizují otázky, které z ní vyplývají a jsou s ní spojené. Výchozí a pravděpodobně nejzásadnější pro budoucí právní posuzování a případnou tvorbu legislativy, je určení právní povahy

[69] ŠTIKA, Martin. Má naprosto svobodná virtuální měna bitcoin místo v právním státě?. *Bulletin advokacie.* 5/2018, s. 29.

[70] CCN. *Satoshi Nakamoto Not Eligible For Nobel Prize.* [Online] Publikováno 17. 11. 2015 [cit. 31. 1. 2023]. Dostupné z: https://www.ccn.com/satoshi-nakamoto-not-eligible-nobel-prize//.

[71] CCN. *UCLA Finance Professor Nominates Satoshi Nakamoto For Nobel Prize.* [Online] Publikováno 09. 11. 2015 [cit. 31. 1. 2023]. Dostupné z: https://www.ccn.com/ucla-finance-professor-nominates-satoshi-nakamoto-nobel-prize/.

[72] CCN. *And Satoshi's True Identity is…* [Online] Publikováno 14. 09. 2019 [cit. 31. 1. 2023]. Dostupné z: https://www.ccn.com/and-satoshis-true-identity-is/.

virtuální měny. Podle toho jak na virtuální měnu budeme nahlížet, tak by se mohla lišit i úprava, jež ji bude regulovat.

3.1 SOUKROMOPRÁVNÍ HLEDISKO

Z hlediska občanskoprávního lze konstatovat, že virtuální měna představuje věc (§ 489 ObčZ) movitou nehmotnou (§ 496 ObčZ) a spíše zastupitelnou (§ 499 ObčZ). Virtuální měny a jejich podkategorie kryptoměny charakteristiky zastupitelnosti spíše splňují. Ovšem ve vztahu k širšímu pojmu virtuální aktivum toto tvrzení slábne, neboť lze pod tento pojem podřadit i virtuální aktiva, která jsou už ze své podstaty nezastupitelná. Příkladem jsou *non-fungible tokens* (NFT), které tento pojem mají již v názvu. U těchto tokenů lze mimo jiné podle jejich povahy například rozpoznat originál od kopií. Zastupitelnost je tedy třeba vždy hodnotit ve vztahu ke konkrétním příkladům. (K rozdílu mezi pojmy zastupitelnost a zaměnitelnost více v bodě 2.1)

Nalezneme však i úvahy, které postupují mnohem dále a polemizují nad otázkou, zda virtuální měna nenaplňuje ze soukromoprávního hlediska znaky cenného papíru (§ 514 ObčZ). Podle Dědiče, Šovara a Mikuly se jedná o velice zásadní otázku. Vzhledem k absenci judikatury a literatury se k dané problematice spolu s kolegy vyjadřuje v článku.[73] Dochází k závěru, že je vyloučeno, aby byly ve světle občanského zákoníku virtuální měny považovány za cenné papíry. Své tvrzení podpírá několika argumenty. Jedním z nich je *„podmínka projevu autonomní vůle emitenta“*. Pro cenné papíry je charakteristické jednání emitenta směřující k vydání určité listiny jako cenného papíru. Nevylučuje se tak možnost, že se někdo může stát vlastníkem bez vůle emitenta nebo jeho vědomí, avšak stále platí podmínka, že musí být listina emitentem alespoň vytvořena. V kontextu virtuálních měn si tak lze jen stěží představit realizaci této podmínky. Projev vůle[74] i proces, jakým cenný papír vzniká, je velice formalizovaný, a vzhledem k povaze

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

[74] Tzv. skripturní akt – jedná se o fyzické zachycení podoby práv, která jsou s cenným papírem provázána. Více viz: KOHAJDA, Michael, KOTÁB, Petr. In.: BAKEŠ, Milan a kol.; *Finanční právo*. 6. vyd. Praha: C. H. Beck, 2012. s. 421–422.

virtuálních měn a v souvislosti se současným nastavením právního rámce nelze tuto podmínku splnit.

Cenný papír představuje listinu, do které je vtěleno právo, a na základě které vzniká závazek mezi vydavatelem (*emitentem*) a další osobou. Typicky majitel, resp. držitel, může prostřednictvím této listiny uplatnit právo z ní plynoucí. Charakteristickou vlastností pro cenné papíry je tedy povinnost poskytnutí plnění vydavatele vůči držiteli. Virtuální měny nesplňují ani tuto podmínku. Vydavatel virtuální měny nemá žádné povinnosti vůči držiteli jednotky virtuální měny. Pro lepší představu lze jako příklad uvést situaci, kdy držitel akcie požaduje vyplacení dividendy, jsou-li vypláceny. V tomto případě je vydavatel povinen poskytnout dané plnění. Naopak v případě držení jednotky virtuální měny žádná taková povinnost nenastává. Hodnotu může držitel realizovat pouze směnou v daný okamžik a je dána nabídkou a poptávkou.

Autoři se dále zabývali otázkou, zda cenný papír může být elektronickou písemností. Cenný papír podle § 514 ObčZ představuje právo spojené s listinou. Listinu samozřejmě i vlivem pokroku už nevnímáme jen v papírové podobě, ovšem je třeba, aby listina naplňovala fyzické aspekty. Listina se tedy musí fyzicky nacházet v konkrétním čase na konkrétním místě. Dále je nutné zmínit, že cenný papír je natolik specifickou listinou, že není možné tuto podmínku relativizovat (např. při aplikaci § 562 ObčZ).

3.2 VEŘEJNOPRÁVNÍ HLEDISKO

Česká právní úprava nabízí možnost zaknihovaných cenných papírů dle zákona o podnikání na kapitálovém trhu. Tento druh cenných papírů sice nemusí splňovat podmínku fyzické existence, dokonce si je v některých aspektech s virtuálními měnami funkčně podobný (lze hovořit o *„virtuálním aktivu spojeném s právem na vyplacení úroku“)*.[75] Narážíme však na striktní zákonné vymezení tohoto pojmu. Zaknihované cenné papíry jsou vedeny v evidenci (Evidence zaknihovaných cenných papírů), kde jsou také dohle-

[75] Bod 3.1 Více viz: Ministerstvo financí České republiky. *Veřejná konzultace - Blockchain, virtuální měny a aktiva.* [Online] Publikováno 30. 11. 2018. Aktualizováno 3. 1. 2019. [cit. 31. 1. 2023]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/kapitalovy-trh/cenne-papiry/2018/verejna-konzultace-blockchain-virtualni-33613.

datelné. Samozřejmě bychom mohli očekávat protiargument, že podobnou evidenci má také Bitcoin nebo Ethereum a další, a tudíž by tento znak mohl být v těchto případech naplněn. Ano, blockchain nabízí velice kvalitní evidenci, ovšem nejedná se o evidenci, kterou stanovuje a uznává zákon. Tudíž ani z veřejnoprávního úhlu pohledu nelze virtuální měnu považovat za cenný papír.

3.3 STANOVISKO ČESKÉ NÁRODNÍ BANKY

ČNB[76] se vyjadřuje především k problematice Bitcoinu jakožto měny, v souvislosti s níž vyvstala řada otázek. Přestože je toto stanovisko zaměřeno na Bitcoin, je možné je vztáhnout i na virtuální měny obecně. Stanovisko ČNB negativně vymezuje virtuální měny a mimo jiné také konstatuje, že nenachází znaky, vzhledem k nimž by bylo možné řadit virtuální měny mezi investiční nástroje. Dále ČNB uvádí, že se nejedená o bezhotovostní peněžní prostředky, elektronické peníze, bezhotovostní obchod s cizí měnou podle zákona o platebním styku ani jinou platební službu. Přestože virtuální měny tedy nejsou investičním nástrojem ve smyslu zákona o podnikání na kapitálovém trhu, je s nimi často spekulováno. Kromě spekulací lze virtuální měnu směňovat za zákonné peníze, případně zboží či služby, nebo je těžit. Virtuální měny nenaplňují žádnou z definic podle směnárenského zákona, jak ČNB ve svém stanovisku uvedla. Režim operací s virtuálními měnami je však s účinností 5. AML směrnice upraven. Nově se vztahuje i na poskytovatele směnárenských služeb mezi virtuálními měnami a měnami s nuceným oběhem, a poskytovatele virtuálních peněženek (čl. 2 odst. 1 bod 3 písm. g) a h) 5. AML směrnice). Dále také 5. AML směrnice stanovuje povinnost dozoru nad těmito subjekty, povinnost jejich registrace a regulace (čl. 47 odst. 1 5. AML směrnice). To ovšem otevírá i otázky, zda vůbec a jakým způsobem bude možno toho docílit.

[76] ČNB. *Obchodování s bitcoiny*. [Online] Publikováno 10. 02. 2014 [cit. 31. 1. 2023]. Dostupné z: https://www.cnb.cz/export/sites/cnb/.galleries/documents/FAQ_download-gallery/obchodovani_s_bitcoiny.pdf.

3.4 STANOVISKO GENERÁLNÍHO FINANČNÍHO ŘEDITELSTVÍ

Vzhledem k tomu, že operace s virtuálními měnami mohou generovat zisk, bylo třeba zodpovědět otázky kolem případného zdanění. Stanovisko Generálního finančního ředitelství uvádí,[77] že fyzické osoby mají tento zisk danit podle § 7 zákona o dani z příjmu fyzických osob,[78] a to jako příjem ze samostatné činnosti.[79] V případě zdanění je rozhodující výsledný zisk, tedy rozdíl mezi hodnotou pořizovací a hodnotou, za kterou byla virtuální měna zpeněžena.[80]

V dalších zdrojích upozorňuje na to, že na virtuální měny, vzhledem k jejich povaze, nelze aplikovat tzv. *časový test*,[81] neboť se jedná o institut, který po třech letech držení cenného papíru zaručuje jeho bezúplatný převod. Přestože přiznání a úhrada daně představuje pro fyzické a právnické osoby povinnost a za nesplnění hrozí příslušné sankce,[82] není snadné tyto příjmy stanovit, přesněji řečeno mnohdy je to velmi pracné. V případě, že osoba provede denně několik transakcí, zisk vypočítává z rozdílu kurzu při nákupu v daném okamžiku a kurzu při prodeji, kdy byla hodnota realizována. Zisky se daní nejen v případech směny virtuální měny za fiat měnu, ale také v případě, kdy nakoupíme za virtuální měnu jinou virtuální měnu. V případě transakcí za celý rok může mnohdy jít o velmi náročnou práci. Dále mají osoby povinnost danit také v okamžiku, kdy

[77] Finanční správa. *Informace GFŘ k daňovému posouzení transakcí s kryptoměnami (např. bitcoin)*. [Online] Publikováno 31. 03. 2022 [cit. 31. 1. 2023]. Dostupné z: https://www.financnisprava.cz/cs/dane/dane/dan-z-prijmu/informace-stanoviska-a-sdeleni/2022/informace-gfr-k-danovemu-posouzeni. PDF dostupné z: https://www.financnisprava.cz/assets/cs/prilohy/d-seznam-dani/Info_kryptomeny_GFR.pdf.

[78] Zákon č. 586/1992 Sb., zákon České národní rady o daních z příjmů.

[79] Měšec.cz. *Jak se daní virtuální měny? Část zisku odvedete vždy, bitcoin je pro berňák věc.* [Online] Publikováno 12. 12. 2017 [cit. 31. 1. 2023]. Dostupné z: https://www.mesec.cz/clanky/jak-se-dani-virtualni-meny-cast-zisku-odvedete-vzdy-bitcoin-je-pro-bernak-vec/.

[80] Finanční správa. *Informace GFŘ k daňovému posouzení transakcí s kryptoměnami (např. bitcoin)*. [Online] Publikováno 31. 03. 2022 [cit. 31. 1. 2023]. Dostupné z: https://www.financnisprava.cz/cs/dane/dane/dan-z-prijmu/informace-stanoviska-a-sdeleni/2022/informace-gfr-k-danovemu-posouzeni. PDF dostupné z: https://www.financnisprava.cz/assets/cs/prilohy/d-seznam-dani/Info_kryptomeny_GFR.pdf.

[81] § 4 odst. 1) písm. w) zákona č. 586/1992 Sb., o daních z příjmů.

[82] Kupř. pokuta za opožděné tvrzení daně, úrok z prodlení aj. § 250 a násl. zákona č. 280/2009 Sb., daňový řád.

dojde ke směně např. bitcoinu za nemovitou věc. Zde se základ pro odvedení daně rovná rozdílu pořizovací ceny v tomto případě bitcoinu a kupní ceny nemovité věci. Pokud jsme například nakoupili bitcoin za 100 000 Kč a jeho hodnota se zvýšila na 1 milion korun, za který si nyní pořídíme nemovitou věc, daníme 900 000 Kč.[83]

Ke dni 1. 1. 2017 je účinné ustanovení zákona o dani z přidané hodnoty, které zakotvuje povinnost, kdy *„příjemce zdanitelného plnění ručí také za nezaplacenou daň z tohoto plnění, pokud je úplata za toto plnění poskytnuta zcela nebo zčásti virtuální měnou podle právního předpisu upravujícího některá opatření proti legalizaci výnosů z trestné činnosti a financování terorismu"*(§ 109 odst. 2 písm. d) ZoDPH). Důvodem je možné zapojení virtuálních měn do tzv. *karuselových podvodů*[84]. Jedná se však stále o ojedinělé ustanovení a je na dalším posouzení, jak důsledně je možné jeho dodržování kontrolovat.

Vzhledem k povaze transakcí finanční úřady většinou nedisponují efektivními nástroji, jak odhalovat případné nepřiznání a následné neodvedení daně. Je tak třeba se zabývat, v případě úvah *de lege ferenda* týkajících se regulace virtuálních měn, nejprve hledáním způsobů, jakými by bylo možné docílit efektivní kontroly. Toto je spíše otázkou technického pokroku než otázkou právní. V současné době je možné odhalení zatajení zisku z virtuálních aktiv obecně z pohybů na bankovních účtech.[85] Tuto skutečnost může zjistit sama banka, nebo orgány finanční správy při výkonu své činnosti, nebo také orgány činné v trestním řízení. Nicméně systematická individuální kontrola finančních toků by byla velmi nákladná a náročná.

---

[83] Peníze.cz. *Vydělali jste na bitcoinu? Před daní Vás nezachrání ani čas.* [Online] Publikováno 3. 02. 2022 [cit. 31. 1. 2023]. Dostupné z: https://www.penize.cz/dan-z-prijmu-fyzickych-osob/430777-bitcoin-a-dane-zisk-z-prodeje-kryptomen-a-danove-priznani.

[84] Tzv. karuselové podvody jsou také nazývány jako podvody kolotočové, nebo chybějícího obchodníka. Jedná se o organizované podvody typicky ve větších skupinách za účelem neodvedení DPH. Charakteristický je také přeshraniční charakter. Více viz Finanční správa. *Karusel (karuselový podvod).* [Online] Publikováno 28. 1. 2016 [cit. 31. 5. 2022]. Dostupné z: https://www.financnisprava.cz/cs/dane/dane/dan-z-pridane-hodnoty/kontrolni-hlaseni-DPH/karusel.

[85] AML zákon.

4. NĚKTERÉ ZAHRANIČNÍ PŘÍKLADY V PŘÍSTUPU K PRÁVNÍ ÚPRAVĚ VIRTUÁLNÍCH MĚN

Státy postupně reagují na dílčí problémy či otázky, které z nárůstu operací s virtuálními penězi plynou. Některé státy Evropské unie transponují 5. AML směrnici v podobě zakotvení jednotlivých dílčích ustanovení. Nicméně i v Evropě se najdou státy s komplexní právní úpravou. Takovým příkladem je Malta.[86] Jak si v otázce úpravy virtuálních měn stojí další státy? A odkud by bylo vhodné čerpat inspiraci? Globální konsenzus napříč světem zatím neexistuje. Zvolené příklady zastupují různé přístupy k regulaci virtuálních měn a dalších aktiv. Jako první příklad bylo zvoleno Japonsko, neboť se jedná o stát, který přijal jako první komplexní právní úpravu. Japonská právní úprava byla vzorem pro maltskou právní úpravu. Dále byla zvolena Jižní Korea, která sice komplexní právní úpravu nepřijala, ale disponuje dílčí úpravou. Jižní Korea byla také zvolena pro svůj přístup, jakým se snaží zajistit uživatelům bezpečnější prostředí. Jako poslední příklad byla zvolena Čína jakožto stát, který virtuální měny a aktiva nyní odmítá. Čína nyní vystupuje proti užívání virtuálních aktiv a označuje transakce s kryptoaktivy za nezákonné. V následující kapitole bude následně rozebrána připravovaná úprava jednotné regulace kryptoaktiv v rámci Evropské unie.

4.1 JAPONSKO

Od roku 2017 je v Japonsku v rámci zákona o platebních službách účinná novela, která zakotvuje definici virtuální měny a oprávnění a regulaci subjektů provozovat takovou směnárenskou činnost. Virtuální měna je definována poměrně obšírně, jako *„i) hodnota majetku, která je omezena pouze na hodnotu v elektronické podobě, s výjimkou uznaných měn a aktiv v elektronické podobě, která může být použita ve vztahu k nespecifikovaným osobám jako platba za účelem protiplnění za nákup nebo leasing zboží nebo za po-*

[86] Ministerstvo financí České republiky. *Veřejná konzultace - Blockchain, virtuální měny a aktiva.* [Online] Publikováno 30. 11. 2018. Aktualizováno 3. 1. 2019. [cit. 31. 1. 2023]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/kapitalovy-trh/cenne-papiry/2018/verejna-konzultace-blockchain-virtualni-33613. s. 11–20.

skytnutí služeb a lze jej také zakoupit a prodat nespecifikovaným osobám jednajícím jako protistrany, které lze převádět prostřednictvím systému elektronického zpracování dat.“ Dále jako „ii) hodnota majetku, kterou lze vzájemně vyměnit za to, co je uvedeno v předchozí položce, s nespecifikovanými osobami jednajícími jako protistrany, a které lze převést pomocí systému elektronického zpracování dat.“[87] Dále jsou směnárny virtuálních měn upraveny v zákoně o prevenci z převodu výnosu z trestné činnosti.[88] Je nutné zmínit, že regulace Japonsku nakonec prospěla. Přilákala větší množství zatím nerozhodných zájemců o virtuální měny, kteří díky regulaci státu získali větší důvěru v tyto investice.

Japonské zákony pracují s pojmem *„fikce cenného papíru“*[89]. Tento institut má pak povahu závazku, ale vztahují se na něj předpisy týkající se cenných papírů. [90]

4.2 JIŽNÍ KOREA

Jižní Korea pracuje jen s dílčí úpravou. Jedním z pravidel, které stojí za zmínku, je spárování elektronické peněženky s bankovním účtem a zákaz držení těchto peněženek cizinci, dětmi a mladistvými.[91] Právní úprava, podobně jako v Japonsku, přinesla důvěru ve virtuální měnu a byla přijata

---

[87] Japanese Law Translation. *Payment Services Act. Act No. 59 of 2009.* [Online] Publikováno 30. 6. 2017 [cit. 31. 1. 2023]. Dostupné z: http://www.japaneselawtranslation.go.jp/law/detail/?id=3078&vm=04&re=02. Dále také viz: Ministerstvo financí České republiky. *Veřejná konzultace - Blockchain, virtuální měny a aktiva.* [Online] Publikováno 30. 11. 2018. Aktualizováno 3. 1. 2019. [cit. 31. 1. 2023]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/kapitalovy-trh/cenne-papiry/2018/verejna-konzultace-blockchain-virtualni-33613. s. 16–18.

[88] Ministerstvo financí České republiky. *Veřejná konzultace - Blockchain, virtuální měny a aktiva.* [Online] Publikováno 30. 11. 2018. Aktualizováno 3. 1. 2019. [cit. 31. 1. 2023]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/kapitalovy-trh/cenne-papiry/2018/verejna-konzultace-blockchain-virtualni-33613. s. 16–18.

[89] Article 2 (2) Payment Services Act. Viz: Japanese Law Translation. *Payment Services Act. Act No. 59 of 2009.* [Online] Publikováno 30. 6. 2017 [cit. 31. 1. 2023]. Dostupné z: http://www.japaneselawtranslation.go.jp/law/detail/?id=3078&vm=04&re=02.

[90] Ministerstvo financí České republiky. *Veřejná konzultace - Blockchain, virtuální měny a aktiva.* [Online] Publikováno 30. 11. 2018. Aktualizováno 3. 1. 2019. [cit. 31. 1. 2023]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/kapitalovy-trh/cenne-papiry/2018/verejna-konzultace-blockchain-virtualni-33613. s. 16–18.

společností pozitivně.[92] Jihokorejská vláda na rozdíl od japonské vlády však vnímá negativně spekulování s kurzy a v minulosti dokonce zvažovala zákaz obchodování s virtuálními měnami. Obávala se negativních finančních dopadů, které by mohla mít závislost na spekulacích s kurzy.[93] K tomuto ovšem nedošlo. V současné době Jižní Korea akceptuje virtuální měny a digitální aktiva a pracuje na právní úpravě směřující k zajištění bezpečného prostředí a vyšší ochrany uživatelů.[94]

V Jižní Koreji mají virtuální měny regulační úpravu, která je považuje za formu digitálního aktiva. S virtuálními měnami je možné legálně nakupovat zboží a služby nebo je investovat. Virtuální měny jsou uchovávány v elektronických peněženkách, které jsou registrovány u regulačních orgánů finanční správy. Uživatelé těchto peněženek mohou převádět své virtuální měny jak na jiné peněženky, tak na bankovní účty. Proces propojení elektronické peněženky s bankovním účtem samozřejmě podléhá příslušné právní úpravě o zpracování osobních údajů.[95] Tato opatření slouží k zajištění bezpečnosti a stability na trhu s virtuálními měnami, přičemž působí i preventivně z hlediska předcházení jejich zneužití. V současné době je vyvíjena snaha směřující k tvorbě právní úpravy zajišťující regulaci a kontrolu tak, aby bylo zajištěno bezpečné prostředí a řádné funkční technické záze-

---

[91] Ministerstvo financí České republiky. *Veřejná konzultace - Blockchain, virtuální měny a aktiva.* [Online] Publikováno 30. 11. 2018. Aktualizováno 3. 1. 2019. [cit. 31. 1. 2023]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/kapitalovy-trh/cenne-papiry/2018/verejna-konzultace-blockchain-virtualni-33613. s. 18.

[92] Kurzy.cz. *V Jižní Koreji začala platit nová pravidla pro obchodování s kryptoměnami. Už žádné anonymní účty.* [Online] Publikováno 31. 1. 2018. [cit. 31. 1. 2023]. Dostupné z: https://www.kurzy.cz/zpravy/444605-v-jizni-koreji-zacala-platit-nova-pravidla-pro-obchodovani-s-kryptomenami-uz-zadne-anonymni-ucty/.

[93] Hospodářské noviny. *Jihokorejská vláda zvažuje zákaz obchodování s kryptoměnami, občané prý příliš riskují.* [Online] Publikováno 11. 1. 2018. [cit. 31. 1. 2023]. Dostupné z: https://byznys.hn.cz/c1-66014340-jizni-korea-chce-zakazat-obchod-s-kryptomenami-navrh-prichazi-po-raziich-u-nejvetsich-burz-v-zemi-kvuli-podezreni-z-danovych-uniku.

[94] Cryptosvět. *Ochrana krypto uživatelů je v Jižní Koreji na 1. místě.* [Online] Publikováno 6. 10. 2022. [cit. 31. 1. 2023]. Dostupné z: https://cryptosvet.cz/ochrana-uzivatelu-je-v-jizni-koreji-na-1-miste/.

[95] Lexology. A *general introduction to the regulation of virtual currencies in South Korea.* [Online] © 2006-2023. [cit. 31. 1. 2023]. Dostupné z: https://www.lexology.com/library/detail.aspx?g=4ab7e422-8668-4db6-a9fd-6a124fffeb01.

mí, zatímco bude uživatelům umožněna volnost a flexibilita v jejich používání.[96]

4.3 ČÍNA

V Číně se stalo téma kryptoměn politickou záležitostí. Od roku 2017 Čína odmítala jakoukoliv činnost spojenou s kryptoměnami. Následně se toto téma stalo národním zájmem a při poskytování osvěty v této souvislosti bylo cíleno na čínské občany.[97] Chvíli to dokonce z politických projevů vypadalo, že dojde v této sféře k posunu.[98] Vzhledem k tomu, jak Bitcoin zasáhl do ekonomické sféry, i Čína se postupně přizpůsobovala pokroku ve snaze tento fenomén regulovat. Následně v září 2021 Čínská centrální banka vydala stanovisko, v němž označila kryptoměnové transakce jako nezákonné (stejně tak i poskytovatele těchto služeb na území Číny), čímž zakázala všechny kryptoměny včetně Bitcoinu.[99] Neznamená to, že by Čína nešla s technologickým pokrokem. Čína se rozhodla vytvořit vlastní digitální jüan (e-CNY), s kterým chce vstoupit na čínský trh.[100]

---

[96] Cryptosvět. *Ochrana krypto uživatelů je v Jižní Koreji na 1. místě.* [Online] Publikováno 6. 10. 2022. [cit. 31. 1. 2023]. Dostupné z: https://cryptosvet.cz/ochrana-uzivatelu-je-v-jizni-koreji-na-1-miste/.

[97] Ministerstvo financí České republiky. *Veřejná konzultace - Blockchain, virtuální měny a aktiva.* [Online] Publikováno 30. 11. 2018. Aktualizováno 3. 1. 2019. [cit. 31. 1. 2023]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/kapitalovy-trh/cenne-papiry/2018/verejna-konzultace-blockchain-virtualni-33613.

[98] LUPA.CZ. *Proč Čína najednou propadla blockchainu a co si od něj slibuje?* [Online] Publikováno 7. 11. 2019. [cit. 31. 1. 2023]. Dostupné z: https://www.lupa.cz/clanky/proc-cina-najednou-propadla-blockchainu-a-co-si-od-nej-slibuje/.

[99] SeznamZprávy. *Čína postavila kryptoměny mimo zákon. Bitcoin padá.* [Online] Publikováno 24. 9. 2021. [cit. 31. 1. 2023]. Dostupné z: https://www.seznamzpravy.cz/clanek/cina-postavila-kryptomeny-mimo-zakon-cena-bitcoinu-pada-175393.

[100] Zítřek. *Boom kryptoměn pokračuje. Vlastní digitální měnu chystá PayPal i Walmart, Čína testuje digitální jüan.* [Online] Publikováno 7. 2. 2022. [cit. 31. 1. 2023]. Dostupné z: https://zitrek.cz/spolecnost/byznys/boom-kryptomen-pokracuje-vlastni-digitalni-menu-chysta-paypal-i-walmart-cina-testuje-digitalni-juan/.

5. PŘIPRAVOVANÁ ÚPRAVA JEDNOTNÉ REGULACE KRYPTOAKTIV V RÁMCI EVROPSKÉ UNIE

Evropská unie (dále také jako *„EU“*) dospěla ke stanovisku, že je na čase oživit evropský hospodářský prostor a zareagovat jednotně na sféru digitálních financí. Dne 24. září 2020 Evropská komise zveřejnila informaci o přijetí Balíčku digitálních financí (v originálu *Digital Finance Package*; dále také jako *„DFP“*).[101] Součástí DFP je strategie pro digitální finance a legislativní návrhy týkající se kryptoaktiv a digitální odolnosti. Evropská unie si klade za cíl být konkurenceschopná v globálním měřítku také ve světě digitálního trhu a směřuje k tomu být tvůrcem globálních standardů. Díky lockdownu v rámci pandemické situace se technologie dostaly skokově do popředí. Z tohoto důvodu se Evropská unie rozhodla na vyvstalý pokrok zareagovat proaktivně, a to právě prostřednictvím DFP a současně i regulovat možná rizika. Spotřebitelům by měl DFP zajistit, kromě ochrany a finanční stability, také širší přístup k moderním finančním produktům.[102] DFP není pouze o sjednocení a regulaci digitálního trhu s financemi a kryptoaktivy, ale také o prevenci možných rizik, která jsou s tímto prostředím spojena.

Balíček se skládá z následujících dílčích částí: strategie digitálního financování, strategie maloobchodních plateb, legislativní návrh regulačního rámce EU pro kryptoaktiva a návrhy regulačního rámce EU pro digitální provozní odolnost. Strategie digitálního financování je sestavena ve světle čtyř základních priorit, které si EU stanovila. Jsou jimi odstranění roztříštěnosti právních úprav na jednotném digitálním trhu. Dalším bodem je vytvoření právního rámce v EU tak, aby usnadnil digitální inovace. V neposlední řadě je další prioritou podpora financování založeného na datech

[101] European Commission. *Digital Finance Package.* [online]. Publikováno 24. 9. 2020. [cit. 31. 1. 2023]. Dostupné z: https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en.

[102] European Commission. *Digital Finance Package: Commission sets out new, ambitious approach to encourage responsible annovation to benefit consumers and businesses.* [online]. Publikováno 24. 9. 2020. [cit. 31. 1. 2023]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684.

a předcházení rizik a řešení možných úskalí digitální transformace. Součástí strategie je také posílení digitální provozní odolnosti finančního sytému.[103]

Vzhledem k zaměření článku bude nyní věnována širší pozornost legislativním návrhům regulačního rámce pro kryptoaktiva. Tato část balíčku obsahuje návrhy následujících nařízení: Návrh nařízení o trzích s kryptoaktivy (v originále *Markets in Crypto-assets*, tzv. *MiCA*), Návrh nařízení o pilotním režimu tržní infrastruktury založené na technologii distribuovaných záznamů, Návrh nařízení o digitální provozní odolnosti (v originále *Digital Operation Resilience Act*, tzv. *DORA*) a pozměňovací směrnice.

Vzhledem k rozebírané problematice se budeme blíže zabývat legislativním Návrhem nařízení o trzích s kryptoaktivy. Jak již bylo zmíněno výše, tento návrh nařízení podporuje pokrok na digitálním trhu a zároveň se snaží poskytnout vyšší transparentnost transakcí a dostupnost povinných informací od obchodníků a ochranu a finanční stabilitu spotřebitelům. Dne 14. března 2022 projednával Ekonomický výbor Evropského parlamentu regulaci kryptoměn. V rámci projednávání bylo také hlasováno o pozměňovacím návrhu, který by obsahoval zákaz tzv. *proof-of-work (PoW)* měn v rámci Evropské unie.[104] Návrh se dotýkal kryptoaktiv, která fungují na principu, v němž uživatel poskytuje svou výpočetní techniku k počítání složitých matematických operací. Výsledkem procesu je ověření transakce. Negativní stránka tohoto procesu spočívá ve spotřebě velkého množství elektrické energie. *PoW* princip je proto z hlediska šetrnosti k životnímu prostředí dlouhodobě kritizován. Je nutno uvést také informaci, že na *PoW* principu pracuje také Bitcoin, pro který by schválení návrhu znamenalo značně negativní dopady. Většina kryptoměn ovšem stojí na principu tzv. *proof-of-stake (PoS)*, který k ověření plateb nepotřebuje tolik výpočetní techniky a je tedy méně energeticky náročný. Výsledkem jednání bylo, že

[103] European Commission. *Digital Finance Package.* [online]. Publikováno 24. 9. 2020. [cit. 31. 1. 2023]. Dostupné z: https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en.

[104] FXstreet.cz. *MiCA, zákaz PoW v EU zamítnut: Bitcoin je prozatím v bezpečí.* [online]. Publikováno 15. 3. 2022. [cit. 31. 1. 2023]. Dostupné z: https://www.fxstreet.cz/zpravodajstvi-127313.html.

Výbor Europarlamentu pro ekonomické záležitosti odmítl začlenit tento návrh do MiCA.[105]

Energetická náročnost se stala jedním z největších problémů, se kterými se potýká trh s virtuálními aktivy. V souvislosti s tím by měl být z tohoto hlediska do budoucna upřednostňován *PoS* princip. PoS princip je sice méně energeticky náročný, ale jsou na něj navázány další problémy a rizika, a to centralizace a možné zneužití systému. Naproti tomu PoW princip sice vyžaduje větší množství energie a je tedy i nákladnější, ale je pro spotřebitele a trh jako celek bezpečnější. Domnívám se, že pro všechny úvahy do budoucna je důležité, aby se regulace vyvíjela tak, aby se minimalizovaly negativní dopady, jako je právě energetická náročnost, a zároveň pro spotřebitele představoval bezpečné prostředí bez zvýšených rizik. Osobně si nemyslím, že zákaz PoW principu je správný směr, jakým se máme vydat. Řešením této situace by mohlo být využití obnovitelných zdrojů energie, přesun těžařských farem do míst, kde je energie levná, snadno dostupná a ekologická. Další možností je snaha o vývoj nových technologií, které budou méně energeticky náročné. Tímto postupem by se mohla stát těžba kryptoměn ekologická a zároveň dlouhodobě udržitelná.

Energetická náročnost těžby kryptoměn je jedním z klíčových faktorů, který nepochybně ovlivňuje fungování trhu s kryptoměnami, a je třeba ji brát v úvahu při zvažování potenciálních investic. Nicméně se domnívám, že se jedná o natolik lukrativní prostředí, že tento problém může významným způsobem přispět k výzkumu, vývoji a tvorbě nízkoenergetických technologií a strategií, které mohou mít využití i mimo tuto oblast. Nelze tedy říci, že energetická náročnost kryptoměn ovlivňuje trh pouze negativně, naopak se domnívám, že může pozitivně přispět jako hnací motor technologického pokroku do budoucna. I dobývání vesmíru je velmi finančně náročné a má své negativní dopady, ale stejně tak každý den těžíme z jeho pozitivních přínosů.

[105] SeznamZprávy. *Hrozba pro bitcoin zažehnána. Europoslanci odmítli kritizovanou regulaci.* [online]. Publikováno 14. 3. 2022. [cit. 31. 1. 2023]. Dostupné z: https://www.seznamzpravy.cz/clanek/ekonomika-osud-kryptomen-je-v-rukach-europoslancu-hlasuji-o-vyrazne-regulaci-193482.

Dále MiCA nabízí difinici pojmu *kryptoaktivum* (v originále *crypto-asset*), který je definován v čl. 3 odst. 1. v bodě 2) MiCA. Kryptoaktivem se ve smyslu MiCA rozumí vyjádření digitální hodnoty nebo práv, které mohou být elektronicky převáděny a ukládány za použití technologie distribuované účetní knihy[106] nebo podobné technologie (čl. 3 odst. 1. bod 2) MiCA). Kryptoaktiva jsou dále rozdělena do čtyř kategorií, a to na *asset-referenced token* (čl. 3 odst. 1. bod 3) MiCA)*, electronic money token* (čl. 3 odst. 1. bod 4) MiCA)*, utility token* (čl. 3 odst. 1. bod 5) *a ostatní tokeny.*[107]

První dvě kategorie lze ve smyslu MiCA v obecném slova smyslu označit za *stablecoiny*. Cílem stablecoinů je, aby byla jejich hodnota zafixována a nebyly volatilní. Udržení stabilní hodnoty je docíleno navázáním tokenu například na hodnotu několika fiat měn, které jsou zákonným platidlem, nebo jedné nebo několika komodit nebo jedné či několika kryptoaktiv nebo kombinací těchto aktiv. *Asset-referenced tokeny (ART)* jsou pro udržení stabilní hodnoty navázány na jiná aktiva, ke kterým mohou patřit i fiat měny. *Electronic money tokeny* udržují svou stabilní hodnotu navázáním na jedinou fiat měnu.[108]

Utility tokeny, nebo také užitné tokeny, jsou kryptoaktiva, která jsou určena k poskytování digitálního přístupu ke zboží nebo službě dostupné prostřednictví DLT a jsou akceptována pouze vydavatelem tohoto tokenu (čl. 3 odst. 1. bod 5) MiCA).[109] Mezi utility tokeny řadíme např. Basic Attention Token (BAT), Binance Coin (BNB) nebo Golem (GNT).

---

[106] Technologie distribuované účetní knihy neboli „DLT" se rozumí druh technologie, která podporuje distribuované zaznamenávání šifrovaných dat. (čl. 3 odst. 1 bod 1) MiCA).

[107] EUR-Lex. *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.* [online]. Publikováno 24. 9. 2020. [cit. 31. 1. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0593.

[108] Medium. *Tokeny s odkazem na aktiva podle nařízení EU o navrhovaných trzích v oblasti kryptografických aktiv.* [online]. Publikováno 10. 2. 2022. [cit. 31. 1. 2023]. Dostupné z: https://medium.com/coinmonks/asset-referenced-tokens-under-the-eus-proposed-markets-in-crypto-assets-regulation-458c317577bb.

[109] EUR-Lex. *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.* [online]. Publikováno 24. 9. 2020. [cit. 31. 1. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0593.

Nařízení MiCA obsahuje celkem devět hlav a 126 článků. Struktura dokumentu je následující: Hlava I. předmět, oblast působnosti a definice (čl. 1-3), Hlava II. Jiná kryptoaktiva než stable coiny a e-money tokeny (čl. 4-14), Hlava III. Stable coiny (čl. 15-42), Hlava IV. E-money tokeny (čl. 43-52), Hlava V. Povolení a provozní podmínky pro poskytovatele služeb souvisejících s kryptoaktivy (čl. 53-75), Hlava VI. Předcházení zneužívání trhu s kryptoaktivy (čl. 76-80), Hlava VII. Příslušné orgány, EBA a ESMA (čl. 81-120), Hlava VIII. Akty v přenesené pravomoci a prováděcí akty (čl. 121), Hlava IX. Přechodná a závěrečná ustanovení (čl. 122-126).[110]

Aktuálně po hlasování Evropského parlamentu dochází k tzv. trialogu mezi Evropskou komisí, Evropským parlamentem a Evropskou radou, který se týká návrhu regulace MiCA. Mezi rozhodující otázky stále patří mj. právě téma udržitelnost životního prostředí ve vztahu ke kryptoměnám.[111] Kromě výše zmíněného by měla být do 1. ledna 2025 zakotvena do Taxonomie EU pro udržitelné činnosti (v originále *EU taxonomy for sustainable activities*) také činnost související s těžbou kryptoměn.[112]

Z hlediska možných *přínosů* jednotné regulace kryptoaktiv v rámci Evropské unie spatřuji zvýšení transparentnosti a důvěryhodnosti. Regulace by mohla poskytnout jasný rámec pro provozování a využívání kryptoaktiv, což by mohlo pomoci zvýšit důvěru veřejnosti v tuto oblast. Dále spatřuji přínos regulace ve zvýšení bezpečnosti kryptoaktiv tím, že by stanovila pravidla pro zabezpečení transakcí a ochranu investic. Domnívám se, že by mohla regulace přispět ke snížení rizika podvodů a nelegální činnosti, při kterých jsou kryptoaktiva použita. Naproti tomu bychom neměli opo-

[110] EUR-Lex. *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.* [online]. Publikováno 24. 9. 2020. [cit. 31. 1. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0593.

[111] Deloitte. *Digital Finance: European Parliament adopts MiCA Regulation, paving the way for an innovation-friendly crypto regulation.* [online]. Publikováno 17. 3. 2022. [cit. 31. 1. 2023]. Dostupné z: https://www2.deloitte.com/lu/en/pages/financial-services/articles/digital-finance-european-parliament-adopts-mica-regulation-innovation-friendly-crypto-regulation.html.

[112] European Commission. *EU taxonomy for sustainable activities.* [online]. Publikováno 12. 6. 2020. [cit. 31. 1. 2023]. Dostupné z: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/sustainable-finance/eu-taxonomy-sustainable-activities_en.

menout také *nedostatky*, které může tato regulace přinést. Jako první problém spatřuji omezení svobody u inovací. Regulace by mohla zpomalit rozvoj v této oblasti, neboť by kroky, které se dosud děly neregulovaně, musely být napřed schváleny. Další negativum spatřuji v administrativní zátěži a na ni logicky navazující zvýšení nákladů. V neposlední řadě vnímám jako velmi zásadní problém ztrátu jisté formy anonymity. Prostřednictvím regulace může být vyžadováno například odhalení a potvrzení identity uživatelů kryptoaktiv, přičemž právě ochrana soukromí je uživateli v této oblasti velmi ceněnou vlastností.

6. MOŽNÁ ÚSKALÍ

6.1 EXEKUCE

Ze zmíněné nemožnosti odhalení, respektive kontroly transakcí a vlastnictví virtuálních měn, už postupně začínají plynout problémy. Štika poukazuje ve svém článku na situaci, kdy je třeba v rámci exekučního řízení zjistit majetek, zajistit jej a následně jej zpeněžit k uhrazení dluhů. V případě, že dlužník bude uchovávat své finance v elektronické peněžence v podobě bitcoinů, nebude možné na tento majetek přijít, natož ho zpeněžit.[113] Jako veliký problém vnímá, že státní orgány nemají možnost spravovat evidenci transakcí, tzv. *blockchain*, jako autorita. Obává se o oprávněné vymáhání pohledávek a práv, které budou věřitelům náležet a domnívá se, že zatím pro takový Bitcoin jaký dnes je, není v právním státě místo. Naproti tomu Jochman uvádí, že mezi hlavní výhody patří právě necenzurovatelnost a nezkonfiskovatelnost bitcoinu. Dále dochází k závěrům, že posouvá demokratický právní stát na zcela novou vyšší úroveň. Obyvatelé tak budou mnohem více nezávislí na státě. Uvádí, že naopak Bitcoin napomáhá ochraně majetku před „zlovůlí“ státu v souvislosti s poukázáním na historický kontext.[114]

[113] ŠTIKA, Martin. Má naprosto svobodná virtuální měna bitcoin místo v právním státě?. *Bulletin advokacie*. 5/2018, s. 29.

[114] JOCHMAN, David. Skutečně nemá „naprosto svobodná virtuální měna bitcoin“ místo v právním státě?. *Bulletin advokacie.* 12/2018, s. 44.

S oběma závěry lze do jisté míry souhlasit. Na jedné straně stojí naprosto pochopitelná obava z nemožnosti státu dosáhnout na peníze v elektronických peněženkách, naproti tomu se lze bez dalšího ztotožnit i s názorem, že tato nemožnost posouvá demokratický stát na zcela novou úroveň. Zásah státu do majetkových práv, jak jsme jej v historii již zažili, je samozřejmě riziko a nezkonfiskovatelnost představuje neskutečnou výhodu. Ve světle současné situace na Ukrajině se může zdát uchování financí v elektronické peněžence při prchání před válkou jako velmi praktické řešení. Považme však, jaké množství osob bude mít dostatek financí, které může do elektronické peněženky uložit (i vzhledem k poplatkům za vklad a výběr). A dále kolik osob z tohoto množství bude disponovat technickým povědomím a všeobecnými znalosti, aby mohli toto řešení využít.

Naproti tomu mohou virtuální měny výrazně zahýbat běžnějšími situacemi. Problém s obnosy uschovanými v elektronických peněženkách však exekucí nekončí, ale naopak začíná. Ač se plně neztotožňuji se všemi závěry Štiky, považuji do jisté míry pro chod státu z dlouhodobého hlediska za rizikovější postup, ve kterém absentuje možnost vykonání exekuce. Tedy situace, kdy stát ztratí nástroj, prostřednictvím kterého se osoby zodpovídají z dluhů, které napáchaly, a to i v případech, kdy třeba nechtějí plnit. V případě, kdy bude plnění závislé na dobrovolnosti, nikoliv na povinnosti, tak jak se strany k tomu zavázaly, se domnívám, že většinou nebude možnost plnění docílit.

Osobně se domnívám, že argument nezkonfiskovatelnosti je silný, ale situací, kdy na něj dojde, bude minimum. Naproti tomu již nyní vzniká velké množství situací v běžném životě, pro které kryptoměny tvoří překážku nebo riziko.

6.2 DĚDICKÉ A RODINNÉ PRÁVO

Uschovávání virtuálních měn v elektronických peněženkách může generovat řadu problémů. Především nemožnost státu vyhledat, zda konkrétní osoba má zřízenou elektronickou peněženku, zda vlastní některou virtuální měnu, a pokud ano, v jaké výši. K tomu, aby byla virtuální měna uživatelsky atraktivní, je také zapotřebí bezpečného místa, kde ji bude možné

uchovat. Elektronické peněženky mají poměrně komplikovaný systém zabezpečení a v případě zapomenutí nebo neznalosti přístupového hesla je skoro nemožné virtuální měnu z peněženky získat. Problém digitálního dědictví se zdaleka netýká jen kryptoměn, ale i přístupů k účtům na hazardních serverech, na burzách apod. Současná právní úprava je zastaralá a otázky digitálního dědictví řeší neuspokojivě.

V případě smrti osoby, která vlastnila virtuální měnu, může nastat hned několik situací. Předně v rámci řízení o pozůstalosti se pozůstalí nemusí dozvědět, že zesnulý vlastnil virtuální měnu, neboť toto není možné nijak centrálně zjistit. Na rozdíl od situace, kdy by zesnulý vlastnil cenné papíry. Tehdy by se notář mohl obrátit na Centrální depozitář cenných papírů. Vlastnictví virtuální měny by však mohlo být zjištěno spíše náhodou, pokud by někdo detailněji zkoumal pohyby na bankovním účtu. V případě, že by zesnulý krátce před smrtí prodal nemovitou věc a finance z prodeje této věci by v pozůstalosti nebyly, mohlo by toto budit otázky a podnítit hledání. Nicméně i v případě, že by v pozůstalosti byla objevena elektronická peněženka, nebudou-li mít pozůstalí přístupové heslo, nebude jim to nijak platné. Dále by mohlo v případě smrti osoby, která vlastnila virtuální měnu v elektronické peněžence a sdělila z nějakého důvodu tuto informaci jiné osobě včetně informace o přístupovém hesle, dojít k trestnému činu vůči majetku zůstavitele a dědic by se tak stal dědicky nezpůsobilý. Na tento trestný čin by se nemuselo ani přijít. Mezi možnými scénáři vnímám v zásadě rozdíl podle toho, zda půjde o hardwarovou nebo softwarovou peněženku. V prvním případě je peněženkou datový nosič, který je fyzicky oddělen od počítače. V druhém případě se může peněženka nacházet přímo v počítači (nainstalovaný program) nebo může osoba vlastnit virtuální aktiva online, a to na různých platformách (Coinbase, Binance, Kraken). Zde si osoba založí účet, ověří údaje a může začít obchodovat. U hardwarových peněženek bude situace nejnáročnější. Z pohybů na účtu sice můžeme usoudit, že máme hledat další finanční prostředky, ale fakticky si tuto skutečnost nemáme jak ověřit. Naopak u virtuálních aktiv uložených na online platformách by bylo možné z pohybů na účtech dovodit, že dotyčný vlastnil účet s virtuálními aktivy na konkrétní platformě. Ovšem otázkou zůstává,

jak budou provozovatelé těchto platforem ochotni s případnými dědici nebo úřady komunikovat. Obecně by to mohlo otevírat prostor pro další druh podvodů. Zde bychom mohli narážet na problém s bezpečnostními pravidly těchto společností a ochranou údajů. Další překážkou budou omezené možnosti postupu českých úřadů, neboť se jedná většinou o společnosti se sídly v zahraničí.

Další otázkou, která v této souvislosti vyvstává, se týká uchování unikátních přístupových hesel k elektronické peněžence, případně účtům. Přístupová hesla by neměla být zazálohovaná v počítači. Odborníci doporučují místa mimo něj, a to papír nebo kovovou destičku. Tato přístupová hesla bude však pravděpodobně obtížné najít a následně propojit s peněženkou nebo účtem.

V případě rodinného práva, resp. společného jmění manželů vznikají velice obdobné problémy. Příkladem může být vypořádání společného jmění manželů (po rozvodu, při úmrtí, po zúžení či zrušení společného jmění), při němž bude zatajen obsah elektronické peněženky.

6.3 DALŠÍ MOŽNÁ RIZIKA

Problémy by mohly obdobně vznikat i v oblasti sociálního zabezpečení, v případě podávání povinného majetkového přiznání, jak již bylo uvedeno v předchozích kapitolách, také v případě zatajování při přiznávání a odvodu daně a v dalších případech. Dále je třeba dát za pravdu i argumentům hovořícím o nejrůznějších bezpečnostních rizicích, právě například při legalizování výnosů z trestné činnosti. Ta jsou bezesporu vysoká. Ovšem i sama virtuální aktiva a peněženky mohou být cílem hackerů, a to i přes jejich zabezpečení. V České republice se již objevuje majetková trestná činnost v této oblasti.[115]

Právními problémy však výčet nekončí. Dále budeme nevyhnutelně muset jednoho dne čelit pokroku. V případě vyvinutí kvantových počítačů by tak došlo k prolomení šifry a Bitcoin či jiná kryptoměna nebo kryptoak-

[115] iDnes.cz. *Soud přehodnotil krádež bitcoinů na zpronevěru, programátor dostal 9 let.* [Online] Publikováno 5. 9. 2019 [cit. 31. 1. 2023]. Dostupné z: https://www.idnes.cz/brno/zpravy/soud-programator-tomas-jirikovsky-bitcoiny-zpronevera.A190905_121842_brno-zpravy_krut.

tivum by se během krátkého času staly bezcennými a investované peníze by zmizely v nenávratnu.

7. MOŽNÁ ŘEŠENÍ

Z hlediska tuzemské právní úpravy virtuálních měn *de lege ferenda* se pravděpodobně nejvíce ztotožňuji s japonskou úpravou, která pro práci s virtuálními měnami používá tzv. *fikci cenného papíru*. Domnívám se, že se do jisté míry jedná o velmi schůdné řešení a směr, jakým by se naše právní úprava mohla v této oblasti nechat inspirovat. Jak již bylo uvedeno výše, český právní řád nám neposkytuje dostatečný prostor k tomu, abychom mohli virtuální měnu považovat za cenný papír, respektive abychom mohli pojem cenného papíru relativizovat. Úprava cenných papírů je poměrně striktní. Snahy o její relativizaci by mohly napáchat řadu škod, nabourat poměrně stabilní praxi a zasáhnout do právní jistoty. Aplikaci úpravy cenných papírů nelze považovat za špatný nápad, neboť to stávající úpravu cenných papírů nijak neovlivní. Kromě toho vzhledem k tomu, jak se virtuální měny chovají, resp. jak je s nimi operováno, je to vhodné.

Dále se domnívám, že je velice praktické zakotvit podobné ustanovení jaké má jihokorejská úprava. Propojení elektronických peněženek s bankovními účty by mohlo znamenat velký krok v zpřehlednění situace, a to i přes snížení míry soukromí. Jak již bylo uvedeno, nyní neexistuje efektivní nástroj, jakým by bylo možné zjistit, zda konkrétní osoba nevlastní finance ještě někde, kam na ně stát nedosáhne. Otázkou zůstává, zda bychom nezůstali u pouhého vědění, že v elektronické peněžence jednotky jsou, ale nebylo by je možno získat. Domnívám se, že vyřešení tohoto problému by mohlo pozitivně prospět oblasti dědického práva. Vyřešilo by to však jen polovinu problému, a to problém se softwarovými elektronickými peněženkami a účtech na online platformách. Stále bychom se nedozvěděli o hardwarových peněženkách. Jediným řešením by bylo pokračovat ještě dál a už při koupi registrovat kupujícího jako držitele hardwarové peněženky, což mi ale přijde velmi přehnané. Na jedné straně je historickým smyslem dědického práva sice materiální zajištění potomstva, nicméně tato regulace a posun k centralizaci popírá původní myšlenku virtuálních měn. Stále mu-

síme mít na paměti, že pořízení a způsob uchování virtuálních měn je svobodnou volbou každé osoby, a to i s riziky, která jsou s tím spojena.

Původní záměr, se kterým virtuální měny a aktiva vznikaly, bylo také, že budou nezávislé na státu, nezdanitelné, decentralizované. Právě v případě exekuce toto může činit velký problém. Informace o konkrétní osobě, soukromí, vlastnictví, lze považovat za určitý druh svobody a shromažďování těchto dat jako omezení. Přesto si myslím, že takové omezení může přispět větší bezpečnosti, jistotě, což ostatně koreluje s ideami teorie společenské dohody. To celé může trhu s kryptoaktivy paradoxně prospět, i když je to proti původnímu záměru tvůrců, neboť to bude pro spotřebitele příznivější a bezpečnější prostředí. Výměnou za vlastní informace získáme možnost lépe vymáhat dlužná plnění či se dozvědět o aktivech v rámci majetkového vypořádání nebo dědického řízení. Předejdeme tak případným podvodům. Existuje bezesporu více způsobů, jak na tento problém hledět, ostatně jak jsem již uvedla výše.

8. ZÁVĚR

Porovnáme-li pojmy virtuální měna a virtuální aktivum navzájem, lze shrnout následující rozdíly. Pojem virtuální měna byl upraven v AML zákoně ve znění platném do 31. 12. 2020. Virtuální měny lze podřadit jako podkategorii k pojmu virtuální aktivum. Od 1. 1. 2021 došlo k terminologické změně a k rozšíření pojmu virtuální měna na virtuální aktivum, přičemž tento pojem byl rozšířen tak, aby pod něj bylo možné zahrnout celou řadu dalších tokenů, jejichž platební funkce je potlačena a naopak je zdůrazněna funkce investiční. Dále z hlediska rozdílů v terminologii lze konstatovat, že pojem kryptoměna je ve vztahu k pojmu virtuální měna užší a lze jej pod něj podřadit. Kryptoměny je dále možné dělit na měny a tokeny. Pojmy digitální měna a digitální peníze jsou podřazené pojmu virtuální aktivum. Konkrétní příklady mohou naplňovat charakteristiky více pojmů. Bitcoin je například jak virtuálním aktivem, tak virtuální měnou, kryptoměnou, současně naplňuje znaky decentralizovaných digitálních peněz a takto bychom mohli pokračovat.

Obecně lze shrnout, že virtuální měny nejsou měnami v právním slova smyslu. Nicméně výjimkou z tohoto tvrzení je Salvador, který se stal vůbec první zemí na světě, která oficiálně přijala jako zákonné platidlo kryptoměnu - Bitcoin.

Otázku, zda jsou virtuální měny penězi, opět nelze krátce zodpovědět. Původní záměr autorů virtuálních měn byl vytvořit univerzální platidlo v digitálním prostoru. Nicméně stejně tak jako se rozšířil pojem, narostlo i množství virtuálních aktiv a s tím se také rozšířily funkce, které mohou plnit. Obecně můžeme virtuální aktiva podle funkce dělit na platební, směnná a investiční, přičemž se mohou tyto funkce i navzájem prolínat. Původní virtuální měny mohou dnes plnit spíše funkci investiční. Ovšem existuje druh virtuálních aktiv, která jsou vytvořena především k funkci platební. Jedná se o stablecoiny. Namísto toho, aby například Bitcoin představoval univerzální platidlo, představuje spíše unikátní komoditu, něco jako diamant nebo zlato. Bitcoin byl dokonce jako jediný za komoditu v roce 2015 oficiálně označen. Na rozdíl od zlata nebo diamantu je však mnohem více volatilní, s čímž se pojí jistá rizika. I přes svou volatilitu však mohou virtuální měny představovat přínos pro chudé země trpící vysokou inflací a špatnou životní úrovní.

Virtuální měny mají asi nejblíže ke komoditám, avšak tento závěr však nelze vztáhnout na virtuální aktiva celkově. Komoditou by mělo být zastupitelné zboží dodávané od různých dodavatelů bez rozdílu kvality tohoto zboží, což by ve vztahu ke konkrétním případům bylo možné i splnit, nikoliv však obecně. Mezi virtuální aktiva řadíme také tzv. NFT, které jsou ze své podstaty a názvu nezastupitelnými tokeny.

Ohledně zakládání komplexní právní úpravy a nových institutů či změny významu již důvěrně známých zažitých pojmů jsem spíše zdrženlivá a považuji to zatím za předčasné. Oblast virtuálních aktiv se velmi dynamicky vyvíjí. Bitcoin sice existuje přibližně dekádu, virtuální měny o něco déle, ale dopady vnímáme výrazněji teprve v posledních letech. Vzhledem k tomuto časovému úseku se jedná o poměrně novou záležitost. Považuji tak za adekvátní dosavadní tvorbu úpravy v podobě dílčích ustanovení, která reagují na vyvstalé problémy a situace. Nedomnívám se však, že tato

úprava je dostatečná, neboť stále existují situace, které uspokojivě vyřešeny nejsou. Tvorba komplexní úpravy je velmi časově náročná a vzhledem k možnému vývoji by mohla narážet na časté aktualizace. Je však na čem pracovat a rozhodně je vhodné sledovat vývoj zahraničních úprav a důsledky, které jednotlivé přístupy měly, mají a budou také mít.

Problematika virtuálních aktiv je velice komplikovaná. Domnívám se, že pro tvorbu legislativy je základní otázkou vymezení podstaty jednotlivých virtuálních aktiv. Dále můžeme zvažovat propojení stávajících technologií na úrovni států s dalšími systémy (např. jako je tomu u propojení elektronických peněženek v Jižní Koreji). Touto cestou můžeme vytvořit bezpečnější prostředí, kde budou efektivně zajišťována práva osob pohybujících se v této oblasti. Pozitivní dopady by tento postup mohl znamenat i v oblasti dědického a rodinného práva. V současné době je velmi náročné zjistit, zda osoba za života vlastnila elektronickou peněženku s virtuálními aktivy, a pokud ano, pravděpodobně se k nim přes zabezpečení nebude možné dostat. V případě, že by alespoň společnosti, které provozují online platformy, měly povinnost jakési centrální evidence, na kterou by se mohl notář v rámci dědického řízení obracet, znamenalo by to posun vpřed. Nicméně stále to nevyřeší situace s hardwarovými peněženkami. Zde se však nabízí otázka, zda je problém natolik palčivý, aby vyžadoval legislativní regulaci. Hledání právních a technologických cest je jedna strana mince, regulace by však neměla být příliš omezující a deanonymizující. Měly bychom nalézt rovnováhu mezi původním záměrem, jistou mírou svobody a zároveň přiměřenou ochranou spotřebitele a bezpečným prostředím.

Paleta oblastí, do kterých virtuální aktiva zasahují, je opravdu pestrá. Kromě výše zmíněných oblastí jsou jimi samozřejmě také oblast trestního práva, exekucí, daní, ale také sféra životního prostředí. Dle mého názoru se jedná o velmi tematicky bohaté a obecně perspektivní odvětví, ať už z hlediska práva nebo z hlediska nových technologií, vědy a výzkumu. Každý pokrok kromě pozitivních přínosů má i negativní dopady, které by však měly být pro další směřování výzvou a příležitostí k překonání problému. Virtuální měny mohou například přispět jako katalyzátor vývoje nových technologií, které budou méně energeticky náročné a přispějí tak k řešení

problému energetické krize. Už nyní lze spatřit pozitivní dopady virtuálních měn například při řešení mezinárodních plateb.

9. SEZNAM POUŽITÝCH ZDROJŮ

9.1 PRAMENY

[1] Důvodová zpráva k zákonu č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu

[2] Důvodová zpráva k zákonu č. 527/2020 Sb., kterým se mění zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů, a další související zákony, zákony související s přijetím zákona o evidenci skutečných majitelů a zákon č. 186/2016 Sb., o hazardních hrách, ve znění pozdějších předpisů

[3] Směrnice Evropského parlamentu a rady (EU) 2018/843 ze dne 30. května 2018, kterou se mění směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu a směrnice 2009/138/ES a 2013/36/EU (tzv. 5. AML směrnice)

[4] Zákon č. 235/2004 Sb., o dani z přidané hodnoty

[5] Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu

[6] Zákon č. 280/2009 Sb., daňový řád

[7] Zákon č. 370/2017 Sb., o platebním styku

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

[9] Zákon č. 586/1992 Sb., zákon České národní rady o daních z příjmů

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

9.2 JUDIKATURA

[11] Rozsudek Soudního dvora (pátého senátu) ze dne 22. října 2015. Skatteverket v. David Hedqvist, ve věci C-264/14

9.3 LITERATURA

[12] BAKEŠ, Milan a kol. *Finanční právo*. 6. vydání. Praha: C. H. Beck, 2012. 552 s. ISBN 978-80-7400-440-7

[13] HLAVINOVÁ, Markéta, KABEŠ, Viktor; PILÍKOVÁ, Jaroslava. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu*. 3. vydání. Praha: C. H. Beck, 2022. 552 s. ISBN 978-80-7400-860-3

[14] JÁNOŠÍKOVÁ, Petra a kol. *Finanční a daňové právo*. 2. vydání. Plzeň: Aleš Čeněk, s.r.o., 2016. 496 s. ISBN 978-80-7380-639-2

[15] STROUKAL, Dominik, SKALICKÝ, Jan. *Bitcoin a jiné kryptopeníze budoucnosti: Třetí rozšířené vydání. Historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. 3. vyd. Praha: Grada Publishing, 2021. 294 s. ISBN 978-80-271-1043-8

[16] TVRDÝ, Jiří, VAVRUŠKOVÁ, Adriana. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu*. 2. vydání. Praha: C. H. Beck, 2018. 584 s. ISBN 978-80-7400-688-3

9.4 ODBORNÉ ČLÁNKY

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

[18] JOCHMAN, David. Skutečně nemá „naprosto svobodná virtuální měna bitcoin“ místo v právním státě?. *Bulletin advokacie.* 12/2018, s. 44

[19] ŠTIKA, Martin. Má naprosto svobodná virtuální měna bitcoin místo v právním státě?. *Bulletin advokacie.* 5/2018, s. 29

9.5 JINÉ ZDROJE

9.5.1 ČESKÉ

[20] CFO world. *Bitcoin a jiné virtuální měny z pohledu práva.* [Online] Publikováno 16. 01. 2017 [cit. 31. 1. 2023]. Dostupné z: https://cfoworld.cz/legislativa/bitcoin-z-pohledu-prava-4199

[21] Clever and smart. *Základy kryptografie pro manažery: hashovací funkce.* [Online] Publikováno 1. 7. 2010 [cit. 31. 1. 2023]. Dostupné z: https://www.cleverandsmart.cz/zaklady-kryptografie-pro-manazery-hashovaci-funkce/

[22] CryptoKingdom. *Co je to pseudonymita?* [Online] Publikováno 15. 10. 2019 [cit. 31. 1. 2023]. Dostupné z: https://cryptokingdom.tech/cs/magazin/zacatecnik/co-je-to-pseudonymita

[23] Cryptosvět. *Ochrana krypto uživatelů je v Jižní Koreji na 1. místě.* [Online] Publikováno 6. 10. 2022. [cit. 31. 1. 2023]. Dostupné z: https://cryptosvet.cz/ochrana-uzivatelu-je-v-jizni-koreji-na-1-miste/

[24] Česká národní banka. *Inflace v prosinci 2022 zpomalila.* [Online] Publikováno 11. 1. 2023 [cit. 31. 1. 2023]. Dostupné z: https://www.cnb.cz/cs/verejnost/servis-pro-media/komentare-cnb-ke-zverejnenym-statistickym-udajum-o-inflaci-a-hdp/Inflace-v-prosinci-2022-zpomalila/

[25] Česká národní banka. *Prognóza ČNB – zima 2023*. [Online] Publikováno 2. 2. 2023 [cit. 31. 1. 2023]. Dostupné z: https://www.cnb.cz/cs/menova-politika/prognoza/

[26] Česká televize. 90'ČT24. *Bitcoin – univerzální platidlo budoucnosti?*. [Online] Publikováno 15. 8. 2017 [cit. 31. 1. 2023]. Dostupné z: https://www.ceskatelevize.cz/porady/11412378947-90-ct24/217411058130815-bitcoin-univerzalni-platidlo-budoucnosti

[27] ČNB. *Obchodování s bitcoiny*. [Online] Publikováno 10. 02. 2014 [cit. 31. 1. 2023]. Dostupné z: https://www.cnb.cz/export/sites/cnb/.galleries/documents/FAQ_downloadgallery/obchodovani_s_bitcoiny.pdf

[28] ČT24. *Kazachstán se stal druhým největším těžařem bitcoinu. Farmy spotřebují osm procent energie v zemi.* [Online] Publikováno 13. 11. 2021 [cit. 31. 1. 2023]. Dostupné z: https://ct24.ceskatelevize.cz/svet/3399608-kazachstan-se-stal-druhym-nejvetsim-tezarem-bitcoinu-farmy-spotrebuji-osm-procent

[29] ČTK. České noviny. *Salvador je ode dneška první zemí na světě, kde lze platit bitcoinem.* [Online] Publikováno 7. 09. 2021 [cit. 31. 1. 2023]. Dostupné z: https://www.ceskenoviny.cz/zpravy/salvador-ktery-zavadi-bitcoin-jako-platidlo-jich-nyni-drzi-400/2086277

[30] DigiSlovník. *Digitální měna.* [Online] Publikováno © 2020 [cit. 31. 1. 2023]. Dostupné z: https://portaldigi.cz/digislovnik/digitalni-mena/

[31] E15. *Investice do bitcoinu jako riziko i šance. Volatilita vytváří obchodní příležitosti.* [Online] Publikováno 31. 3. 2021 [cit. 31. 5. 2022]. Dostupné z: https://www.e15.cz/kryptomeny-investice

[32] E15.cz. *Bitcoinmaty se množí. Hotovost za digitální měnu jde směnit už na 16 500 místech.* [Online] Publikováno 16. 3. 2021. [cit. 31. 1. 2023]. Dostupné z: https://www.e15.cz/kryptomeny/bitcoinmaty-se-mnozi-hotovost-za-digitalni-menu-jde-smenit-uz-na-16-500-mistech-1378796

[33] Euro.cz. *Inflace ve Venezuele zpomalila, přesto loni dosáhla 234 procent. Velké problémy má stále i Turecko.* [Online] Publikováno 25. 1. 2023 [cit. 31. 1. 2023]. Dostupné z: https://www.euro.cz/clanky/inflace-ve-venezuele-zpomalila-presto-loni-dosahla-234-procent-velke-problemy-ma-stale-i-turecko/

[34] Evropská centrální banka. *Co jsou peníze?* [Online] Publikováno 24. 11. 2015, aktualizováno 20. 6. 2017 [cit. 31. 1. 2023]. Dostupné z: https://www.ecb.europa.eu/ecb/educational/explainers/tell-me-more/html/what_is_money.cs.html

[35] Finanční analytický úřad. *MONEYVAL*. [Online] Publikováno © 2022 [cit. 31. 1. 2023]. Dostupné z: https://www.financnianalytickyurad.cz/moneyval

[36] Finanční správa. *Informace GFŘ k daňovému posouzení transakcí s kryptoměnami (např. bitcoin)*. [Online] Publikováno 31. 03. 2022 [cit. 31. 1. 2023]. Dostupné z: https://www.financnisprava.cz/cs/dane/dane/dan-z-prijmu/informace-stanoviska-a-sdeleni/2022/informace-gfr-k-danovemu-posouzeni. PDF dostupné z: https://www.financnisprava.cz/assets/cs/prilohy/d-seznam-dani/Info_kryptomeny_GFR.pdf

[37] Finanční správa. *Karusel (karuselový podvod)*. [Online] Publikováno 28. 1. 2016 [cit. 31. 1. 2023]. Dostupné z: https://www.financnisprava.cz/cs/dane/dane/dan-z-pridane-hodnoty/kontrolni-hlaseni-DPH/karusel

[38] Finex.cz. *36. díl Seriálu technické analýzy – Co je to volatilita.* [Online] Publikováno 7. 9. 2019 [cit. 31. 1. 2023]. Dostupné z: https://finex.cz/technicka-analyza-volatilita/

[39] Finex.cz. *Anonymní kryptoměny: jak privátní transakce fungují a nakolik jsou spolehlivé?* [Online] Publikováno 28. 11. 2020 [cit. 31. 1. 2023]. Dostupné z: https://finex.cz/anonymni-kryptomeny-jak-privatni-transakce-funguji-a-nakolik-jsou-spolehlive/

[40] Finex.cz. *Inflace: Co je to inflace? Jaké jsou její příčiny a jaké může mít dopady?*. [Online] Aktualizováno 1. 11. 2022 [cit. 31. 1. 2023]. Dostupné z: https://finex.cz/inflace/

[41] Finex.cz. *Non-fungible tokeny (NFT): Co to je, jak fungují a vyplatí se do nich investovat?* [Online] Publikováno © 2014-2023 [cit. 31. 1. 2023]. Dostupné z: https://finex.cz/rubrika/nft/

[42] Forbes. *Brutální propad bitcoinu. Kryptoměna je prvním poraženým ekonomické krize*. [Online] Publikováno 16. 3. 2020 [cit. 31. 1. 2023]. Dostupné z: https://www.forbes.cz/brutalni-propad-bitcoinu-kryptomena-je-prvnim-porazenym-ekonomicke-krize/

[43] FXstreet.cz. *Inflace v Turecku v prosinci klesla na 64,3 procenta, nejvíce od roku 1995.* [Online] Publikováno 3. 1. 2023 [cit. 31. 1. 2023]. Dostupné z: https://www.fxstreet.cz/inflace-v-turecku-v-prosinci-klesla-na-643-procenta-nejvice-od-roku-1995.html

[44] FXstreet.cz. *MiCA, zákaz PoW v EU zamítnut: Bitcoin je prozatím v bezpečí.* [online]. Publikováno 15. 3. 2022. [cit. 31. 1. 2023]. Dostupné z: https://www.fxstreet.cz/zpravodajstvi-127313.html

[45] FXstreet.cz. *První fond v Česku umožňuje investici do kryptoměn.* [Online] Publikováno 31. 1. 2018 [cit. 31. 1. 2023]. Dostupné z: https://www.fxstreet.cz/prvni-fond-v-cesku-umoznuje-investici-do-kryptomen.html

[46] Hospodářské noviny. *Jihokorejská vláda zvažuje zákaz obchodování s kryptoměnami, občané prý příliš riskují.* [Online] Publikováno 11. 1. 2018. [cit. 31. 1. 2023]. Dostupné z: https://byznys.hn.cz/c1-66014340-jizni-korea-chce-zakazat-obchod-s-kryptomenami-navrh-prichazi-po-raziich-u-nejvetsich-burz-v-zemi-kvuli-podezreni-z-danovych-uniku

[47] iDNES.cz. *Cena zlata v korunách zlomila dosavadní rekordy. Může růst i nadále*. [Online] Publikováno 19. 5. 2020 [cit. 31. 1. 2023]. Dostupné z: https://www.idnes.cz/ekonomika/zahranicni/zlato-cena-rekord-krize-investice-pandemie-covid-19-koruna-dolar.A200519_153409_eko-zahranicni_mato

[48] iDnes.cz. *Soud přehodnotil krádež bitcoinů na zpronevěru, programátor dostal 9 let.* [Online] Publikováno 5. 9. 2019 [cit. 31. 1. 2023]. Dostupné z: https://www.idnes.cz/brno/zpravy/soud-programator-tomas-jirikovsky-bitcoiny-zpronevera.A190905_121842_brno-zpravy_krut

[49] iKrypto.cz. *Kde všude můžeme platit bitcoinem*. [Online] Publikováno 16. 3. 2019 [cit. 31. 1. 2023]. Dostupné z: https://www.ikrypto.cz/kde-vsude-muzeme-platit-bitcoinem/

[50] Investiční web. *Bitcoin byl oficiálně označen za komoditu. Vrátí se jeho dřívější sláva?* [Online] Publikováno 21. 09. 2015 [cit. 31. 1. 2023]. Dotupné z: https://www.investicniweb.cz/ekonomika-politika/bitcoin-byl-oficialne-oznacen-za-komoditu-vrati-se-jeho-drivejsi-slava

[51] ITBIZ. *Komodita.* [Online] Publikováno 13. 09. 2011 [cit. 31. 1. 2023]. Dostupné z: https://www.itbiz.cz/slovnik/ekonomie/komodita

[52] Kriptomat. *Jak investovat do kryptoměn pro dlouhodobý zisk.* [Online] Publikováno © 2023 [cit. 31. 1. 2023]. Dostupné z: https://kriptomat.io/cs/kryptomeny/jak-investovat-do-kryptomen/

[53] Krypto-world.info. *Hašovací funkce, principy, příklady a kolize.* [Online] Publikováno 19. 03. 2005 [cit. 31. 1. 2023]. Dostupné z: http://crypto-world.info/klima/2005/cryptofest_2005.htm

[54] Kurzy.cz. *Bitcoinmaty, bitcoin bankomaty v ČR.* [Online] © 2000 – 2022. [cit. 31. 1. 2023]. Dostupné z: https://www.kurzy.cz/bitcoinmaty/

[55] Kurzy.cz. *V Jižní Koreji začala platit nová pravidla pro obchodování s kryptoměnami. Už žádné anonymní účty.* [Online] Publikováno 31. 1. 2018. [cit. 31. 1. 2023]. Dostupné z: https://www.kurzy.cz/zpravy/444605-v-jizni-koreji-zacala-platit-nova-pravidla-pro-obchodovani-s-kryptomenami-uz-zadne-anonymni-ucty/

[56] LUPA.CZ. *Proč Čína najednou propadla blockchainu a co si od něj slibuje?* [Online] Publikováno 7. 11. 2019. [cit. 31. 1. 2023]. Dostupné z: https://www.lupa.cz/clanky/proc-cina-najednou-propadla-blockchainu-a-co-si-od-nej-slibuje/

[57] Medium. *Tokeny s odkazem na aktiva podle nařízení EU o navrhovaných trzích v oblasti kryptografických aktiv.* [online]. Publikováno 10. 2. 2022. [cit. 31. 1. 2023]. Dostupné z: https://medium.com/coinmonks/asset-referenced-tokens-under-the-eus-proposed-markets-in-crypto-assets-regulation-458c317577bb

[58] Měšec.cz. *Jak se daní virtuální měny? Část zisku odvedete vždy, bitcoin je pro berňák věc.* [Online] Publikováno 12. 12. 2017 [cit. 31. 1. 2023]. Dostupné z: https://www.mesec.cz/clanky/jak-se-dani-virtualni-meny-cast-zisku-odvedete-vzdy-bitcoin-je-pro-bernak-vec/

[59] Měšec.cz. *V obchodech už zaplatíte kryptoměnou. V Česku jsou jich zatím necelé 4 tisíce.* [Online] Publikováno 23. 10. 2021 [cit. 31. 1. 2023]. Dostupné z: https://www.mesec.cz/clanky/v-obchodech-uz-zaplatite-kryptomenou-v-cesku-je-jich-zatim-necelych-4-tisice/

[60] Ministerstvo financí České republiky. *Veřejná konzultace - Blockchain, virtuální měny a aktiva.* [Online] Publikováno 30. 11. 2018. Aktualizováno 3. 1. 2019. [cit. 31. 1. 2023]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/kapitalovy-trh/cenne-papiry/2018/verejna-konzultace-blockchain-virtualni-33613

[61] Novinky.cz. *Salvador by neměl používat bitcoin jako zákonné platidlo, burcoval MMF.* [Online] Publikováno 25. 11. 2021 [cit. 31. 1. 2023]. Dostupné z: https://www.novinky.cz/internet-a-pc/clanek/salvador-by-nemel-pouzivat-bitcoin-jako-zakonne-platidlo-burcoval-mmf-40379097

[62] Peníze.cz. *Vydělali jste na bitcoinu? Před daní Vás nezachrání ani čas.* [Online] Publikováno 3. 02. 2022 [cit. 31. 1. 2023]. Dostupné z: https://www.penize.cz/dan-z-prijmu-fyzickych-osob/430777-bitcoin-a-dane-zisk-z-prodeje-kryptomen-a-danove-priznani

[63] SeznamZprávy. *Čína postavila kryptoměny mimo zákon. Bitcoin padá.* [Online] Publikováno 24. 9. 2021. [cit. 31. 1. 2023]. Dostupné z: https://www.seznamzpravy.cz/clanek/cina-postavila-kryptomeny-mimo-zakon-cena-bitcoinu-pada-175393

[64] SeznamZprávy. *Hrozba pro bitcoin zažehnána. Europoslanci odmítli kritizovanou regulaci.* [online]. Publikováno 14. 3. 2022. [cit. 31. 1. 2023]. Dostupné z: https://www.seznamzpravy.cz/clanek/ekonomika-osud-kryptomen-je-v-rukach-europoslancu-hlasuji-o-vyrazne-regulaci-193482

[65] Tradearena.cz. *Co je digitální měna, kryptoměna nebo token*. [Online] Publikováno 29. 7. 2019 [cit. 31. 1. 2023]. Dostupné z: https://www.tradearena.cz/rubriky/aktuality/co-je-digitalni-mena-kryptomena-nebo-token_806.html

[66] Zítřek. *Boom kryptoměn pokračuje. Vlastní digitální měnu chystá PayPal i Walmart, Čína testuje digitální jüan.* [Online] Publikováno 7. 2. 2022. [cit. 31. 1. 2023]. Dostupné z: https://zitrek.cz/spolecnost/byznys/boom-kryptomen-pokracuje-vlastni-digitalni-menu-chysta-paypal-i-walmart-cina-testuje-digitalni-juan/

9.5.2 CIZOJAZYČNÉ

[67] Cambridge Dictonary. *Commodity*. [Online] Publikováno 2019 [cit. 31. 1. 2023]. Dostupné z: https://dictionary.cambridge.org/dictionary/english/commodity

[68] CCN. *And Satoshi's True Identity is…* [Online] Publikováno 14. 09. 2019 [cit. 31. 1. 2023]. Dostupné z: https://www.ccn.com/and-satoshis-true-identity-is/

[69] CCN. *Bitcoin Creator Satoshi is 'Already Dead', Claims BitMEX CEO.* [Online] Publikováno 23. 09. 2019 [cit. 31. 1. 2023]. Dostupné z: https://www.ccn.com/bitcoin-creator-satoshi-dead/

[70] CCN. *Satoshi Nakamoto Not Eligible For Nobel Prize.* [Online] Publikováno 17. 11. 2015 [cit. 31. 1. 2023]. Dostupné z: https://www.ccn.com/satoshi-nakamoto-not-eligible-nobel-prize//

[71] CCN. *UCLA Finance Professor Nominates Satoshi Nakamoto For Nobel Prize.* [Online] Publikováno 09. 11. 2015 [cit. 31. 1. 2023]. Dostupné z: https://www.ccn.com/ucla-finance-professor-nominates-satoshi-nakamoto-nobel-prize/

[72] CoinMarketCap. *Today´s Cryptocurrency Prices by Market Cap.* [Online] Publikováno © 2022 [cit. 31. 1. 2023]. Dostupné z: https://coinmarketcap.com/

[73] Deloitte. *Digital Finance: European Parliament adopts MiCA Regulation, paving the way for an innovation-friendly crypto regulation.* [online]. Publikováno 17. 3. 2022. [cit. 31. 1. 2023]. Dostupné z: https://www2.deloitte.com/lu/en/pages/financial-services/articles/digital-finance-european-parliament-adopts-mica-regulation-innovation-friendly-crypto-regulation.html

[74] Dictonary.com. *Commodity*. [Online] Publikováno 2019 [cit. 31. 1. 2023]. Dostupné z: https://www.dictionary.com/browse/commodity

[75] EUR-Lex. *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937.* [online]. Publikováno 24. 9. 2020. [cit. 31. 1. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0593

[76] European Commission. *Digital Finance Package.* [online]. Publikováno 24. 9. 2020. [cit. 31. 1. 2023]. Dostupné z: https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

[77] European Commission. *Digital Finance Package: Commission sets out new, ambitious approach to encourage responsible annovation to benefit consumers and businesses.* [online]. Publikováno 24. 9. 2020. [cit. 31. 1. 2023]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684

[78] European Commission. *EU taxonomy for sustainable activities.* [online]. Publikováno 12. 6. 2020. [cit. 31. 1. 2023]. Dostupné z: https://ec.europa.eu/info/business-economy-euro/banking-and-finance/sustainable-finance/eu-taxonomy-sustainable-activities_en

[79] Exploding topics. *How Many Cryptocurrencies are There In 2022?* [Online] Publikováno 25. 3. 2022 [cit. 31. 1. 2023]. Dostupné z: https://explodingtopics.com/blog/number-of-cryptocurrencies

[80] Exploding topics. *How Many Cryptocurrencies are There In 2023?* [Online] Publikováno 25. 11. 2022 [cit. 31. 1. 2023]. Dostupné z: https://explodingtopics.com/blog/number-of-cryptocurrencies

[81] Japanese Law Translation. *Payment Services Act. Act No. 59 of 2009.* [Online] Publikováno 30. 6. 2017 [cit. 31. 1. 2023]. Dostupné z: http://www.japaneselawtranslation.go.jp/law/detail/?id=3078&vm=04&re=02.

[82] Lexology. A *general introduction to the regulation of virtual currencies in South Korea.* [Online] © 2006-2023. [cit. 31. 1. 2023]. Dostupné z: https://www.lexology.com/library/detail.aspx?g=4ab7e422-8668-4db6-a9fd-6a124fffeb01

[83] Technopedia.com. *Cryptocurrency.* [Online] Publikováno 2019 [cit. 31. 1. 2023]. Dostupné z: https://www.techopedia.com/definition/27531/cryptocurrency

[84] TechTerms. *Cryptography*. [Online] Publikováno 2019 [cit. 31. 1. 2023]. Dostupné z: https://techterms.com/definition/cryptography

https://doi.org/10.5817/RPT2023-1-3

PŘÍSTUP ŠIROKÉ VEŘEJNOSTI K ÚDAJŮM O SKUTEČNÝCH MAJITELÍCH A PRÁVO NA OCHRANU SOUKROMÍ

ADAM JAREŠ[1]

Soud:	Soudní dvůr Evropské unie (velký senát)
Věc:	Spojené věci C 37/20 a C 601/20, Luxembourg Business Registers, ECLI:EU:C:2022:912
Datum:	22. 11. 2022
Dostupnost:	curia.europa.eu

1. ÚVOD

Dne 22. listopadu 2022 vydal Soudní dvůr Evropské unie rozhodnutí o předběžných otázkách, které se týkalo přístupu široké veřejnosti k údajům o skutečných majitelích právnických osob.[2] Při rozhodování SDEU poměřoval konflikt práva na soukromí a práva na ochranu osobních údajů s obecným zájmem na transparentnosti vlastnické struktury s ohledem na boj proti praní špinavých peněz a financování terorismu. V českém právním prostředí jsou požadavky evropské legislativy v této oblasti upravené v zákoně o evidenci skutečných majitelů[3], jehož cílem byla řádná transpozice požadavků týkajících se evidování skutečných majitelů do čes-

[1] JUDr. Adam Jareš, Ph.D., Ústav práva a technologií Právnické fakulty Masarykovy univerzity, kontaktní e-mail: adam.jares@mail.muni.cz.

[2] Rozsudek SDEU (velkého senátu) ze dne 22. listopadu 2022 ve spojených věcech C-37/20 a C-601/20, Luxembourg Business Registers, ECLI:EU:C:2022:912.

[3] Zákon č. 37/2021 Sb., o evidenci skutečných majitelů (dále jen „zák. o ESM“).

kého právního řádu. Na základě tohoto zákona byla zřízena Evidence skutečných majitelů jako informační systémem veřejné správy.[4]

Česká evidence skutečných majitelů je veřejně přístupná každému a je možné z ní čerpat některé osobní údaje skutečných majitelů zapsaných v evidenci.[5] Rozhodnutí může mít do budoucna vliv na další fungování Evidence skutečných majitelů a jejích obdob napříč Evropskou unií, respektive na rozsah přístupu k údajům z evidencí.

2. PRÁVNÍ ZÁKLAD VĚCI

Základ věci spočívá v 5. AML směrnici[6], z jejíchž recitálů vyplývá, že mezi její cíle patří nejen odhalování a vyšetřování praní peněz, ale také prevence jeho vzniku, jelikož posílení transparentnosti by mohlo být významným odstrašujícím momentem.[7] Veřejný přístup k informacím o skutečných majitelích umožňuje mimo jiné, aby tyto informace byly ve větší míře zkoumány občanskou společností, včetně tisku nebo organizací občanské společnosti. Tím může napomoci vyšetřování a přispět k boji proti zneužívání společností a jiných právnických osob k praní peněz a financování terorismu. Zároveň může mít reputační účinky vzhledem k tomu, že každý, kdo s právnickou osobou bude uzavírat transakce, bude znát totožnost jejích skutečných majitelů.[8]

Podle 4. AML směrnice[9] platilo, že členské státy zajistí, aby informace o skutečném vlastnictví byly vždy k dispozici mimo jiné kterékoli osobě nebo organizaci, která může prokázat oprávněný zájem. Přijetím 5. AML

[4] § 11 odst. 1 zák. o ESM.

[5] § 14 odst. 1 zák. o ESM.

[6] Směrnice Evropského parlamentu a rady (EU) 2018/843 ze dne 30. května 2018, kterou se mění směrnice (EU) 2015/849 o předcházení využívání finančního systému k praní peněz nebo financování terorismu a směrnice 2009/138/ES a 2013/36/EU (dále jen „5. AML směrnice“).

[7] Recitál č. 5 5. AML směrnice.

[8] Recitál č. 30 5. AML směrnice.

[9] Směrnice Evropského parlamentu a Rady (EU) 2015/849 ze dne 20. května 2015 o předcházení využívání finančního systému k praní peněz nebo financování terorismu, o změně nařízení Evropského parlamentu a Rady (EU) č. 648/2012 a o zrušení směrnice Evropského parlamentu a Rady 2005/60/ES a směrnice Komise 2006/70/ES (dále jen „4. AML směrnice“).

směrnice došlo k posunu v tom smyslu, že informace o skutečných majitelích mají být vždy k dispozici jakékoli osobě z široké veřejnosti.

5. AML směrnice zároveň stanoví, že za výjimečných okolností stanovených vnitrostátním právem mohou členské státy stanovit na základě individuálního posouzení případu výjimku z takovéhoto přístupu ke všem nebo některým informacím o skutečném majiteli. Výjimku lze stanovit v případě, že by přístup široké veřejnosti vystavil skutečného majitele nepřiměřenému riziku, riziku podvodu, únosu, vydírání, obtěžování, násilí nebo zastrašování nebo pokud je skutečným majitelem nezletilá nebo jinak právně nezpůsobilá osoba, a to na základě podrobného hodnocení výjimečné povahy daných okolností. Rozhodnutí o výjimce musí být přezkoumatelné v rámci správního přezkumu a zároveň musí být zajištěna soudní ochrana.

3. ŘEŠENÉ PŘEDBĚŽNÉ OTÁZKY

V rámci předběžných otázek předložených SDEU šlo právě o tyto výjimky z přístupu široké veřejnosti, a to v případě Lucemburska a jeho Registru skutečných majitelů[10].

Tamní zákon dovoluje registrované právnické osobě nebo skutečnému majiteli požádat za výjimečných okolností, aby byl přístup k informacím o skutečném majiteli omezen pouze na vnitrostátní orgány, úvěrové a finanční instituce a další orgány veřejné moci. A to v případě, že by tento přístup vystavil skutečného majitele nepřiměřenému riziku, riziku podvodu, únosu, vydírání, obtěžování, násilí nebo zastrašování.[11]

Žádosti dvou právnických osob o zamezení přístupu byly zamítnuty. Soud pak v rámci řízení o žalobách proti zamítavým rozhodnutím předložil předběžné otázky Soudnímu dvoru. Ty se týkaly výkladu pojmů „výjimečné okolnosti“, „nepřiměřené riziko“, ale také poměru veřejného přístupu k osobním údajů skutečných majitelů k právu na respektování soukromého

[10] *Registre des bénéficiaires effectifs*. Dostupný z https://www.lbr.lu/.

[11] Bod 19 anotovaného rozhodnutí.

a rodinného života a na ochranu osobních údajů podle Listiny základních práv Evropské unie.[12,13]

4. ÚVAHY SDEU O PRÁVU NA OCHRANU SOUKROMÍ A ZÁJMU NA TRANSPARENTNOSTI VLASTNICKÉ STRUKTURY

Omezení těchto základních práv je možné, nicméně pouze při zohlednění testu proporcionality vyplývajícího z článku 52 Listiny. Ten říká, že každé omezení výkonu práv a svobod uznaných Listinou musí být stanoveno zákonem a respektovat podstatu těchto práv a svobod. A při dodržení zásady proporcionality mohou být omezení zavedena pouze tehdy, pokud jsou nezbytná a skutečně odpovídají cílům obecného zájmu uznávaných Evropskou unií, nebo potřebě ochrany práv a svobod druhého.

SDEU se tak postupně věnoval úvahám ohledně jednotlivých aspektů dostupnosti údajů o skutečném vlastnictví a jejich poměru k právu na soukromí[14] a ochranu osobních údajů[15] a zda zásah do těchto práv prostřednictvím dostupnosti těchto údajů naplňuje požadavky článku 52 Listiny[16].

Nejprve SDEU konstatoval, že omezení je stanoveno zákonem, a tedy vyhovuje zásadě legality.[17]

Dále se SDEU věnoval úvaze, zda zásah do těchto práv respektuje jejich podstatu. Dovodil přitom, že zásah, který s sebou přináší přístup široké veřejnosti k informacím o skutečných majitelích, nenarušuje samotnou podstatu základních práv v článcích 7 a 8 Listiny.[18]

---

[12] Listina základních práv Evropské Unie ze dne 7.6.2016, C 202/389 (dále jen „Listina“).

[13] Body 24 a 33 anotovaného rozhodnutí.

[14] Srov čl. 7 Listiny: *„Každý má právo na respektování svého soukromého a rodinného života, obydlí a komunikace.“*

[15] Srov čl. 8 Listiny: *„1. Každý má právo na ochranu osobních údajů, které se ho týkají. 2. Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.“*

[16] Srov čl. 52 odst. 1 Listiny: *„Každé omezení výkonu práv a svobod uznaných touto listinou musí být stanoveno zákonem a respektovat podstatu těchto práv a svobod. Při dodržení zásady proporcionality mohou být omezení zavedena pouze tehdy, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého.“*

[17] Bod 49 anotovaného rozhodnutí.

[18] Body 52 a 54 anotovaného rozhodnutí.

V dalším kroku SDEU zvažoval, zda k omezení práv dochází z důvodu obecného zájmu uznaného Evropskou unií. Zde uvedl, že stanovením přístupu široké veřejnosti k informacím o skutečných majitelích usiluje unijní normotvůrce o předcházení praní peněz a financování terorismu tím, že prostřednictvím zvýšené transparentnosti vytvoří takové prostředí, které bude méně náchylné ke zneužití k těmto účelům. Tento cíl přitom podle SDEU představuje cíl obecného zájmu, jímž lze odůvodnit i závažné zásahy do základních práv zakotvených v článcích 7 a 8 Listiny.[19]

SDEU v této souvislosti však zároveň upozorňuje na to, že Rada Evropské unie v tomto kontextu výslovně odkazuje na zásadu transparentnosti, která umožňuje občanům blíže se účastnit rozhodovacího procesu a zaručuje, že správní orgány budou mít ve vztahu k občanům v demokratickém systému větší legitimitu, účinnost a odpovědnost.[20] V souvislosti se zásadou transparentnosti SDEU uvádí, že ji podle něj nelze v tomto kontextu jako takovou považovat za cíl obecného zájmu, jímž by bylo možné odůvodnit zásah do základních práv. Přístup k údajům o skutečných majitelích má totiž za cíl zpřístupnit široké veřejnosti údaje týkající se totožnosti soukromých skutečných majitelů, jakož i povahy a rozsahu jejich účasti ve společnostech nebo jiných právnických osobách. Nesměřuje tedy na transparentnost činností veřejnoprávní povahy.[21]

Dále se SDEU věnoval posouzení vhodnosti, nezbytnosti a přiměřenosti zásahu do základních práv garantovaných Listinou. Zde šlo primárně o posouzení přiměřenosti opatření vedoucího k zásahu do práv zaručených v článcích 7 a 8 Listiny, dodržení požadavků vhodnosti a nezbytnosti i požadavku přiměřenosti těchto opatření ve vztahu ke sledovanému cíli.[22]

Nejprve tedy SDEU ověřil, zda přístup široké veřejnosti k informacím o skutečných majitelích je vhodný k dosažení sledovaného cíle obecného zájmu. Zde SDEU konstatoval, že přístup široké veřejnosti k informacím o skutečných majitelích je vhodný k tomu, aby přispěl k dosažení cíle

[19] Body 58 a 59 anotovaného rozhodnutí.

[20] Bod 60 anotovaného rozhodnutí.

[21] Body 61 a 62 anotovaného rozhodnutí.

[22] Body 63 až 66 anotovaného rozhodnutí.

obecného zájmu, kterým je předcházení praní peněz a financování terorismu, a to z důvodu, že veřejná povaha tohoto přístupu a zvýšená transparentnost, jež z něj vyplývá, přispívají k vytvoření prostředí méně náchylného ke zneužití k těmto účelům.[23]

Následně SDEU zvažoval, zda je zásah do práv zaručených v článcích 7 a 8 Listiny omezen na to, co je nezbytně nutné, a to v tom smyslu, zda by tohoto cíle nebylo možné rozumně dosáhnout stejně účinným způsobem jinými prostředky, které méně zasahují do těchto základních práv subjektů údajů. Zde již SDEU dospěl k závěru, že nelze mít za to, že zásah do práv zaručených v článcích 7 a 8 Listiny vyplývající z přístupu široké veřejnosti k informacím o skutečných majitelích, je omezen na to, co je nezbytně nutné.[24] V této souvislosti si SDEU kladl otázku, zda nebylo vhodnější omezit přístup k předmětným údajům kritériem „oprávněného zájmu".[25]

V závěru rozhodnutí se SDEU věnoval úvaze o přiměřenosti dotčeného zásahu, zejména s ohledem na to, zda přístup široké veřejnosti k informacím o skutečných majitelích je založen na vyváženém poměření sledovaného cíle obecného zájmu a dotčených základních práv a zda existují dostatečné záruky proti riziku zneužití.[26]

V této souvislosti SDEU především upozornil, že z 5. AML směrnice vyplývá, že široká veřejnost musí mít povolený přístup alespoň k informacím o jméně, měsíci a roce narození, zemi bydliště a státní příslušnosti skutečného majitele a o povaze a rozsahu účasti skutečného majitele. Členské státy tak mohou za podmínek stanovených vnitrostátním právem zpřístupnit další informace umožňující zjištění totožnosti skutečného majitele. Z použití výrazu „alespoň" přitom vyplývá, že tato ustanovení umožňují zpřístupnit veřejnosti údaje, které nejsou dostatečně vymezené ani identifikovatelné. Hmotněprávní pravidla upravující zásah do práv za-

[23] Bod 67 anotovaného rozhodnutí.

[24] Bod 76 anotovaného rozhodnutí.

[25] Body 68 až 72 anotovaného rozhodnutí.

[26] Bod 77 anotovaného rozhodnutí.

ručených v článcích 7 a 8 Listiny proto podle SDEU nesplňují požadavek jasnosti a přesnosti.[27]

SDEU dále k vyvažování cíle obecného zájmu a zásahu do základních práv dodává, že předcházení praní peněz a financování terorismu je sice cíl obecného zájmu, nicméně ten přísluší přednostně veřejným orgánům a subjektům, jako jsou úvěrové či finanční instituce, kterým jsou v důsledku jejich aktivit ukládány konkrétní povinnosti v dané oblasti.[28]

5. ZÁVĚR SDEU

Závěr SDEU je tedy takový, že je neplatné ustanovení 5. AML směrnice o povinnosti členských států zajistit široké veřejnosti přístup k informacím o skutečných majitelích společností a jiných právnických osob zapsaných v rejstříku. S ohledem na tento závěr se SDEU dalším předběžným otázkám dále nevěnoval.[29]

6. REFLEXE ROZHODNUTÍ

Rozhodnutí mezi protikorupčními nevládními neziskovými organizacemi vyvolalo přinejmenším zklamání a obavy.[30] Vezmeme-li však v úvahu rozhodovací praxi SDEU například v oblasti *data retention*[31] nebo *Privacy Shield*[32] akcentující důležitost vysoké míry ochrany soukromí a osobních údajů, nemusí být rozhodnutí překvapivé.

---

[27] Body 81 a 82 anotovaného rozhodnutí.

[28] Bod 83 anotovaného rozhodnutí.

[29] Body 88 až 91 anotovaného rozhodnutí.

[30] Např. TRANSPARENCY INTERNATIONAL. Why are EU Public Registers Going Offline, and What's Next for Corporate Transparency? In: *transparency.org* [online]. 2022 [cit. 14. 2. 2023]. Dostupné z https://www.transparency.org/en/blog/cjeu-ruling-eu-public-beneficial-ownership-registers-what-next-for-corporate-transparency.

[31] Především rozsudek Soudního dvora (velkého senátu) ze dne 8. dubna 2014 ve spojených věcech C-293/12 a C-594/12, *Digital Rights Ireland*; rozsudek Soudního dvora (velkého senátu) ze dne 21. prosince 2016 ve spojených věcech C-203/15 a C-698/15, *Tele2 Sverige*; či rozsudek Soudního dvora (velkého senátu) ze dne 6. října 2020 ve spojených věcech C-511/18, C-512/18 a C-520/18, *La Quadrature du Net*.

[32] Rozsudek Soudního dvora (velkého senátu) ze dne 6. října 2015 ve věci C-362/14, Schrems; Rozsudek Soudního dvora (velkého senátu) ze dne 16. července 2020 ve věci C-311/18, *Schrems II*.

Role neziskového sektoru při odhalování složitých schémat praní špinavých se však ukazuje jako významná. Pokud by tak do budoucna měl být přístup k údajům o skutečných majitelích pro neziskový sektor omezen či značně ztížen, bude tím do jisté míry popřen i jeden z účelů dostupnosti těchto údajů, kterým je transparentnost vlastnických struktur, prostřednictvím které může docházet k předcházení či odhalování praní peněz.

Rozhodnutí však pravděpodobně neznamená konec přístupu relevantních zástupců občanského sektoru k údajům o skutečném vlastnictví. Z rozhodnutí se jeví, že SDEU by se zřejmě zdálo vhodnější, aby přístup k údajům nebyl poskytnut široké veřejnosti bez dalšího, ale pouze na základě prokázaného oprávněného zájmu. To by mohlo představovat rozumný kompromis a vyvážení zájmu na ochranu soukromí, resp. osobních údajů se zájmem na transparentnosti vlastnických struktur. Tento návrat k úpravě 4. AML směrnice by však nesměl znamenat, že bude docházet k obstrukcím při přístupu k relevantním údajům.

K posunu od přístupu k údajům na základě oprávněného zájmu dle 4. AML směrnice k neomezenému přístupu široké veřejnosti podle 5. AML směrnice Evropská komise v řízení argumentovala tím, že by bylo obtížné právě definovat kritérium „oprávněného zájmu“. Ačkoliv Evropská komise zvažovala možnost navrhnout jednotnou definici tohoto kritéria, nakonec tak neučinila z důvodu, že toto kritérium by bylo obtížně proveditelné a jeho použití by mohlo vést ke svévolným rozhodnutím.[33] SDEU však tento argument nepřijal s tím, že případná obtížnost přesného nastavení případů a podmínek, za nichž může mít veřejnost přístup k informacím o skutečných majitelích, nemůže ospravedlnit přístup široké veřejnosti k těmto informacím.[34] V této souvislosti zároveň SDEU ale uvedl, že jak tisk, tak organizace občanské společnosti, které mají spojitost s prevencí a bojem proti praní peněz a financování terorismu, mají na přístupu k informacím o skutečných majitelích oprávněný zájem.[35]

[33] Bod 71 anotovaného rozhodnutí.

[34] Bod 72 anotovaného rozhodnutí.

[35] Bod 74 anotovaného rozhodnutí.

Ve věci dalšího vývoje v této oblasti však bude zřejmě nutné vyčkat schválení další AML směrnice, která by měla mimo jiné reagovat i na anotované rozhodnutí. Napříč členskými státy je přístup různý. Svůj registr skutečných vlastníků veřejnosti znepřístupnilo v reakci na anotované rozhodnutí například Irsko[36], Rakousko[37], Kypr[38]. V České republice jsou na základě zák. o ESM dostupné komukoliv údaje o skutečném majiteli právnické osoby v rozsahu jména, státu bydliště, roku a měsíce narození, státního občanství a údaje související s postavením skutečného majitele či s jeho majetkovou účastí.[39] V okamžiku dokončení tohoto textu se nejeví, že tento přístup k údajům by v České republice měl být nějakým způsobem omezen. Pro odhalování složitých schémat praní špinavých peněz je však nutné, aby nebyla přístupná jen česká Evidence skutečných majitelů, ale aby byl možný jednoduchý přístup do obdobných evidencí v ostatních členských státech, v ideálním případě aby vznikla propojená evidence napříč Evropskou unií.

[36] Viz *Central Register of Beneficial Ownership of Companies and Industrial and Provident Societies* dostupný z https://rbo.gov.ie.

[37] FINANZMINISTERIUM. Information on the implications of the judgment of the Court of Justice of the European Union in joined cases C-37/20 and C-601/20 of November 22, 2022. In: *bmf.gv.at* [online] 2022 [cit. 14. 2. 2023]. Dostupné z https://www.bmf.gv.at/en/topics/financial-sector/beneficial-owners-register-act/Public-access.html.

[38] THE DEPARTMENT OF REGISTRAR OF COMPANIES AND INTELLECTUAL PROPERTY. Suspension of access to the Beneficial Owners register for the general public. In: *companies.gov.cy* [online] 2022 [cit. 14. 2. 2023]. Dostupné z https://www.companies.gov.cy/en/knowledgebase/news/suspension-of-access-to-the-beneficial-owners-register-for-the-general-public.

[39] Srov. § 13 a 14 zák. o ESM.

https://doi.org/10.5817/RPT2023-1-4

PŘEHLED AKTUÁLNÍ JUDIKATURY I/2023

ANNA BLECHOVÁ, MARTIN ERLEBACH, ŠIMON CHVOJKA, VOJTĚCH JUŘIČKA, ANEŽKA KARPJÁKOVÁ, FRANTIŠEK KASL, ANDREJ KRIŠTOFÍK, PAVEL LOUTOCKÝ, JAKUB MÍŠEK, TEREZA NOVOTNÁ, SOFIE PETROVÁ, JAN SVOBODA, ZUZANA VLACHOVÁ, JAKUB VOSTOUPAL, ONDŘEJ WOZNICA, VERONIKA PŘÍBAŇ ŽOLNERČÍKOVÁ

1. PRÁVO DUŠEVNÍHO VLASTNICTVÍ A AUTORSKÉ PRÁVO

LOUBOUTIN VS AMAZON: PŘÍMÁ ODPOVĚDNOST A PORUŠENÍ OCHRANNÉ ZNÁMKY

Soud: Soudní dvůr Evropské unie
Věc: C-148/21 a C-184/21
Datum: 22. 6. 2022
Dostupnost: curia.europa.eu

Christian Louboutin je návrhář obuvi, jehož nejznámější výrobek jsou dámské boty na vysokém podpatku s vnějším podešvem červené barvy odpovídající kódu 18-1663TP vzorníku Pantone.[1] Tato barva je zapsána jako ochranná známka v Beneluxu a ochranná známka Evropské unie.[2] Společnost Amazon provozuje internetový portál, kde dochází k prodeji jak jejich vlastních výrobků, tak výrobků třetích stran. Oba druhy produktů na svých stránkách společnost inzeruje. Zasílání výrobků třetích stran je zajiš-

[1] Bod 6 anotovaného rozhodnutí.

[2] Bod 7 anotovaného rozhodnutí.

ťováno buď samotnými stranami nebo za součinnosti společnosti Amazon. Společnost Amazon výrobky skladuje ve svých skladech a výrobky odesílá zákazníkům.[3]

Spor, který byl ve spojených věcech C-148/21 a C-184/21 řešen a předložen Soudnímu dvoru jako předběžná otázka, byl založen na interpretaci čl. 9 odst. 2 nařízení o ochranné známce EU 2017/1001. Konkrétně se dotčené soudy ptaly na to, za jakých podmínek může být provozovatel internetového tržiště shledán přímo odpovědným podle daného článku za zobrazení reklamy a dodání zboží porušujícího práva, které je nabízeno k prodeji a uváděno na trh z podnětu a pod kontrolou prodejců, kteří jsou třetími osobami a využívají služeb tohoto provozovatele.[4] Jinými slovy, předběžné otázky mířily na zjištění podmínek pro uplatnění oprávnění majitelů ochranných známek EU k tomu, aby zabránili třetím osobám v užívání jakéhokoli označení, které je shodné nebo podobné jejich ochranné známce, ve vztahu k výrobkům nebo službám, které jsou shodné, podobné nebo nepodobné (s některými dalšími požadavky) těm, pro které je ochranná známka EU zapsána.

Dle čl. 9 odst. 2 nařízení o ochranné známce EU 2017/1001 vyplývá ze zápisu ochranné známky EU pro jejího vlastníka právo bránit ochranou známku před neoprávněným užitím třetími stranami.

Soudní dvůr se v tomto kontextu zaměřil především na výklad slova užití, kde upřesnil, že se jedná o aktivní jednání s přímou či nepřímou kontrolou nad aktem představujícím užívání.[5] Dále se soud zabýval problematikou spojitosti mezi poskytovatelem služby (online tržiště) a produktu jeho zákazníků. Soudní dvůr konstatoval, že taková spojitost *„existuje, pokud provozovatel on-line tržiště prostřednictvím služby optimalizace pro vyhledávače na internetu a prostřednictvím klíčového slova totožného s ochrannou známkou jiné osoby propaguje výrobky této značky prodávané jeho zákazníky na jeho on-line tržišti. Taková reklama totiž vytváří pro uživatele internetu, kteří provádějí vyhledávání na základě tohoto klíčového slova, zjevnou asociaci mezi těmito vý-*

[3] Body 8 a 9 anotovaného rozhodnutí.

[4] Body 17 a 21 anotovaného rozhodnutí.

[5] Bod 27 anotovaného rozhodnutí.

robky označenými ochrannou známkou a možností jejich nákupu prostřednictvím uvedeného tržiště.“[6] Tento jev pak vede k tomu, že přiměřeně pozorný uživatel nemá šanci zjistit, zdali se jedná o produkt vlastníka ochranné známky, či nikoli.

Soudní dvůr ve svém rozhodnutí došel k závěru, že provozovatel online tržiště by mohl být přímo odpovědný ve smyslu čl. 9 odst. 2 nařízení o ochranné známce EU 2017/1001 na základě jednotného způsobu prezentace svých výrobků a výrobků třetích stran.[7] Toto rozhodnutí může být tak vnímáno jako silný nástroj pro vymáhání porušení práv k ochranným známkám. Zároveň je pak zajímavé zmínit, že tento výklad daného ustanovení je vybočením z dosavadní judikatury týkající se problematiky bezpečného přístavu a rozhodnutí je kontradiktorní k závěrům Stanoviska generálního advokáta Szpunara[8] i závěrům odborné veřejnosti[9].

Autorka: AB

SDĚLOVÁNÍ DÍLA VEŘEJNOSTI V DOPRAVNÍCH PROSTŘEDCÍCH A INSTALACE ZVUKOVÝCH ZAŘÍZENÍ

Soud: Soudní dvůr Evropské unie
Věc: C-775/21 a C-826/21
Datum: 20. 4. 2023
Dostupnost: curia.europa.eu

Rumunští kolektivní správci se rozhodli vymáhat licenční poplatky za sdělování děl na palubě různých dopravních prostředků.[10] Iniciovali proto před

[6] Bod 44 anotovaného rozhodnutí.

[7] Bod 51 anotovaného rozhodnutí.

[8] Bod 101, Stanovisko generálního advokáta M. Szpunara ze dne 2. června 2022 k spojené věci C-148/21 a C-184-21.

[9] Viz ROSASTI, Eleonora, The Louboutin/Amazon cases (C-148/21 and C-184/21) and Primary Liability Under EU Trade Mark Law (April 8, 2022). (2022) 44(7) European Intellectual Property Review, str. 435-440, Dostupné z: https://ssrn.com/abstract=4078987.

[10] Body 28 a 36 anotovaného rozhodnutí.

rumunskými soudy řízení o platbě licenčních poplatků za hudební nahrávky na palubě letadel a následně také vlaků.[11] Soudní dvůr řízení spojil.

Položené předběžné otázky lze rozdělit do tří skupin. V prvním řízení byla položena otázka, zda šíření hudebních nahrávek během letu je sdělováním díla veřejnosti.[12] V obou řízeních pak byly položeny otázky, zda lze z pouhé přítomnosti zvukových zařízení na palubě také dovodit sdělování díla veřejnosti.[13] Závěrem v druhém řízení také padla otázka, zda lze ve vnitrostátní úpravě zavést vyvratitelnou domněnku, že existence zvukového systému na palubě představuje sdělování díla veřejnosti.[14]

K první předběžné otázce, teda zda šíření během letu je sdělováním díla veřejnosti, Soudní dvůr konstatoval, že šíření hudebních nahrávek jako hudební kulisy v dopravních prostředcích skutečně sdělováním díla veřejnosti je.[15] K druhé skupině předběžných otázek Soudní dvůr dovodil, že pouhá instalace zvukového zařízení na palubě dopravního prostředku nemůže být současně vědomým zprostředkováním chráněných děl zákazníkům, tedy sdělováním díla veřejnosti.[16] K poslední otázce, tedy zda lze stanovit vyvratitelnou domněnku ve vnitrostátním právu Soudní dvůr dovodil, že taková vyvratitelná domněnka by rozšířila obsah pojmu sdělování veřejnosti dle InfoSoc směrnice[17], a tedy není slučitelná s evropským právem.[18]

Rozhodnutí Soudního dvora se, stejně jako dřívější řízení zaměřená na otázky sdělování díla veřejnosti, soustředí na recitál 27 InfoSoc směrnice. V tomto případě však Soudní dvůr pouze z recitálu 27 dovodil, že ke sdělování díla nedochází.[19] V tom se odlišuje od jiných řízení, ve kterých navíc extenzivně posuzoval, zda instalace zařízení je také zprostředkováním pří-

[11] Body 28 a 35 anotovaného rozhodnutí.

[12] Bod 34 anotovaného rozhodnutí.

[13] Body 34 a 40 anotovaného rozhodnutí.

[14] Bod 40 anotovaného rozhodnutí.

[15] Bod 57 anotovaného rozhodnutí.

[16] Bod 71 anotovaného rozhodnutí.

[17] 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

[18] Body 80 a 83 anotovaného rozhodnutí.

[19] Body 67 a 68.

stupu ke chráněným dílům, přičemž následně i z pouhé instalace zařízení dovodil sdělování díla veřejnosti.[20]

Autor: OW

REŽIM SPOLUVLASTNICTVÍ OCHRANNÝCH ZNÁMEK

Soud: Soudní dvůr Evropské unie
Věc: C-686/21
Datum: 27. 4. 2023
Dostupnost: curia.europa.eu

LEGEA je národní ochrannou známkou a ochrannou známkou Evropské unie, která je v podílovém spoluvlastnictví čtyř osob disponujících rovnými podíly.[21] V roce 1993 tito spoluvlastníci poskytli k užívání ochranných známek výlučnou licenci na dobu neurčitou společnosti Legea.[22] V roce 2006 jeden z nich projevil nesouhlas s trváním této licenční smlouvy.[23]

V roce 2009 byly podány vzájemné žaloby společností Legea a jediným spoluvlastníkem ochranných známek usilujícím o ukončení licenční smlouvy, v nichž se spoluvlastník domáhal mimo jiného i určení, že společnost Legea užívá ochranné známky neoprávněně.[24] Soud prvního stupně dospěl k závěru, že společnost opravdu po projevení nesouhlasu dotčeného spoluvlastníka užívá ochranné známky neoprávněně.[25] Odvolací soud se naopak domníval, že vůle tří ze čtyř spoluvlastníků k pokračování licenční smlouvy postačuje.[26]

Nejvyšší soud v Itálii položil Soudnímu dvoru předběžnou otázku, zda k dispozici s výlučným právem vyplývajícím z ochranné známky Evropské

[20] Např. body 42 a 46 rozhodnutí C-306/05 (SGAE).

[21] Bod 15 anotovaného rozhodnutí.

[22] Bod 16 anotovaného rozhodnutí.

[23] Bod 17 anotovaného rozhodnutí.

[24] Bod 18 anotovaného rozhodnutí.

[25] Bod 19 anotovaného rozhodnutí.

[26] Bod 20 anotovaného rozhodnutí.

unie je třeba rozhodnutí „pouhé“ většiny spoluvlastníků, anebo je nutný jednomyslný souhlas všech spoluvlastníků. [27]

Podstatou právního posouzení bylo vyřešení otázky podmínek individuálního výkonu výlučného práva, kterým disponují spolumajitelé ochranné známky společně s ohledem na unijní úpravu. Pokud jde o nařízení o ochranné známce EU, to výslovně uznává spoluvlastnictví ochranné známky EU, ale – stejně jako směrnice – neobsahuje žádná ustanovení upravující podmínky jeho výkonu spoluvlastníky.[28]

Soudní dvůr při posouzení ochranné známky jako předmětu vlastnictví došel k závěru, že vzhledem k tomu, že neexistuje ustanovení unijního práva, které by upravovalo podmínky, za nichž spoluvlastníci ochranné známky přijímají rozhodnutí o poskytnutí nebo ukončení licence k užívání uvedené ochranné známky, jedná se o neharmonizovanou oblast práva, která v důsledku toho spadá do působnosti práva vnitrostátního.[29]

Soudní dvůr tak konstatoval, že režim spoluvlastnictví národní ochranné známky, jakož i ochranné známky Evropské unie spadá do působnosti vnitrostátního práva.[30]

Autorka: SP

[27] Bod 22 anotovaného rozhodnutí.

[28] Bod 36 anotovaného rozhodnutí.

[29] Bod 37 anotovaného rozhodnutí.

[30] Bod 40 anotovaného rozhodnutí.

MEZINÁRODNÍ PŘÍSLUŠNOST PRO ŘÍZENÍ O PORUŠENÍ PRÁV K OCHRANNÉ ZNÁMCE EU

Soud: Soudní dvůr Evropské unie
Věc: C-104/22 (Lännen MCE)
Datum: 27. 4. 2023
Dostupnost: curia.europa.eu

Finská společnost Lännen[31] vlastní ochrannou známku EU „Watermaster". U finského obchodního soudu[32] podala žalobu pro údajné porušení práv k ní ve Finsku. První žalovaná Senwatec[33] užívala placené odkazy v internetovém vyhledávači provozovaném pod finskou národní doménou nejvyšší úrovně.[34] Po zadání výrazu „Watermaster" se jako první výsledek objevila reklama na výrobky společnosti Senwatec.[35] Z reklamy ani z internetových stránek společnosti jednoznačně nevyplývalo, kam výrobky dodává a zda činnost zaměřuje na finský trh.[36] U druhé žalované Berky byl jedním z výsledků vyhledání[37] výrazu „Watermaster" odkaz na Flickr.com (nikoli reklamní odkaz) obsahující fotografie výrobků této společnosti. Ke snímkům byly připojeny meta tagy obsahující klíčová slova, včetně „Watermaster".[38]

Žalované namítaly místní nepříslušnost soudu.[39] Soud přerušil řízení a podal k Soudnímu dvoru tři předběžné otázky[40] k výkladu čl. 125 odst. 5 nařízení 2017/1001,[41] dle kterého lze vést řízení rovněž před soudy členského státu, na jehož území došlo k porušení práv nebo zde porušení

[31] Celým názvem Lännen MCE Oy.

[32] Markkinaoikeus, předkládající soud.

[33] Obě žalované (Berky GmbH a Senwatec GmbH & Co. KG) mají sídlo v Německu.

[34] V tomto případě www.google.fi.

[35] Bod 12 anotovaného rozhodnutí.

[36] Body 13 a 43 anotovaného rozhodnutí.

[37] Opět prostřednictvím vyhledávače www.google.fi.

[38] Body 14 a 15 anotovaného rozhodnutí.

[39] Bod 17 anotovaného rozhodnutí.

[40] Bod 23 anotovaného rozhodnutí.

[41] Nařízení Evropského parlamentu a Rady (EU) 2017/1001 ze dne 14. června 2017 o ochranné známce Evropské unie, dále jen „nařízení 2017/1001".

hrozí.[42] Podstatou bylo, zda, používá-li třetí osoba bez souhlasu označení totožné s ochrannou známkou EU vlastníka v reklamě či nabídkách k prodeji na internetu pro totožné/podobné výrobky, může proti ní vlastník podat žalobu ve státě, kde se nacházejí spotřebitelé/podnikatelé, jimž jsou reklamy či nabídky určeny, i neuvádí-li třetí osoba výslovně, že tam lze její výrobky dodat,[43] a jaké okolnosti zohlednit při posuzování, zda je reklama spotřebitelům/podnikatelům v tomto státě určena.[44]

Odkazuje na předchozí judikaturu Soudní dvůr uvedl, že při posuzování, zda k vytýkanému jednání došlo na území státu soudu, jsou údaje o zeměpisných oblastech, do nichž jsou produkty dodávány, klíčovým kritériem.[45] Nejsou-li uvedeny, je třeba spojitost s daným členským státem prokázat prostřednictvím dalších okolností.[46] Musí se přitom jednat ze strany původce porušení o aktivní jednání.[47] Jako další relevantní okolnosti Soudní dvůr posuzoval výše uvedená jednání žalovaných.[48]

Soudní dvůr uzavřel, že aktivní jednání třetí osoby spočívající v zaplacení provozovateli internetového vyhledávače s národní doménou nejvyšší úrovně jiného členského státu, než kde je usazena, aby se tamní veřejnosti zobrazil odkaz na její internetové stránky a umožnil přístup k její nabídce,

---

[42] Jedná se o alternativní pravidlo soudní příslušnosti k základnímu pravidlu obsaženému v čl. 125 odst. 1 nařízení, viz bod 31 anotovaného rozhodnutí a rozsudek ze dne 5. září 2019, AMS Neve Ltd a další, C-172/18, bod 41.

[43] Bod 24 anotovaného rozhodnutí.

[44] Bod 34 anotovaného rozhodnutí.

[45] Bod 42 anotovaného rozhodnutí, Soudní dvůr k tomu odkazuje na rozsudek ze dne 12. července 2011, L'Oréal a další, C-239/09, bod 65.

[46] Body 43–44 anotovaného rozhodnutí. Soudní dvůr odkázal především na rozsudek ze dne 7. prosince 2010, Pammer a Hotel Alpenhof, C-585/08 a C-144/09, bod 93, kde byl [byť při výkladu nařízení Evropského parlamentu a Rady (EU) č. 1215/2012 ze dne 12. prosince 2012 o příslušnosti a uznávání a výkonu soudních rozhodnutí v občanských a obchodních věcech, dále jen „nařízení Brusel I bis“] vymezen demonstrativní výčet indicií nasvědčujících, že činnost podnikatele se zaměřuje na členský stát, v němž má spotřebitel bydliště; k tomu viz bod 46 anotovaného rozhodnutí. Soudní dvůr zdůraznil, že byť jsou pravidla obsažená v nařízení 2017/1001 *lex specialis* k nařízení Brusel I bis (bod 25 anotovaného rozhodnutí), obě nařízení užívají obdobné pojmy. Při výkladu nařízení 2017/1001 je tudíž relevantní též nařízení Brusel I bis (bod 45 anotovaného rozhodnutí).

[47] Bod 40 anotovaného rozhodnutí a rozsudek ze dne 5. září 2019, AMS Neve Ltd a další, C-172/18, bod 44 a tam citovaná judikatura.

[48] Bod 47 anotovaného rozhodnutí.

je dostatečným spojením s tímto státem pro účely čl. 125 odst. 5 nařízení 2017/1001.[49] Naopak použití dotčeného výrazu jako meta tagu u snímků na serveru pro sdílení fotografií online s generickou doménou nejvyšší úrovně, na nějž směřoval pouze přirozený odkaz, bez dalšího nepostačuje.[50]

Autorka: ZV

2. SOUKROMÍ A OSOBNÍ ÚDAJE

DATA Z REGISTRU SKUTEČNÝCH MAJITELŮ

Soud:	Soudní dvůr Evropské unie
Věc:	C-37/20 a C-601/20 (Luxembourg Business Registers)
Datum:	22. 11. 2022
Dostupnost:	curia.europa.eu

Soudní dvůr rozhodoval o spojených věcech, jejichž společným jmenovatelem bylo povinné zveřejňování informací o skutečných majitelích dotčených společností ve smyslu čl. 30 pozměněné směrnice č. 2015/849. Společnosti tvrdily, že hromadným zpřístupněním těchto údajů vzniká riziko pro dotčené fyzické osoby a způsobuje tak zásah do jejich práva na ochranu osobních údajů ve smyslu čl. 8 Listiny základních práv EU.

Směrnice č. 2015/849 byla změněna směrnicí č. 2018/843, aby byla zajištěna vyšší transparentnost údajů o skutečných majitelích a tím i docházelo k předcházení korupčního a dalšího trestného jednání. Klíčovým byl čl. 30 odst. 5, který v původní verzi dával členským státům povinnost zajistit přístup k údajům z registrů krom OČTŘ a osobám provádějícím hloubkovou kontrolu též „*kterékoli osobě nebo organizaci, která může prokázat oprávněný zájem*“. Upravená verze však poslední možnost rozšířila na poskytování „*jakékoli osobě z široké veřejnosti*“.

Národní soud položil Soudnímu dvoru sérii otázek směřujících k interpretačnímu vyjasnění ustanovení čl. 30 pozměněné směrnice č. 2015/849 zejména ve vztahu k ustanovením nařízení č. 2016/679 (GDPR)

[49] Body 49, 50 a 54 anotovaného rozhodnutí.

[50] Body 51, 52 a 54 anotovaného rozhodnutí.

a k možnosti výjimek z povinného zveřejňování údajů. Soudní dvůr odpovídal na první otázku ve věci C-601/20, která spočívala v tom, zda je čl. 30 odst. 5 směrnice 2015/849 po novele v souladu s požadavky čl. 7 a 8 Listiny základních práv EU.

V rámci posouzení otázky Soudní dvůr nejprve připomíná, že zpřístupnění osobních údajů třetím stranám představuje zásah do základních práv zakotvených v čl. 7 a 8 Listiny.[51] Zpřístupnění údajů online komukoli pak činí tento zásah intenzivnější.[52] Soudní dvůr následně provádí komplexní zhodnocení předmětné úpravy. Nejprve konstatuje, že je dodržena zásada legality[53] a není narušena podstata základních práv garantovaných čl. 7 a 8 Listiny.[54] Soudní dvůr identifikoval jako cíl hodnocené úpravy předcházení praní peněz a financování terorismu takovým způsobem, že „*prostřednictvím zvýšené transparentnosti [úprava] vytvoří takové prostředí, které bude méně náchylné ke zneužití k těmto účelům*“.[55] Soudní dvůr pak provádí klasický třístupňový test proporcionality, při kterém několikrát opakuje legitimitu a důležitost tohoto regulatorního cíle. Nejprve dochází k závěru, že hodnocená úprava je vhodná, tedy umožňuje dosáhnout předpokládaného cíle.[56] V kontextu hodnocení potřebnosti Komise argumentovala tím, že ke změně došlo protože bylo nesnadné zajistit jednotnou a dostatečně širokou interpretaci pojmu „oprávněný zájem“, což vedlo k obavě o snížení účinnosti regulace v různých členských státech.[57] Soudní dvůr nicméně tento argument nepřijal a uvedl, že překládané řešení není z hlediska jeho zásahu nezbytně nutné k dosažení předpokládaného cíle.[58] Konečně v rámci samotného poměřování Soudní dvůr dochází k závěru, že

[51] Bod 39 anotovaného rozhodnutí.

[52] Body 42-43 anotovaného rozhodnutí.

[53] Bod 48 anotovaného rozhodnutí.

[54] Bod 54 anotovaného rozhodnutí.

[55] Bod 58 anotovaného rozhodnutí.

[56] Bod 67 anotovaného rozhodnutí.

[57] Bod 68 anotovaného rozhodnutí.

[58] Bod 76 anotovaného rozhodnutí.

hodnocené řešení nenabízí dostatečné záruky účinné ochrany základních práv a nepřiměřeně do nich zasahuje.[59]

Soudní dvůr v návaznosti na uvedenou argumentaci svým výrokem zneplatnil ustanovení směrnice 2018/843, kterým došlo k novele čl. 30 odst. 5 směrnice 2015/849. Bezprostředním důsledkem je zřejmě protiprávnost takové národní úpravy, která toto ustanovení prováděla do národních právních řádů. Do budoucna je anotované rozhodnutí zajímavé z hlediska legálnosti poskytování osobních údajů v kvalitě otevřených dat, kdy Soudní dvůr dále stanoví limity možné praxe.

Autor: JM

OCHRANA OSOBNÍCH ÚDAJŮ VE VEŘEJNÝCH REJSTŘÍCÍCH

Soud: Soudní dvůr Evropské unie
Věc: C-37/20 a C-601/20
Datum: 22. 11. 2022
Dostupnost: curia.europa.eu

Jedná sa o spojenú vec dvoch luxemburských spoločností, ktoré sa domáhali obmedzenia verejnosti informácií obsiahnutých vo verejnom registri skutočných majiteľov, výhradne na štátne orgány a nie širokú verejnosť.[60] V oboch prípadoch vrcholný luxemburský súd podal predbežnú otázku. Nakoľko predbežné otázky smerovali k rovnakej podstate, i keď z rozdielnej argumentácie, jednanie o predbežnej otázke bolo Súdnym dvorom spojené.

V prvom prípade, kedy sa skutočný majiteľ spoločnosti odvolával najmä na skutočnosť, že široké uverejnenie informácií o skutočnom majiteľovi[61] predstavuj skutočnú a aktuálnu hrozbu rizika, že skutočný majiteľ a jeho rodina budú vystavený možnému podvodu, únosu, vydieraniu, obťažovaniu a ďalším rizikám[62], mimo iné aj preto, že v rámci svojho postavenia často

[59] Bod 86 anotovaného rozhodnutí.

[60] Bod 27 Rozhodnutia.

[61] K ich rozsahu viz bod 16 Rozhodnutia.

[62] Bod 20 Rozhodnutia.

cestuje do zemí s nestabilným režimom a vysokou kriminalitou.[63] V tejto veci predkladá súd otázku ako si má vykladať pojmy „*neprimerané riziko*“, „*výnimočné okolnosti*“ a „*riziko*“, najmä potom vo svetle čl. 30 odst. 9 pozmenenej Smernice 2015/849.[64]

Obdobného obmedzenia sa domáha aj skutočný majiteľ spoločnosti v druhom prípade, ktorý má zato, že takto široké, resp. verejné sprístupnenie jeho údajov je v rozpore s jeho základným právom na ochranu súkromia a rodinného života (čl. 7) a právom na ochranu osobných údajov (čl. 8), a tiež má zato že sa jedná o porušenie niektorých základných zásad GDPR podľa jeho článku 5.[65] To mimo iné aj z dôvodu, že účelom predmetného registru má byť ochrana pred legalizáciou výnosov z trestnej činnosti, pričom má sťažovateľ za to, že táto úloha nie je plnené verejnosťou, ktorej sú údaje sprístupňované. Predbežná otázka teda smeruje k výkladu práva na súkromie a rodinný život v kontexte smernice 2018/843 a jej cieľa predchádzania legalizácie výnosov, a zároveň či čl. 5 GDPR nebráni širokému zverejňovaniu údajov bez možnosti získavania niektorých údajov, ako napríklad záujem, od žiadateľov.

V odpovedi na tieto otázky Súdny dvor najprv zdôrazňuje, že už samotné sprístupnenie údajov, bez ohľadu na ich využitie, je zásahom do práv podľa čl. 7 a 8[66] a teda sprístupnenie podľa predmetnej smernice je zásahom do týchto práv.[67] Ďalej tento zásah považuje za závažný, práve z dôvodu, že sú údaje sprístupňované všetkým bez ohľadu na ich cieľ, ktorý nemusí sledovať pôvodný dôvod ich zverejnenia.[68] Súdny dvor následne pristupuje k testu proporcionality, nakoľko sa nejedná o absolútne práva.[69] V rámci toho upozorňuje súd na legálnosť zverejňovania a vo vzťahu k čl. 7 a 8 nezhladáva porušenie, nakoľko údaje s ktorými sa narába sú bezpro-

[63] Bod 21 Rozhodnutia.

[64] Bod 23 a 24 Rozhodnutia.

[65] Bod 29 a 30 Rozhodnutia.

[66] Bod 39 Rozhodnutia.

[67] Bod 40 a 41 Rozhodnutia.

[68] Bod 42 a 44 Rozhodnutia.

[69] Bod 46 a násl.

stredne potrebné k naplneniu účelu zákona.[70] Podľa Súdneho dvora tiež k tomuto narábaniu dochádza podľa pravidiel stanovených GDPR.[71] Súdny dvor dochádza prostredníctvom teleologického výkladu k záveru, že obecné sprístupnenie údajov je vhodným postupom, nakoľko cieľom smernice je vytvorenie transparentného prostredia a budovanie dôvery vo finančné trhy, čo sú ciele plnené obecný zverejnením.[72] Ako posledné, Súdny dvor poukazuje na možnosť obmedzenia prístupu prostredníctvom registrácie[73] alebo stanovenia výnimiek pre „výnimočné okolnosti", ktorých definícia tvorí jednu z otázok, u čoho Súdny dvor poznamenáva, že sa jedná o otázku pre národného zákonodarcu.[74]

Autor: AK

PRÁVO NA INFORMACE O PŘÍJEMCÍCH OSOBNÍCH ÚDAJŮ ČI TOLIKO KATEGORIÍCH PŘÍJEMCŮ?

Soud: Soudní dvůr Evropské unie
Věc: C-154/21
Datum: 12. 1. 2023
Dostupnost: curia.europa.eu
Souvislost s: C-487/2021

Původní spor začal v roce 2019, když se RW obrátil na Österreichische Post (dále jen jako „žalovaná") s žádostí dle čl. 15 GDPR o přístup ke zpracovávaným osobním údajům a, v případě sdělení těchto údajů třetím osobám, také k totožnosti příjemců těchto údajů.[75] Žalovaná odpověděla v omezeném rozsahu s odkazem na internetové stránky, totožnost konkrétních příjemců dat však nevydala.[76]

[70] Bod 52 Rozhodnutia.
[71] Bod 53 Rozhodnutia.
[72] Bod 58 a 67 Rozhodnutia.
[73] Bod 80 Rozhodnutia.
[74] Bod 86 a násl. Rozhodnutia.
[75] Bod 17 anotovaného rozhodnutí.
[76] Bod 18 anotovaného rozhodnutí.

RW v reakci podal žalobu k rakouským soudům, aby byla žalovaná povinována vydat totožnost příjemců zpřístupněných osobních údajů. Žalovaná v průběhu řízení RW informovala o kategoriích příjemců osobních údajů, kvůli čemuž soudy první a druhé instance žalobu zamítly. RW se tak obrátil na rakouský Nejvyšší soud, který řízení přerušil a položil Soudnímu dvoru předběžnou otázku ohledně výkladu čl. 15 odst. 1 písm. c) a čl. 14 písm. e) GDPR, tedy zda tyto musí být vykládány tak, „*že právo na přístup je omezeno na informace o kategoriích příjemců, pokud konkrétní příjemci nejsou v době zamýšleného sdělení ještě známi, ale že se nutně musí vztahovat i na informace o příjemcích těchto informací, pokud již byly údaje sděleny?*“[77,78]

Soudní dvůr uznal, že zatímco textace čl. 14 odst. 1 písm. e) neumožňuje stanovit prioritu mezi pojmy „příjemci“ a „kategorie příjemců“, v souladu se zásadou transparentnosti a oproti čl. 13 a 14 zakládá čl. 15 subjektu údajů skutečné právo na přístup v kontextu zpracovávaných osobních údajů, což mj. znamená, že „*subjekt údajů musí mít na výběr, zda chce získat informace pokud možno o konkrétních příjemcích, kterým byly nebo budou uvedené údaje zpřístupněny, nebo informace o kategoriích příjemců.*“[79] Navíc, jak Soudní dvůr již v minulosti judikoval, právo podle čl. 15 musí subjektu údajů nabízet možnost ověřit jak správnost osobních údajů, tak i zákonnost jejich zpracování, zejména pak zda byly zpřístupněny oprávněným příjemcům.[80,81] Toto právo je efektivně základem řady dalších práv vyplývajících z GDPR (mj. právo na opravu, výmaz či omezení zpracování) a pro jejich

[77] Článek 14 odst. 1 písm. e) GDPR stanovuje: „*Jestliže osobní údaje nebyly získány od subjektu údajů, poskytne správce subjektu údajů informace o případných příjemcích nebo kategoriích příjemců osobních údajů.*“
Článek 15 odst. 1 písm. c) GDPR stanovuje: „*Subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům a k následujícím informacím – příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích*“

[78] Body 22-27 anotovaného rozhodnutí.

[79] Body 30-36 anotovaného rozhodnutí.

[80] Viz rozsudky ze dne 17. července 2014, YS a další, C-141/12 a C-372/12, EU:C:2014:2081, bod 44, jakož i ze dne 20. prosince 2017, Nowak, C-434/16, EU:C:2017:994, bod 57, a rozsudek ze dne 7. května 2009, Rijkeboer, C-553/07, EU:C:2009:293, bod 49.

[81] Bod 37 anotovaného rozhodnutí.

dosažení je pak nutné, aby měl subjekt údajů právo na sdělení totožnosti konkrétních příjemců osobních údajů.[82]

Soudní dvůr na základě této argumentace uzavřel, že právo subjektu údajů na přístup k osobním údajům, které se ho týkají podle čl. 15 odst. 1, zakládá povinnost správce sdělit tomuto subjektu totožnost konkrétních příjemců, ledaže je nemožné je identifikovat či správce doloží, že žádosti subjektu údajů jsou zjevně nedůvodné či nepřiměřené.[83]

Autor: JV

PROCESNÍ KOLIZE OBČANSKOPRÁVNÍ A SPRÁVNĚPRÁVNÍ OCHRANY PRÁV VYPLÝVAJÍCÍCH Z GDPR

Soud: Soudní dvůr Evropské unie
Věc: C-132/21
Datum: 12. 1. 2023
Dostupnost: curia.europa.eu

Pan BE žádal o audiozáznam zasedání valné hromady akciové společnosti, jíž je akcionářem, společnost mu však vyhověla pouze částečně a poskytla mu prostřihaný záznam, na kterém byly patrné toliko jeho vstupy (konkrétně otázky), nikoliv však reakce.[84] Obrátil se tak na maďarský Národní úřad pro ochranu údajů a svobodu informací s tím, že společnost porušila GDPR a měla by být povinována vydat daný záznam, dozorový úřad však jeho žádost zamítl.[85] V reakci na to BE podal dvě žaloby, jednu namířenou proti rozhodnutí úřadu a druhou k civilnímu soudu podle čl. 79 odst. 1 GDPR proti rozhodnutí správce údajů. Druhé žalobě již soud vyhověl z důvodu, že správce porušil právo BE na přístup k osobním údajům.[86]

Dané rozštěpení kauz, a konkrétně vyhovění žalobě v občanskoprávním řízení, však představovalo procesní oříšek, který zarazil i předkládající soud

[82] Body 38 a 39 anotovaného rozhodnutí.

[83] Bod 51 anotovaného rozhodnutí.

[84] Body 11 a 12 anotovaného rozhodnutí.

[85] Bod 13 anotovaného rozhodnutí.

[86] Body 14-16 anotovaného rozhodnutí.

(který rozhodoval správněprávní část sporu), neboť stál před otázkou sladění posouzení legality rozhodnutí správce údajů civilním soudem se správním řízením a zejména, zda má jeden procesní prostředek závaznost či přednost před druhým.[87] Rozhodl se tak řízení přerušit a položil Soudnímu dvoru předběžnou otázku, zda prostředek správní ochrany upravený v článku 77 GDPR je prostředkem pro uplatnění práv vyplývajících z veřejného práva a prostředek soudní ochrany v článku 79 GDPR zase ze soukromého práva.[88] Na to pak ještě navázal další otázkou ohledně přednosti jednotlivých řízení, konkrétně zda mají být jednotlivá řízení na sobě plně nezávislá, či by mělo mít rozhodnutí dozorového úřadu přednost (v kontextu čl. 51 odst. 1 a čl. 58 odst. 2 písm. b) a d) GDPR).[89]

Soudní dvůr v první řadě přikročil kvůli pochybnostem Evropské komise k přeformulování otázek[90].[91] K věci samotné pak Soudní dvůr uvádí, že všechny prostředky z článků 77, 78 a 79 musí být uplatnitelné, aniž by byly dotčeny prostředky ostatní.[92] Ze znění těchto ustanovení je pak patrné, že nezakládají přednostní ani výlučnou příslušnost, ni pravidlo přednostního posouzení úřadem či soudem.[93] Oproti situaci, kdy je jedna věc předložena dozorovým úřadům či soudům několika členských států (a kdy normotvůrce výslovně upravuje mechanismy spolupráce aj.), je tak v souladu se zásadou procesní autonomie, aby si každý stát upravil procesní prostředky, které mohou existovat zároveň a nezávisle na sobě, tak, aby byla zajištěna vysoká úroveň ochrany práv vyplývajících z unijního řádu.[94] Existence více nezávislých paralelních procesů je navíc v souladu s posílením pozice sub-

[87] Body 16-18 anotovaného rozhodnutí.

[88] Body 19-22 anotovaného rozhodnutí.

[89] Bod 22 anotovaného rozhodnutí.

[90] *„Zda čl. 77 odst. 1, čl. 78 odst. 1 a čl. 79 odst. 1 nařízení 2016/679, musí být ve světle článku 47 Listiny základních práv (dále jen „Listina“), vykládány v tom smyslu, že procesní prostředky zakotvené v uvedených čl. 77 odst. 1 a čl. 78 odst. 1 a dále v čl. 79 odst. 1, mohou být uplatněny zároveň a nezávisle, nebo zda má jeden z nich přednost.“*

[91] Body 23-31 anotovaného rozhodnutí.

[92] Body 32-35 anotovaného rozhodnutí.

[93] Bod 35 anotovaného rozhodnutí.

[94] Body 37-47 anotovaného rozhodnutí.

jektu údajů i plného soudního přezkumu, tato pravidla však nesmí ohrozit užitečný účinek a efektivní ochranu zaručenou GDPR.[95,96]

V předkládané věci jsou jednotlivá řízení koncipována jako na sobě právně nezávislá, avšak vázaná jedním skutkovým stavem, což nevylučuje možnost navzájem si odporujících rozhodnutí.[97] Takový stav by však vedl k narušení právní jistoty a oslabení ochrany práv GDPR stanovených.[98] Soudní dvůr tak uzavřel, že instituty ochrany práv zakotvených články 77, 78 a 79 GDPR umožňují jejich souběžné a nezávislé využití, ale je na členských státech, aby toto procesní nastavení neohrozilo účinnost ochrany práv zaručených GDPR, soudržné a jednotné uplatňování jeho ustanovení či právo na účinný prostředek nápravy před soudem ve smyslu čl. 47 Listiny základních práv.

Autor: JV

STŘET ZÁJMŮ U POVĚŘENCE PRO OCHRANU OSOBNÍCH ÚDAJŮ

Soud: Soudní dvůr Evropské unie
Věc: C-453/21
Datum: 9. 2. 2023
Dostupnost: curia.europa.eu

Pan FC u společnosti X-FAB vykonával funkci předsedy podnikové rady. V červnu 2015 byl jmenován pověřencem pro ochranu osobních údajů. V prosinci 2017 byl s okamžitým účinkem odvolán pro střet zájmů na základě neslučitelnosti funkce předsedy podnikové rady a pověřence. To bylo následně dopisy zopakováno v květnu 2018 v souladu s čl. 38 GDPR, které

[95] Body 43-48 anotovaného rozhodnutí.

[96] V tomto smyslu viz rozsudek ze dne 14. července 2022, EPIC Financial Consulting, C-274/21 a C-275/21, EU:C:2022:565, bod 73 a citovaná judikatura.

[97] Body 52 a 53 anotovaného rozhodnutí.

[98] Body 54-57 anotovaného rozhodnutí.

se mezitím stalo použitelným.[99] Pan FC podal žalobu na určení, že je stále pověřencem společnosti X-FAB.

Soud prvního stupně a odvolací soud žalobě podané FC vyhověly. Společnost X-FAB se dovolala k soudu Bundesarbeitsgericht (Spolkový pracovněprávní soud v Německu), který předložil předběžné otázky na výklad čl. 38 GDPR.[100]

Výklad Soudního dvora se týkal především druhé věty daného ustanovení GDPR, ve které stojí, že pověřenec "[v] *souvislosti s plněním svých úkolů není správcem nebo zpracovatelem propuštěn ani sankcionován*." Nejprve se zabýval tím, zda je přípustná odlišná vnitrostátní právní úprava odvolání pověřence. Soudní dvůr zde navázal na svou nedávnou judikaturu,[101] kde dovodil, že pověřenec musí být chráněn před jakýmkoliv rozhodnutím, kterým by byl ukončen výkon jeho funkce, které by mu způsobovalo újmu, nebo které by představovalo sankci. Tento výklad je přitom potvrzen kontextem, do něhož uvedené ustanovení zapadá, a zejména právním základem, na jehož základě unijní normotvůrce GDPR přijal.[102] Tudíž stanovení pravidel o ochraně pověřence zaměstnaného správcem nebo zpracovatelem před odvoláním spadá pod ochranu fyzických osob při zpracování osobních údajů pouze v rozsahu, v němž taková pravidla směřují k zachování funkční nezávislosti pověřence.[103] Z toho vyplývá, že členský stát může stanovit zvláštní ochranná ustanovení v oblasti odvolávání pověřence, pokud tato ustanovení neohrozí dosažení cílů GDPR.[104] Příkladem ochrana pověřence, která by bránila jakémukoli odvolání pověřence v případě, že by již nemohl plnit své povinnosti a úkoly nezávislým způsobem z důvodu střetu zájmů, by ohrozila dosažení tohoto cíle.[105]

[99] Viz bod 13 anotovaného rozhodnutí.

[100] Viz bod 15 anotovaného rozhodnutí.

[101] Rozsudek CJEU ze dne 22. června 2022 ve věci Leistritz, C-534/20, EU:C:2022:495 a zde citovaná rozhodnutí.

[102] Viz bod 28 anotovaného rozhodnutí.

[103] Viz bod 30 anotovaného rozhodnutí.

[104] Viz bod 32 anotovaného rozhodnutí.

[105] Viz bod 34 anotovaného rozhodnutí.

Dále Soudní dvůr pojednával o tom, za jakých podmínek lze konstatovat existenci „střetu zájmů“ ve smyslu čl. 38 odst. 6 GDPR.[106] GDPR nestanoví zásadní neslučitelnost výkonu funkce pověřence s výkonem jiných funkcí u správce nebo zpracovatele.[107] Ovšem v souladu s cílem sledovaným čl. 38 odst. 6 GDPR nelze pověřenci svěřit plnění úkolů nebo povinností, které by mohly narušit plnění povinností, které plní jako pověřenec.[108] Z toho zejména vyplývá, že pověřenec nemůže plnit úkoly nebo povinnosti, které by ho vedly k určování účelů a prostředků zpracování osobních údajů.[109] Určení existence střetu zájmů pak musí být provedeno případ od případu s přihlédnutím k organizační struktuře podniku a případných vnitřních pravidel.[110]

Soudní dvůr tak poskytl další významné vodítko pro roli pověřence a zachování jeho specifického postavení v rámci organizačních struktur správce.

Autor: FK

POVINNOST ZOHLEDNIT ZÁJMY SUBJEKTŮ ÚDAJŮ V SOUVISLOSTI S DOKAZOVÁNÍM V OBČANSKOPRÁVNÍM ŘÍZENÍ

Soud: Soudní dvůr Evropské unie
Věc: C-268/21
Datum: 2. 3. 2023
Dostupnost: curia.europa.eu

Společnost Norra Stockholm Bygg AB (dále jen „Fastec“) postavila budovu pro společnost Per Nycander AB (dále jen „Nycander“). Pro vedení elektro-

[106] Viz bod 38 anotovaného rozhodnutí.
[107] Viz bod 40 anotovaného rozhodnutí.
[108] Viz bod 41 anotovaného rozhodnutí.
[109] Viz bod 44 anotovaného rozhodnutí.
[110] Viz bod 45 anotovaného rozhodnutí.

nické evidence zaměstnanců pracujících na dané stavbě byla společností Fastec zmocněna společnost Entral AB.[111]

Fastec se žalobou k soudu prvního stupně domáhala zaplacení dlužné částky po Nycander. Nycander tento požadavek rozporovala.[112] Navrhla proto soudu, aby bylo Entral AB nařízeno předložit evidenci zaměstnanců Fastec jako důkaz.[113] Tento návrh Fastec odmítl pro rozpor s čl. 5 odst. 1 písm. b) GDPR.[114] Soud prvního stupně Entral AB nařídil evidenci předložit,[115] odvolací soud toto rozhodnutí potvrdil. Fastec podala dovolání ke švédskému Nejvyššímu soudu.[116]

Nejvyšší soud řízení přerušil a podal k Soudnímu dvoru dvě předběžné otázky. Nejprve se ptal, zda se ustanovení čl. 6 odst. 3 a 4 GDPR aplikují na situaci, kdy má být v občanskoprávním řízení jako důkaz předložena evidence zaměstnanců obsahující osobní údaje třetích osob, jež byly shromážděny za účelem daňové kontroly.[117] Pokud by odpověď na první otázku byla kladná, tak se soud táže, zda ustanovení čl. 5 a 6 GDPR ukládají soudu povinnost zohlednit zájmy subjektů údajů. A pokud ano, zda unijní právo či GDPR stanovuje nějaké zvláštní požadavky.[118]

K první předběžné otázce Soudní dvůr dovodil, že se předmětná ustanovení na danou situaci aplikují,[119] jelikož je účel, kterému slouží zpracování údajů v řízení před soudem prvního stupně, odlišný od účelu, pro který

[111] Bod 15 anotovaného rozhodnutí.

[112] Bod 16 anotovaného rozhodnutí. Společnost Nycander argumentovala tím, že skutečný počet hodin odpracovaný zaměstnanci Fastec je nižší, než uvádějí.

[113] Bod 17 anotovaného rozhodnutí. Evidence měla sloužit jako důkaz uvádějící skutečný počet hodin, jež zaměstnanci Fastec odpracovali. Měla být předložena v zásadě v nezměněné podobě, nebo se zakrytými národními identifikačními čísly dotyčných osob.

[114] Bod 18 anotovaného rozhodnutí. Rozpor Fastec shledává v tom, že takové zpřístupnění údajů soudem není v souladu s účelem, za kterým byly osobní údaje v něm obsažené shromážděny. Tím je daňová kontrola činnosti společnosti švédskou finanční správou.

[115] Soud nařídil předložit evidenci pouze těch zaměstnanců, kteří v předmětném období pracovali na dané stavbě.

[116] Body 19 a 20 anotovaného rozhodnutí.

[117] Body 24 a 25 anotovaného rozhodnutí.

[118] Body 24 a 42 anotovaného rozhodnutí.

[119] Bod 41 anotovaného rozhodnutí.

byly shromážděny.[120] Dané zpracování proto musí 1) mít základ ve vnitrostátním právu[121], 2) představovat nutné a přiměřené opatření v demokratické společnosti[122] a 3) chránit nezávislost soudnictví a soudních řízení[123], anebo zajišťovat vymáhání občanskoprávních nároků.[124] Zda jsou tyto podmínky splněny musí dle Soudního dvora posoudit Nejvyšší soud.[125]

K druhé předběžné otázce Soudní dvůr stanovil, že pro výkon práva na účinnou soudní ochranu a práva na spravedlivý proces je třeba, aby měl jednotlivec přístup k nezbytným důkazům. Tyto důkazy však mohou obsahovat osobní údaje třetích osob.[126] Aby zpracování údajů bylo zákonné, musí soud zohlednit dotčené protichůdné zájmy subjektů údajů, než nařídí předložení předmětných důkazů.[127] Vyvážení těchto zájmů se může lišit dle okolností případu a druhu řízení.[128] Zároveň je třeba zohlednit požadavky vyplývající ze zásad proporcionality[129] a minimalizace.[130]

Autor: VJ

---

[120] Bod 36 anotovaného rozhodnutí.

[121] Ve smyslu čl. 6 odst. 1 písm. e) GDPR ve spojení s čl. 6 odst. 3 GDPR. Základ zde představuje kapitola 38 švédského občanského soudního řádu (označován jako „RB“), viz bod 38 anotovaného rozhodnutí. Zda se jedná o vnitrostátní právo hmotné, či procesní, nehraje roli, jelikož ustanovení čl. 6 odst. 3 písm. b) a odst. 4 GDPR mezi nimi nerozlišuje, viz bod 40 anotovaného rozhodnutí.

[122] Ve smyslu čl. 6 odst. 4 GDPR.

[123] Ve smyslu čl. 23 odst. 1 GDPR. Dle soudu tento cíl skýtá jak ochranu výkonu spravedlnosti před vnitřními i vnějšími vlivy, tak řádný výkon spravedlnosti. Viz bod 38 anotovaného rozhodnutí.

[124] Body 37 a 38 anotovaného rozhodnutí.

[125] Bod 39 anotovaného rozhodnutí.

[126] Bod 53 anotovaného rozhodnutí.

[127] Body 46 a 59 anotovaného rozhodnutí.

[128] Body 47 a 59 anotovaného rozhodnutí.

[129] Body 49 a 59 anotovaného rozhodnutí. Zásada proporcionality se uplatní, protože právo na ochranu osobních údajů není právem absolutním, viz bod 4 odůvodnění GDPR.

[130] Body 54 a 59 anotovaného rozhodnutí. Dle zásady minimalizace přísluší vnitrostátnímu soudu povinnost určit, zda je zpřístupnění osobních údajů 1) přiměřené, 2) schopné dosáhnout cíle stanoveného vnitrostátním právem, a 3) omezené pouze na rozsah nezbytný pro účel jejich zpracování (jinými slovy, zda cíle nelze dosáhnout způsobem, který představuje méně závažné porušení ochrany osobních údajů velkého počtu třetích osob, např. výslechem vybraných svědků), viz body 54 a 55 anotovaného rozhodnutí.

SOULAD PUBLIKACE OSOBNÍCH ÚDAJŮ NA WEBOVÝCH STRÁNKÁCH S RESPEKTEM K SOUKROMÍ

Soud: Evropský soud pro lidská práva
Věc: L.B. v. Hungary, č. 36345/16
Datum: 9. 3. 2023
Dostupnost: hudoc.echr.coe.int

Maďarská Národní daňová a celní správa uveřejnila roku 2014 stěžovatelovy osobní údaje na svých webových stránkách v seznamu dlužníků s ohledem na to, že stěžovatel dlužil státu na daních více než 10 milionů forintů (cca 30 000 EUR), toto v souladu s platnou právní úpravou maďarského daňového řádu. Jednalo se o daňové identifikační číslo a adresa bydliště stěžovatele. Tyto informace byly dále roku 2016 použity internetovým médiem k vytvoření mapy neplatičů.[131]

V předchozím řízení rozhodl čtvrtý senát Evropského soudu pro lidská práva (dále jen „ESLP“) pěti hlasy proti dvěma, že nedošlo k porušení článku 8 EÚLP[132], když shledal, že za daných okolností případu nezatížilo zveřejnění osobních údajů stěžovatele jeho soukromý život podstatně více, než bylo nezbytné k prosazení legitimního zájmu státu. Dne 31. května 2021 byl případ na žádost stěžovatele postoupen Velkému senátu ESLP.[133]

Stěžovatel se odvolával na čl. 8 EÚLP (Právo na respektování soukromého a rodinného života), který zní „*1. Každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence. 2. Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.*“[134]

[131] Body 25–28 anotovaného rozhodnutí.

[132] Evropská úmluva o lidských právech.

[133] Bod 75 anotovaného rozhodnutí.

[134] Bod 77 anotovaného rozhodnutí.

V tomto případě se Velký senát ESLP věnoval zejména otázce zásahu do stěžovatelova práva z hlediska nezbytnosti pro demokratickou společnost.[135] Konkrétně se jednalo zejména o zveřejňování adres bydliště uvedených neplatičů a proporcionalita takového zásahu s ohledem na zamýšlený účinek tohoto uveřejnění, který měl být dle maďarského parlamentu odstrašující. Dle Velkého senátu ESLP nebylo prokázáno, že by byl zohledněn dopad režimu zveřejňování podle maďarského daňového řádu na právo na soukromí, a zejména riziko zneužití adresy bydliště daňového dlužníka jinými osobami z řad veřejnosti. Rovněž nebyl zohledněn potenciální dosah média použitého k šíření dotčených informací, konkrétně skutečnost, že zveřejnění osobních údajů na internetových stránkách finančního úřadu znamená, že bez ohledu na motivy získání přístupu k informacím má kdokoli na celém světě, kdo má přístup k internetu, rovněž neomezený přístup k informacím o jménu i adrese bydliště každého daňového dlužníka uvedeného v seznamu, přičemž riziko opětovného zveřejnění je přirozeným, pravděpodobným a předvídatelným důsledkem původního zveřejnění.[136]

Vzhledem k systematickému zveřejňování údajů o daňových poplatnících, které zahrnovalo adresy bydliště daňových poplatníků, nebyl Velký senát ESLP přesvědčen, že důvody, na které se maďarský zákonodárce odvolával při přijímání režimu zveřejňování, byly dostatečné k tomu, aby prokázaly, že zásah, který je předmětem stížnosti, byl "nezbytný v demokratické společnosti" a že orgány žalovaného státu dosáhly spravedlivé rovnováhy mezi dotčenými konkurujícími si zájmy. Velký senát ESLP proto shledal porušení stěžovatelova práva na respektování soukromého života dle čl. 8 EÚLP.[137]

Autorka: TN

[135] Bod 115 a násl. anotovaného rozhodnutí.

[136] Body 132–135 anotovaného rozhodnutí.

[137] Body 139 a 140 anotovaného rozhodnutí.

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PŘI ONLINE VÝUCE (PODMÍNKY ČL. 88 GDPR)

Soud: Soudní dvůr Evropské unie
Věc: C-34/21
Datum: 30. 3. 2023
Dostupnost: curia.europa.eu

V roce 2020 ministr školství a kultury německé spolkové země Hesensko stanovil formální rámec výuky během pandemie covid-19. Součástí tohoto rámce byla možnost žáků se účastnit na výuce prostřednictvím videokonference, pokud nebyla možná jejich osobní přítomnost. Taková forma výuky byla podmíněna souhlasem zletilého studenta nebo souhlasem zákonného zástupce u nezletilých studentů. Oproti tomu požadavek souhlasu učitelů s účastí na této formě výuky nebyl požadován.[138]

Zdůvodněním pro absenci požadavku souhlasů u učitele byla ustanovení hesenského zákona o ochraně osobních údajů a spolkového zákona o ochraně osobních údajů, které umožňovaly zpracování osobních údajů zaměstnanců škol kvůli nutnosti takového zpracování pro plnění jejich povinností z pracovního poměru.[139] Tato ustanovení byla přijata ve formě zpřesnění zpracování osobních údajů zaměstnanců předpokládaných GDPR v článku 88. Rada pro zaměstnance školství v Hesensku pro tuto absenci souhlasu podala žalobu ve správním soudnictví, která vyústila v předložení dvou předběžných otázek.

Těmito otázkami jsou:

- Je nutné, aby konkretizační předpis podle čl. 88 odst. 1 GDPR splňoval podmínky v čl. 88 odst. 2 GDPR?
- Pokud vnitrostátní norma nesplňuje podmínky čl. 88 odst. 2 GDPR, může být i přesto použitelná?

[138] Body 14 a 15 anotovaného rozhodnutí.

[139] § 23 hesenského zákona o ochraně osobních údajů a § 86 spolkového zákona o ochraně osobních údajů.

Soudní dvůr nejdříve zdůraznil, že ustanovení čl. 88 GDPR se uplatní i na zaměstnance ve veřejném sektoru vzhledem k autonomnímu výkladu evropského práva.[140]

K samotným otázkám se pak Soudní dvůr vyjádřil tak, že pro přijetí konkretizačních norem podle čl. 88 odst. 1 GDPR existují 3 podmínky. První podmínkou je skutečná konkretizace reflektující specifika určitého sektoru, ve kterém zaměstnanci působí, nejen zopakování obecných požadavků GDPR.[141] Další dvě podmínky vychází z čl. 88 odst. 2 GDPR a sice, že konkretizační předpisy musí směřovat k ochraně práv a svobod zaměstnanců, tedy ne ke zhoršení standardu přiznaného GDPR, a zároveň musí být přijata opatření zajišťující proporcionalitu těchto opatření.[142] Pokud tedy podmínky podle čl. 88 odst. 2 společně s podmínkou skutečné konkretizace nejsou splněny nemůže jít o konkretizační normu podle tohoto článku GDPR.

K druhé otázce Soudní dvůr připomněl aplikační přednost evropského práva, která by za nesplnění podmínek z čl. 88 odst. 2 vedla k nemožnosti aplikovat tento nepravý konkretizační předpis.

Přestože Soudní dvůr zdůraznil, že konkrétní posouzení naplnění podmínek pro přijetí konkretizační normy je na vnitrostátním soudě, též naznačil, že posuzovaná ustanovení spolkového a hesenského zákona mají atributy pouhého opakování obecných podmínek z GDPR a neměla by se proto aplikovat.[143]

Autor: ME

PORUŠENÍ GDPR JAKOŽTO VZNIK ÚJMY

Soud: Soudní dvůr Evropské unie
Věc: C-300/21
Datum: 4. 5. 2023
Dostupnost: curia.europa.eu

[140] Body 44 a 45 anotovaného rozhodnutí.

[141] Bod 74 anotovaného rozhodnutí.

[142] Bod 64 anotovaného rozhodnutí.

[143] Body 80 a 81 anotovaného rozhodnutí.

Österreichische Post zpracovávala údaje o politických preferencích rakouských obyvatel, a to na základě statistické explorace. Jeden ze subjektů údajů, který ke zpracování neudělil souhlas, se cítil dotčen, protože mu byla daným způsobem přisouzena spřízněnost s určitou politickou stranou.[144,145] V této souvislosti žaloval Österreichische Post na zaplacení nehmotné újmy.

Předmětný spor byl řešen před rakouskými soudy. V rámci jeho řešení vyvstaly předběžné otázky týkající se náhrady újmy v důsledku porušení GDPR[146].[147] Těmi se v anotovaném rozsudku zabýval Soudní dvůr. Podstatou předběžných otázek bylo, zda k přiznání práva na náhradu újmy postačuje pouhé porušení GDPR.[148] Dále se Soudní dvůr zabýval tím, zda právo na náhradu nehmotné újmu dle GDPR brání aplikaci vnitrostátních pravidel podmiňujících náhradu tím, že újma dosáhla určité míry.[149] Nakonec Soudní dvůr rozebral, zda se pro určení výše náhrady újmy použijí vnitrostátní předpisy (za dodržení zásady rovnocennosti a efektivity).[150]

Povinnost nahradit újmu související s porušením pravidel o zpracování osobních údajů je definována v čl. 82 odst. 1 GDPR. Doslova je stanoveno, že: *„Kdokoli, kdo v důsledku porušení tohoto nařízení utrpěl hmotnou či nehmotnou újmu, má právo obdržet od správce nebo zpracovatele náhradu utrpěné újmy.“*

Soudní dvůr uvedl, že pro vznik náhrady újmy je potřeba naplnění tří kumulativních podmínek: i) porušení GDPR, ii) vznik újmy a iii) kauzální nexus mezi porušením a újmou.[151] Proto dovodil, že pouhé porušení GDPR

[144] V tomto případě nebyly údaje předány dalším osobám.

[145] Body 11 a 12 anotovaného rozsudku.

[146] 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).

[147] Bod 20 anotovaného rozsudku.

[148] Bod 28 anotovaného rozsudku.

[149] Bod 43 anotovaného rozsudku.

[150] Bod 52 a násl. anotovaného rozsudku.

[151] Bod 32 anotovaného rozsudku.

není dostatečným podkladem pro přiznání práva na náhradu újmy.[152] Dále popsal, že pojem újma není spojován s odkazem na vnitrostátní právo a musí být vykládán jednotně a autonomně v rámci unijního práva.[153] Přiznání práva na náhradu újmy tedy nemůže být, na základě vnitrostátních předpisů, navázáno na dosažení určité míry.[154] GDPR nestanovuje pravidla pro vyčíslení výše náhrady újmy. Vzhledem k absenci této úpravy má být rozsah náhrady určen na základě práva členského státu.[155]

Anotovaný rozsudek přináší dodatečný pohled na otázky náhrady újmy za porušení předpisů o zpracování osobních údajů, které vyvstaly např. v britském případě Lloyd v Google. V teoretické rovině Soudní dvůr pro přiznání práva na náhradu újmy jasně uvedl nutnost naplnění tří kumulativních podmínek. Zůstává však otázkou, zda v praxi naplnění první podmínky automaticky (nebo alespoň ve většině případů) neimplikuje i naplnění zbylých podmínek, např. v souvislosti s omezením svobody vůle dotčeného subjektu údajů ohledně jeho možnosti nakládání s předmětnými daty.

Autor: JS

ODPOVĚDNOST SPRÁVCE V PŘÍPADĚ NEDŮSLEDNÉHO SPLNĚNÍ POVINNOSTÍ PODLE ČL. 26 A 30 NAŘÍZENÍ GDPR

Soud: Soudní dvůr Evropské unie
Věc: C-60/22
Datum: 4. 5. 2023
Dostupnost: curia.europa.eu

Žalobci byla německým Spolkovým úřadem zamítnuta jeho žádost o mezinárodní ochranu.[156] Spolkový úřad při zamítnutí žádosti vycházel z elektronického spisu „MARIS“ (dále jen „elektronický spis“), který obsahoval

[152] Bod 42 anotovaného rozsudku.
[153] Body 30 a 44 anotovaného rozsudku.
[154] Bod 51 anotovaného rozsudku.
[155] Viz body 52-29 anotovaného rozsudku.
[156] Bod č. 27 anotovaného rozhodnutí.

osobní údaje o žalobci v daném řízení.[157] Žalobce proti rozhodnutí úřadu podal žalobu k německému správnímu soudu, jemuž byl následně elektronický spis zaslán v rámci společného postupu podle čl. 26 Nařízení GDPR[158] prostřednictvím elektronické soudní a správní poštovní schránky spravovanou veřejným subjektem, jež je součástí moci výkonné.[159]

Dle německého soudu však Spolkový úřad nepředložil úplný záznam o činnostech zpracování týkající se daného spisu, a proto bylo jednání úřadu v rozporu s Nařízením GDPR, přesněji se zásadami zpracování osobních údajů dle čl. 5 odst. 1[160] ve spojení s čl. 26[161] a čl. 30[162] daného nařízení.[163] Německý soud se proto rozhodl obrátit se v dané věci na Soudní dvůr EU s žádostí o zodpovězení předběžných otázek. Primární byla otázka, zda má chybějící nebo neúplné plnění povinností[164] odpovědnosti správce za následek protiprávnost zpracování údajů, a tudíž může subjekt údajů žádat výmaz těchto údajů v souladu čl. 17 odst. 1 písm. d) Nařízení GDPR[165] nebo omezení jejich zpracování podle čl. 18 odst. 1 písm. b) Nařízení GDPR?[166,167]

Soudní dvůr v případě této otázky konstatoval, že nesplnění povinnosti podle čl. 26 nebo 30 Nařízení GDPR ze strany správce nepředstavuje pro-

[157] Bod č. 28 anotovaného rozhodnutí.

[158] Celým názvem 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.

[159] Bod č. 29 anotovaného rozhodnutí.

[160] Čl. 5 odst. 1 Nařízení GDPR stanovuje obecné zásady pro zpracování osobních údajů, mezi které mimo jiné patří jejich zpracování konkrétním, zákonným a transparentním způsobem (čl. 5 odst. 1 písm. a)).

[161] Čl. 26 Nařízení GDPR ukládá, v případě dvou a více správců, povinnost mezi sebou uzavřít transparentní ujednání o společném postupu v rámci kterého mimo jiné vymezí úlohy společných správců, jejich vztahy a své podíly na odpovědnosti za povinnosti poskytovat informace uvedené v čl. 13 a 14 Nařízení GDPR.

[162] Čl. 30 Nařízení GDPR stanovuje správci povinnost vést záznam o činnostech zpracování. Záznam dle daného článku obsahuje např. jméno a kontaktní údaje správce, účely zpracování, popis kategorie subjektů údajů a osobních údajů, kategorie příjemců a další.

[163] Bod č. 32 a 33 anotovaného rozhodnutí.

[164] Např. neexistence ujednání o společném postupu dle čl. 26 GDPR nebo neexistence nebo nekompletnost o činnostech zpracování dle čl. 30 Nařízení GDPR.

[165] Čl. 17 odst. 1 písm. d) Nařízení GDPR dovoluje právo na výmaz, pokud byly dané osobní údaje zpracovány protiprávně.

tiprávní zpracování, které přiznává subjektu údajů právo na výmaz či omezení zpracování, jelikož takové porušení samo o sobě neznamená, že správce porušil zásadu odpovědnosti dle čl. 5 odst. 2, ve spojení s čl. 5 odst. 1 písm. a) a čl. 6 odst. 1 Nařízení GDPR.[168,169]

Návazně se německý soud v žádost dotázal, zda má porušení čl. 5, 26 nebo 30 GDPR správcem za následek, že soud smí k daným osobním údajům přihlédnout pouze, pokud subjekt údajů s tímto použitím explicitně souhlasí.[170] K dané otázce Soudní dvůr dospěl k závěru, že v případě, že správce nesplnil povinnosti, které mu vyplývají z čl. 26 nebo 30 Nařízení GDPR není zákonnost zohlednění takových údajů vnitrostátním soudem podmíněna souhlasem subjektu údajů.[171]

Autorka: AKar

PRÁVO NA VYDÁNÍ KOPIE ZPRACOVÁVANÝCH OSOBNÍCH ÚDAJŮ PODLE ČL. 15 ODST. 3 GDPR

Soud: Soudní dvůr Evropské unie
Věc: C-487/2021
Datum: 4. 5. 2023
Dostupnost: curia.europa.eu
Souvislost s: C-154/21

Společnost CRIF jakožto poradenská agentura poskytuje na žádost klientů informace o solventnosti třetích osob, za kterýmžto účelem zpracovávala

[166] Čl. 18 odst. 1 písm. b) Nařízení GDPR stanovuje právo na omezení zpracování v případě, že je zpracování protiprávní a subjekt údajů odmítá výmaz a žádá místo toho pouze omezení jejich použití.

[167] Bod č. 38 anotovaného rozhodnutí.

[168] Čl. 6 odst. 1 Nařízení GDPR uvádí, že zpracování údajů je považováno za zákonné, pokud splňuje alespoň jednu z podmínek uvedených v tomto článku. Mezi tyto podmínky patří např. udělení souhlasu subjektu se zpracováním jeho osobních údajů pro konkrétní účel nebo nezbytnost zpracování pro splnění pro splnění úkolů ve veřejném zájmu nebo výkonu moci veřejné.

[169] Bod č. 61 až 69 anotovaného rozhodnutí.

[170] Bod č. 38 anotovaného rozhodnutí.

[171] Bod č. 71 až 75 anotovaného rozhodnutí.

osobní údaje žalobce F. F.[172] Ten v roce 2018 požádal o přístup ke zpracovávaným osobním údajům včetně e-mailů a výpisů z databází, společnost CRIF žádosti vyhověla, ovšem zpřístupnila pouze souhrnný seznam jeho zpracovávaných osobních údajů, nikoliv kopie všech dokumentů tyto údaje obsahující.[173]

Žalobce v reakci podal stížnost k rakouskému úřadu pro ochranu osobních údajů (dále jen „DSB"), ten ji však zamítl.[174] Žalobce tak podal proti tomuto rozhodnutí žalobu k rakouskému Spolkovému správnímu soudu, který řízení přerušil a položil Soudnímu dvoru čtyři předběžné otázky týkající se výkladu zejména čl. 15 odst. 3 GDPR[175,176]:

- Zahrnuje výraz „kopie" pouze fotokopii apod., či je možné zahrnout i širší chápání tohoto pojmu (tedy např. opis či transkript)?
- Zahrnuje právo subjektu údajů na vydání kopie zpracovávaných údajů[177] i právo na vydání veškerých dokumentů, v nichž se dané údaje nacházejí (příp. databázi)?
- V případě negativní odpovědi na druhou otázku, může být ve světle související judikatury[178] a zásadami GDPR přesto v určitých situacích nezbytné subjektu údajů vydat rovněž úryvky z textu nebo celé dokumenty?
- Zahrnuje pojem „informace" v případě elektronického podání subjektu údajů pouze zpracovávané osobní údaje podle čl. 15 odst. 3 GDPR, či např. i metadata?

---

[172] Bod 9 anotovaného rozhodnutí.

[173] Body 10-12 anotovaného rozhodnutí.

[174] Body 12 a 13 anotovaného rozhodnutí.

[175] *„Správce poskytne kopii zpracovávaných osobních údajů. Za další kopie na žádost subjektu údajů může správce účtovat přiměřený poplatek na základě administrativních nákladů. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob*."

[176] Body 14-17 anotovaného rozhodnutí.

[177] Jednalo by se tedy o věrnou reprodukci osobních údajů, ke kterých musí být poskytnut přístup podle čl. 15 odst. 1 GDPR.

[178] Ve smyslu rozsudku Soudního dvora ze dne 20. prosince 2017, Nowak (C-434/16, EU:C:2017:994).

Soudní dvůr spojil první tři otázky, neboť je dle jeho názoru není možné vnímat odděleně.[179] Přestože soud uznal, že je nutné vykládat pojmy „osobní údaje“ i „kopie“ široce[180], a to zvláště v kontextu související judikatury[181], což subjektu údajů přiznává právo na poskytnutí věrné reprodukce svých osobních údajů v širším smyslu, není možné výkladem samotného třetího odstavce článku 15 překročit rozsah práva založeného odstavcem prvním.[182] Zatímco první odstavec definuje rozsah a předmět práva, třetí odstavec upřesňuje praktické podmínky pro splnění povinnosti správce, a nerozšiřuje tak smysl pojmu „kopie“ na dokument jako takový, ale pouze na osobní údaje, které obsahuje a které musí být úplné.[183] Tyto údaje však musí subjektu údajů umožnit ověření správnosti a zákonnosti zpracování daných osobních údajů, což si mj. žádá, aby byly dané údaje poskytovány stručně a srozumitelně.[184,185] A tím pádem v situacích, kdy by samotné osobní údaje nebyly bez kontextu subjektu údajů srozumitelné, je předpokladem práva na získání věrné reprodukce zpracovávaných osobních údajů i právo získat kopii výpisů z dokumentů či celých dokumentů.[186] Soudní dvůr ovšem jedním dechem dodává, že je nezbytné zohlednit i případná dotčená práva a svobody jiných osob.[187]

Ke čtvrté otázce již Soudní dvůr toliko dodal, že pojem „informace“ musí být vykládán v tom smyslu, že se vztahuje pouze na osobní údaje, jejichž kopii musí správce poskytnout podle první věty třetího odstavce.[188]

Autor: JV

---

[179] Body 18 a 19 anotovaného rozhodnutí.

[180] Generální advokát v bodech 36 až 39 upozorňuje, že se široká definice „osobních údajů“ vztahuje i na veškeré informace ze zpracování osobních údajů vyplývající, viz bod 26 anotovaného rozhodnutí.

[181] Viz rozsudek ze dne 20. prosince 2017, Nowak, C-434/16, EU:C:2017:994, bod 34.

[182] Body 18-32 anotovaného rozhodnutí.

[183] Body 30-32 anotovaného rozhodnutí.

[184] Viz rozsudek ze dne 12. ledna 2023, Österreichische Post (Informace o příjemcích osobních údajů), C-154/21, EU:C:2023:3, bod 37 a citovaná judikatura.

[185] Body 34-38 anotovaného rozhodnutí.

[186] Body 41-43 anotovaného rozhodnutí.

[187] Body 43-45 anotovaného rozhodnutí.

[188] Body 46-53 anotovaného rozhodnutí.

3. INFORMACE VEŘEJNÉHO SEKTORU

PŘÍSTUP KE ZDRAVOTNICKÝM DATŮM Z REGISTRU NZIS

Soud: Ústavní soud
Věc: Pl.ÚS 25/21 (40/2023 Sb.)
Datum: 17. 1. 2023
Dostupnost: nalus.usoud.cz

Ústavní soud rozhodoval o případu týkajícího se práva na přístup k informacím podle zákona č. 106/1999 Sb. z Národního zdravotnického informačního systému ("NZIS"). Ústavní soud se v tomto kontextu zabýval návrhem Městského soudu v Praze na zrušení § 73 odst. 7 zákona č. 372/2011 Sb., o zdravotních službách, který uvádí, že se informace o údajích v NZIS poskytují pouze o struktuře dat. Na základě tohoto ustanovení pak bylo v původním případě odmítnuto poskytnutí statistických informací o ročním počtu úmrtí mezi lety 2014 až 2019. Navrhovatel pak argumentoval tím, že uvedené omezení práva na informace je protiústavní, protože se nevejde do žádného důvodu uvedeného v čl. 17 odst. 4 LZPS, který právo na informace umožňuje omezit.

Předmětem sporu byla otázka možnosti omezení práva na informace podle čl. 17 odst. 4 LZPS a zda se ustanovení § 73 odst. 7 zákona č. 372/2011 Sb. vejde do jeho aplikačního rozsahu.

Ústavní soud dospěl k závěru, že návrh na zrušení předmětného ustanovení není důvodný.[189] Samotná argumentace a její praktické dopady však směřují jinam, než by se mohlo na první pohled zdát. Ústavní soud předně připomíná, že pokud zásah do práv plynoucích z čl. 17 LZPS a čl. 10 odst. 1 Úmluvy nebude splňovat podmínky zde uvedené, tj. pokud nebude stanoven zákonem, nebude sledovat legitimní cíl zakotvený v těchto ustanoveních a současně nebude nezbytný v demokratické společnosti, aby těchto cílů dosáhl, pak půjde o porušení těchto článků.[190] Ústavní soud následně

[189] Bod 31 anotovaného rozhodnutí.

[190] Bod 36 anotovaného rozhodnutí.

odkazuje na svoji předchozí judikaturu (zejm. v podobě nálezu sp. zn. Pl. ÚS 2/10), který *pro futuro* stanovil postup pro situace obdobné s právě řešeným případem.[191] Dle Ústavního soudu je třeba vycházet ze zásady, že „*informace se poskytují a každé případné omezení tohoto práva je pak nutné vykládat restriktivním způsobem*“, přičemž k omezení může dojít jen za podmínek stanovených v čl. 17 odst. 4 LZPS, tedy jen v případech stanovených zákonem a zároveň kdy je to nezbytné v demokratické společnosti pro ochranu jiných práv a hodnot.[192] Ústavní soud pak zkoumá a hledá důvod, který by založil nezbytnost takové výluky (např. ochrana osobních údajů[193]), ale nenachází je. Předmětné ustanovení tak nemůže založit legitimní základ pro odmítnutí žádosti o informace. Ústavní soud přezkoumávané ustanovení nezrušil, protože existuje jeho ústavně konformní výklad, který spočívá v korektní aplikaci § 12 zákona č. 106/1999 Sb.

Ústavní soud potvrdil, že zákonné výjimky pro poskytování informací musí korespondovat s požadavky čl. 17 odst. 4 LZPS a tím je zákonodárce omezen před účelovými zásahy do práva na informace.

Autor: JM

SVOBODNÝ PŘÍSTUP K PORODNICKÝM DATŮM

Soud: Ústavní soud
Věc: III. ÚS 836/21
Datum: 11. 4. 2023
Dostupnost: nalus.usoud.cz

Tomuto rozhodnutí ÚS je věnována mediální pozornost kvůli důležitosti rozhodnutí pro budoucí získávání zdravotnických dat nezdravotnickými subjekty, i kvůli datům samotným. Stěžovatelka A. Š. si vyžádala od Ústavu zdravotnických informací a statistiky („ÚZIS“) údaje o počtu porodů v letech 2014 a 2015, a spolu s názvem porodnice informace o počtu

[191] Bod 40 anotovaného rozhodnutí.

[192] Bod 42 anotovaného rozhodnutí.

[193] Bod 47 anotovaného rozhodnutí.

zdravotnických výkonů učiněných při porodu, příkladem provedení císařského řezu či nástřihu hráze, a navazující statistiky.[194]

Vydání informací ÚZIS vyhověl částečně[195], zpřístupněním souhrnných dat za dané roky, bez uvedení porodnic.[196] Odkázal na zákon o zdravotních službách[197], který podle § 73 odst. 8 umožňuje získání dat pouze v podobě, ze které nelze určit konkrétní fyzickou nebo právnickou osobu. Stěžovatelka podala odvolání k Ministerstvu zdravotnictví.[198] Zamítavé rozhodnutí MZ napadla u Městského soudu v Praze, který žalobu také zamítl[199] s odůvodněním, že stěžovatelka má možnost údaje vyžádat u jednotlivých porodnic dle zákona o státní statistické službě.[200] Stěžovatelka podala kasační stížnost na Nejvyšší správní soud[201], kde mimo jiné argumentovala, že samotný § 73 odst. 8 zákona o zdravotních službách je protiústavní a porušuje právo na informace garantované čl. 17 Listiny[202]. Po opětovném zamítnutí[203] podala stížnost k ÚS. Žádala i odstranění požadavku anonymizace právnických osob ze zákona o zdravotních službách.[204]

ÚS konstatoval, že omezit právo dle čl. 17 Listiny a dle § 12 informačního zákona[205] lze jenom zákonem.[206] Každé takové omezení je nutné vykládat restriktivně.[207] ÚS se neztotožnil s výkladem, že název porodnic je dů-

[194] Bod 2 anotovaného rozhodnutí.

[195] Rozhodnutím ze dne 4. 5. 2017 č. j. UZIS/003773/2017.

[196] Bod 2 anotovaného rozhodnutí.

[197] Zákon č. 372/2011 Sb., zákon o zdravotních službách a podmínkách jejich poskytování

[198] Bod 2 anotovaného rozhodnutí. Stížnost byla rozhodnuta dne 7. 6. 20217 čj. J. MZDR 26678/2017-2/PRO.

[199] Rozsudek Městského soudu v Praze ze dne 14. 6. 2019 č. j. 6 A 155/2017-61.

[200] Městský soud v Praze odkazoval na § 17 odst. 2 Zákona č. 89/1995 Sb., zákon o státní statistické službě.

[201] Body 4–5 anotovaného rozhodnutí.

[202] Listina základních práv a svobod 2/1993 Sb.

[203] Rozsudek Nejvyššího správního soudu ze dne 28. 1. 2021 č.j. 3 As 232/2019-40

[204] Bod 5 anotovaného rozhodnutí a následující.

[205] Zákon č. 106/1999 Sb., zákon o svobodném přístupu k informacím.

[206] Body 14–17 anotovaného rozhodnutí.

[207] Bod 21 anotovaného rozhodnutí, s odvoláním na Nález Ústavního soudu ze dne 17. 1. 2023 sp. zn. Pl. ÚS 25/21.

věrná informace, kterou je potřeba chránit před zásahem do dobré pověsti.[208] Soudy argumentovaly též možností dezinterpretace dat a dalšími riziky.[209] ÚS neshledal argumenty legitimními. Zájem porodnic na ochraně pověsti není rovnocenný ústavně zakotvenému právu na informace. Převaha práva na informace je zjevná i bez provedení testu proporcionality.[210] Ustanovení § 73 odst. 8 zákona o zdravotních službách však není potřeba měnit, protože existuje ústavně konformní výklad.[211]

Ústavní soud zrušil předchozí rozsudky soudů i rozhodnutí správních orgánů.[212] ÚS také konstatoval, že zveřejnění informací o zákrocích a rozsahu jejich provádění v jednotlivých porodnicích je nepochybně ve veřejném zájmu.[213] To bylo ostatně hlavním argumentem stěžovatelky.[214]

Autorka: VPŽ

4. ELEKTRONICKÉ DŮKAZY

NAHRÁVKA HOVORU BEZ SOUHLASU DRUHÉ STRANY JAKO PŘÍPUSTNÝ DŮKAZ V TRESTNÍM ŘÍZENÍ

Soud: Nejvyšší soud
Věc: 7 Tdo 501/2021
Datum: 26. 5. 2021
Dostupnost: nsoud.cz

V dané věci byl obviněný uznán Městským soudem v Brně[215] vinným za přečin pojistného podvodu dle § 210 odst. 1 písm. c) trestního zákoníku (dále

[208] Bod 28 anotovaného rozhodnutí.
[209] Body 7 a 26 anotovaného rozhodnutí.
[210] Body 30–31 anotovaného rozhodnutí.
[211] Bod 38 anotovaného rozhodnutí, Verdikt Ústavního soudu, bod III.
[212] Verdikt Ústavního soudu, body I. a II.
[213] Bod 33 anotovaného rozhodnutí.
[214] Bod 10 anotovaného rozhodnutí.
[215] Rozsudek Městského soudu v Brně ze dne 10. 11. 2020, č. j. 91 T 66/2020-139.

jen „TZ“)[216] a byl mu uložen trest odnětí svobody v délce trvání 3 měsíců s podmíněným odkladem.[217] Pojistného podvodu se dle soudu obviněný dopustil tím, že v listopadu 2019 elektronicky požádal společnost Generali Česká pojišťovna, a. s. (dále jen „pojišťovna“) o vyplacení pojistného plnění z důvodu pojistné události. Jednalo se o úraz pravého kolene s trvalými následky, ke kterému došlo v červnu 2019.[218] V rámci šetření pojistné události proběhl v lednu 2020 mezi obviněným a pracovníkem pojišťovny telefonní hovor, při kterém obviněný nepravdivě uvedl, že se s pravým kolenem v minulosti nikdy neléčil, přestože v roce 2002 podstoupil jeho operaci.[219]

Obviněný podal proti rozsudku odvolání. Soud druhé instance jej však zamítl jako nedůvodné.[220] Následně bylo obviněným podáno dovolání k Nejvyššímu soudu s odůvodněním, že zjištěný skutek nelze považovat za trestný čin, a to z důvodu, že v dané věci nedošlo k naplnění subjektivní stránky trestného činu (tj. zavinění ve formě alespoň nepřímého úmyslu), jelikož v řízení nebylo prokázáno úmyslné sdělení nepravdivé informace při výše zmíněném telefonickém hovoru.[221] Obviněný navíc tvrdil, že trpí poruchami paměti a vzhledem k tomu, že od dané operace uplynulo již 18 let, si ji v daném okamžiku pouze nevybavil, nikoliv ji nezmínil v úmyslu zatajit tuto skutečnost.[222]

V dovolání obžalovaný taktéž namítl, že soud prvního stupně postavil závěr o vině na základě pouze jednoho důkazu, jímž byl výše uvedený telefonický záznam. Obviněný vyslovil pochybnost o splnění zákonných náležitostí tohoto důkazu, jelikož volající (pracovník pojišťovny) mu zřetelně a srozumitelně nesdělil, že je hovor nahráván a taktéž si od obviněného ne-

[216] Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.

[217] Bod č. 2 anotovaného rozhodnutí.

[218] Tamtéž.

[219] Tamtéž.

[220] Usnesení Krajského soudu v Brně dne 2. 2. 2021, č. j. 8 To 13/2021-164.

[221] Bod č. 4 anotovaného rozhodnutí.

[222] Tamtéž.

vyžádal souhlas k pořízení záznamu.[223] Dle tvrzení obviněného byl hovor mimo jiné veden provokativně a útočným záměrem.[224]

Nejvyšší soud dovolání odmítl pro jeho zjevnou neopodstatněnost.[225] Ve vztahu k námitce absence úmyslu dovolací soud uvedl, že obviněný je svéprávnou osobou, která již v minulosti měla zkušenost s uzavíráním pojištění a uplatňování požadavků na plnění z těchto smluv. Obviněný taktéž nemohl být telefonátem zaskočen, jelikož po uplatnění jeho pojistného nároku mohl předpokládat, že pojišťovna bude tyto skutečnosti následně ověřovat, mimo jiné telefonicky. Navíc z nahrávky vyplývá, že obviněného k odpovědi nikdo nenutil, a tudíž mohl uvést, že si na danou skutečnost nevzpomíná, popř. že má problémy s pamětí.[226]

Nejvyšší soud taktéž zkoumal splnění zákonných náležitostí záznamu hovoru, jež byl v řízení použit jako důkaz. Dle odůvodnění soudu je s ohledem na ustanovení § 89 odst. 2 TŘ[227] přípustným důkazním prostředkem i záznam telefonického rozhovoru, který byl pořízen jedním z jeho účastníků bez souhlasu druhého účastníka téhož telefonického rozhovoru. Soud v rámci řízení taktéž zkoumal, zda byl důkaz získán nezákonným donucením nebo hrozbou takového donucení.[228] Nejvyšší soud však dospěl k závěru, že znak nezákonného donucení nelze v obdobné situaci shledat pouze v tom, že volající pracovník pojišťovny explicitně nesdělil obžalovanému, že je hovor nahráván a nedotázal se jej na souhlas s pořízením takového záznamu, a to zejména pokud své postavení a smysl hovoru zřetelně deklaroval a celá komunikace byla zjevně srozumitelná.[229] Nelze se dle soudu ztotožnit ani s námitkou, že byl hovor provokativní s útočným záměrem,

[223] Bod č. 4 anotovaného rozhodnutí.

[224] Tamtéž.

[225] Podle § 265i odst. 1 písm. e) TŘ.

[226] Bod č. 12 anotovaného rozhodnutí.

[227] Dle daného ustanovení *„za důkaz může sloužit vše, co může přispět k objasnění věci, zejména výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání.*“

[228] Dle § 89 odst. 3 TŘ „*Důkaz získaný nezákonným donucením nebo hrozbou takového donucení nesmí být použit v řízení s výjimkou případu, kdy se použije jako důkaz proti osobě, která takového donucení nebo hrozby donucení použila*.“

[229] Bod č. 13 anotovaného rozhodnutí.

pokud si pojišťovna hodlala pouze ověřit poskytnuté informace o pojistné události, u nichž měla pochybnosti o jejich pravdivosti.

Autorka: AKar

ODŮVODNĚNÍ ODPOSLECHŮ A JEHO LIMITY

Soud: Soudní dvůr Evropské unie
Věc: C-349/21
Datum: 16. 2. 2022
Dostupnost: curia.europa.eu

Bulharská prokuratura předložila specializovanému trestnímu soudu žádosti o povolení využití vyšetřovacích prostředků včetně uvedení podstatných důvodů, kterými byla zejména nemožnost získat relevantní důkazy jiným způsobem za účelem odposlechu osob podezřelých ze spáchání závažných trestních činů. Tyto žádosti byly posouzeny předsedou specializovaného trestního soudu. Bylo vydáno povolení odposlechů telefonních hovorů na základě předpřipraveného vzoru, který nicméně v souladu s právní úpravou neobsahoval odkaz na skutkové a právní okolnosti a nebyl individualizován.[230] Důkazy získané z odposlechů byly pak využity v rámci obžaloby jako důkazy pro prokázání účasti na zločinecké skupině, poskytování úplatků a pro další závažné trestné činy.

Bulharský specializovaný trestní soud předkládající Soudnímu dvoru předběžnou otázku v další instanci nejprve posuzoval platnost postupu a zdůraznil, že nelze individualizovaně ověřit důvody konkrétně použité pro nařízení odposlechu. Kladl si ovšem otázku, jestli právě absence individualizovaného odůvodnění (které je ale v souladu s bulharským právem) rozhodnutí není v rozporu s evropskou právní úpravou, a to konkrétně čl. 15 odst. 1 směrnice 2002/58/ES.[231] Taková rozhodnutí pak potenciálně omezují dotčeným osobám práva a svobody zakotvené v Listině základních

[230] Bod 25 odůvodnění.

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

práv a svobod Evropské unie („Listina“) a mohou se dostat do rozporu s evropským právem.[232]

Na základě předchozího bulharský soud položil Soudnímu dvoru předběžnou otázku a dotázal se, jestli je taková praxe bulharských soudů „*podle níž soud povolí sledování, zaznamenávání a uchovávání telefonních hovorů podezřelých osob prostřednictvím předem vypracovaného obecného vzorového textu, ve kterém se bez jakékoli individualizace pouze tvrdí, že byla dodržena zákonná ustanovení*“[233] v souladu s evropskou právní úpravou a jestli pak takové informace mohou být použity v rámci dokazování dané skutkové podstaty.

Soudní dvůr zdůraznil, že povolení odposlechů předchází odůvodněná žádost, včetně důvodu a nutnosti využití a identifikace konkrétních osob.[234] Soud tak rozhodoval na základě odůvodněné a podrobné žádosti i když samotné rozhodnutí odůvodněno nebylo[235]. Zásadní je pak, a to v souladu s čl. 47 Listiny, aby osoba, jíž se odposlech dotýká, byla schopna „*pochopit důvody, proč bylo použití těchto prostředků povoleno, aby mohla případně toto povolení užitečně a účinně napadnout*“[236]. Pokud tedy, přestože rozhodnutí nebylo odůvodněno individualizovaně, je možné, aby daná osoba pochopila důvody a právní okolnosti nařízení odposlechu, stejně tak jako dobu, po který je nařízen, dojde k naplnění zákonných požadavků, pokud takové informace, jakož i absence individualizovaného rozhodnutí budou jednoznačně uvedeny.

Soudní dvůr konstatoval, že daná vnitrostátní praxe není v rozporu s unijní úpravou za situace, kdy podmínky pro nařízení odposlechu mohou být “*snadno a jednoznačně vyvozeny z přečtení rozhodnutí ve vzájemném spojení s žádostí o povolení, přičemž posledně zmíněná žádost musí být po udělení povolení zpřístupněna osobě, vůči které bylo použití zvláštních vyšetřovacích*

[232] Konkrétněji více víz bod 32 odůvodnění.

[233] Bod 34 odůvodnění, první předběžná otázka.

[234] Bod 49 a 50 odůvodnění.

[235] Bod 51 odůvodnění.

[236] Bod 55 odůvodnění.

prostředků povoleno"[237] a tudíž mohou sloužit jako důkaz v rámci řízení. Soudní dvůr tak stanovil, že je v souladu s unijní úpravou, pokud odůvodnění rozhodnutí obsahuje jen dobu platnosti a prohlášení o dodržení zákonných ustanovení (což bylo odůvodněno a konkretizováno v žádosti) a zároveň pokud dané byly schopny pochopit osoby, jichž se rozhodnutí týká a vše jim bylo dostupno. Odůvodnění není nutno obsáhnout v samotném rozhodnutí, ale případně jen v žádosti, což postačuje, pokud se proti ní samotný soud nijak nevymezí (čímž de facto odůvodnění přebírá).

Autor: PL

5. OSTATNÍ

OBJEKTIVNÍ ODPOVĚDNOST OBJEDNATELŮ A FAKTICKÝCH ŠIŘITELŮ ZA ZÁKONNOST ZASÍLÁNÍ OBCHODNÍCH SDĚLENÍ

Soud: Nejvyšší správní soud
Věc: 6 As 18/2022-43
Datum: 16. 3. 2023
Dostupnost: nssoud.cz

Stěžovatelka byla uznána vinnou rozhodnutím Úřadu pro ochranu osobních údajů za to, že v letech 2016 a 2017 šířila obchodní sdělení v rozporu se zákonem[238] – neměla souhlas adresátů a neuváděla totožnost odesílatele a platnou adresu pro odhlášení zasílání obchodních sdělení. Za to jí byla uložena pokuta ve výši 1.400.000 Kč.[239] S rozkladem ani následnou žalobou nebyla stěžovatelka úspěšná.

Nejvyšší správní soud se zabýval třemi námitkami. První je otázka mírnějšího charakteru pozdější úpravy, druhá je nutnost identifikace konkrétní osoby jednající za právnickou osobu pro dovození odpovědnosti

[237] Bod 65 odůvodnění.

[238] A to konkrétně § 11 odst. 1 písm. a), b) a d) zákona č. 480/2004 Sb., o některých službách informační společnosti, ve znění do 30. 6. 2017.

[239] Bod 1 anotovaného rozhodnutí.

a třetí charakter objektivní odpovědnosti. Ani jedna z nich přitom nebyla shledána důvodnou.

Kasační soud neshledal, že by novější právní úprava byla příznivější. Dle rozhodného znění zákona[240] není nutné zjišťovat konkrétní fyzickou osobu, která založila odpovědnost právnické osoby, což navazuje na koncepci objektivní odpovědnosti dle dřívější úpravy.[241] Pozdější úprava tak pro stěžovatelku nebyla z hlediska podmínek odpovědnosti příznivější při stanovování druhu ani výměry trestu.[242] Dále soud konstatoval, že správní spis zcela jasně dokládá šíření reklamních sdělení v rozporu se zákonem.[243] Za to je přitom stěžovatelka objektivně odpovědná, jelikož šiřitelé obchodních sdělení (ať už objednavatelé nebo faktičtí šiřitelé) musí ověřovat, zda rozesílání obchodních sdělení probíhá zákonným způsobem, a to včetně existence souhlasu adresátů.[244] Dlužno dodat, že stěžovatelka velmi obecně namítala i nepřiměřenost pokuty, pročež kasační soud s poukazem na dispoziční zásadu a obecné vypořádání obecných námitek pouze stručně uvedl, že uložená pokuta v první čtvrtině zákonné sazby není excesivní ani likvidační.[245]

Kromě vyvrácení argumentace stěžovatelky prostou aplikací zákonných předpisů tak Nejvyšší správní soud (trochu mimoděk) svým výkladem aproboval rozšiřující výklad objektivní odpovědnosti za distribuci nezákonných obchodních sdělení, a to mimo faktické šiřitele i na objednatele takového šíření, což nemusí být na první pohled ze zákona zřejmé.

Autor: ŠCh

[240] § 20 odst. 6 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich.

[241] Bod 19 anotováno rozhodnutí.

[242] Bod 19 anotováno rozhodnutí.

[243] Bod 22 anotovaného rozhodnutí.

[244] Bod 23 anotovaného rozhodnutí.

[245] Bod 25 anotovaného rozhodnutí.

MOŽNOST SPOLKU POSKYTOVAT SVÝM ČLENŮM INTERNETOVÉ PŘIPOJENÍ JAKO HLAVNÍ ČINNOST

Soud: Nejvyšší správní soud
Věc: 3 Afs 284/2022-99
Datum: 14. 4. 2023
Dostupnost: nssoud.cz

Stěžovatel je zapsaným spolkem, který tisícům svých členů poskytoval – za zaplacení platby označované jako „členský příspěvek“ – připojení k internetu.[246] Správce daně doměřil daň z příjmu právnických osob a penále za zdaňovací období 2014 a 2015.[247]

Hlavní spor spočívá v tom, zda platby za poskytování internetu v podobě „členských příspěvků“ jsou osvobozeny od daně z příjmu či nikoliv.

Nejvyšší správní soud v souladu s recentní judikaturou[248] dospěl k závěru, že stěžovatel při poskytování internetu fakticky vykonává podnikatelskou činnost, a proto příjem podléhá dani z příjmu.[249]

Odůvodnění kasační soud opřel o to, že výjimku[250] z obecného principu zdanění[251] je nutné vykládat restriktivně.[252] Ze spolkového rejstříku a stanov sice vyplývá, že účelem spolku je široký a spočívá v mnoha aktivitách souvisejících s poskytováním přístupu k internetu.[253] K naplňování tohoto účelu ovšem nedocházelo, jelikož stěžovatelova aktivita se omezovala pouze na poskytování připojení k internetu a podstatná většina členů na chodu

[246] Bod 1 a 62 anotovaného rozhodnutí.

[247] Bod 3 anotovaného rozhodnutí. Penále byly následně odvolacím orgánem vypuštěny – viz bod 5 anotovaného rozhodnutí.

[248] Rozsudky Nejvyššího správního soudu ze dne 4. 4. 2023, č. j. 6 Afs 92/2022-51 a z téhož dne č. j. 7 Afs 165/2022-46, na které je poukázáno v bodě 38 anotovaného rozhodnutí.

[249] Bod 57 anotovaného rozhodnutí.

[250] § 19 odst. 1 zákona č. 586/1992 Sb., o daních z příjmů.

[251] § 18 odst. 1 zákona o daních z příjmů.

[252] Bod 39 anotovaného rozhodnutí.

[253] Bod 45 anotovaného rozhodnutí.

spolku nijak neparticipovala,[254] nepočítala s tím,[255] a stěžovatel si toho byl vědom.[256] Jelikož tato činnost stěžovatele a na to navázané příjmy nikterak nepodporovaly jeho hlavní činnost deklarovanou stanovami, nenaplnil stěžovatel podmínky zákona pro osvobození těchto „členských příspěvků" od daně z příjmu.[257] Nejvyšší správní soud v odůvodnění poukázal i na potřebu zachování rovnosti vůči ostatním poskytovatelům internetu.[258]

Již tak není možné obcházet obecné zdanění příjmů tím, že formálně jsou platby za služby poskytované spolkem vykazovány jako členské příspěvky. Na takové příjmy se neaplikuje výjimka. Závěr tohoto rozhodnutí nicméně není, že spolky nemohou poskytovat svým členům přístup k internetu, ale chtějí-li mít členské poplatky osvobozené od daně z příjmu, nesmí jít o jejich hlavní činnost, kterou fakticky zakrývají podnikatelskou činnost.

Autor: ŠCh

[254] Bod 46 anotovaného rozhodnutí.

[255] Bod 48 anotovaného rozhodnutí.

[256] Bod 55 anotovaného rozhodnutí.

[257] Bod 57 anotovaného rozhodnutí.

[258] Bod 62 anotovaného rozhodnutí.

ESSAYS I/2023

CONTENTS

MATCH-FIXING IN TRADITIONAL SPORTS AND E-SPORTS: A COMPARISON OF CONSEQUENCES[1]

ONDŘEJ HÁJEK[2]

1. INTRODUCTION

Thoughts of influencing everything around us are fundamental to the human mind. It is unsurprising that over the years, people have come up with the idea of influencing even sports, especially sports results. Moreover, in recent decades, the influence of sports has developed hand in hand dynamically with the development of betting on sports events, with internet betting being essential.

The importance of online betting was fully demonstrated during the Covid-19 pandemic when it was practically the only way to bet on sporting events during the most significant restrictions.[3] However, the betting world stumbled upon the fact that the whole planet, including sporting events, came to a standstill at the beginning. Unlike traditional sports, e-sports has the advantage that, with few exceptions (potentially gaming

[1] Esej byla zpracována v semestru jaro 2023 v rámci předmětu MVV793K Internet Gaming and Entertainment Law. / The essay was written in the spring 2023 semester for the course MVV793K Internet Gaming and Entertainment Law.

[2] Ondřej Hájek is a student at the Faculty of Law, Masaryk university, contact e-mail: 493819@mail.muni.cz

[3] For example, in the Czech Republic during the so-called first wave, most betting offices closed on their own, in the case of the second wave, this was done on the basis of government resolution. Cf. Resolution No 1332 of the Government of the Czech Republic of 14th December 2020.

houses, boot camps etc.), playing matches at online events[4] has not been restricted due to the risk of infection.

Due to event cancellations and the effort of bookmakers to compensate for these cancellations, e-sport betting has started to receive much more attention than before, both from bookmakers and bettors. For bookmakers, it meant listing brand-new betting opportunities and understanding the games themselves; for bettors, it meant gaining confidence in an area of betting they would otherwise not have paid much attention to it. It meant that much capital went into the area from both sides, where capital naturally attracts the opportunity for its "easy" acquisition by influencing the match.

The author feels the need to highlight this topic, especially given the circumstances in previous paragraphs, where an e-sport match is not far from a potential crime.

In its first chapter, the paper explains the concept of match-fixing and distinguishes it from spot-fixing; in the second chapter, the paper introduces some of the key decisions on the issues fulfilling the "merits" of match-fixing and its consequences in the field of classical sport. In the third chapter, the article will focus on match-fixing in e-sports and its consequences in terms of sanctions. This will be immediately followed by chapter four, where the author will try to compare these consequences from the previous two chapters with each other.

The author intends to use an analytical method mainly concerning existing and decided cases.

2. WHAT IS MATCH-FIXING? AND WHAT IS SPOT-FIXING, THEN?

The central concept throughout the paper is the term match-fixing, for which the critical element is behaviour that leads to influencing matches. This is a very general definition; however, the author considers it practically impossible to define match-fixing in much more detail due

[4] E-sport matches can take two different forms, online and offline. In the first case, players join the game from anywhere, while in the second, everyone plays in the same arena, for example.

to the many ways the result can be influenced. In this sense, the author believes that one of the most concise definitions is the one in the Cambridge Dictionary, which reads as follows: *"dishonest activity to make sure that one team wins a particular sports match."*[5]

One of the more precise definitions then is that of Article 3(4) of the Council of Europe Convention on the Manipulation of Sporting Competitions, which, although it nowhere uses the term match-fixing, is nevertheless close in meaning when it states: *"Manipulation of sports competitions" means an intentional arrangement, act or omission aimed at an improper alteration of the result or the course of a sports competition in order to remove all or part of the unpredictable nature of the aforementioned sports competition with a view to obtaining an undue advantage for oneself or for others."*[6]

The complexity of match-fixing itself and its forms is also represented by its division, where it is impossible to imagine only a betting lobby. However, it is a very significant part. For example, according to Hill, match-fixing in football can be divided into arranged match-fixing and gambling match-fixing.[7] According to the classification in the previous sentence, the first case is explained in more detail by Giel, Dallmeyer, Memmert and Breuer, for example. They stated: *"One party of the contest bribes either (a) the opponent party to underperform or (b) the referee to make biased decisions in its favor. Both actions aim at securing the bribing party's victory ("cheating to win")*.[8] In the second case, Hill sees match-fixing as a way to profit from the betting business.[9] However, the author considers that this classification applies to any sport, definitely to all team sports. Hill's limi-

[5] Cambridge Advanced Learner´s Dictionary & Thesaurus - Match-fixing. *Cambridge University Press* [online]. 2023. [cit. 16. 4. 2023]. Available at: https://dictionary.cambridge.org/dictionary/english/match-fixing

[6] Article 3(4) of the Council of Europe Convention on the Manipulation of Sporting Competitions.

[7] HILL, Declan. Jumping into Fixing. In: *Trends in Organized Crime* [online]. 2015, vol. 3. [cit. 16. 4. 2023]. p. 214-215. Available at: https://link.springer.com/article/10.1007/s12117-014-9237-5

[8] GIEL, Thomas, et al. Corruption and Self-Sabotage in Sporting Competitions – An Experimental Approach to Match-fixing Behavior and the Influence of Deterrence Factors. *Journal of Sports Economics* [online]. 2023, vol. 4. [cit. 16. 4. 2023]. p. 498. Available at: https://journals.sagepub.com/doi/full/10.1177/15270025221134239

tation to football was due to the paper's focus. This opinion is confirmed by Giel, Dallmeyer, Memmert and Breuer, who take this classification as the basis for match-fixing as a whole.[10]

From match-fixing itself, spot-fixing should be strongly distinguished. The Collins Dictionary understands spot-fixing as unfairly influencing a sporting contest without affecting the final result.[11] Several important facts are already apparent from this. Firstly, spot-fixing does not primarily aim to influence a sporting event's overall outcome. However, according to the author, it cannot be ruled out that such indirect influence will occur.

Secondly, suppose spot-fixing targets events not primarily intended to influence the match's outcome. In that case, it means that the above-described way of arranged match-fixing should not apply here because the bribing party is primarily concerned with winning. On the other hand, the second method mentioned above is the right one in this case because it aims to profit from the betting business, where the word "spot" in the term spot-fixing can be understood as single events that can be influenced and on which bookmakers write odds. As an example of such events on which bets can be placed in the betting business, there is a plethora of events depending on the concrete sport - for example, the number of corner kicks or the first throw-in in a football match, the number of penalty minutes in hockey, the number of points scored by players in basketball, or the result of a particular game or a fifteen in tennis.

Thirdly, an individual player can do spot-fixing, especially on occasions such as the first throw-in, etc., effortlessly, even in team sports. It cannot be clearly argued that match-fixing cannot be performed by a single player within a team sport (for example, the goalkeeper in football has, of course,

---

[9] HILL, Declan. Jumping into Fixing. In: *Trends in Organized Crime* [online]. 2015, vol. 3. [cit. 16. 4. 2023]. p. 214-215. Available at: https://link.springer.com/article/10.1007/s12117-014-9237-5

[10] GIEL, Thomas, et al. Corruption and Self-Sabotage in Sporting Competitions – An Experimental Approach to Match-fixing Behavior and the Influence of Deterrence Factors. *Journal of Sports Economics* [online]. 2023, vol. 4. [cit. 16. 4. 2023]. p. 498. Available at: https://journals.sagepub.com/doi/full/10.1177/15270025221134239

[11] Collins English Dictionary - Spot fixing. *HarperCollins Publishers* [online]. 2023. [cit. 16. 4. 2023]. Available at: https://www.collinsdictionary.com/dictionary/english/spot-fixing

a rather significant role in whether the opponent scores), but usually with much more significant complications than in the case of spot-fixing. Spot-fixing is also, in the author's opinion, significantly more challenging to detect in terms of player misconduct, partly because these unique opportunities are monitored to a much lesser extent (to illustrate - try to think about the last football match you watched how many corners were played and whether a strange situation preceded any of them, how the playing team got to it), partly because even a player's "mistake" can occur when he acts differently than he should as a professional. In short, it is not easy to prove intent if there is no evidence of player communication with the betting business.

This paper focuses on match-fixing, the more intensive variant of the two, so it will continue to work only with this concept. However, the author felt the need to distinguish the two key terms of this chapter, partly because of the limited familiarity with spot-fixing and partly afterwards for completeness. Conversely, the author will not distinguish between types of match-fixing in later chapters, where the concept will be pursued in terms of effect rather than cause.

3. MATCH FIXING IN CLASSICAL SPORT

3.1 KEY CASES OF MATCH-FIXING AND ITS CONSEQUENCES

In this chapter, the author will briefly highlight some of the significant cases of match-fixing in the current millennium in the so-called classical sports, focusing primarily on the consequences that have resulted for athletes. In the following subsection, the author will attempt to generalise and summarise these implications in comparison with e-sports in the next chapter.

According to the author, the first case worth mentioning is "The Whistle Scandal", which started in Brazilian football in 2005. This case involved two referees influencing the results to benefit of betting interests in return for payment. In particular, the central figure here was referee Edílson Pereira de Carvalho, who was, among other things, an international referee for

FIFA. His 11 matches in Brazil's top football competition, the Serie A, were annulled by a decision of the Supreme Court of Sporting Justice and subsequently had to be replayed.[12]

As a result, they were both banned for life from professional football[13] and "*accused by the Public Ministry of larceny, conspiracy to commit a crime and fraudulent misrepresentation.*"[14] However, the Court of Justice of São Paulo dismissed the charges because the circumstances indicated that no crime had been committed (due to the absence of a fitting offence).[15] All that remained was an attempt to obtain compensation for "material and moral damages to the fans" through a public civil lawsuit when they were viewed as consumers. In addition, the football associations concerned were also to be held liable for this sum, both at the state and federal levels.[16] Both sports organisations were eventually acquitted by the Superior Tribunal of Justice of Brazil of paying compensation for the 11 cancelled matches.[17]

In response to this case, Law No. 10.671/03 ("Fans' Statute") was subsequently amended, whereby Articles 41C to 41E now contain match-fixing offences with punishments.[18]

---

[12] HOMEWOOD, Brian. Brazilian referee admits that he fixed matches. In: *The Guardian*. [online]. 30. 9. 2005. [cit. 20. 5. 2023]. Available at: https://www.theguardian.com/football/2005/sep/30/newsstory.sport7

[13] ROHTER, Larry. Brazilians May Be Accustomed to Corrupt Officials, but Draw the Line at Soccer Referees. In: The *New York Times* [online]. 11. 10. 2005. [cit. 20. 5. 2023]. Available at: https://www.nytimes.com/2005/10/11/world/americas/brazilians-may-be-accustomed-to-corrupt-officials-but-draw.html

[14] GODINHO, Leticia, Cassio, BARBOSA. Topics for an Academic Agenda: *The* Prevention of Match Fixing in Brazil. In: *Match-Fixing in International Sports: Existing Processes, Law Enforcement, and Prevention Strategies* [online]. 2013. [cit. 20. 5. 2023]. p. 238. Available at: https://www.researchgate.net/publication/286507480_Topics_for_an_Academic_Agenda_The_Prevention_of_Match_Fixing_in_Brazil

[15] Ibidem.

[16] CONSULTOR JURIDICO. The judgment of the Court of First Instance. In: *conjour.com.br* [online].1. 3. 2011. [cit. 20. 5. 2023]. Available at: https://www.conjur.com.br/2011-mar-01/justica-condena-cbf-ex-juiz-empresario-pagar-160-milhoes

[17] VITAL, Danilo. STJ afasta dano moral coletivo por fraude na arbitragem do Brasileiro de 2005. In: conjour.com.br [online]. 27. 10. 2020. [cit. 13. 6. 2023]. Available at: https://www.conjur.com.br/2020-out-27/stj-afasta-dano-moral-coletivo-fraude-brasileirao-2005

[18] Cf. Arcticles 41C to 41E, Law No. 10.671/03 ("Fans' Statute").

Another case the author feels is worth mentioning is this time from the field of individual sport, namely darts. Here it involved two consecutive cases of match-fixing in a short period by two different players, namely Kyle McKinstry and Wessel Nijman. Both of these players fixed matches, McKinstry precisely two and Nijman one, and the Darts Regulation Authority (further as "DRA") received a report on the players based on suspicious bets on their matches. Both players admitted to match-fixing; however, McKinstry only admitted to fixing one of the matches in question and refusing to provide the DRA with his phone details.[19,20]

Nijman was given a 5-year ban by the DRA with the possibility of reducing his sentence by half if he engaged in educational and anti-corruption activities.[21] Despite his denial of influencing one game, McKinstry was found to have influenced both. There was also a violation of the rule on his part by refusing to provide his phone data. His punishment was thus considerably more severe than that imposed in the Nijman case. McKinstry was banned by the DRA for six and a half years for influencing the matches and for a further 18 months for failing to provide data from his phone.[22]

These two examples from darts are given here precisely because, as far as the author is aware, everything has been dealt with within the sports organisation itself or through its intended control mechanisms, not by other legal instruments.

As a final example, the author would like to mention a case that falls more under spot-fixing; however, as clear from the above, it is only a milder form of match-fixing that does not primarily affect the match's outcome.

---

[19] DRA. DRA Statement on Nijman. In: The *Darts Regulation Authority* [online]. 27. 10. 2020. [cit. 20. 5. 2023]. Available at: http://www.thedra.co.uk/dra-update-on-nijman

[20] DRA. Updated DRA Statement – Kyle McKinstry. In: The *Darts Regulation Authority* [online]. 25. 11. 2020. [cit. 20. 5. 2023]. Available at: http://www.thedra.co.uk/updated-dra-statement-kyle-mckinstr

[21] DRA. DRA Statement on Nijman. In: The *Darts Regulation Authority* [online]. 27. 10. 2020. [cit. 20. 5. 2023]. Available at: http://www.thedra.co.uk/dra-update-on-nijman

[22] DRA. Updated DRA Statement – Kyle McKinstry. In: The *Darts Regulation Authority* [online]. 25. 11. 2020. [cit. 20. 5. 2023]. Available at: http://www.thedra.co.uk/updated-dra-statement-kyle-mckinstr

In August 2010, a cricket test match between England and Pakistan was played in London. Sports agent Mazhar Majeed was filmed by undercover reporters providing them with information in return for a cash payment that two Pakistan players would deliberately deliver *no-balls*[23] at some point in the match.[24]

The International Cricket Council has banned three players of the Pakistan team, namely captain Salman Butt and players Mohammad Asif and Mohammad Amir.[25] Butt was banned for ten years, with half of the sentence suspended on the condition that he does not commit further breaches of the code and participates in an anti-corruption programme. Asif was banned for seven years, with two years suspended on the same terms as Butt's sentence. Amir was given a 5-year ban.[26] Subsequently, Butt and Asif's appeal to the Court of Arbitration for Sport in Lausanne did not help either, with both appeals being dismissed.[27,28]

The case did not end there, however, as the Scotland Yard and Crown Prosecution Service took an interest in all three players and sports agent

---

[23] In cricket, the term no ball means a delivery played against the rules. Overstepping typically commits it; however, there are numerous ways to commit a no ball.

[24] CRINCIFO STAFF. Lord's Test at centre of fixing allegations In: *ESPN Cricinfo* [online]. 28. 8. 2010. [cit. 20. 5. 2023]. Available at: https://www.espncricinfo.com/story/lord-s-test-at-centre-of-fixing-allegations-474890

[25] BBC. ICC bans Salman Butt, Mohammad Asif & Mohammad Amir. In: *BBC News Sport* [online]. 5. 2. 2011. [cit. 20. 5. 2023]. Available at: http://news.bbc.co.uk/sport2/hi/cricket/other_international/pakistan/9388422.stm

[26] International Cricket Council ("ICC") v. Salman Butt, Mohammad Asif and Mohammad Amir. [online]. 5. 2. 2011. [cit. 20. 5. 2023]. Available at: http://icc-live.s3.amazonaws.com/cms/media/about_docs/518b6fcd97012-International%20Cricket%20Council%20v%20Salman%20Butt,%20Mohammad%20Asif%20and%20Mohammad%20Amir%20-%20Determination%20of%20the%20independent%20anti-corruption%20tribunal.pdf

[27] Salman Butt v. International Cricket Council (ICC), CAS 2011/A/2364. [online]. 17. 4. 2013. [cit. 24. 5. 2023]. Available at: https://jusmundi.com/en/document/decision/en-salman-butt-v-international-cricket-council-icc-award-wednesday-17th-april-2013-1#decision_9734

[28] Mohammad Asif v. International Cricket Council (ICC), CAS 2011/A/2362. [online].17. 4. 2013. [cit. 24. 5. 2023]. Available at: https://jusmundi.com/en/document/decision/en-mohammad-asif-v-international-cricket-council-icc-award-wednesday-17th-april-2013-1

Mazhar Majeed.[29] On 1 November 2011, they were all found guilty by a jury of conspiracy to cheat at gambling and conspiracy to receive corrupt payments and sentences were handed down at Southwark Crown Court by Judge Cook on 3 November 2011. Butt received a total of 2 years and six months in prison, Amir received a total of six months in a young offenders institution, Asif received a total of 1 year in prison, and Majeed received a total of two years and eight months in prison.[30] Majeed, Amir and Butt were not helped by appeals, all of which were dismissed.[31,32]

To conclude this subchapter, it is appropriate to look at the current situation in the Czech Republic, where the proceeding against Roman Berbr, the former vice-president of the Football Association of the Czech Republic, is ongoing. The prosecution accuses Berbr of being at the top of an organised group that was supposed to influence matches in the Czech Republic's second and third-highest football competitions between 2019 and 2020.[33] The author is, however, fully aware that the presumption of innocence still applies to the current case.

3.2 CONCLUSION ON THE CONSEQUENCES

The examples given in the previous subsection were not chosen at random, as they show that sporting and criminal sanctions can be considered within sports. The question of what sanction will be applied depends on many factors. To some extent, these will be objective factors, such as the scale of the activity in question or the seriousness of the activity, but also factors of

[29] PRESS TRUST OF INDIA. Scotland Yard passes on evidence to prosecutors. In: *NDTV Sports* [online]. 17. 9. 2010. [cit. 24. 5. 2023]. Available at: https://sports.ndtv.com/cricket/scotland-yard-passes-on-evidence-to-prosecutors-1588633

[30] R v Mohammad Amir, Salman Butt. [2011] EWCA Crim 2914. Royal Courts of Justice. [online]. 23. 11. 2011. [cit. 20. 5. 2023]. Available at: https://caselaw.nationalarchives.gov.uk/ewca/crim/2011/2914

[31] Ibidem.

[32] R v Majeed, R v Westfield. [2012] EWCA Crim 1186. Royal Courts of Justice. [online]. 31. 5. 2012. [cit. 20. 5. 2023]. Available at: https://caselaw.nationalarchives.gov.uk/ewca/crim/2012/1186

[33] ČTK. Berbr plzeňskému soudu řekl, že se necítí vinen, vypovídat bude v úterý. In: *České noviny* [online]. 17. 4. 2023. [cit. 20. 5. 2023]. Available at: https://www.ceskenoviny.cz/zpravy/2352711

a less objective nature, such as the public or media coverage of the sport in particular, which in many cases plays a driving role in the process towards punishing athletes.

However, sporting sanctions will outweigh criminal sanctions by many orders of magnitude. For example, in 2022, Sportradar, a company that focuses, among other things, on the detection of match-fixing, recorded 169 sanctions based on the data it audited, of which 154 were sporting sanctions. Only 15 were criminal sanctions.[34] Based on its data, The same company states in its 2021 statistics that there have been 492 sporting sanctions and 50 criminal sanctions over the last 17 years. This is, therefore, a trend where sporting sanctions outnumber criminal ones.[35]

The author considers this fact to be determined by inappropriate constructions of the facts of the offences and then by the circumstance that criminal law operates on the ultima ratio principle, i.e., as the most severe possible sanction for the most serious cases. At the same time, he also considers this is since the proof in criminal proceedings has shifted boundaries compared to the evidence of wrongdoing within sports associations or organisations.

4. MATCH-FIXING IN E-SPORTS

4.1 SOME SPECIFICS OF ESPORTS IN RELATION TO MATCH-FIXING

The author of the text thinks it is appropriate to briefly comment on the specifics of esports and their relation to match-fixing, mainly because the whole work tries to contrast esports with traditional sports.

Firstly, the e-sports industry is a relatively new industry and is experiencing a surge of interest from the media, sponsors, and fans. As part of this growth, people who see this as an opportunity to make a quick buck are naturally tapping into the industry. This view is shared, for example, by Oskar

[34] SPORTRADAR. Betting Corruption and Match-Fixing in 2021: A review by Sportradar Integrity Services. In: *Sportradar* [online]. 03/2022. [cit. 20. 5. 2023]. p. 13. Available at: https://goto.sportradar.com/SR_Betting_Corruption_and_Match-Fixing_in_2021

[35] Ibidem, p. 19.

Fröberg, the Founder and CEO of esports data provider Abios.[36] The risk of match-fixing is thus not negligible from the start.

Secondly, e-sports are quite necessarily related to technology to a much greater extent than any traditional sport, which can be both an advantage and a disadvantage compared to conventional sports. The author considers that games as such, to which e-sports are subsequently linked, have brought with them an entirely new way of match-fixing, namely cheats. Cheats, of course, aim to affect at least the player's performance, but in most cases, they have the potential to affect the outcome of the entire game.[37]

Lastly, the author considers that in contrast to traditional sports, where people already perceive match-fixing and influencing matches in general as a relatively severe problem that can occasionally be subject to criminal sanctions, this is not the case in electronic sports. The author has the impression that one part of the public still does not understand e-sports. The other part still sees around it a kind of aura of "just a game", where they do not consider match-fixing in e-sports as such a problem that should be solved by criminal sanctions (or maybe significant sanctions in general).

There is, of course, a significant difference within continents, where the Asian world, which is the hegemon in the gaming world,[38] has been able to adapt and works quite well within national organisations. Of particular note is the Korean e-Sports Association (KeSPA), which works closely with government agencies.[39]

---

[36] Abios: Combatting match-fixing and cheating in esports is crucial. In: *Esports Insider* [online]. 18. 1. 2022. [cit. 27. 5. 2023]. Available at: https://esportsinsider.com/2022/01/abios-combatting-match-fixing-and-cheating-in-esports-is-crucial

[37] SCHÖBER, Timo, Georg, STADTMANN. The dark side of e-sports – An analysis of cheating, doping & match-fixing activities and their countermeasures. *International Journal of Esports* [online]. 23. 7. 2022, vol. 1, issue no. 1. [cit. 27. 5. 2023]. Available at: https://www.ijesports.org/article/98/html

[38] CHEEMA, Sukhbir. The world's largest internet gamers: 4 Southeast Asian nations dominate top spots. In: *Mashable SEA* [online]. 5. 10. 2022. [cit. 27. 5. 2023]. Available at: https://sea.mashable.com/life/21530/the-worlds-largest-internet-gamers-4-southeast-asian-nations-dominate-top-spots

[39] SCHÖBER, Timo, Georg, STADTMANN. The dark side of e-sports – An analysis of cheating, doping & match-fixing activities and their countermeasures. *International Journal of Esports* [online]. 23. 7. 2022, vol. 1, issue no. 1. [cit. 27. 5. 2023]. Available at: https://www.ijesports.org/article/98/html

The international organisation Esports Integrity Commission (ESIC) is also worth mentioning here. Still, the main problem is that large video game companies that also act as event organisers (such as Riot Games) are not members.[40]

4.2 KEY CASES OF MATCH-FIXING AND ITS CONSEQUENCES

The first high-profile case that received much media attention was the 2010 StarCraft match-fixing case. In this case, a total of 14 people were accused of influencing the results in exchange for financial sums. According to the official investigation, the betting turnover made by this match-fixing reached up to 140 million South Korean Won (over $123 000). The case was particularly significant because it was the first confirmed case of match-fixing by professional gamers in the country of e-sports and gaming in general, South Korea.[41]

In response, there were severe punishments that did not just stay at the sporting level. A lifetime ban from the Korean pro-gaming scene was handed out to 11 players by the KeSPA,[42] and some players got fines ranging from 2 to 12.5 million South Korean Won. Two players were then given community service sentences of 120 hours, and two players were given mandatory participation in gambling treatment of 40 hours, among other penalties. There were also four suspended prison sentences, two for six months with a probationary period of one year, one for 12 months with a probationary period of two years, and one for 18 months with a probationary period of three years.[43]

---

[40] ESIC. Members & Supporters. [online]. 2023. [cit. 20. 5. 2023]. Available at: https://esic.gg/members/

[41] YONHAP NEWS AGENCY. Prosecutors charge 14 people in StarCraft match-fixing scandal. In: *Yonhap News Agency* [online]. 16. 5. 2010. [cit. 27. 5. 2023]. Available at: https://en.yna.co.kr/view/AEN20100516001000320

[42] GOSU GAMERS. sAviOr admits to match-fixing. In: *Gosu Gamers* [online]. 25. 6. 2010. [cit. 27. 5. 2023]. Available at: https://www.gosugamers.net/news/12308-savior-admits-to-match-fixing

[43] Match Fixing Scandal. In: Liquipedia.net [online]. 10. 4. 2019. [cit. 27. 5. 2023]. Available at: https://liquipedia.net/starcraft/Match_Fixing_Scandal

Another interesting case to point out is the case of Alexey Berezin, known by his Dota2 game nickname "Solo". He was caught betting $100 against his team in 2013, and then his team lost, with his performance described as "suspiciously horrible". However, it was a game where neither team cared about anything, as advancement was no longer possible for either team.[44]

Only sporting sanctions were applied here, and these were later reduced. Solo was banned for life, his teammates for three years, and the organisation under which the players played for one year.[45] As noted, Solo's sanction was eventually reduced to one year while at the same time acknowledging that it was the individual player's misconduct, not the entire organisation, which was cleared.[46] However, even this did not do much for the athlete himself, as the gaming organisation decided not to continue Solo within the team.[47]

The 2012 MLG Summer Championship final in League of Legends was also very controversial. Two North American teams, "Dignitas" and "Team Curse," made it to the finals. Five games were played under the Best of 5 rules in the finals, and Team Curse won. After a Team Curse player confessed, it was discovered that there was an agreement between the teams before the series began. This caused, among other things, the series' first game to be played non-standardly.[48]

The tournament organisers responded to this discovery by disqualifying both teams. At the same time, the teams were stripped of their prize money and points earned during the tournament, which were subsequently alloca-

[44] SCHUMACHER, Dennis. Update: roX.KIS issues statement. In: *JoinDOTA* [online]. 15. 6. 2013. [cit. 27. 5. 2023]. Available at: https://www.joindota.com/news/9989-update-rox-kis-issues-statement

[45] Ibidem.

[46] GOSU GAMERS. Solo's Starladder ban reduced to one year. In: *Gosu Gamers* [online]. 23. 6. 2013. [cit. 27. 5. 2023]. Available at: https://www.gosugamers.net/dota2/news/24589-solo-s-starladder-ban-reduced-to-one-year

[47] "SUN_TZU". Solo out of RoX.KiS. In: *JoinDOTA* [online]. 21. 6. 2013. [cit. 27. 5. 2023]. Available at: https://www.joindota.com/news/10165-solo-out-of-rox-kis

[48] HAFER, Leana. Top two League of Legends teams from MLG Summer disqualified for "collusion". In: *PC Gamer* [online]. 27. 8. 2012. [cit. 27. 5. 2023]. Available at: https://www.pcgamer.com/top-two-league-of-legends-teams-from-mlg-summer-disqualified-for-collusion/

ted to teams from third place downwards.[49] The problem with this behaviour, however, is mainly the fact that the removal of points and prize money was the only legal consequence in this case, so the punitive nature did not manifest itself much.[50]

On this point, the author will allow himself only a small personal remark. Criminal law is indeed the instrument of the ultima ratio, as the author has already stated in the previous text. Thus, if other legal (or semi-legal in the form of sporting penalties) instruments are sufficient, criminal sanctions should not necessarily be resorted to. However, what is to be distinguished in the above case is that a "mere disqualification" resulted in the loss of funds and points from the tournament in question. Unlike a "ban" from subsequent tournaments, disqualification does not preclude a team from participating in future tournaments. In addition, the team lost funds and points it had earned in the tournament (although it is necessary to have the results for this). Thus, the author wonders how much effect the above punishment has in terms of the other teams that did not achieve the funds and points by their performance (for example, the team "TEAM4NOT.NA" in the above tournament). In other words, if fraudulent behaviour occurs (which is probably the closest to the above), would it be classified as a sufficient punishment for the perpetrators that the funds that were fraudulently stolen be returned to the victims? The author believes that such a penalty is wholly insufficient.

The author has chosen a recent case as a final example of match-fixing in e-sports. Malcolm Chung Wai Kiat, known within VALORANT as "germsg", was the captain of the Resurgence team that participated in the Epulze Royal SEA Cup in September 2020. Germsg's friend and teammate advised him to bet on his loss and deliberately lose to secure the money from the bet. Since germsg saw no other way to get the money from his friend

[49] Ibidem.

[50] MARTIN, Alan. Fair play and fixing: The growing pains of eSports. In: *RedBull.com* [online]. 2. 8. 2016. [cit. 27. 5. 2023]. Available at: https://www.redbull.com/int-en/fair-play-and-fixing-the-growing-pains-of-esports

who owed him money, he decided to use his intentional loss idea. Moreover, as captain, the team obeyed him without any problem.[51]

As a consequence, both players were banned for three years from all Valorant Champions Tour events by RIOT Games as the owner and developer of VALORANT.[52] On 26 May 2023, germsg was sentenced to 4 months in prison for one of the charges when he pleaded guilty to accepting payments in violation of the Prevention of Corruption Act. At the same time, another charge of acting against the Remote Gambling Act was considered. His friend and the team member who instigated the said conduct was sentenced to a minimum of 6 months of reformative training a day earlier after pleading guilty.[53]

However, at the end of this section, there are positive cases where teams or individuals have rejected match-fixing. For example, the case from the 2020 ESL ONE Germany tournament in DOTA 2, where match-fixers contacted players before the elimination matches, can be seen as evidence. Three players were offered 1 000 000 rubles, roughly 13 000 US dollars. This is even more than the prize money a team receives for finishing in the top 8 in that tournament. Instead of accepting here, there was a rejection and publication of said offer, which is the right approach.[54]

---

[51] WI-LIAM, Teh. Team captain of Resurgence, Germsg jailed after being found guilty of match-fixing. In: *Gosu Gamers* [online]. 26. 5. 2023. [cit. 27. 5. 2023]. Available at: https://www.gosugamers.net/valorant/news/68171-team-captain-of-resurgence-germsg-jailed-after-being-found-guilty-of-match-fixing

[52] DAS, Abhimannu. Riot Games Hands Three-Year Ban to "germsg" and "Dreamycsgo" for Match-Fixing in Valorant. In: *AFK Gaming* [online]. 17. 6. 2021. [cit. 27. 5. 2023]. Available at: https://afkgaming.com/esports/news/riot-games-hands-three-year-ban-to-germsg-and-dreamycsgo-for-match-fixing-in-valorant

[53] CHAI, Ruth. S'porean Valorant team captain, 24, jailed for match-fixing to win gambling bets. In: *Mothership* [online]. 27. 5. 2023. [cit. 27. 5. 2023]. Available at: https://mothership.sg/2023/05/spore-valorant-pro-gamers-throw-match-jail/

[54] CHEN, Patrik. Matchfixers offer $13,000 to Yellow Submarine Players during ESL One Germany. In: *esports.com* [online]. 20. 10. 2020. [cit. 27. 5. 2023]. Available at: https://www.esports.com/en/matchfixers-offer-13000-to-yellow-submarine-players-during-esl-one-germany-138830

4.3 CONCLUSION ON THE CONSEQUENCES

In the previous subsection, the author tried to summarise some essential cases or, according to the author, interesting for the world of e-sports, again mainly in the direction of consequences. The author feels that he has again found examples for all sorts of sanctions and non-sanctions, both sporting and criminal.

The author considers that there is a great inconsistency in imposing penalties for these actions. This is mainly due to the widely differing legal provisions. While Asian countries can punish the conduct in question quite harshly, if necessary, with criminal sanctions, which is due, among other things, to the fact that e-sports and gaming, in general, are an idol for them, criminal sanctions are not applied in the vast majority of countries. Punishment is thus referred to as the sporting level, which may or may not be sufficient. Again, as in the case of traditional sports, this depends on the circumstances of individual cases, and the author believes that the imposition of sanctions should never operate as a generalised process without considering the specifics of the case.

5. SO IS THERE A DIFFERENCE BETWEEN THE CONSEQUENCES?

If the author has to consider whether the sanctions for match-fixing are different in traditional sports and e-sports, the first thought that comes to his mind is that they are not in general. He considers that both parts have to deal with very similar problems.

In general, the author feels that, in principle, sports sanctions can handle both sectors reasonably well, where this should be an automatic consequence naturally. However, in the most severe cases, which would also require, for example, the use of criminal law resources, the said conduct often encounters an inability to fit the said conduct under the facts of the offence.

A kind of shyness about criminal law is evidenced, among other things, by the fragmentation of how the issue is viewed by criminal law demonstrated by comparison by KEA European affairs. However, this is somewhat

older material, and the author feels that he is still able to show the problem more clearly.[55] In the Czech Republic, for example, match-fixing is dealt with mainly under § 331-334 of the Criminal Code, where the vague term "a matter of general interest" used here has been interpreted by the courts to mean that sports (specifically football) can also be subsumed under that term.[56] The author does not dispute the inclusion of sports. However, he wonders a little whether gaming (the essence of e-sports) would also fall easily within the definition.

Thus, the author asks whether it is not better to go the route of particular facts than to subordinate match-fixing to the existing general ones. The author believes that, at least from the point of view of prevention, this would have a better chance of working because it would be quite clear what the norm punishes. The potential perpetrator would be more easily aware that the norm punishes the conduct.

At the same time, the author points to the fragmentation in the form of punishments, where different offences under which match-fixing is classified provide other punishments, which according to the author, is only partially appropriate. However, criminal policy is, of course, a matter for individual states.

Shared problems also remain when it comes to proving match-fixing itself, as there are almost infinitely many influences that can affect performance without the behaviour being match-fixing. Thus, in both sectors, one has to rely mainly on the movement of the money in the betting markets or on leaked conversations where the conduct in question is arranged.

However, subtle differences between the consequences are apparent at a glance. First of all, it is necessary to mention that, unlike traditional sports, e-sports have the advantage of being able to skip the historical search for the right solution and make extensive use of those that already exist. It

[55] KEA. Match-fixing in sport: A mapping of criminal law provisions in EU 27. *KEA European Affairs* [online]. 3. 2012. [cit. 20. 5. 2023]. p. 23 - 38 Available at: https://ec.europa.eu/assets/eac/sport/library/studies/study-sports-fraud-final-version_en.pdf

[56] GANGER, Jiří. Match fixing a jeho trestněprávní aspekty. diplomová práce, *Právnická fakulta Masarykovy university* [online]. 2018. [cit. 28. 5. 2023]. p. 47. Available at: https://is.muni.cz/auth/th/rv3ds/430831_Ganger_Jiri_Diplomova_prace_final.pdf

is also worth mentioning the opposite view, namely that criminal law was beginning to adapt in part in individual states, which also took time, and e-sports came into a period when this adaptation process was already underway.

It is clear from this that e-sports have set a much higher bar compared to traditional sports much earlier and usually punish offences quite strictly. Still, the question is how the process would have looked if they had not come into at least partially adapted legislation. Also significant, according to the author, is the fact that e-sports are partly forced to behave in this way due to fears about their PR, where they are far from having the position of traditional sports, and hesitation could damage them significantly.

The author considers that the most significant difference between these consequences is that within e-sports, there is a highly fragmented state of who imposes sporting sanctions. If we take traditional sports, it will almost always be the sporting association within which the offence occurred (e.g., the Disciplinary Commission of the Football Association of the Czech Republic). In contrast, in the case of e-sports, it is a kind of strange combination where some sporting sanctions are imposed by national associations where they exist (e.g., KeSPA). However, sporting sanctions are also imposed by the tournament organisers themselves if the sporting sanctions relate to their tournaments (e.g., a ban on participation in those tournaments). In addition, some sporting sanctions are imposed by the game's owner and its developer (e.g., RIOT Games). If we add to this the different games, which will be different for each, it is a highly fragmented structure. The author believes that this fragmentation is very detrimental to e-sports.

However, according to the author, it is undeniable that the consequences of match-fixing in sports and e-sports are very similar and cannot be easily distinguished from each other.

6. CONCLUSION

The author of the text tried to compare the consequences of match-fixing in classical sports with the consequences of match-fixing in esports. For this purpose, in the first chapter, he first discussed what match-fixing is and

stopped at its distinction from spot-fixing. Then, in the next chapter, he focused on selected well-known match-fixing cases and their consequences, first discussing these in the first part and then summarising the consequences in general in the second part. In the third chapter, the same has been done for match-fixing in the case of e-sports, with the difference that in the introduction of this chapter, certain specifics that the author believes apply to e-sports have been defined.

The fourth and final substantive chapter then attempted to compare the implications of the cases within the second and third chapters and to draw out the differences in the punishment of match-fixing in the sporting and e-sports environment.

The author considers that the text concludes that there are significant similarities between the sanctions imposed in traditional sports and e-sports. The distinction between the two is made concerning region and context of circumstances, with only hardly noticeable differences compared to the similarities.

7. BIBLIOGRAPHY

[1] "SUN_TZU". Solo out of RoX.KiS. In: *JoinDOTA* [online]. 21. 6. 2013. [cit. 27. 5. 2023]. Available at: https://www.joindota.com/news/10165-solo-out-of-rox-kis

[2] ABIOS. Abios: Combatting match-fixing and cheating in esports is crucial. In: *Esports Insider* [online]. 18. 1. 2022. [cit. 27. 5. 2023]. Available at: https://esportsinsider.com/2022/01/abios-combatting-match-fixing-and-cheating-in-esports-is-crucial

[3] BBC. ICC bans Salman Butt, Mohammad Asif & Mohammad Amir. In: *BBC News Sport* [online]. 5. 2. 2011. [cit. 20. 5. 2023]. Available at: http://news.bbc.co.uk/sport2/hi/cricket/other_international/pakistan/9388422.stm

[4] Cambridge Advanced Learner's Dictionary & Thesaurus -Match-fixing. *Cambridge University Press* [online]. 2023. [cit. 16. 4. 2023]. Available at: https://dictionary.cambridge.org/dictionary/english/match-fixing

[5] CHAI, Ruth. S'porean Valorant team captain, 24, jailed for match-fixing to win gambling bets. In: *Mothership* [online]. 27. 5. 2023. [cit. 27. 5. 2023]. Available at: https://mothership.sg/2023/05/spore-valorant-pro-gamers-throw-match-jail/

[6] CHEEMA, Sukhbir. The world's largest internet gamers: 4 Southeast Asian nations dominate top spots. In: *Mashable SEA* [online]. 5. 10. 2022. [cit. 27. 5. 2023]. Available at: https://sea.mashable.com/life/21530/the-worlds-largest-internet-gamers-4-southeast-asian-nations-dominate-top-spots

[7] CHEN, Patrik. Matchfixers offer $13,000 to Yellow Submarine Players during ESL One Germany. In: *esports.com* [online]. 20. 10. 2020. [cit. 27. 5. 2023]. Available at: https://www.esports.com/en/matchfixers-offer-13000-to-yellow-submarine-players-during-esl-one-germany-138830

[8] Collins English Dictionary - Spot fixing. *HarperCollins Publishers* [online]. 2023. [cit. 16. 4. 2023]. Available at: https://www.collinsdictionary.com/dictionary/english/spot-fixing

[9] CONSULTOR JURIDICO. the judgment of the Court of First Instance. In: *conjour.com.br* [online].1. 3. 2011. [cit. 20. 5. 2023]. Available at: https://www.conjur.com.br/2011-mar-01/justica-condena-cbf-ex-juiz-empresario-pagar-160-milhoes

[10] CRINCIFO STAFF. Lord's Test at centre of fixing allegations In: *ESPN Cricinfo* [online]. 28. 8. 2010. [cit. 20. 5. 2023]. Available at: https://www.espncricinfo.com/story/lord-s-test-at-centre-of-fixing-allegations-474890

[11] ČTK. Berbr plzeňskému soudu řekl, že se necítí vinen, vypovídat bude v úterý. In: *České noviny* [online]. 17. 4. 2023. [cit. 20. 5. 2023]. Available at: https://www.ceskenoviny.cz/zpravy/2352711

[12] DAS, Abhimannu. Riot Games Hands Three-Year Ban to "germsg" and "Dreamycsgo" for Match-Fixing in Valorant. In: *AFK Gaming* [online]. 17. 6. 2021. [cit. 27. 5. 2023]. Available at: https://afkgaming.com/esports/news/riot-games-hands-three-year-ban-to-germsg-and-dreamycsgo-for-match-fixing-in-valorant

[13] DRA. DRA Statement on Nijman. In: The *Darts Regulation Authority* [online]. 27. 10. 2020. [cit. 20. 5. 2023]. Available at: http://www.thedra.co.uk/dra-update-on-nijman

[14] DRA. Updated DRA Statement – Kyle McKinstry. In: The *Darts Regulation Authority* [online]. 25. 11. 2020. [cit. 20. 5. 2023]. Available at: http://www.thedra.co.uk/updated-dra-statement-kyle-mckinstr

[15] ESIC. Members & Supporters. [online]. 2023. [cit. 20. 5. 2023]. Available at: https://esic.gg/members/

[16] GANGER, Jiří. Match fixing a jeho trestněprávní aspekty. diplomová práce, *Právnická fakulta Masarykovy university* [online]. 2018. [cit. 28. 5. 2023]. Available at: https://is.muni.cz/auth/th/rv3ds/430831_Ganger_Jiri_Diplomova_prace_final.pdf

[17] GIEL, Thomas, et al. Corruption and Self-Sabotage in Sporting Competitions – An Experimental Approach to Match-fixing Behavior and the Influence of Deterrence Factors. *Journal of Sports Economics* [online]. 2023, vol. 4. [cit. 16. 4. 2023]. p.497–525. Available at: https://journals.sagepub.com/doi/full/10.1177/15270025221134239

[18] GODINHO, Leticia., BARBOSA, Cassio. Topics for an Academic Agenda: The Prevention of Match Fixing in Brazil. In: *Match-Fixing in International Sports: Existing Processes, Law Enforcement, and Prevention Strategies* [online]. 2013. [cit. 20. 5. 2023]. p. 229 – 245. Available at: https://www.researchgate.net/publication/286507480_Topics_for_an_Academic_Agenda_The_Prevention_of_Match_Fixing_in_Brazil

[19] GOSU GAMERS. sAviOr admits to match-fixing. In: *Gosu Gamers* [online]. 25. 6. 2010. [cit. 27. 5. 2023]. Available at: https://www.gosugamers.net/news/12308-savior-admits-to-match-fixing

[20] GOSU GAMERS. Solo's Starladder ban reduced to one year. In: *Gosu Gamers* [online]. 23. 6. 2013. [cit. 27. 5. 2023]. Available at: https://www.gosugamers.net/dota2/news/24589-solo-s-starladder-ban-reduced-to-one-year

[21] HAFER, Leana. Top two League of Legends teams from MLG Summer disqualified for "collusion". In: *PC Gamer* [online]. 27. 8. 2012. [cit. 27. 5. 2023]. Available at: https://www.pcgamer.com/top-two-league-of-legends-teams-from-mlg-summer-disqualified-for-collusion/

[22] HILL, Declan. Jumping into Fixing. In: *Trends in Organized Crime* [online]. 2015, vol. 3. [cit. 16. 4. 2023]. p.212-228. Available at: https://link.springer.com/article/10.1007/s12117-014-9237-5

[23] HOMEWOOD, Brian. Brazilian referee admits that he fixed matches. In: The *Guardian*. [online]. 30. 9. 2005. [cit. 20. 5. 2023]. Available at: https://www.theguardian.com/football/2005/sep/30/newsstory.sport7

[24] International Cricket Council ("ICC") v. Salman Butt, Mohammad Asif and Mohammad Amir. [online]. 5. 2. 2011. [cit. 20. 5. 2023]. Available at: http://icc-live.s3.amazonaws.com/cms/media/about_docs/518b6fcd97012-International%20Cricket%20Council%20v%20Salman%20Butt,%20Mohammad%20Asif%20and%20Mohammad%20Amir%20-%20Determination%20of%20the%20independent%20anti-corruption%20tribunal.pdf

[25] KEA. Match-fixing in sport: A mapping of criminal law provisions in EU 27. *KEA European Affairs* [online]. 3. 2012. [cit. 20. 5. 2023]. Available at: https://ec.europa.eu/assets/eac/sport/library/studies/study-sports-fraud-final-version_en.pdf

[26] MARTIN, Alan. Fair play and fixing: The growing pains of eSports. In: *RedBull.com* [online]. 2. 8. 2016. [cit. 27. 5. 2023]. Available at: https://www.redbull.com/int-en/fair-play-and-fixing-the-growing-pains-of-esports

[27] Match Fixing Scandal. In: *Liquipedia.net* [online]. 10. 4. 2019. [cit. 27. 5. 2023]. Available at: https://liquipedia.net/starcraft/Match_Fixing_Scandal

[28] Mohammad Asif v. International Cricket Council (ICC), CAS 2011/A/2362. [online].17. 4. 2013. [cit. 24. 5. 2023]. Available at: https://jusmundi.com/en/document/decision/en-mohammad-asif-v-international-cricket-council-icc-award-wednesday-17th-april-2013-1

[29] PRESS TRUST OF INDIA. Scotland Yard passes on evidence to prosecutors. In: *NDTV Sports* [online]. 17. 9. 2010. [cit. 24. 5. 2023]. Available at: https://sports.ndtv.com/cricket/scotland-yard-passes-on-evidence-to-prosecutors-1588633

[30] R v Majeed, R v Westfield. [2012] EWCA Crim 1186. Royal Courts of Justice. [online]. 31. 5. 2012. [cit. 20. 5. 2023]. Available at: https://caselaw.nationalarchives.gov.uk/ewca/crim/2012/1186

[31] R v Mohammad Amir, Salman Butt. [2011] EWCA Crim 2914. Royal Courts of Justice. [online]. 23. 11. 2011. [cit. 20. 5. 2023]. Available at: https://caselaw.nationalarchives.gov-.uk/ewca/crim/2011/2914

[32] ROHTER, Larry. Brazilians May Be Accustomed to Corrupt Officials, but Draw the Line at Soccer Referees. In: The *New York Times* [online]. 11. 10. 2005. [cit. 20. 5. 2023]. Available at: https://www.nytimes.com/2005/10/11/world/americas/brazilians-may-be-accustomed-to-corrupt-officials-but-draw.html

[33] Salman Butt v. International Cricket Council (ICC), CAS 2011/A/2364. [online]. 17. 4. 2013. [cit. 24. 5. 2023]. Available at: https://jusmundi.com/en/document/decision/en-salman-butt-v-international-cricket-council-icc-award-wednesday-17th-april-2013-1#decision_9734

[34] SCHÖBER, Timo, Georg, STADTMANN. The dark side of e-sports – An analysis of cheating, doping & match-fixing activities and their countermeasures. *International Journal of Esports* [online]. 23. 7. 2022, vol. 1, issue no. 1. [cit. 27. 5. 2023]. Available at: https://www.ijesports.org/article/98/html

[35] SCHUMACHER, Dennis. Update: roX.KIS issues statement. In: *JoinDOTA* [online]. 15. 6. 2013. [cit. 27. 5. 2023]. Available at: https://www.joindota.com/news/9989-update-rox-kis-issues-statement

[36] SPORTRADAR. Betting Corruption and Match-Fixing in 2021: A review by Sportradar Integrity Services. In: *Sportradar* [online]. 3. 2022. [cit. 20. 5. 2023]. Available at: https://goto.sportradar.com/SR_Betting_Corruption_and_Match-Fixing_in_2021

[37] VITAL, Danilo. STJ afasta dano moral coletivo por fraude na arbitragem do Brasileiro de 2005. In: conjour.com.br [online]. 27. 10. 2020. [cit. 13. 6. 2023]. Available at: https://www.conjur.com.br/2020-out-27/stj-afasta-dano-moral-coletivo-fraude-brasileirao-2005

[38] WI-LIAM, Teh. Team captain of Resurgence, Germsg jailed after being found guilty of match-fixing. In: *Gosu Gamers* [online]. 26. 5. 2023. [cit. 27. 5. 2023]. Available at: https://www.gosugamers.net/valorant/news/68171-team-captain-of-resurgence-germsg-jailed-after-being-found-guilty-of-match-fixing

[39] YONHAP NEWS AGENCY. Prosecutors charge 14 people in StarCraft match-fixing scandal. In: *Yonhap News Agency* [online]. 16. 5. 2010. [cit. 27. 5. 2023]. Available at: https://en-.yna.co.kr/view/AEN20100516001000320

THE TOGGLEABLE FILTER BUBBLE: PERSONALIZED INFORMATION ON AN OPT-IN BASIS[57]

VOJTĚCH JUŘIČKA[58]

1. INTRODUCTION

We now live in an increasingly digitized society. As the internet has made sharing and seeking information more effortless than ever, people spend more and more time there searching for various information, be it for education or entertainment. The information that can be found there varies significantly in type and quality. As such, filtering of the information has been introduced. This can be mainly seen in search engines such as Google, which automatically select webpages to add to their index, from which the search results are picked out.[59] Similarly, social media personalize the feed that is shown to the user through a scoring system managed by an algorithm using machine learning.[60] The term *filter bubble* was first introduced by Eli Pariser,[61] and since then, filter bubbles, echo chambers, algori-

[57] Esej byla zpracována v semestru podzim 2022 v rámci předmětu MVV1368K Privacy and Personal Data Law. / The essay was written in the autumn 2022 semester for the course MVV1368K Privacy and Personal Data.

[58] Vojtěch Juřička is a student at the Faculty of Law, Masaryk university, contact e-mail: 480557@mail.muni.cz

[59] GOOGLE. In-depth guide to how Google Search works. *Google Search Central* [online]. 2022. [cit. 10. 12. 2022]. Available at: https://developers.google.com/search/docs/fundamentals/how-search-works

[60] FACEBOOK. Good Questions, Real Answers: How Does Facebook Use Machine Learning to Deliver Ads? *Facebook Business* [online]. 2022. [cit. 10. 12. 2022]. Available at: https://www.facebook.com/business/news/good-questions-real-answers-how-does-facebook-use-machine-learning-to-deliver-ads

[61] FARNAM STREET. How Filter Bubbles Distort Reality: Everything You Need to Know. In: *Fs.blog* [online]. 2022. [cit. 10. 12. 2022]. Available at: https://fs.blog/filter-bubbles/

thmic personalization, and similar topics have been the subject of public debate.

The main concern mentioned regarding these topics is the informational isolation of an individual resulting in narrow access to different sources and perspectives, which strengthens the individual's own opinions.[62] This can lead to a polarization of society, creating several hostile groups of people which are unable to reach common ground on a specific topic. This is also referred to as *Cyberbalkanization*.[63] Albeit the aforementioned topics are often debated, divisive opinions exist regarding their severity or even existence.[64] This essay aims to explore the idea of whether the phenomenon of filter bubbles should be regulated through an opt-in or opt-out system.

2. TERMINOLOGY

First and foremost, it is necessary to define the term *filter bubble*. The term is often interchanged with another term, *echo chamber*, so these two will be described together. Bruns states that a filter bubble is created when a group of people chooses to prefer communication with each other and thus excludes outsiders.[65] On the other hand, Fletcher defines a filter bubble as a result of algorithmic filtering, where news that a person dislikes or disagrees with is filtered out, resulting in a narrow scope of information reaching the person.[66]

An echo chamber, according to Bruns, is a situation where a group of people choose to prefer connection with each other and thus exclude other

---

[62] FLETCHER, Richard. The truth behind filter bubbles: Bursting some myths. In: *Reuters Institute for the Study of Journalism* [online]. 2020. [cit. 10. 12. 2022]. Available at: https://reutersinstitute.politics.ox.ac.uk/news/truth-behind-filter-bubbles-bursting-some-myths

[63] BOZDAG, Engin. VAN DEN HOVEN, Jeroen. Breaking the filter bubble: democracy and design. *Ethics and Information Technology* [online]. 18. 12. 2015, no. 17. [cit. 10. 12. 2022]. p. 249-265. Available at: https://link.springer.com/content/pdf/10.1007/s10676-015-9380-y.pdf?pdf=button

[64] BRUNS, Axel. Filter bubble. *Internet Policy Review* [online]. 29. 11. 2019, vol. 8, no. 4. [cit. 10. 12. 2022]. Available at: https://policyreview.info/concepts/filter-bubble

[65] Ibidem.

[66] FLETCHER, Richard. The truth behind filter bubbles: Bursting some myths. In: *Reuters Institute for the Study of Journalism* [online]. 2020. [cit. 10. 12. 2022]. Available at: https://reutersinstitute.politics.ox.ac.uk/news/truth-behind-filter-bubbles-bursting-some-myths

people.[67] Fletcher's definition of echo chambers is a state where exposition to liked and agreeable news distorts the perception of reality, resulting in a belief that reality only consists of agreeable news. That disagreeable news does not exist or is exaggerated.[68]

In these definitions, the authors' similar approaches can be seen. A filter bubble filters out specific information from the mass pool of all information, thus has the effect of narrowing the information intake. The echo chamber then amplifies the filtered information, which then seems like the opposing information does not exist or its advocates are in the minority. Thus, these two phenomena have the effect of making the world seem, as if everyone had the same views and opinions as the person in question.

Another set of terms needed to be clarified are self-selected personalization and pre-selected personalization, as defined by Borgesius et al. The term self-selected personalization describes the intentional choice to filter information that a person encounters. This is something that everybody does, more or less consciously, by picking what news outlets, news stories, internet comments etc. to read. This is a result of selective exposure, a common human tendency to avoid information challenging their own point of view and to seek out affirmative information instead. Pre-selected personalization is not done by the person themselves, but by websites, advertisers, or other different actors, with or without the use of algorithms. Oftentimes, it is done so without the person's choice, input, consent or even knowledge.[69]

3. THE NECESSITY OF FILTER BUBBLE REGULATION

Some, however, are of the opinion that the filter bubbles and echo chambers are not as important and as dangerous of an issue. Bruns states

[67] BRUNS, Axel. Filter bubble. *Internet Policy Review* [online]. 29. 11. 2019, vol. 8, issue no. 4. [cit. 10. 12. 2022]. Available at: https://policyreview.info/concepts/filter-bubble

[68] FLETCHER, Richard. The truth behind filter bubbles: Bursting some myths. In: *Reuters Institute for the Study of Journalism* [online]. 2020. [cit. 10. 12. 2022]. Available at: https://reutersinstitute.politics.ox.ac.uk/news/truth-behind-filter-bubbles-bursting-some-myths

[69] BORGESIUS, Frederik J. Z., et al. Should we worry about filter bubbles? *Internet Policy Review* [online]. 31. 5. 2016, vol. 5, issue no. 1. [cit. 10. 12. 2022]. Available at: https://policyreview.info/pdf/policyreview-2016-1-401.pdf

that they are merely a secondary problem that diverts attention from the more pressing social and societal issues to mere technological factors. That is, if they even exist in the form they are made out to be by the prevalent social debate, as there is not enough empirical evidence supporting the existence of filter bubbles and echo chambers as observable phenomena in public communication. On the contrary, the global societal and political discourse concerning these two phenomena has assumed that they exist and harmfully impact society. According to Bruns, this discrepancy implies a moral panic connected with the transition to a new technological medium, akin to the introduction of the paper press, and an overly simplistic interpretation of the effects of this new technology. Moreover, the concepts of a filter bubble and an echo chamber were not introduced by internet communications experts but by an activist and tech entrepreneur Eli Pariser and a legal scholar Cass R. Sunstein.[70]

Fletcher argues similarly while citing Bruns. He adds that excessive focus on filter bubbles can lead us to misunderstand the mechanisms at play, as the platforms like social media and search engines are not the sole cause but only a part of the picture.[71]

The abovementioned information, however, does not mean that we should abandon the notion of studying and regulating filter bubbles and echo chambers. As both Bruns and Fletcher pointed out, it is needed to tackle the issue more broadly. It is also possible that some form of legal regulation of these phenomena and subsequent changes in user behaviour will prompt researchers to change their methodology and thus come to more conclusive results.

Then, perhaps it is better to phrase the research question differently: Should the pre-selected algorithmic personalization be regulated through an opt-in or opt-out system?

---

[70] BRUNS, Axel. Filter bubble. *Internet Policy Review* [online]. 29. 11. 2019, vol. 8, issue no. 4. [cit. 10. 12. 2022]. Available at: https://policyreview.info/concepts/filter-bubble

[71] FLETCHER, Richard. The truth behind filter bubbles: Bursting some myths. In: *Reuters Institute for the Study of Journalism* [online]. 2020. [cit. 10. 12. 2022]. Available at: https://reutersinstitute.politics.ox.ac.uk/news/truth-behind-filter-bubbles-bursting-some-myths

4. REGULATING PRE-SELECTED ALGORITHMIC PERSONALIZATION THROUGH AN OPT-IN OR OPT-OUT REGIME

The aforementioned choice, consent, and consequentially knowledge can be granted to the person in question through a mandatory opt-in or opt-out system. If the user would be initially asked whether they want to engage in the personalization, they would become aware of its existence. Moreover, if a choice is presented, then the user can decide whether they want to undertake the risk of receiving the personalized content and thus end up in a filter bubble and an echo chamber (if they exist and pose a substantial risk, as was mentioned above), or receive content in a non-personalized manner.

Disabling pre-selected personalization, however, has its drawbacks. Even with pre-selected personalization active, people still engage in self-selected personalization. This can be observed in the fact that, arguably, nobody opens every single link that appears in their feed. However, with the pre-selected personalization turned off, the self-selected personalization becomes more prominent. The social media feed would likely become less engaging, and the user experience on the site could be worse because, as Fletcher stated, people only possess a limited amount of time, and would thus encounter less engaging content.[72] This could lead to people spending less time on the social media site in question. Whether that is a good or bad thing is a whole other matter.

On the other hand, giving users the possibility of experiencing pre-selected and non-pre-selected content side by side would give them the ability to compare the two experiences and choose which one they prefer. This degree of control could also, to a certain degree, mitigate the public unrest about the control of the flow of information by big corporations and, for example, their involvement in rigging elections and the like.

Regarding the question of whether opt-in or opt-out should be preferred by default, opt-in may be the better choice. That is due to the nature of hu-

[72] FLETCHER, Richard. The truth behind filter bubbles: Bursting some myths. In: *Reuters Institute for the Study of Journalism* [online]. 2020. [cit. 10. 12. 2022]. Available at: https://reutersinstitute.politics.ox.ac.uk/news/truth-behind-filter-bubbles-bursting-some-myths

man interaction with pop-up windows. In the case of a default opt-out system, upon the installation of the app, users might skip the opt-out button without even paying any attention to it, similarly to cookie pop-up windows. As such, the default opt-in would result in the hurried user engaging with non-personalized content, thus minimizing the risks posed by skewed personalized content.

In the case of search engines, however, the option of disabling the pre-selected personalization makes less sense. If we take Google as an example, the relevancy of a search result is determined by hundreds of factors like quality, relevancy to the user's query, user's location, language, device etc. But if this degree of personalization ensures that *"searching for "bicycle repair shops" would show different results to a user in Paris than it would to a user in Hong Kong"*, then turning this personalization off would mean that the user would most likely end up with results that are irrelevant to him. As this would make the search engine nearly unusable, it can be concluded that a complete opt-out is not feasible in the case of search engines.

5. CONCLUSION

The essay tackled the question, of whether the filter bubbles should be regulated through an opt-in or opt-out system. First, the essay compared and clarified the terms of a filter bubble and an echo chamber before defining the terms self-selective and pre-selective personalization. Then the essay discussed whether it is necessary to regulate the filter bubble at all, as there is not much empirical evidence that the phenomenon exists in the sense in which it is commonly used and discussed. Lastly, the essay argued the use of an opt-in and opt-out system regarding pre-selective personalization in social media and search engines.

An opt-in or opt-out system possesses some notable benefits for the users of social media platforms. Such a choice could make the users aware that the content is being personalized and give them better control over what information they receive. While disabling the personalization also has drawbacks, most notably in the form of making the content less engaging, its toggleable nature compensates for the disadvantages of both sides, as it

allows the user to choose the option that they prefer. The side-to-side comparison can also provide the user with valuable insight. As such, I believe that such implementation would not disadvantage the users in any way. However, such a system is not a feasible solution when it comes to search engines, as it would render the search results less relevant and the engine's function less effective.

6. BIBLIOGRAPHY

[1] BORGESIUS, Frederik J. Z., et al. Should we worry about filter bubbles? *Internet Policy Review* [online]. 31. 5. 2016, vol. 5, issue no. 1. [cit. 10. 12. 2022]. ISSN: 21976775. Available at: https://policyreview.info/pdf/policyreview-2016-1-401.pdf

[2] BOZDAG, Engin. VAN DEN HOVEN, Jeroen. Breaking the filter bubble: democracy and design. *Ethics and Information Technology* [online]. 18. 12. 2015, issue no. 17. [cit. 10. 12. 2022]. p. 249-265. ISSN: 1572-8439 Available at: https://link.springer.com/content/pdf/10.1007/s10676-015-9380-y.pdf?pdf=button

[3] BRUNS, Axel. Filter bubble. *Internet Policy Review* [online]. 29. 11. 2019, vol. 8, issue no. 4. [cit. 10. 12. 2022]. ISSN: 21976775 Available at: https://policyreview.info/concepts/filter-bubble

[4] FACEBOOK. Good Questions, Real Answers: How Does Facebook Use Machine Learning to Deliver Ads? *Facebook Business* [online]. 2022. [cit. 10. 12. 2022]. Available at: https://www.facebook.com/business/news/good-questions-real-answers-how-does-facebook-use-machine-learning-to-deliver-ads

[5] FARNAM STREET. How Filter Bubbles Distort Reality: Everything You Need to Know. In: *Fs.blog* [online]. 2022. [cit. 10. 12. 2022]. Available at: https://fs.blog/filter-bubbles/

[6] FLETCHER, Richard. The truth behind filter bubbles: Bursting some myths. In: *Reuters Institute for the Study of Journalism* [online]. 2020. [cit. 10. 12. 2022]. Available at: https://reutersinstitute.politics.ox.ac.uk/news/truth-behind-filter-bubbles-bursting-some-myths

[7] GOOGLE. In-depth guide to how Google Search works. *Google Search Central* [online]. 2022. [cit. 10. 12. 2022]. Available at: https://developers.google.com/search/docs/fundamentals/how-search-works

FEDERATED LEARNING AND DATA MINIMISATION IN AUTOMATED DECISION MAKING[73]

ANNA MEDBØE TAMULY[74]

1. INTRODUCTION

To avoid bias in automatic decisions (hereafter "ADM"), we not only need a vast amount of data, but the data we use must be meaningful. In an article in the Hastings Law Journal, Ignacio Cofone defines meaningful data as "counterintuitively, a data sample that is unrepresentative of the pool because it looks like what we believe the pool would look like had it not embedded structural inequalities."[75]

This requirement of meaningful collection of data is also in accordance with one of the key principles in the EU General Data Protection Regulation (hereafter "GDPR").[76] The principle of "data minimisation" in GDPR Art. 5.1.c) states that "Personal data shall be: adequate, relevant and limited to what is necessary in relation to the purposes for which they are proces-

[73] Esej byla zpracována v semestru podzim 2022 v rámci předmětu MVV1368K Privacy and Personal Data Law. / The essay was written in the autumn 2022 semester for the course MVV1368K Privacy and Personal Data.

[74] Anna Medbøe Tamuly is a student at University of Bergen, contact e-mail: my.tamuly@hotmail.com

[75] COFONE, Ignacio N. Algorithmic Discrimination Is an Information Problem. *Hastings Law Journal*. 8. 2019, vol. 70, issue no. 6. p. 1389-1444.

[76] Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

sed"[77]. On the basis of this, it is not legal to uncritically and without limits collect a large amount of data in order to develop Artificial Intelligence ("AI") that will carry out the processes of ADM.

However, one can argue that the need for data maximisation (big data) to avoid bias and to get good ADM contradicts the GDPR principle of data minimisation. How do we know when the data we have collected is sufficient enough to do ADM? When do we have enough data? And what is a "good and unbiased" automatic decision?

To remedy this issue and to comply with the data minimisation principle, many firms have attempted to develop AI that can perform ADM using so-called "federated learning". This essay is going to examine if federated learning can be a solution to comply with the data minimisation principle in GDPR art. 5.1.c) when using ADM.

2. FEDERATED LEARNING: THE SOLUTION TO COMPLY WITH THE DATA MINIMISATION PRINCIPLE WHILE USING ADM?

2.1 DEFINITIONS

2.1.1 AUTOMATED DECISION-MAKING

ADM is defined in *EDPS guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*.[78] EDPB defines ADM together with profiling as these two concepts are closely related. However, ADM alone can be understood as "the ability to make decisions by technological means without human involvement".[79] Furthermore, they state that automated decisions "can be made with or without profiling; profiling can take place without making automated decisions. However, profiling and automated decision-making are not necessarily separate activities."[80]

---

[77] Ibidem, art. 5(1).

[78] EDPB. Guidelines 2016/679 on Automated individual decision-making and Profiling for the purposes of Regulation. In: *ec.eruopa.eu* [online]. 3. 10. 2017 [cit. 7. 11. 2022] p. 8. Available at: https://ec.europa.eu/newsroom/article29/items/612053

[79] Ibidem.

[80] Ibidem.

2.1.2 ARTIFICIAL INTELLIGENCE (AI) VS. MACHINE LEARNING

AI can be defined as "the field of developing computers and robots that are capable of behaving in ways that both mimic and go beyond human capabilities."[81] This means that AI can "analyze and contextualise data to provide information but also can do ADM and trigger "actions without human interference."[82]

Machine learning is a subcategory of AI. Machine learning is often used to create good and functional AI. In order to succeed in this, it is necessary to also use other tools besides machine learning, such as deep learning, neural networks, computer vision, and natural language processing.[83] Machine learning "uses algorithms to automatically learn insights and recognize patterns from data, applying that learning to make increasingly better decisions."[84]

2.1.3 FEDERATED LEARNING

Federated learning was developed by Google in 2016.[85] Google used the method to train a machine learning model on data located on mobile phones, but without uploading the data to a centralised network.[86] The purpose was to build machine learning models that were updated based on data stored on the users' mobile phones without having to share this data.[87]

---

[81] COLUMBIA UNIVERSITY, The Fu Foundation, School of Engineering and Applied Science Artificial Intelligence (AI) vs. Machine Learning. In: *ai.engineering.columbia.edu* [online]. 2022. [cit. 7. 11. 2022]. Available at: https://ai.engineering.columbia.edu/ai-vs-machine-learning/

[82] Ibidem.

[83] Ibidem.

[84] Ibidem.

[85] MCMAHAN, Brendan, Daniel RAMAG. Federated Learning: Collaborative Machine Learning without Centralized Training Data. In: *Google Research Blog* [online]. 6. 4. 2017. [cit. 8. 11. 2022]. Available at: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

[86] Ibidem.

[87] Ibidem.

To train a standard machine learning model, it's required to centralise the data used in training in a data centre or on a machine.[88] Two of the Google Research Scientists explain in a Google Research blog article that federated Learning, unlike standard machine learning, "enables mobile phones to collaboratively learn a shared prediction model while keeping all the training data on the device, decoupling the ability to do machine learning from the need to store the data in the cloud.[89]" They further state that this "goes beyond the use of local models that make predictions on mobile devices (...) by bringing model training to the device as well."[90]

In conclusion, federated learning is a way to minimise the use of data sharing while at the same time maximising the output. In other words, firms using federated learning will be able to train their AI to do much better ADM and, at the same time, minimise the sharing of data.

2.2 THE DEVELOPMENT AND USE OF FEDERATED LEARNING

When used by Google, federated learning works like this: a user downloads the current model of an app. The app improves by learning from the data on the user's phone. Based on the learning, the model "summarises the changes as a small focused update".[91] It is only this small focused update that will be sent back to the shared Google cloud, "using encrypted communication, where it is immediately averaged with other user updates to improve the shared model."[92] This means that all the personal data of a user will remain on their phone and no sharing of personal data will be done to improve the machine learning model.

An example of using federated learning to improve ADM could be when getting insurance for liability for car accidents online. Many insurance

[88] Ibidem.

[89] MCMAHAN, Brendan, Daniel RAMAG. Federated Learning: Collaborative Machine Learning without Centralized Training Data. In: *Google Research Blog* [online]. 6. 4. 2017. [cit. 8. 11. 2022]. Available at: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

[90] Ibidem.

[91] Ibidem.

[92] Ibidem.

providers already use ADM to give out insurance like this. However, there is a high risk of negative bias in this ADM. One of the main problems is that one insurance provider alone doesn't have enough meaningful data to make their system for ADM good enough or reliable enough. By using federated learning, they can collaborate with other insurance providers when developing the system without sharing the personal data of their customers. This will both be in line with the data minimisation principle and, at the same time, increase the scope for what ADM can be used for.

2.3 RISKS, ADVANTAGES AND DISADVANTAGES

As argued above, federated learning can lead to significant improvements in the systems that carry out ADM. This is because it is possible to gain access to much larger amounts of meaningful data without having to share the data and, therefore at the same time, operate in line with the data minimisation principle. However, there is also a great risk when using federated learning.

Often companies use cloud computing to be able to combine all the learning the system has done individually, e.g., on an individual phone in Google's case. Google uses Google Cloud and sends encrypted packages from individual phones to the shared cloud.[93] In this process, there are many risks. If, for example, an insurance provider does not encrypt its data in an adequate manner, they risk sharing personal data about its clients with other insurance providers. This is very problematic from a personal data point of view but can also be problematic from a competition law point of view. The definition of personal data in GDPR is broad. As soon as some of the information can be related to an "identified or identifiable natural person" either "directly or indirectly" its personal data.[94]

To be able to develop the ADM process from federated learning, it is also required that the data points are the same. In other words, there must

[93] MCMAHAN, Brendan, Daniel RAMAG. Federated Learning: Collaborative Machine Learning without Centralized Training Data. In: *Google Research Blog* [online]. 6. 4. 2017. [cit. 8. 11. 2022]. Available at: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

[94] GDPR, art. 4 (1).

be predefined data categories. The Norwegian Data Protection Authority addressed this challenge in a sandbox project.[95] The project was in collaboration with a company that wanted to streamline and improve the way banks can counter money laundering and terrorist financing. However, this challenge is equally relevant for others who want to use federated learning, as shown in the example of insurance providers that want to improve their ADM when granting insurance for liability for car accidents online.

The problem arises because there are different practices related to which data is collected. In order for federated learning to work as intended, it is necessary to coordinate which data categories the banks process. If a model developed in bank A shall be trained in bank B, B needs the same data categories that A used when developing the model.[96] However the need for each category of personal data only arises when a bank builds a model which uses (and needs to use) this exact category.[97] Some categories will always be needed when issuing car insurance, while others will be necessary more rarely or maybe never in some banks. If this is the case, one can argue that it will be a breach of the data minimisation principle to collect this data to improve the ADM for the one bank that does not use this data category normally.

An opposite reflection is as follows; if, by using federated learning, it is possible to create better systems for ADM that have less bias and are more precise, could it be a breach of the data minimisation principle to not use federated learning? The result of this would have been that everyone who had the ability to use federated learning or other technologies that minimise the sharing of data when developing their ADM systems, would have had to use it.

---

[95] NORWEGIAN DATA PROTECTION AUTHORITY. Finterai, sluttrapport: Maskinlæring uten datadeling (English translation: Finterai, final report: Machine learning without data sharing), In: *Sandbox for responsible artificial intelligence* [online]. 11. 10. 2022 [cit. 10. 11. 2022]. Available at: https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ferdige-prosjekter-og-rapporter/finterai-sluttrapport/om-foderert-laring/

[96] Ibidem.

[97] Ibidem.

3. CONCLUSION

The use of federated learning has great potential to ensure that big data can be used to make good ADM systems without breaching the principle of data minimisation. This is because the data used does not need to be shared, and the models can the trained in a bank or a phone's individual system before the learning outcome is shared with the main model.

However, there are some risks, such as how much one can trust the cloud used to share individual training and the systems used to encrypt the data.

On the other hand, Google has already successfully used federated learning for years, and with technological development, the areas in which federated learning can be used will also increase. In this essay, I have used the use of ADM when getting insurance for liability for car accidents online as an example, but there are indefinably more areas where federated learning can be used.

In order to develop good enough AI and good enough systems for ADM, large amounts of meaningful data are required. This is where the problem concerning the data minimisation principle and that the AI and ADM often get biases arises. My prediction for the future is that the more the use of AI and ADM increases, the more there is a need for federated learning and other similar technologies to make these systems good enough, that they do not have biases and, at the same time, comply with GDPR.

4. BIBLIOGRAPHY

[1] COFONE, Ignacio N. Algorithmic Discrimination Is an Information Problem. *Hastings Law Journal*. 8. 2019, vol. 70, issue no. 6. p. 1389-1444.

[2] COLUMBIA UNIVERSITY, The Fu Foundation, School of Engineering and Applied Science Artificial Intelligence (AI) vs. Machine Learning. In: *ai.engineering.columbia.edu* [online]. 2022. [cit. 7. 11. 2022]. Available at: https://ai.engineering.columbia.edu/ai-vs-machine-learning/

[3] EDPB. Guidelines 2016/679 on Automated individual decision-making and Profiling for the purposes of Regulation. In: *ec.eruopa.eu* [online]. 3. 10. 2017 [cit. 7. 11. 2022] p. 8. Available at: https://ec.europa.eu/newsroom/article29/items/612053

[4] MCMAHAN, Brendan, Daniel RAMAG. Federated Learning: Collaborative Machine Learning without Centralized Training Data. In: *Google Research Blog* [online]. 6. 4. 2017. [cit. 8. 11. 2022]. Available at: https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

[5] NORWEGIAN DATA PROTECTION AUTHORITY. Finterai, sluttrapport: Maskinlæring uten datadeling (English translation: Finterai, final report: Machine learning without data sharing), In: *Sandbox for responsible artificial intelligence* [online]. 11. 10. 2022 [cit. 10. 11. 2022]. Available at: https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ferdige-prosjekter-og-rapporter/finterai-sluttrapport/om-foderert-laring/

[6] Regulation (EU) 2016/679, of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

CHATGPT AS LAWYER'S ASSISTANT[98]

TENA KRZNARIĆ[99]

1. INTRODUCTION

In the last few months, ChatGPT has caused a big storm in the public (even though it is not a barely new thing) from those who are enthusiastic about the phenomenon to those who are quick to criticize that many jobs will disappear due to artificial intelligence, including legal professionals. It didn't take long for it to be banned in Italy for violating GDPR and other similar concerns around the world. At the same time, AI successfully passed the bar exam in America. Looking at technological progress, it has great significance. This does not mean that it will take over legal affairs, but it certainly has great potential to transform it.

2. TECHNOLOGY BEHIND GPT

There are many mistakes in the media regarding names used in this matter and in any case, they are not synonyms. The first version that occurred was called GPT, which means generative pre-trained transformer. Later versions were called GPT-2, GPT-3, ChatGPT, and the most recent GPT4. In order to understand the possibilities that those models offer, it is necessary to understand the technology behind them and the differences from previous versions.

---

[98] Esej byla zpracována v rámci stáže autorky v Legal Institute LexRatio Institute for Legal and Information Technology in Maribor, Slovenia. / The essay was written during the author's internship in Legal Institute LexRatio Institute for Legal and Information Technology in Maribor, Slovenia.

[99] Tena Krznarić is a student at the Faculty of Law, University of Zagreb, contact e-mail: tena.krznaric@student.pravo.hr

The first term necessary for understanding the technology behind GPT is natural language processing. Natural language processing is a branch of artificial intelligence that combines computational linguistics with statistical, machine learning and deep learning models, which enable computers to process human language in the form of text or voice data and to understand its full meaning, complete with the speaker or writer's intent and sentiment derived meaning, context, or sentiment in textual data or conversations with humans using grammars and graph structures.[100] GPT-3 and GPT-4 are large language models, the variation of natural language processing, capable of recognising, summarising, translating, predicting and generating text and other content based on knowledge gained from massive datasets. ChatGPT is a natural language processing tool driven by AI technology that allows you to have human-like conversations and much more with the chatbot. The language model can answer questions and assist you with tasks like composing emails, essays, and code.[101] Simplified, ChatGPT is a chatbot driven by GPT-3 language model. The GPT-4 language model is used in another ChatGPT version, ChatGPT Plus.

When ChatGPT was asked how it can support lawyers, its answer mentioned the following categories: legal research, document drafting, case preparation, due diligence, legal writing and proofreading, legal compliance, and client communications.

As GPT is a trained model and is built on a massive dataset, ChatGPT is trained through reinforced learning which means it works based on input data, and the result can be used as input in the next analysis to improve its performance. The algorithm uses a trial and error method to come to a clear objective and can be used in natural language processing in cases such as predictive text, text summarization, question answering and machine translation.[102]

[100] LEGAL INSTITUTE LEXRATIO. Glossary. In: *lexratio.eu* [online]. 2022 [cit. 31. 5. 2023]. Avalabale at: https://lexratio.eu/knowledge-base/glossary/

[101] Ibidem.

[102] Ibidem.

Since its 'knowledge' depends on the inputs, its help depends on its and humans' understanding of the term.

3. LEGAL RESEARCH

Legal research for ChatGPT is the process of identifying and analyzing legal sources and materials to find answers to specific legal questions, understand legal principles, support legal arguments, and provide guidance for legal decision-making. As a result, it can quickly search and analyze vast amounts of legal information, which gives a researcher quick access to information. It also includes case law research, statutes and regulations, legal commentary and scholarly articles. It can provide relevant legal precedents, interpretations, and insights to support legal research efforts.

A recent New York case showed that answers obtained via ChatGPT's legal research help should be additionally verified. In the mentioned case, a lawyer used ChatGPT for case research and while asking ChatGPT to confirm if the case its answer refers to is real and to provide a source it did, though the lawyer himself did not check for the source.[103] It is yet to be seen if there will be any consequences for the lawyer and ChatGPT itself. That being said, a Texas federal judge already imposed a "Mandatory Certification Regarding Generative Artificial Intelligence." This means all submissions to the court must have an amendment saying that they were drafted by a human or that the parts drafted using generative AI were checked by a human.[104]

[103] DRAY, Brandon. Lawyer Faces Sanctions After Admitting Using ChatGPT For 'Bogus' Legal Research. In: *Daily wire* [online]. 29. 5. 2023. [cit. 31. 5. 2023]. Available at: https://www.dailywire.com/news/lawyer-faces-sanctions-after-admitting-using-chatgpt-for-bogus-legal-research

[104] COLDEWEY, David. No ChatGPT in my court: Judge orders all AI-generated content must be declared and checked. In: *techcrunch*.com [online] 31. 5. 2023. [cit. 3. 6. 2023]. Available at: https://techcrunch.com/2023/05/30/no-chatgpt-in-my-court-judge-orders-all-ai-generated-content-must-be-declared-and-checked/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8

4. DOCUMENT DRAFTING

When it comes to document drafting, ChatGPT's answer perceives its support to lawyers as it can generate an initial draft of a document based on the user's request, such as a non-disclosure agreement or an arbitration clause. The precision of the draft depends on the question asked and the details provided.

It is important to remember that all the information that should stay private should not be inserted; as it was mentioned earlier, it is trained through reinforced learning, and it may result in a situation where such information can be used as input.

In other ways, ChatGPT can help in structuring and formatting documents, language and grammar, cross-referencing and reviewing the final version of a document.

5. CASE PREPARATION

Case preparation does not include only the legal research covered above. It can include organization and summarization of materials or suggesting case strategy. When it comes to case summarizing, it can review court opinions, pleadings etc., it can extract key information like the background of the case, legal issues of the case, key points of court reasoning and do legal analysis. In connection to the case strategy, ChatGPT can assist a lawyer in various ways, such as case theory development, by examining the evidence and formulating arguments for the desired outcome. Potentially it can provide insights into alternative dispute resolution or settlement negotiations.

6. DUE DILIGENCE

Due Diligence can be assisted by ChatGPT in many areas. To start with, it can help by reviewing documents like contracts, agreements, intellectual property etc. and analysing them to identify obligations, rights, and crucial provisions. Furthermore, it can help with risk assessment by reviewing li-

tigation history, regulatory filings and other relevant documents. It can prepare a due diligence report by summarizing previous findings.

7. LEGAL WRITING

When it comes to legal writing and proofreading, practically all the above-mentioned assistance could be conducted. But ChatGPT can also review and proofread legal documents, briefs, memos, and other written materials to help ensure clarity, coherence, and accuracy through content enhancement, citations, language and grammar checks etc.

8. LEGAL COMPLIANCE

In the matter of legal compliance, ChatGPT can help navigate through legal and regulatory frameworks by providing information on specific laws, industry standards, and compliance requirements. It can assess current compliance practices and identify gaps or areas of concern, assist in developing systems and processes for ongoing compliance monitoring and reporting and provide guidance on data privacy and security compliance.

9. CLIENT COMMUNICATION

Client communication is one of the most important parts of work, as the result of work depends on good communication. Chatbots cannot replace face-to-face communication, but they can help with simple written communication by generating clear and concise explanations of legal concepts and processes to help clients better understand their legal matters or preparing client correspondence and responses to inquiries.

10. CRITICS

The benefit of using ChatGPT is that it does not support only the English language, although it is its main working language, but many others like Croatian, Czech, German, and Spanish. Despite all the languages included, the efficiency of ChatGPT depends on the quality of input data in the requested language. The problem arising from using other languages is that it confuses similar languages. For example, it mixes Croatian and Ser-

bian. Even though it is not something worrying, it shows the importance of detailed reading and could be proven problematic when providing answers due to non-distinction data from which it learned. Not to mention, the response time in English is quicker than, for example, in Croatian.

The biggest problem that came up in legal research is that ChatGPT has up-to-date information until September 2021. This represents a huge obstacle for lawyers, especially in the continental legal circle, where legal acts constantly change. For example, Croatian Law on Renting Apartments[105] does not track changes from 2020, although it should be covered by the time frame.

ChatGPT itself recognizes potential challenges in using it for legal purposes. The first challenge can be a lack of contextual understanding as it generates responses based on patterns and information from the training data and may not understand the specific context or unique details of a particular legal case or jurisdiction. The second challenge is ethical and professional responsibility as humans have to verify suggested answers and information. The third problem is privacy and confidentiality. This was briefly covered above, as one has to be careful with providing data to the chatbot. Such concern occurred in Italy, which led to the ban of ChatGPT, specifically because the app had experienced a data breach involving user conversations and payment information.[106] The fourth challenge is the limitation in legal advice. ChatGPT can provide general legal information and suggestions, but it constantly warns that it is not a substitute for professional legal advice. Every legal case is specific, and all circumstances are essential. Layperson is not aware of the complexity and changes related to the case and can misinterpret given information or be mistaken regarding the applicable law. This especially has the effect because ChatGPT is not up-to-date after September 2021.

[105] Law on Renting Apartments, NN 91/96, 48/98, 66/98, 22/06, 68/18, 105/20

[106] MCCALLUM, Shiona. ChatGPT banned in Italy over privacy concerns. In: *BBC News* [online]. 1. 4. 2023. [cit. 31. 5. 2023]. Avaialable at: https://www.bbc.com/news/technology-65139406

11. CONCLUSION

AI is a powerful tool, and the world must embrace its existence and further development. The truth is that some professions will disappear at one point in time, but new ones will surface, and legal ones are not among those.

Legal professionals do a lot of repetitive actions and similar cases that could be eased by using AI tools. It doesn't have to be ChatGPT, as there are other chatbots, too. ChatGPT is just free and easily accessible. When professionals use AI tools, they just have to be precise and careful. Professionals have to read answers in detail and check them, as potentially, they will be provided with wrong answers. They have to use their professional knowledge in order to benefit from these tools.

There are many benefits to using AI, efficiency and time-saving, accessibility and availability to continual learning, and these benefits feel both lawyers and their clients.

Yes, there are many concerns regarding the use of such technology, but we are on a long road ahead of useful regulation, which will not slow down innovation, especially in the European Union, where privacy is a top topic.

12. BIBLIOGRAPHY

[1] LEGAL INSTITUTE LEXRATIO. Glossary. In: *lexratio.eu* [online]. 2022 [cit. 31. 5. 2023]. Avalabale at: https://lexratio.eu/knowledge-base/glossary/

[2] DRAY, Brandon. Lawyer Faces Sanctions After Admitting Using ChatGPT For 'Bogus' Legal Research. In: *Daily wire* [online]. 29. 5. 2023. [cit. 31. 5. 2023]. Available at: https://www.dailywire.com/news/lawyer-faces-sanctions-after-admitting-using-chatgpt-for-bogus-legal-research

[3] COLDEWEY, David. No ChatGPT in my court: Judge orders all AI-generated content must be declared and checked. In: *techcrunch.*com [online] 31. 5. 2023. [cit. 3. 6. 2023]. Available at: https://techcrunch.com/2023/05/30/no-chatgpt-in-my-court-judge-orders-all-ai-generated-content-must-be-declared-and-checked/?guccounter=1&guce_referrer=aHR0cHM6Ly-93d3cuZ29vZ2xlLmNvbS8

[4] Law on Renting Apartments, NN 91/96, 48/98, 66/98, 22/06, 68/18, 105/20

[5] MCCALLUM, Shiona. ChatGPT banned in Italy over privacy concerns. In: *BBC News* [online]. 1. 4. 2023. [cit. 31. 5. 2023]. Avaialable at: https://www.bbc.com/news/technology-65139406

RECENZE ZÁVĚREČNÝCH PRACÍ I/2023

OBSAH SEKCE

DRACHOVSKÁ, K: DIGITÁLNÍ POZŮSTALOST

JAN DVOŘÁK[1]

DRACHOVSKÁ, K.: Digitální pozůstalost. 2023, diplomová práce, Univerzita Karlova, Právnická fakulta, 63 s.

ANOTACE

Stále více společenských vztahů se přesouvá online a stejně, jako se vyvíjí technologie, musí v reakci na to řešit nové výzvy též právo. Jednu z takových výzev, která navazuje na masivní pokrok v online světě, představuje digitální pozůstalost. Proto si jako ústřední bod celé práce kladu otázku, co se stane s digitálním majetkem, tedy hodnotami, které v rámci svých online aktivit každý z nás vytváří, v případě naší smrti. Tuzemská platná právní neobsahuje žádná speciální ustanovení pro dědění digitálního majetku. Přechod na právní nástupce proto závisí na příslušných ustanoveních, na jejichž základě posuzujeme právní nástupnictví mortis causa dnes. Výběr konkrétní právní normy přitom závislosti na předmětu digitální pozůstalosti. Platná a účinná právní úprava toho času neobsahuje ani legální definici pojmu digitální pozůstalost. Obecně lze pod tímto pojmem chápat všechna digitálně uložená data, která mohou být součástí zůstavitelovy sféry právní dispozice. Rozsah tohoto pojmu tedy naplňuje celá škála hodnot různé povahy. Proto rozlišuji tři skupiny digitálních aktiv, pro něž lze definovat společná pravidla dědění. První a nejrozsáhlejší část věnuji dědění internetových účtů určených ke komunikaci (konkrétně e-mailové účty a účty na sociálních sítích). Dále se zabývám děděním kryptoměn s akcentem na praktická úskalí jejich přechodu mortis causa. Třetí skupinu, jíž věnuji samostatnou pozornost, tvoří účty s předplatnými a online úložiště. Hlavním cílem práce je identifikovat většinu sporných otázek, přinést nové pohledy do rozbíhající se debaty

[1] prof. JUDr. Jan Dvořák, CSc. je profesorem na Katedře občanského práva Právnické fakulty Univerzity Karlovy, kontaktní e-mail: dvorak@prf.cuni.cz.

právní doktríny, jakož i najít odpověď na většinu vyřčených otázek. Práce vzájemně konfrontuje existující pohledy tuzemské i zahraniční právní vědy i praxe, načež se snaží najít řešení, které bude nejvíce vyhovovat současné koncepci dědického práva v občanském zákoníku. V návaznosti na to poskytuje práce i praktické tipy, jak čelit a předcházet nejzávažnějším úskalím, jež se s děděním digitálních aktiv pojí.

KLÍČOVÁ SLOVA

Pozůstalost; digitální majetek; principy dědického práva

ABSTRACT

More and more social relations are moving online and, just as technology is evolving, the law must also respond to new challenges. One of such challenges, that builds on the massive advances in the online world, is digital inheritance. Therefore, as a focal point of the whole thesis, I ask what happens to digital assets, i.e. the values that each of us creates in our online activities, in the event of our death. Czech law does not contain any special provisions for the inheritance of digital assets. Therefore, succession depends on the relevant provisions under which we assess succession mortis causa today. The choice of a particular legal rule depends on the subject matter of the digital estate. The legislation at the time does not even contain a legal definition of the term of digital estate (digital inheritance). In general, this term can be understood as all digitally stored data that may be part of the testator's sphere of legal disposition. The scope of this term is therefore filled by a whole range of values of different nature. Therefore, I distinguish three groups of digital assets for which common rules of inheritance can be defined. I devote the first and most extensive section to the inheritance of internet accounts intended for communication (specifically, e-mail accounts and social networking accounts). I then address the inheritance of cryptocurrencies, with an emphasis on the practical pitfalls of their passage mortis causa. The third group, to which I devote particular attention, consists of subscription accounts and online (cloud) storage. The main goal of the thesis is to identify most of the contentious issues, to bring new insights to the burgeoning debate of legal doctrine, as well as to answer most of the questions raised.

The thesis confronts the existing perspectives of domestic and foreign legal scholarship and practice with each other and then attempts to find a solution that will best suit the current concept of inheritance law in the Civil Code of the Czech Republic. Following this, the thesis also provides practical tips on how to face and prevent the most serious pitfalls related to the inheritance of digital assets.

KEY WORDS

Inheritance; Digital Assets; Principles of Inheritance Law

Plná verze práce je dostupná z: https://dspace.cuni.cz/handle/20.500.11956/178955

Zvolené téma považuji za originální, novátorské a původní. Navíc jde o téma, kterému se česká odborná literatura věnuje jen sporadicky, i když notářská praxe se již s problematikou digitální pozůstalosti musí vyrovnávat. Je proto pochopitelné, že autorka čerpala především z německé odborné literatury a přihlédla i k některým německým soudním rozhodnutím. I proto považuji zpracování zvoleného tématu za obtížné jak po stránce teoretické, tak i praktické.

Ke zdařilému sepsání zvoleného tématu je nezbytným předpokladem výborná znalost právní teorie, proto autorka v úvodu popisuje teoretické přístupy k dědění digitálního majetku, seznamuje čtenáře s německou obligační teorií, jakož i s čínskou věcně právní teorii, tuto část práce završuje pohledem na dědění digitálních aktiv podle českého právního řádu. V úvodu autorka předkládá čtenáři vymezení pojmu digitální pozůstalosti a digitálního majetku.

Za významnou považuji tu část práce, ve které autorka zkoumá přechod digitální pozůstalosti *sub specie* tradičních principů dědického práva (ve světle zásad dědického práva formulovaných v klasické učebnici Emanuela Tilsche).[2] Podle jejího názoru lze i při dědění digitální pozůstalosti vystačit

[2] Viz např. TILSCH, Emanuel. *Dědické právo rakouské se stanoviska srovnávací vědy právní*. Praha: Wolters Kluwer, 2015. 168 s. ISBN: 978-80-7478-713-3.

s platnou právní úpravou. Zpracování části věnované dědění internetových komunikačních účtů zasluhuje plné uznání pro svou přehlednost, jasnost a dobré zdůvodnění. Problematice dědění kryptoměn, které jsou z digitálního majetku zřejmě nejznámější, se věnuje podrobným výkladem na straně 36 a následujících. Tato problematika se z pohledu notářské praxe jeví jako nejvíce aktuální. Při rozboru dědění účtů s předplatným a přístupů k online databázím navazuje otázkami souvisejícími s autorským právem, jakož i se smluvními podmínkami.

Podrobný závěr práce shrnuje poznatky, k nimž se autorka po předchozí analýze a právně srovnávacím pohledu dopracovala. Autorka zde upozorňuje, že zákonodárce nestanovil speciální právní pravidla, podle kterých bychom měli posuzovat dědění digitálních aktiv. Správně zdůrazňuje princip univerzální sukcese v jejímž důsledku dědic nastupuje do smluvního postavení zůstavitele, proto má právo na přístup k účtu včetně jeho obsahu, v tom se autorka shoduje se závěry německé judikatury, nepřejímá však její závěr, že dědic není oprávněn účet nadále využívat k vlastní aktivní komunikaci.

Za hodnou dalšího rozpracování vnímám problematiku účtu jako součásti pozůstalosti a zejména problematiku osobního pouta uživatele s účtem. Podle názoru autorky toto pouto není tak silné, abychom dovodili, že účet není součástí pozůstalosti. Tato její myšlenka rezonuje v práci na řadě míst, považoval bych za vhodné, aby se k této otázce autorka ještě podrobněji vyjádřila. Samostatnou a nelehkou problematikou je dále dědění kryptoměny, které je v rámci úspěšného řízení o pozůstalosti podmíněno znalostí takzvaného privátního klíče, který je však mnohdy dědicům nedostupný. Vyvstává tak otázka, jak postupovat v takovém případě?

Formální stavba práce je dobře podána, čtenář ocení i jasnou systematiku práce. Předloženou práci považuji za mimořádně zdařilou a hodnotnou. Výrazně přesahuje běžný standard diplomových prací. Oceňuji, že autorka při své inspiraci převážně z německé právní praxe nepřejímá její závěry automaticky a posuzuje je kriticky s vědomím odlišnosti české právní úpravy. Autorkou uvedený příklad (rozhodnutí německého Spolkového soudního dvora uvedený na straně 14 práce) je velmi instruktivní

pro formování obligační teorie. Oceňuji rovněž, že autorka ve vhodných souvislostech doplňuje svůj výklad i o vazbu na ustanovení týkající se ochrany spotřebitele.[3]

[3] Srov. problematiku smluvních podmínek, které mají povahu adhezních smluv.

FORMÁNEK, D.: PRÁVO NA INFORMACE A OSOBNÍ ÚDAJE

JAKUB HARAŠTA[4]

FORMÁNEK, D.: Právo na informace a osobní údaje. 2022, diplomová práce, Masarykova univerzita, Právnická fakulta, 85 s.

ANOTACE

Tato diplomová práce se zabývá otázkami střetu práva na informace a práva na ochranu soukromí a osobních údajů. Věnuje se především, ve světle aktuální judikatury, analýze podmínek pro poskytování informací veřejného sektoru, které obsahují osobní údaje, nebo které by mohly zasáhnout do práva na soukromí dotčených osob. Důraz je kladen na poskytování údajů o platových poměrech, jehož podmínky byly stanoveny soudní praxí, především přelomovým nálezem Ústavního soudu ze dne 17. 10. 2017, sp. zn. IV. ÚS 1378/16.

KLÍČOVÁ SLOVA

Právo na informace; zákon 106; platový nález; ochrana osobních údajů; platový test

ABSTRACT

This diploma thesis deals with the issues of the conflict between the right to information and the right to protection of privacy and personal data. In particular, in the light of current case law, it analyzes the conditions for the provision of public sector information which contains personal data or which could interfere with the right to privacy of the persons concerned. Emphasis is placed

[4] JUDr. Mgr. Jakub Harašta, Ph.D. je odborným asistentem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity, kontaktní e-mail: jakub.harasta@law.muni.cz.

on the provision of data about salary conditions, the conditions of which have been determined by court practice, especially the groundbreaking judgement of the Constitutional Court of 17 October 2017, file no. IV. ÚS 1378/16

KEY WORDS

Freedom of Access to Information; Act No. 106; Salary Judgment; Personal Data Protection; Salary Test

Plná verze práce je dostupná z: https://is.muni.cz/auth/th/ozi1r/

Nález Ústavního soudu ze dne 17. října 2017, ve věci sp. zn. IV. ÚS 1378/16, je lépe známý pod populárním názvem *Platový nález*. Ústavní soud se v něm vymezil vůči názoru Nejvyššího správního soudu,[5] že test proporcionality není při aplikaci § 8b zákona č. 106/1999 Sb. nutné provádět, a to z důvodu, že jej již provedl zákonodárce, když dané ustanovení formuloval. Jak Ústavní soud uvedl, *„[ž]ádným zákonem totiž nelze abstraktně vyloučit ochranu základních práv a svobod, zaručenou ústavním pořádkem. V každém jednotlivém případě střetu ústavně zaručených práv musejí soudy a jiné orgány veřejné moci zvážit význam a intenzitu dotčených práv.*" Z tohoto pak Ústavní soud dovodil, že povinné osoby dle zákona č. 106/1999 mohou odmítnout poskytnout informace o platu a odměnách zaměstnance, pokud nejsou kumulativně splněny čtyři podmínky: (a) účelem vyžádání informace je přispět k diskuzi o věcech veřejného zájmu, (b) informace samotná se týká veřejného zájmu, (c) žadatel o informaci plní úkoly či poslání dozoru veřejnosti či roli tzv. „společenského hlídacího psa", a (d) informace existuje a je dostupná.

Ústavní soud tak byl ve svých závěrech v *Platovém nálezu* přímočarý. Přímočarým naopak nebylo to, jak se závěry Ústavního soudu projeví na praxi jednotlivých povinných osob, případně v rámci přezkumu jejich praxe ve správním soudnictví. Diplomová práce *Právo na informace a osobní údaje*

[5] Viz Rozsudek Nejvyššího správního soudu ze dne 22. října 2014, sp. zn. 8 As 55/2012.

tak usilovala o odpověď právě na otázku následné praxe a vlivu, který na ni *Platový nález* bude mít.

Platový nález v zásadě vedl k vytvoření paralelního postupu pro vyřizování rozsáhlé skupiny žádosti podle zákona č. 106/1999 Sb. Diplomant sám v práci konstatoval, že zejména pro povinné subjekty s nedostatečnými personálními či odbornými kapacitami představuje zohlednění *Platového nálezu* v procesu vyřizování žádosti o informace výzvu.[6] *Platový nález* také představoval zásadní změnu v judikatuře. Nutně tak vedl k přehodnocení předcházející rozhodovací praxe a vyžadoval od správních soudů přizpůsobení se novému stavu.

Diplomant si za výzkumnou otázku stanovil, zda jsou podmínky stanovené Ústavním soudem v *Platovém nálezu* omezené na poskytování informací o platových poměrech, nebo zda se aplikují šířeji na všechny případy poskytování informací s osobními údaji.[7] Časový rozestup pěti let, které uplynuly od vydání *Platového nálezu* k napsání diplomové práce, však umožňuje pozorovat a analyzovat také dopady, které bylo možné v době vydání nálezu pouze odhadovat, a které s touto výzkumnou otázkou přímo nesouvisí.

V úvodních částech je diplomová práce věnována základním východiskům práva na informace[8] a také základním východiskům ochrany osobnosti, projevů osobní povahy, soukromí a osobních údajů.[9] Jakkoli je právní úpravu i její relevantní principy vhodné připomenout, diplomant se zde dle mého názoru pustil do až nepodstatných detailů. Čtenářům s problematikou na obecné úrovni obeznámeným tak lze doporučit tyto části při čtení vynechat.

Kapitola 3 je věnována pravidlům poskytování osobních údajů dle zákona č. 106/1999 Sb.[10] Diplomant v ní mapuje způsoby, jakým jsou informace veřejné správy obsahující osobní údaje a potenciálně způsobilé zasáhnout do soukromí osoby, poskytovány. Text je věnován popisu mechanismů ob-

[6] Viz s. 79 recenzované práce.

[7] Viz s. 15-16 recenzované práce.

[8] Viz s. 17-22 recenzované práce.

[9] Viz s. 23-32 recenzované práce.

[10] Viz s. 33-41 recenzované práce.

sažených v § 8a odst. 1 (označováno jako „základní obecné pravidlo“) a v § 8a odst. 2, § 8b a § 10 (označeno jako „speciální pravidla“) zákona č. 106/1999 Sb. Vzhledem k tomu, že § 8a odst. 2 byl do zákona č. 106/1999 Sb. přidán až po vydání *Platového nálezu*,[11] byl zde určitě značný prostor pro zmatky ve výkladu ohledně vzájemných souvislostí a návazností. Diplomant však tyto vazby vysvětlil velmi systematicky a s lehkostí, kterou mu závidím. Přesto mám však pocit (který u mě od napsání posudku na tuto diplomovou práci pouze zesílil), že by zejména této kapitole slušel syntetický závěr v podobě grafického znázornění (např. za použití BPMN notace).

Kapitola 4 je následně věnována kolizi práva na informace s právem na ochranu osobních údajů.[12] Tato kapitola je částečně tvořena rekapitulací a popisem *Platového nálezu*[13] a až následně přichází ke slovu informace o navazující judikatuře a dotváření platového testu, který Ústavní soud zformuloval.[14] Diplomant se v této kapitole extenzivně věnuje dopadu *Platového nálezu* na následnou rozhodovací praxi zejména Nejvyššího správního soudu. I popis *Platového nálezu* zmiňuje některé problematické momenty, které Ústavní soud svým nálezem vytvořil. Následně pak diplomant analyzuje, jakým způsobem se s těmito problémy vypořádal právě Nejvyšší správní soud.

Kapitola 5 je věnována plánovaným legislativním změnám,[15] konkrétně vládnímu návrhu novely zákona č. 106/1999 Sb. zahrnujícímu nový § 8c. Diplomant přijímá odůvodnění vlády, která uvedla, že problém vyžadující zařazení nového ustanovení spočívá „*ve složitosti posouzení jednotlivých podmínek platového testu povinnými subjekty*“.[16] Tuto argumentaci dále rozvíjí a analyzuje přípravné dokumenty. Vzhledem k tomu, že § 8c se s účinností

[11] Byl přidán zákonem č. 111/2019 Sb., který s účinností od 24. dubna 2019 měnil některé zákony v souvislosti přijetím zákona č. 110/2019 Sb., o zpracování osobních údajů.

[12] Viz s. 42-67 recenzované práce.

[13] Viz s. 42-61 recenzované práce.

[14] Viz s. 62-67 recenzované práce.

[15] Viz s. 68-72 recenzované práce.

[16] Viz s. 68 recenzované práce.

od 1. ledna 2023 stal součástí zákona č. 106/1999 Sb.,[17] mohlo by se zdát, že této části není potřeba věnovat pozornost. Naopak mám za to, že tato část je jednou z nejcennějších, protože diplomant se ustanovení věnuje velmi podrobně, a právě v kontextu tvořenému dalším výkladem obsaženým v diplomové práci.

Kapitola 6 pak obsahuje rekapitulaci základních argumentů práce a odpověď na výzkumnou otázku.[18] Diplomant dospěl k závěru, že podmínky stanovené v *Platovém nálezu* je možné použít nejen na všechny případy poskytování informací obsahujících osobní údaje, ale také při kolizi s jinými chráněnými zájmy.[19] Výslovně také uzavírá, že v případě, kdy žadatel žádá informaci za účelem jejího užití ve veřejné diskusi (tedy pokud realizuje svobodu projevu), zastává automaticky funkci „veřejného hlídacího psa".[20] S předloženými závěry se lze ztotožnit, bohužel však nejsou ve všech krocích argumentovány vyčerpávajícím způsobem. Následuje Závěr, kde již autor pouze rekapituluje základní myšlenky a prezentuje některé širší úvahy, ke kterým v průběhu psaní práce dospěl.[21]

Od *Platového nálezu* již uplynula řada let a kritickou reflexi v tomto rozsahu (a této kvalitě zpracování) si určitě zaslouží. Reakce povinných osob i správních soudů na tento nález ukázala, že problematika veřejné kontroly výkonu veřejné moci je stále živá. Přes soupeřící zájmy a mnohé excesy je dle mého z práce jasně patrné, že je společným úkolem všech zúčastněných, aby textace, aplikace a interpretace zákona č. 106/1999 Sb. odpovídala potřebám moderní (tedy informované) společnosti.

[17] Nabytím účinnosti zákona č. 241/2022 Sb.

[18] Viz s. 73-77 recenzované práce.

[19] Viz s. 76 recenzované práce.

[20] Viz s. 76 recenzované práce.

[21] Viz s. 78-79 recenzované práce.

SOUKUPOVÁ, M.: ČLÁNEK 17 SMĚRNICE O AUTORSKÉM PRÁVU NA JEDNOTNÉM DIGITÁLNÍM TRHU

JELIZAVETA JUŘIČKOVÁ[22]

SOUKUPOVÁ, M.: Článek 17 směrnice o autorském právu na jednotném digitálním trhu. 2022, diplomová práce, Masarykova univerzita, Právnická fakulta, 160 s.

ANOTACE

Diplomová práce se zabývá čl. 17 směrnice (EU) 2019/790 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu. Čl. 17 zavádí odpovědnost poskytovatelů služeb pro sdílení obsahu online za neoprávněná sdělení nebo zpřístupnění děl chráněných autorským právem nebo jiných předmětů ochrany veřejnosti, pokud jsou nahrány uživatelem. Čl. 17 je v práci podroben kritické analýze spojené s úvahou o jeho možné kvalifikaci a možném konfliktu se základními lidskými právy a svobodami. Pozornost je věnována také transpozici a sporu o jeho neplatnost probíhajícímu před Soudním dvorem Evropské unie. Poslední kapitola je zaměřena na otázku, zda je možné dosáhnout účelu čl. 17 jinou cestou.

[22] Mgr. Jelizaveta Juřičková je doktorandkou na Ústavu práva a technologií Právnické fakulty Masarykovy Univerzity, kontaktní e-mail: 528873@mail.muni.cz.

KLÍČOVÁ SLOVA

Jednotný digitální trh; DSM směrnice; autorské právo; čl. 17; monitoring a filtrace; poskytovatel služeb pro sdílení obsahu online; sdělování veřejnosti; odpovědnost za obsah nahraný třetí stranou

ABSTRACT

The thesis deals with Article 17 of Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market. Article 17 establishes the liability of online content-sharing service providers for unauthorised act of communication or making available to the public of copyrighted works or other protected subject matter when uploaded by a user. Article 17 is, in this thesis, subjected to a critical analysis associated with a consideration of its possible qualification and possible conflict with fundamental human rights and freedoms. Attention is also paid to its transposition and the dispute over its invalidity pending before the Court of Justice of the European Union. The final chapter focuses on the question of whether the purpose of Article 17 can be achieved by other means.

KEY WORDS

Digital Single Market; DSM Directive; Copyright Law; Article 17; Monitoring and Filtering; Online Content Sharing Service Provider; Communication to the Public; Liability for the Content Uploaded by the Third Party

Plná verze práce je dostupná z: https://is.muni.cz/auth/th/xuene/

Práce je věnována vysoce kontroverznímu a aktuálnímu tématu v oblasti autorského práva, článku 17 směrnice (EU) 2019/790 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu. Článek 17 zavádí pro vybranou kategorii poskytovatelů služeb informační společnosti nový režim právní odpovědnosti za díla nahraná jejich uživateli. Autorka si klade za cíl určit, zda bylo možné účelu článku 17 dosáhnout jinými prostředky.

Autorka nejprve čtenáře uvádí do problematiky článku 17 DSM směrnice. Velmi zevrubně líčí historii vzniku tohoto ustanovení, včetně kontroverze kolem důvodnosti zavedení této úpravy. Představuje základní argument nositelů práv, tedy nutnost zmírnění tzv. *value gap*, *„situace, kdy na internetu neustále stoupá počet nezákonně zveřejněných děl, zatímco příjmy nositelů práv k oněm dílům naopak klesají,“*[23] stejně jako námitky akademiků, kteří tvrdí, že *value gap* není dostatečně empiricky podložen. Dodáním tohoto kontextu autorka vytváří plastický obraz okolností a protichůdných zájmů, ze kterých článek 17 vzešel.

Další kapitola práce rozebírá strukturu článku 17. Článek 17 vyjímá podmnožinu poskytovatelů služeb informační společnosti, tzv. poskytovatele služeb pro sdílení obsahu online, z „bezpečného přístavu“, který je chrání před odpovědností za díla nahrávaná koncovými uživateli na jejich platformy, a stanovuje, že provádějí sdělování a zpřístupňování děl veřejnosti. Poskytovatel může odpovědnosti za díla nahrávaná jeho uživateli předejít, a to přednostně získáním svolení ke sdělování nebo zpřístupnění děl veřejnosti od nositelů autorských práv. Pokud není svolení poskytnuto, může poskytovatel svoji odpovědnost omezit alternativními prostředky, konkrétně vynaložením nejlepšího úsilí k zamezení nahrání díla, o kterém mu autor poskytl relevantní a nezbytné informace a znemožněním přístupu k dílu na základě oznámení autora v kombinaci s vynaložením nejlepšího úsilí k zamezení jeho opětovnému nahrání. Jak uvádí autorka, k plnění povinností vyplývajících z článku 17 je nutné využití technologií filtrace obsahu nahrávaného uživateli.[24]

Následující část práce se zabývá akademickou diskuzí o klasifikaci práva na sdělování díla veřejnosti, se kterým článek 17 operuje, což je dle autorky důležité pro jeho správnou transpozici a aplikaci. Autorka v této části představuje argumenty zastánců názoru, že článek 17 je *lex specialis* k obecnému právu na sdělování díla veřejnosti dle článku 3 InfoSoc směrnice, i pojetí, dle kterého je právo na sdělování veřejnosti dle článku 17 *sui*

[23] Viz s. 18 recenzované práce.

[24] Viz s. 32 recenzované práce.

generis. Byť je tato diskuze zajímavá, není zcela jasné, jakou úlohu hraje při zodpovězení výzkumné otázky.

Poté autorka přechází k otázce kompatibility článku 17 se základními lidskými právy, tedy svobodou projevu a informací, právem na ochranu osobních údajů a svobodou podnikání, a s tím souvisejícího soudního sporu[25] Polska, Komise a Parlamentu o to, zda článek 17 má být zneplatněn na základě nepřípustného zásahu do svobody projevu. Prostřednictvím relevantní literatury a judikatury SDEU naznačuje, že článek 17 ve své konečné podobě zřejmě není vhodným prostředkem k nastolení rovnováhy mezi zájmy poskytovatelů a nositelů práv, čímž je zdůrazněna relevance nastolené výzkumné otázky.

Následně jsou v práci rozebrány tři transpozice článku 17 — česká, německá a francouzská. Význam zahrnutí porovnání transpozic, zejména té německé a francouzské, je ozřejměn v další části práce, protože jednou z navrhovaných možností nápravy nedostatků článku 17 je právě jeho extenzivní výklad při transponování.

Závěrem se autorka dostává ke zodpovězení výzkumné otázky, tedy zda by bylo možné účelu článku 17, kterým je *„nutnost přizpůsobení autorského práva digitálnímu věku a jeho užití na platformách a nutnost vypořádat hodnotovou propast“*,[26] dosáhnout jiným způsobem, a to s menším zásahem do základních lidských práv a svobod zúčastněných stran. Autorka zkoumá čtyři možná řešení: transpozici členskými státy jdoucí nad rámec textace článku 17, dvě varianty novelizace DSM směrnice a nahrazení článku 17 zcela odlišným režimem. Tato kapitola představuje pestrou paletu návrhů na řešení různých autorů, přičemž autorka práce řešení sice komentuje, ale nedává explicitně přednost žádnému z nich.

Obecně je na práci výjimečná poctivost a kvalita zpracování. Hlavní předností práce je, že poskytuje opravdu ucelený vhled do problematiky článku 17. Autorka správně uvádí, že přínos její práce může veliký i pro praxi (např. když v kapitole 2.1 zevrubně rozebírá definiční znaky poskytovatele služeb sdílení obsahu online). Ocenit lze i autorčinu snahu pro-

[25] Rozsudek SDEU (velkého senátu) ze dne 26.4.2022 ve věci C-401/19

[26] Viz s. 119 recenzované práce.

niknout do praktických otázek neprávní povahy, např. do fungování technologií, které lze využívat k filtraci obsahu. Proto lze přečtení práce doporučit každému, kdo má zájem si vytvořit přehled o novém režimu odpovědnosti za autorskoprávně chráněný obsah na internetu.

V práci výrazně převažuje kritická diskuze nad deskripcí. Autorka se dokáže na velmi vysoké úrovni vypořádat s názory odborníků, např. rozbor stanoviska generálního advokáta ve věci C-401/19 staví z podstatné části výhradně na vlastní argumentaci, která je logická a přesvědčivá. Práce také obsahuje řadu zajímavých a inovativních myšlenek, které jsou v tuto chvíli předmětem živého akademického zájmu – např. vytvoření jednotné databáze autorskoprávně chráněných děl.

Množství zohledněných zdrojů je impozantní a jejich zpracování velmi přehledné a systematické. Je potřeba zdůraznit, že většina zdrojů je cizojazyčná, což je pro diplomovou práci v českém prostředí dost neobvyklé. Po jazykové stránce je práce na vysoké úrovni, obsahuje pouze několik drobných chyb a překlepů, což je ovšem pochopitelné s ohledem na rozsah textu.

ERLEBACH, M.: OCHRANA OSOBNÍCH ÚDAJŮ V DIGITAL MARKETS ACT A DIGITAL SERVICES ACT

PAVEL LOUTOCKÝ[27]

ERLEBACH, M. Ochrana osobních údajů v Digital Markets Act a Digital Services Act. 2023, magisterská práce, Masarykova univerzita, Právnická fakulta, 101 s.

ANOTACE

Předkládaná práce má za cíl analyzovat dopad nových nařízení o digitálních trzích a digitálních službách Evropské unie do právního rámce ochrany osobních údajů, jak jej aktuálně definuje obecné nařízení o ochraně osobních údajů. Práce nabízí úvahy de lege ferenda nad překryvem vymáhacích mechanismů v těchto třech nařízeních a možná řešení tohoto překryvu zasazená do kontextu existujícího právního rámce Evropské unie a judikatury Soudního dvora Evropské unie.

KLÍČOVÁ SLOVA

DMA; DSA; GDPR; osobní údaje; ne bis in idem; dvojí vymáhání

ABSTRACT

The aim of this thesis is to analyse the impact of the new Digital Markets Act and Digital Services Act by the European Union on the legal framework of personal data protection as currently defined by the General Data Protection Regulation. The thesis offers de lege ferenda considerations on the overlapping enforcement mechanisms in these three regulations and possible solutions to these

[27] JUDr. Pavel Loutocký, Ph.D., BA (Hons) je odborným pracovníkem na Ústavu práva a technologií Právnické fakulty Masarykovy Univerzity, kontaktní e-mail: loutocky@muni.cz.

overlaps in the context of the existing European Union legal framework and the case law of the Court of Justice of the European Union.

KEY WORDS

DMA; DSA; GDPR; Personal Data; Ne bis in idem; Double Enforcement

Plná verze práce je dostupná z: *https://is.muni.cz/auth/th/sy33j/*

Téma práce a její zaměření je zvoleno velmi vhodně a je vzhledem k překotnému vývoji evropské legislativy je nutno považovat jej za aktuální a potřebné, ke zpracování ale ovšem náročné. Práce se zaměřuje na důležité otázky související s koexistencí obdobných požadavků obsažených v konkrétně identifikovaných právních předpisech – v nařízení GDPR a v aktuálním Digital Markets Act a Digital Services Act. Je patrné, že autor se v problematice detailně orientuje, což se ve valné míře vhodně projevilo v samotném textu. Autor prezentuje ucelený pohled na vybranou problematiku a identifikuje klíčové problémy včetně možností jejich řešení.

Za cíl práce si autor zvolil, že bude „*analyzovat dopad nových nařízení o digitálních trzích (dále jen „DMA“) a nařízení o digitálních službách (dále jen „DSA“) do právního rámce ochrany osobních údajů, jak jej aktuálně definuje GDPR a úvahy de lege ferenda nad vymáháním regulace osobních údajů ve všech těchto třech nařízeních.*“[28] Takto nastavené cíle byly autorem naplněny, vhodně a systematicky prezentuje jednotlivé průniky a souvislosti v rámci vybraných předpisů, dále v práci identifikuje jejich relevanci a hodnotí jejich dopady a problematické aspekty.

Práce je (kromě úvodu a závěru) rozdělena do čtyř základních částí.

V úvodní části (kapitole 2) je charakterizován evropský digitální balíček a jeho šíře a komplexnost, tedy vnitřní rozpory mezi danými předpisy lze předpokládat, což autor dále specifikuje a zaměřuje na problematiku osobních údajů obsažených v GDPR a specificky ve vybrané právní úpravě v nařízeních DMA a DSA, která jsou v další části představena. V rámci nově

[28] Viz s. 16 recenzované práce.

představených předpisů budou relevantní povinnosti vznikat nejdříve pro velmi velké subjekty, posléze se pak až do plné účinnosti v roce 2024 budou postupně aplikovat na subjekty menší. „*Dále je v práci poukázáno na některá stěžejní ustanovení těchto dvou nařízení, která mají sloužit k ochraně soukromí nebo osobních údajů. Těmito konkrétními ustanoveními se pak práce bude zabývat dále.*“[29]

V kapitole 3 autor rozebírá vybraná ustanovení DMA[30] a DSA[31] a úpravu obsaženou v GDPR, a to za „*účelem odhalení případných střetů nebo nejasných vztahů v rámci vymáhacích mechanismů těchto nařízení.*“[32] Těmi je pak konkrétně myšlena zejména taková situace, kdy by mohlo dojít k sankcionování povinného subjektu dle dvou různých předpisů (tedy potenciálně ke kumulaci sankcí apod.).

Právě problematice dvojího vymáhání sankcí na základě zkoumané právní úpravy se věnuje autor v další kapitole (4), respektive v této kapitole autor rozebírá metody, které by zabránily nejistotě, jakým způsobem konflikty mezi právními úpravami a jejich vymáhacími mechanismy řešit. Účelem této kapitoly tak je především dojít k použitelnosti identifikovaných ustanovení tak, aby byla zachována vnitřní sounáležitost a bezrozpornost celého právního rámce ochrany osobních údajů – GDPR jako *lex generalis* a DMA a DSA potenciálně jako *lex specialis*. V této kapitole se také autor zpětně zabýval širšími souvislostmi nové právní úpravy a důvody jejího přijetí především v souvislosti s regulací tzv. „strážců přístupu“ a velmi velkých online platforem (ale nejen jich), jelikož právě z účelu přijímané právní úpravy je možné potenciálně dovodit, jakým způsobem k dvojí úpravě přistupovat.

---

[29] Viz s. 17 recenzované práce.

[30] V rámci tohoto předpisu jako problematické identifikuje článek 5 odstavec 2 „*(kombinování osobních údajů bez souhlasu), 6 odstavec 9 (přenositelnost údajů), odstavec 10 (předání osobních údajů bez souhlasu), odstavec 11 (předání neanonymizovaných dat) a článek 7 odstavec 8 (princip minimalizace údajů).*“ Viz s. 58 recenzované práce.

[31] V rámci tohoto předpisu jako problematickou identifikuje především „*absenci efektivních mechanismů spolupráce s orgány pověřenými ochranou osobních údajů. To je přitom společný problém pro DMA i DSA. Přímý střet s úpravou GDPR nebyl v DSA nikde nalezen.*“ Viz s. 58 recenzované práce.

[32] Viz s. 17 recenzované práce.

V návaznosti na předešlé v kapitole 5 autor diskutuje, že přestože dvojí vymáhání je nechtěným jevem, může se v závěru jednat o úmysl evropského zákonodárce. Rozebírá pak více důsledky právě toho, že by se jednalo o jev zamýšlený, včetně představení analogické argumentace v souvislosti s rozhodovací praxí Soudního dvora Evropské unie. Přestože se tak jedná o validní přístup, je poměrně velkým zásahem především do právní jistoty a do práva na spravedlivý proces a autor správně v samotném závěru nabízí korelaci pomocí soft law při zachování dvojího vymáhání jako mimořádného stavu. Je tak nutno dle jeho závěru vytvořit ideálně tzv. koordinační soft law – mělo by se jednat o set výkladových pravidel, který by měl efektivně koordinovat postupy při vymáhání ekvivalentních ustanovení proti obdobnému subjektu.

Autor pak závěrem velmi konkrétně uvádí, že „u *překryvů mezi DMA a GDPR se jedná o případy, kdy je dvojí vymáhání nezbytné. K dostatečnému zachování práv dotčených subjektů a udělování proporčních sankcí je ovšem stále třeba přijmout koordinační soft law, které by napomohlo správnému fungování daných vymáhacích vztahů. Pro chybějící koordinaci mezi DSA a GDPR při jejich vymáhání bylo soft law také identifkováno jako vhodný nástroj ke stabilnímu udržení vykládaných ustanovení mezi DSA a GDPR.*“[33]

Právní úprava a její problémy jsou v této práci prezentovány systematicky a přehledně, autor postupuje vhodně metodologicky od obecného ke konkrétnímu. Přečtení práce tak lze jen doporučit, a to i vzhledem k tomu, že je patrné, že autor se v tématu orientuje velmi dobře a je schopen komplexně uchopit komplikovanou právní úpravu, která je z GDPR, DMA a DSA (a jejích průniků) patrná. Práce se sice může zdát převážně jako analytická, v závěru ale autor vhodně hodnotí problematické aspekty a doporučuje některé návrhy pro řešení překryvů mezi identifikovanou právní úpravou. Závěrečná část pojednávající o soft law by si zasloužila možná detailnější rozbor, a to i pro to, že je důležitá mj. pro DSA, jehož rozbor je v závěrečných částech textu poněkud upozaděn. Právě soft law by mělo být odpovědí na řešení problému překryvu právních úprav. Pravděpodobně pak také bude jednat o přístup (a to vzhledem k aktuální legislativní aktivitě

[33] Viz s. 86 recenzované práce.

Evropské komise), který by neměl být využitelný jen v představované problematice.

STANKOVÁ, P: KRIMINALIZACE ÚTOKŮ NA INFORMAČNÍ SYSTÉMY

JIŘÍ MULÁK[34]

STANKOVÁ, P: Kriminalizace útoků na informační systémy. 2023, diplomová práce, Univerzita Karlova, Právnická fakulta, 106 s.

ANOTACE

Diplomová práce se zabývá problematikou kriminalizace útoků na informační systémy. Aktuálnost tématu je podtržena rapidním vývojem informačních a komunikačních technologií a přesunem každodenních aktivit do virtuálního prostředí. V současné době kybernetická kriminalita představuje rostoucí nebezpečí nejenom pro jednotlivce, ale také pro stát. Cílem práce je představit kybernetické útoky a trestněprávně je klasifikovat. Dále je pozornost koncentrována na procesněprávní stránku útoků, zejména na jejich odhalování, vyšetřování a postup při mezinárodní spolupráci. Opomenut není ani nadnárodní a mezinárodní rámec v boji proti kybernetické kriminalitě. Snahou práce je zjistit, jakým problematickým aspektům čelí tuzemská právní úprava a jaký budoucí vývoj lze v oblasti kyberzločinu očekávat. Úvodní část objasňuje základní pojmy, se kterými práce hojně pracuje. Následně jsou představeny klíčové mezinárodní instrumenty v boji proti kybernetické kriminalitě. Těžiště je věnováno představení jednotlivých druhů kybernetických útoků a jejich následné trestněprávní klasifikaci. Navazující část přibližuje procesní rovinu problematiky, přičemž vymezená část obsahuje taktéž poznatky z kriminologie, jako je typologie pachatelů a jejich motivů. Zmíněna je taktéž problematika aktuálních trendů v kyberprostoru, jako jsou cloudová úložiště, virtuální měny a virtuální krádeže. Závěrem jsou předsta-

[34] JUDr. Jiří Mulák, Ph.D. je odborným asistentem na Katedře trestního práva Právnické fakulty Univerzity Karlovy, kontaktní e-mail: mulakj@prf.cuni.cz.

veny statistické údaje týkající se nápadu kybernetické trestné činnosti v České republice během posledních let a předpokládaného budoucího vývoje. Kapitola současně reflektuje i vývoj kybernetické trestné činnosti v souvislosti s koronavirovým onemocněním COVID-19 a probíhajícím válečným konfliktem na Ukrajině. Mimo to jsou prezentovány vize a cíle České republiky v oblasti kybernetické bezpečnosti.

KLÍČOVÁ SLOVA

Kybernetická kriminalita; kyberútok; kyberprostor

ABSTRACT

This master thesis deals with the issue of criminalization of attacks on information systems. The topicality of the topic is supported by the rapid development of information and communication technologies and the shift of everyday activities to the virtual environment. Nowadays, cybercrime poses a growing danger not only to individuals but also to the state. The aim of this thesis is to introduce cyberattacks and to classify them from the perspective of the criminal law. Furthermore, attention is concentrated on the procedural aspect of the attacks, in particular on their detection, investigation and the procedure of international cooperation. The transnational and international frameworks in the fight against cybercrime are also considered. The thesis seeks to identify what problematic aspects domestic legislation faces and what future developments in the field of cybercrime can be expected. The introductory section explains the basic terms that are used extensively in the thesis. Subsequently, key international instruments in the fight against cybercrime are introduced. The focus is on introducing the different types of cyberattacks and their subsequent criminal classification. The subsequent part introduces the procedural level of the issue, while this part also includes findings from criminology, such as the typology of perpetrators and their motives. The issue of current trends in cyberspace such as cloud storage, virtual currencies and virtual theft is also mentioned. Finally, statistical data concerning the incidence of cybercrime in the Czech Republic in recent years and possible future developments are presented. At the same time, the chapter also reflects on the development of cybercrime in the context of the COVID-19 coronavirus dis-

ease and the ongoing war conflict in Ukraine. In addition, the vision and goals of the Czech Republic in the field of cyber security are presented.

KEY WORDS
Cybercrime; Cyberattack; Cyberspace

Plná verze práce je dostupná z: https://dspace.cuni.cz/handle/20.500.11956/179367

Diplomová práce představuje rozbor problematiky kyberkriminality, což je aktuální i společensky závažné téma. Jde o téma aktuální, neboť v oblasti informačních technologií neustále dochází k dalšímu rozvoji a rozmachu v oblasti kriminality. Zřetelné jsou stále sofistikovanější způsoby jejího páchání, na což je nezbytné kontinuálně reagovat jak v oblasti prevence a kriminalistických metod vyšetřování, tak také v oblasti rozhodovací praxe a podřazování nových případů pod stávající trestné činy či reaktivním vytváření nových skutkových podstat.

Problematika útoků na informační systémy je problematikou závažnou, aktuální a rovněž i náročnou na zpracování, neboť jde o jednu z nejkomplexnějších oblastí trestního práva v 21. století. Vyžaduje totiž znalosti trestního práva hmotného i procesního a také znalosti z oborů kriminologie, kriminalistiky, mezinárodního práva a informačních technologií. Diplomantka při psaní práce vycházela zejména ze standardních metod při zpracování odborného textu jak je analýza a deskripce. Pracovala přitom s nadprůměrným počtem pramenů, mezi nimiž jsou kromě tuzemských zdrojů a judikatury zastoupeny ve značné míře také prameny zahraniční.

Diplomová práce je s výjimkou úvodu a závěru členěna do sedmi na sebe logicky navazujících kapitol, které jsou dále členěny na podkapitoly. Úvodní část objasňuje základní pojmy (kyberkriminalita či kyberprostor), se kterými diplomantka v rámci práce dále pracuje. Následně jsou představeny klíčové mezinárodní instrumenty v boji proti kybernetické kriminalitě (v kontextu EU a Rady Evropy). Těžiště diplomové práce je věnováno představení jednotlivých druhů kybernetických útoků a jejich následné trestně-

právní klasifikaci. Je postihnut hacking obecně, dále také phishing, sniffing, DoS a DDoS, či malware. Navazující část přibližuje procesní rovinu problematiky, přičemž vymezená část obsahuje taktéž poznatky z kriminologie, jako je typologie pachatelů a jejich motivů. Zmíněna je taktéž problematika aktuálních trendů v kyberprostoru, které zahrnují typicky cloudová úložiště, virtuální měny a virtuální krádeže. Závěrem jsou představeny statistické údaje týkající se nápadu kybernetické trestné činnosti v ČR za poslední léta, jakož i predikce budoucího vývoje. Kapitola současně reflektuje i vývoj kybernetické trestné činnosti v souvislosti s koronavirovým onemocněním COVID-19 a probíhajícím válečným konfliktem na Ukrajině. V práci jsou dále prezentovány rovněž cíle ČR v oblasti kybernetické bezpečnosti.

Předložená práce představuje velmi zdařilé zpracování zvoleného tématu. Diplomantka prokázala, že se ve zvolené problematice velmi dobře orientuje. Je třeba ocenit počet použitých zdrojů včetně zdrojů zahraničních. Orientace v problematice je pak prokazována rovněž tím, že autorka do práce vhodně zakomponovala i aktuální trendy a informace, např. BitB jako aktuální trendy phishingu, nově přijatou Strategii prevenci kriminality, problematiku Covid-19 a další.

Autorka též prokázala velký přehled v technických normách a metodologii zajišťování digitálních stop. Předložená práce splňuje všechny obsahové i formální náležitosti, které jsou kladeny na tento typ kvalifikační práce.

PEŠKOVÁ, M: TRANSPOZICE INSTITUTU ENERGETICKÉHO SPOLEČENSTVÍ DO ČESKÉHO PRÁVNÍHO ŘÁDU

VÁCLAV ŠMEJKAL[35]

PEŠKOVÁ, M: Transpozice institutu energetického společenství do českého právního řádu. 2022, diplomová práce, Univerzita Karlova, Právnická fakulta, 185 s.

ANOTACE

Hlavním tématem diplomové práce je institut energetických společenství a jeho transpozice do českého právního řádu. Energetickými společenstvími se rozumí občanské energetické společenství podle směrnice Evropského parlamentu a Rady (EU) 2019/944 ze dne 5. června 2019 o společných pravidlech pro vnitřní trh s elektřinou a o změně směrnice 2012/27/EU a společenství pro obnovitelné zdroje upravené směrnicí Evropského parlamentu a Rady (EU) 2018/2001 ze dne 11. prosince 2018 o podpoře využívání energie z obnovitelných zdrojů. Ani jedna z uvedených směrnic nebyla v ČR v době psaní práce plně transponovaná, ačkoliv transpoziční lhůty v obou případech již uplynuly. První kapitola diplomové práce rozebírá obecně transpozici unijních směrnic z teoretického pohledu včetně metod transpozice a úpravy procesu transpozice směrnic na národní úrovni. Druhá kapitola se zabývá už samotnou unijní právní úpravou energetických společenství. Identifikovány jsou společné charakteristiky a také základní rozdíly mezi oběma typy energetických společenství včetně důsledků, které z těchto rozdílů plynou pro přípravu transpozičního právního předpisu. Třetí část práce analyzuje zahraniční zkušenosti s energetickými společenstvími ve vybraných zemích EU, konkrétně v Německu, Rakousku, Portugalsku a Slovensku. Pozornost je věnována nejen praktickým zkušenostem s existencí energetických

[35] doc. JUDr. Václav Šmejkal, Ph.D. je docentem na Katedře evropského práva Právnické fakulty Univerzity Karlovy, kontaktní e-mail: smejkalv@prf.cuni.cz.

společenství, ale zejména v současnosti platné nebo nově navrhované právní úpravě. Ve čtvrté, závěrečné kapitole jsou okomentovány rámcové představy o transpozici energetických společenství podle věcného záměru nového energetického zákona a uvedena doporučení autorky, která by mohla být zohledněna při transpozici abstraktních unijních ustanovení o energetických společenstvích do českého právního řádu. Příloha diplomové práce potom obsahuje konkrétní návrh paragrafového znění úpravy energetických společenství na zákonné úrovni. Tím je naplněn cíl práce, jímž je poskytnout praktické návrhy legislativních řešení k transpozici energetických společenství do nového energetického zákona a tím pozitivně ovlivnit průběh jeho legislativního procesu a celkovou kvalitu právní úpravy.

KLÍČOVÁ SLOVA

Energetické společenství; transpozice; směrnice; nový energetický zákon

ABSTRACT

The main topic of the diploma thesis is the legal concept of energy communities and its transposition into Czech law. The term "energy communities" means both citizen energy communities according to the Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU and renewable energy communities as defined by the Directive (EU) 2018/2001 of the European Parliament and of the Council of 11 December 2018 on the promotion of the use of energy from renewable sources. None of the mentioned directives has, at the time this thesis has been written fully transposed in the Czech Republic, although the transposition deadlines in both cases have already passed. The first chapter of the diploma thesis discusses the transposition of EU directives in general and from a theoretical point of view, including transposition methods and a description of the process of transposition of directives at the national level. The second chapter deals with the EU legal provisions regulating the energy communities themselves. Common characteristics, as well as basic differences between both types of energy communities, are identified, including the consequences of these differences for the preparation of transposition legislation. The third

part of the thesis analyses foreign experience with energy communities in selected EU countries, specifically in Germany, Austria, Portugal, and Slovakia. Attention is paid not only to practical experiences with the existence of energy communities but especially to currently effective or newly proposed legislation. In the fourth and final chapter, the framework ideas on the transposition of energy communities according to the white paper of the new Energy Act are commented on and the author's recommendations how to transpose the abstract EU provisions on energy communities into the Czech legal order are given. The annexe of the diploma thesis then contains an articulated version of a draft act regulating energy communities. This fulfils the goal of the diploma thesis, which is to provide practical proposals for legislative solutions for the transposition of energy communities into the new Energy Act and thereby positively influence its legislative process and the overall quality of legislation.

KEY WORDS

Energy Community; Transposition; Directive; New Energy Act

Plná verze práce je dostupná z: https://dspace.cuni.cz/handle/20.500.11956/180041

Téma posuzované práce je nepochybně aktuální, neboť se týká probíhajících prací na transpozici EU směrnic spadajících do „balíku" Čisté energie pro všechny Evropany (CEP). Tato aktuálnost je navíc zvýrazněna stávající kritickou situací na trzích s elektřinou a plynem, jakož i kontroverzností debat o klimatické změně a s ní související potřebou přechodu k obnovitelným zdrojům energie atd.

Zvolené téma, tak jak bylo autorkou vymezeno, vyžaduje především skvělou obeznámenost s evropskou a národní legislativou v energetickém sektoru a dále s procesem transpozice směrnic EU 2019/944 a 2018/2001 do právních řádů členských zemí EU, samozřejmě včetně probíhajících prací na transpozici v ČR. Vedle toho zpracování práce s daným obsahem přepokládá dobrou orientaci v právu EU, v právu obchodních korporací, občanském a správním právu. Co do teorie se posuzovaná práce nesnaží na-

stolovat a řešit doktrinální otázky, směřuje spíše k pragmatickému, legislativně-technickému zpracování tématu, a to až po návrh paragrafového znění klíčových částí energetického zákona.[36] I „nejteoretičtější" kapitola 1 o transpozici unijních směrnic je spíše přehledovým úvodem (svého druhu „*literature review*") než organickou částí výzkumu.

Z hlediska systematiky je práce členěna do čtyř hlavních obsahových kapitol, kterými se autorka snaží pokrýt téma od obecných otázek transpozice směrnic EU, přes ukázky praktického převzetí směrnic o OES[37] a SOZ[38] ve vybraných členských státech EU, až po velmi konkrétní návrhy řešení zcela detailních otázek v budoucích zákonech ČR. Jedná se o členění přehledné, v němž každá kapitola je „samonosná" svým obsahovým zaměřením a plní v rámci práce jako celku určitou roli.

Co do formálního členění práce by bylo vhodné, kdyby autorka používala více úrovní podkapitol, resp. mezi-titulků, protože některé její podkapitoly jsou z hlediska komfortu čtenáře příliš dlouhé.[39] Jiné pak spojují více témat, která by lépe mohla být pojednána v samostatných podkapitolách.[40]

Po stránce čistě formální je práce napsána velmi kvalitním odborným jazykem, bez rušivých chyb a překlepů. Podání autorky je v popisných i analytických pasážích velmi jisté a logické, ačkoli množství zkratek, výrazů a slovních spojení obtížně srozumitelných neprofesionálům v oboru energetiky[41] vyžaduje od čtenáře nejen neustálé přelistovávání na více než pětistránkový seznam zkratek, ale i občasné dohledávání energetické terminologie na internetu.

Práce je zcela nepochybně odborně vysoce fundovaným rozborem otázek spojených s OES a SOZ ve smyslu výše uvedených směrnic EU a také otázek jejich transpozice do právních řádů členských států. V obeznámenosti s touto problematikou, v přístupu ke zcela konkrétním informacím,

[36] Srov. Příloha 1, s. II-V.

[37] Tzn. Občanské energetické společenství.

[38] Tzn. Společenství pro obnovitelné zdroje energie.

[39] Za všechny příkladem přes 10 stran dlouhá podkapitola 2.3.

[40] Např. podkapitola 4.1.1, která na více než sedmi stranách rozebírá otázky členství v OES a současně kontroly nad ním.

[41] Např. „agregace poskytované flexibility" na s. 54.

odborným studiím, materiálům regulačních úřadů atd., je autorka v domácí akademické obci zřejmě bezkonkurenční.

V návaznosti na výše uvedené je tedy nepochybné, že práce přináší nové a původní poznání, které není triviální ani běžně dostupné a činí tak způsobem, který odpovídá odborné analýze nastolených problémů. Autorka prokázala potřebnou orientaci i v oborech práva souvisejících s tématikou regulace v energetice, ať se jedná o právo EU, české právo obchodních korporací, právo občanské a správní. Práce s prameny je příkladná,[42] dotažení analýz do aktuální současnosti nepochybné.

Velmi sympatické je vkládání grafických znázornění a tabulek do textu, které pro čtenáře vhodně strukturují množství informací v textu obsažených a v něčem nahrazují i chybějící mezi-titulky či jiné způsoby vnitřního členění textu. Nedostatky práce je možné spatřovat tedy spíše v jejím koncepci a formálním pojetí než v kvalitě jejího sdělení. Předně je zřejmé, že práce mohla být kratší, aniž by její klíčové sdělení utrpělo.

Kratší mohla být úvodní kapitola věnovaná otázkám transpozice směrnice do právních řádů členských států. Jak již bylo uvedeno výše, působí jako rozsáhlý samostatný celek (či „*literature review*“), na nějž je sice v dalších kapitolách tu a tam odkazováno, nikoli však v míře, která by ospravedlňovala jeho dvacetistránkový rozsah a obsah odpovídající spíše práci věnované něčemu jinému než velmi technickému a pragmatickému rozboru toho, jak převést do národního právního řádu instituty OES a SOZ.

V každém případě musí čtenář vnímat jako zcela neorganický ostrý předěl mezi kapitolami 1 a 2 práce, které jako by k sobě ani nepatřily. Bylo by tudíž čtenářsky vstřícnější a pro celkové vnímání dalšího obsahu práce vhodnější, pokud by úvodní kapitola byla věnována spíše úvodu do unijní úrovně regulace energetiky s její specifickou terminologií a jejími dopady do národní úrovně. Rovněž měly být v úvodu instituty OES a SOZ alespoň stručně, ale srozumitelně, definovány, protože v práci se tak děje až na s. 30, ačkoli od počátku jde v textu především o ně.

Zkrácení by se mohlo týkat i pasáží, které jsou svou povahou spíše technické či legislativně technické a připomínají tak dílčími informacemi nabi-

[42] Srov. 328 odkazů na 140 stranách textu.

tou příručku či oponenturu pro potřeby pracovníků Ministerstva průmyslu a obchodu než právní výzkum. Neřeší totiž ani tak otázky právní, jako poskytuje přehled možných přístupů, jak do právního jazyka převést prakticky fungující technicko-organizační řešení. V kontrastu k nim je pro čtenáře-právníka velmi osvěžující typicky právní analýza obsažená např. v podkapitole 4.1.2, věnované tomu, jaká právní forma by v právu ČR nejvíce pasovala na OES resp. SOZ.

Jako dílčí připomínky je možné zmínit např. skutečnosti neodpovídající poznámku o malém využívání formy S.E. (Societas Europaea) v ČR,[43] když naopak i ze snadno dostupných zdrojů[44] lze zjistit letitou pravdu, že v ČR se setrvale registruje násobně více S.E. než ve zbylých 26 členských státech EU dohromady. Dále nepovažuji za vhodné přejít v závěrečné kapitole práce[45] na kritický rozbor aktuálních opatření vlády na snížení a stabilizaci cen energií pro koncové odběratele. Závěr má sloužit ke shrnujícímu vysvětlení toho nakolik provedená analýza umožnila naplnit záměr práce, odpovědět na výzkumnou otázku atd., nikoli ke kritickému nastolování nových, v práci neřešených témat.

Uvedené připomínky však oponent považuje za podstatné spíše *pro futuro*, pokud by autorka chtěla výzkum svého tématu prodloužit ve formě rigorózní nebo disertační práce. V celkovém hodnocení práce rozhodně nemění jednoznačné ocenění velmi přínosného, samostatného a zejména informačně velmi vydatného díla.

[43] Srov. s. 118 recenzované práce.

[44] Srov. https://en.wikipedia.org/wiki/Societas_Europaea

[45] Viz s. 139 recenzované práce.

SUSSKIND, R. E.: TOMORROW'S LAWYERS: AN INTRODUCTION TO YOUR FUTURE[1]

ANNA BLECHOVÁ[2]

SUSSKIND, R. E.: Tomorrow's Lawyers: An Introduction to your Future. Oxford: Oxford University Press, 2023, 320 s. eISBN 978-0-19-267999-4

1. ÚVOD

„The future is already here – it's just not evenly distributed.“[3,4] Známý citát Wiliama Gibsona, který nejen, že je uveden v novém vydání knihy Richarda E. Susskinda, Tomorrows Lawyers[5], ale i poměrně trefně vystihuje její hlavní myšlenku. Budoucnost už tu totiž je, je v mladých nadějných právnících, kteří mají tu moc právní odvětví odvážně měnit a transformovat v návaznosti na nejnovější trendy.

Richard Susskind je britský profesor práva, jehož kariéra je spojená s právem informačních technologií. Je to autor mnoha úspěšných monografií, článků a také přednášek.[6] Kniha, kterou jsem měla možnost pro účely této recenze přečíst, zachycuje jen jednu z částí jeho myšlenek o bu-

[1] Tento článek vznikl v rámci projektu "Právo a technologie XI“, MUNI/A/1293/2022.

[2] Mgr. Anna Blechová je prezenční doktorandkou na Ústavu práva a technologií, Právnické fakulty Masarykovy univerzity, kontaktní e-mail: anna.blechova@law.muni.cz.

[3] Volně je možné přeložit jako „Budoucnost už je mezi námi – jen zatím není rovnoměrně distribuována“.

[4] Broadband blues. *The Economist* [online]. 2021 [cit. 20.06.2023]. Dostupné z: https://www.economist.com/business/2001/06/21/broadband-blues

[5] SUSSKIND, Richard E. *Tomorrow's lawyers : an introduction to your future /*. Oxford: Oxford University Press, 2023, s. 145. Všechny citace z recenzované knihy byly přeloženy autorkou této recenze.

[6] Richard Susskind. In: [cit. 20.06.2023]. Dostupné z: https://www.susskind.com

doucnosti právního odvětví.[7] Tomorrow‘s lawyers poprvé vyšlo v roce 2012, druhá iterace byla publikována v roce 2017 a poslední verze vyšla v březnu roku 2023.[8] Ačkoli pro dnešního čtenáře, který se pohybuje v oblasti IT práva, nebude kniha pravděpodobně žádným třeskavým textem, lze si snadno představit, že v době, kdy Facebook ještě nebyl META a Zoom byl teprve v plenkách, tomu mohlo být zcela jinak. Je ale nutné přiznat, že kniha je napsaná velmi čtivě a přináší mnoho podnětů k zamyšlení.

Kniha samotná je rozdělena systematicky do třech částí. První část má název *„Radikální změny na právním trhu“*, druhá část je věnována definici nového prostředí a závěrečná část pak přibližuje vyhlídky pro mladé právníky[9]. Celkově je kniha rozložena do 22 tematických kapitol.

2. ČÁST PRVNÍ: RADIKÁLNÍ ZMĚNY NA PRÁVNÍM TRHU

Úvod knihy autor otevírá tvrzením, že právní instituce a právníci se změní radikálněji v méně než dvou dekádách než za minulá dvě století.[10] S autorem nelze jinak než souhlasit co se týče toho, že právní profese právě prochází změnou. Nicméně spíše než změnu institucí a právníků a jejich profese můžeme pozorovat změnu nástrojů, které používají, a prostředí, ve kterém se pohybují. Podstata právních profesí zůstane, a měla by zůstat, neměnná. Následně se pak autor věnuje třem proměnným, které danou změnu řídí. Jmenovitě se jedná o (i) „míň-za-víc“ výzvu, (ii) liberalizaci, a (iii) technologie. Všechny tři zmíněné proměnné jsou pak vedeny skrze celou knihu jako pojící prvky.

---

[7] SUSSKIND, Richard E. *Tomorrow’s lawyers*. p. ix-x. Ostatní autorovy knihy, blíže přibližující dané téma jsou např. SUSSKIND, Richard. *Online Courts and the Future of Justice*. New York: Oxford University Press, 2019.; SUSSKIND, Richard. *The Future of Law: Facing the Challenges of Information Technology*. Oxford, New York: Oxford University Press, 1998.; SUSSKIND, Richard E. 1961-. *The future of the professions : how technology will transform the work of human experts /*. Oxford University Press, 2015.

[8] SUSSKIND, Richard E. *Tomorrow’s lawyers,* p. vii-x.

[9] Důležité je zmínit, že Susskind ve své knize pojmem „Young Lawyers“(mladí právníci) nemyslí pouze mladé právníky dle věku a zkušeností, ale i ty, kteří se mladí cítí nezávisle na dvou výše zmíněných proměnných. Ibid., s. 1–2.

[10] Ibid., s. 1.

Zvláštní důraz autor klade na „více-za-méně“ výzvu, kterou vnímá jako primární impuls pro změnu fungování právního trhu.[11] Tento prvek je Susskindem popisován ve spojitosti s touhou zákazníků po větším množství informací za méně peněz. Tento jev není spojen pouze s nechutí zákazníků vynaložit potřebné prostředky, ale především s faktem, že potřebné prostředky často k dispozici vůbec nemají.[12] Zároveň pak autor předpokládá, že poptávka po právních službách v kontextu komplexních problémů může vzrůstat.[13] V návaznosti na předchozí dva faktory by pak více-za-méně výzva mohla fungovat jako motivace pro právníky, aby zásadně změnili styl své práce (i za využití technologií) a zaměřili se více na možnosti spolupráce a nabízení svých služeb jako „licencí“ ke svému know-how. Tato myšlenka se následně odráží i ve třetí kapitole knihy, která se věnuje obchodním strategiím pro zaručení úspěšného právního podnikání v kontextu autorem předpokládaných změn.

V jedné z dalších kapitol této části se Susskind (oproti předchozím verzím knihy) věnuje konkrétně pandemii COVID-19. Celou kapitolu autor otevírá konstatováním, že celosvětová pandemie urychlila nasazení vybraných technologií, na které ve svých pracích upozorňoval již dříve.[14] Nicméně vzápětí zmiňuje, že toto urychlení nasazení některých technologií (ačkoli se jedná o pozitivní změnu) v právním prostředí není možné vnímat jako žádnou revoluci. V tomto s autorem knihy nelze jinak než souhlasit. I když plno právníků po celém světě začalo více využívat technologie a pracovat i z domova, jejich styl práce se často nezměnil a pouze došlo k aktualizaci pracovních nástrojů. Ta pravá revoluce, jak je popsáno v této knize, je pak spojená především s hlubšími změnami práce, a to především změnou pracovního stylu a přístupu. Zajímavé je pak Susskindovo tvrzení, že celosvětovou pandemii je možné vnímat jako nenaplánovaný pilotní

[11] Ibid., s. 27.

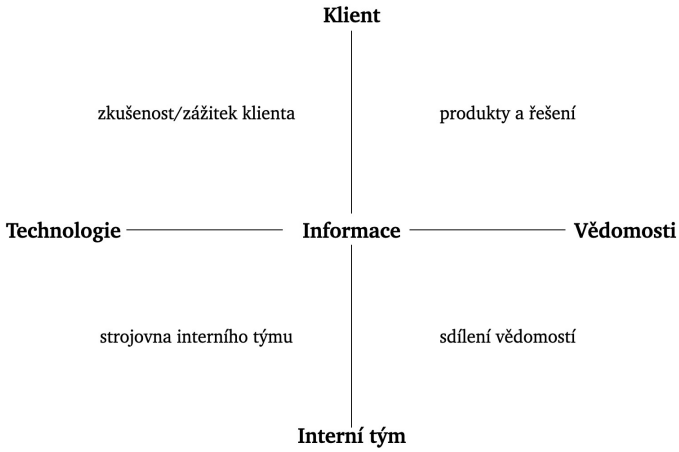
[12] Ibid., s. 12–13.

[13] Ibid., s. 13–14.

[14] Ibid., s. 28–29.

program pro změnu právních profesí.[15] Otázkou zůstává, zda byl ale tento program úspěšný, či nikoli.

Poslední kapitola této části nese název „síť“[16,17] a osobně ji považuji za jednu z nejzajímavějších. Susskind v této části postupně a velmi trpělivě rozebírá vztah mezi zpracováním informací a jejich zhodnocením. Základní „souřadnicovou síť“ pak nastiňuje graf v obrázku č. 1.



Obrázek č. 1, zdroj: SUSSKIND, Richard E. *Tomorrow's lawyers*, s. 84

Autor představuje, jak s informací pracovat v kontextu interního zpracování a hodnocení, a jak z pohledu externího (z pohledu klientského).[18] Dále v souřadnicové síti demonstruje vztah mezi vědomostmi a technologiemi. Na základě tohoto rozdělení pak autor vymezuje čtyři kvadranty, které definují jednotlivé oblasti. Příkladem je vztah mezi zpracováním informace ve spojitosti s interním zhodnocením a technologií. Tuto oblast Susskind obecně považuje za „strojovnu interního týmu“ a konkrétně se dle něj jedná

[15] Ibid., s. 30.

[16] V originálním znění kapitola nese název „Grid“.

[17] SUSSKIND, Richard E. *Tomorrow's lawyers*, s. 79 a násled.

[18] Ibid., s. 79–85.

například o management dokumentů, marketingové databáze, hardware network. Oproti tomu protilehlý kvadrant, tedy vztah mezi zpracováním informací v kontextu klienta a vědomostí, označuje pojmem produkty a řešení.[19] Právě v rámci tohoto kvadrantu by měla přicházet inovativní řešení a nové obchodní modely posouvající právní odvětví. Příkladem změn, které připadají v úvahu, jsou například využití ODR, automatizace dokumentů, využití umělé inteligence, či nasazení prediktivních systémů.[20]

3. ČÁST DRUHÁ: NOVÉ PROSTŘEDÍ

Druhá část knihy se zaměřuje na vymezení a zkoumání prostředí právního odvětví. Desátá kapitola knihy tak popisuje například postavení a vliv startupů v kontextu budoucnosti právního odvětví a označuje je za primární hnací motory radikálních změn.[21] Na světě v tuto chvíli operuje cca 3000-4000 právních startupů, což je zásadně více než v době prvního vydání knihy, kdy jich byly pouze nižší stovky.[22] Krom toho v současné době tyto společnosti začínají být zajímavou investiční příležitostí.[23,24] V závěru kapitoly autor pak startupy rozděluje do dvou kategorií. První kategorie zahrnuje ty startupy, které budou skutečně narušovat a odstraňovat potřeby tradičního dodavatelského řetězce tradičních právníků. Jedná se o budoucí právní Amazony a Ubery. Cílem těchto startupů není samoúčelná likvidace pracovních příležitostí právníků, i když to může být do jisté míry důsledkem. Primárním cílem a hnacím imperativem, je splnění výzvy "více za méně", která byla zmíněna již v první části knihy.[25] Druhá kategorie pak zahrnuje ty startupy, které přinášejí revoluční řešení, které si dokážou poradit

[19] Ibid., s. 84–85.

[20] Ibid., s. 86–87.

[21] Ibid., s. 122–123.

[22] Ibid., s. 123–124.

[23] Ibid., s. 124–125.

[24] CROFT, Jane. Why are investors pouring money into legal technology? *Financial Times* [online]. 2022 [cit. 21.06.2023]. Dostupné z: https://www.ft.com/content/b6f0796e-0265-40c6-ad4c-a900cd788c39; GAMMER, Isabelle. Making a positive business case for tech investment. In: *LexisNexis Blogs* [online]. 2. 5. 2023 [cit. 21.06.2023]. Dostupné z: https://www.lexisnexis.co.uk/blog/future-of-law/tech-investment-how-lawyers-can-make-the-case

[25] SUSSKIND, Richard E. *Tomorrow's lawyers*, s. 127–128.

i s velkými problémy, u kterých současný systém zpravidla selhává, jako je např. přístup k justici.[26] V návaznosti na situaci spojenou s právními startupy se lze ztotožnit s autorovým přesvědčením o tom, že právě právní startupy jsou jedním z nejenergičtějších a nejvíc inspirujících zákoutí právního světa.

Několik kapitol této části je pak věnováno oblasti online soudnictví. Jak autor předesílá již v úvodu recenzované knihy[27], této oblasti se dopodrobna věnoval už ve své předchozí knize „Online Courts and the Future of Justice“[28]. Susskind v této části knihy adresuje jeden z nejpalčivějších problémů dnešního justičního systému a tím je přístup k justici jako takové.[29] Řešením této situace pak autor vidí ve využití technologií a rozšíření justičního systému o jeho online asynchronní podobu soudu. Zároveň autor zdůrazňuje, že pouhé přesunutí soudu do online prostředí komunikačních platforem jako Zoom není žádnou „revolucí“. Budoucnost řešení sporů totiž spočívá v jiných aspektech, než je jen přesunutí soudního procesu z fyzických soudních síních do online prostředí.[30] Zároveň se autor okrajově nastiňuje i téma, zdali je soud místo nebo služba.[31]

Poslední kapitola této části se věnuje tématu budoucnosti práva s důrazem na změnu přístupu k této profesi. Autor zde vychází ze své dřívější publikace s názvem „The Future of Law“[32] a zaměřuje se na konkrétní oblasti, u kterých očekává změnu v přístupu. Vzhledem k tomu, že původní kniha vznikla v 90. letech minulého století, má autor možnost k určité reflexi a ohlédnutí se za více než čtvrtstoletím od vyřčení svých původních prognóz. Příkladem takových prognóz je změna právního servisu z poradního na informativní, změna přístupu z jeden-na-jednoho na jeden-na-mnoho, změna finančního schématu z hodinových sazeb na sazby za jednotlivé

[26] Ibid., s. 128–129.

[27] Ibid., s. 6.

[28] SUSSKIND, Richard. *Online Courts and the Future of Justice*.

[29] SUSSKIND, Richard E. *Tomorrow's lawyers*, s. 139 a násled.

[30] Ibid., s. 159–160.

[31] Ibid., s. 161–164. Blíže k této polemice viz BLECHOVÁ, Anna. *Online soudnictví jako výzva pro justici*. 2022. Diplomová práce. Masarykova univerzita. Právnická fakulta, s. 23–32.

[32] SUSSKIND, Richard. *The Future of Law*.

služby. V rámci právního procesu pak autor předpovídal přesun od tištěných právních materiálů a zdrojů k těm elektronickým. [33]

4. ČÁST TŘETÍ: VYHLÍDKY PRO MLADÉ PRÁVNÍKY

Závěrečná část knihy se pak věnuje vyhlídkám pro mladé právníky. Autor tuto část lehce cynicky otevírá tvrzením, že zlaté časy právní profese již pominuly. Což může být pro čerstvého absolventa práv poněkud skličující tvrzení.[34] Nicméně je třeba si uvědomit, že za zenitem jsou zlaté časy klasických právních profesí. Co se týče těch nových, budoucích právních profesí, tam se situace liší.[35] Autor přichází se seznamem 15 budoucích „právnických" profesí. Příkladem jsou R&D pracovník, právní projektový manažer nebo vizualizátor právních dat.[36] Zajímavá je pak například pozice hybridního právníka, kdy Susskind apeluje na mladé právníky, aby si rozšířili znalosti o neprávnický obor.[37] V kontextu dané knihy jistě dávají smysl oblasti jako jsou informační technologie, psychologie nebo například sociologie. Nicméně je třeba se zmínit, že tento apel je realizovatelný především za situace, kdy jsou právní vzdělávací programy na vysokých školách rozděleny na bakalářské a magisterské studium. V případě zemí, kde jsou dlouhé magisterské právní programy, se situace částečně komplikuje, jelikož ne všichni studenti mají možnosti a schopnosti vést souběžně dvě studia rozdílných oborů. Tito studenti či mladí právníci, pak ale samozřejmě mají možnost ve vzdělávání po dokončení magisterského právního studia.

Právě vzdělání právníků je pak další oblastí, které se autor věnuje. Pozastavuje se především nad tím, že dnešní britské právnické fakulty nepřipravují studenty, až na výjimky, pro budoucí právní profese. Krom toho tuto úvahu podpořil i faktem, že právnické fakulty objektivně produkují víc právníků, než je volných míst na trhu práce.[38] V navazujících částech textu

[33] SUSSKIND, Richard E. *Tomorrow's lawyers*, s. 178–184.

[34] Ibid., s. 187.

[35] Ibid., s. 187–190.

[36] Ibid., s. 190.

[37] Ibid., s. 193–195.

[38] Ibid., s. 219–221.

si pak autor pokládá jednu z klíčových otázek celé knihy: *„Čím se má stát velké množství mladých právníků“? Vzděláváme začínající právníky, aby se stali tradičními, konzultativními poradci, kteří se specializují na jednoduché právní problémy jednotlivých jurisdikcí, pracují v režimu na míru šitých řešení klientovi a kteří si účtují hodinovou sazbu? Nebo připravujeme příští generaci právníků na to, aby se z nich stali flexibilnější, týmoví, technologicky vyspělí, obchodně zdatní, hybridní profesionálové, kteří jsou schopni překračovat právní a profesní hranice a tvořit nový právní trh?“*[39] Ačkoli autor na tyto otázky jasnou odpověď nedává, rozhodně se jedná o úvahu k zamyšlení. Zároveň předkládá několik možných řešení dané situace. Jako příklad je možné uvést rozšíření tradičního právního vzdělání o dobrovolný modul, který studentům předá nějakou z dovedností pro 21. století.[40]

Poslední kapitola celé knihy se pak věnuje tématu umělé inteligence a dlouhodobým predikcím. Autor předpovídá, že do roku 2040 není nadnesené nebo naivní uvažovat nad skutečností, že právní profese se změní k nepoznání. Co se týče umělé inteligence, Susskind předpokládal, že tento fenomén bude využíván v kontextu analýzy dokumentů, predikčních systémů a automatizace dokumentů.[41] Vzhledem k tomu, že k takovému využití umělé inteligence již dochází, je nezbytné se podívat na další možnosti jejího využití. To autor vidí ve vytvoření komplexních systémů, které v dlouhodobém horizontu dokáží nahradit práci většiny právníků.[42] Ačkoli autor v knize zmiňuje i generativní AI[43], je škoda, že kniha byla dokončena před velkým boomem ChatGPT. Vzhledem k autorově erudici a představivosti by pak jistě byla zajímavá úvaha, jak rychlé rozšíření tohoto nástroje může ovlivnit budoucnost právní profese.

[39] Ibid., s. 224.

[40] Ibid., s. 225–229.

[41] Ibid., s. 255–256.

[42] Ibid., s. 258–260.

[43] Ibid., s. 23–24.

5. ZÁVĚR

Tomorrow's Lawyers je určitě kniha, která stojí za pozornost. Zkušenosti a expertíza autora jsou nepopiratelné, i tak je ale možná na místě budoucího čtenáře této knihy varovat, že některé části mají tendenci problémy částečně zjednodušovat, což pak vede k vytváření nejasností a nepřesvědčivých tvrzení. Příkladem může být kapitola o umělé inteligenci, vzdělávání nebo například online soudnictví.

Nicméně, jak autor sám předpokládá, jedná se o knihu, která má především vést k zamyšlení a podpoře fantazie. Tento cíl kniha jistě naplňuje, ať už je to podnětem k úvahám o budoucnosti soudnictví, využití AI, vzdělávání současných právníků nebo změně obchodního modelu současných právních kanceláří.

Závěrem pak nemohu jinak, než se přiklonit k autorově závěrečnému apelu. I když se budete jako právní „revolucionáři" cítit osamělí, je důležité abyste se připojili k rostoucímu hnutí lidí, kteří „vylepšují spravedlnost" tím, že aplikují technologie při hledání nových cest pro právo, naši nejdůležitější společenskou instituci.[44]

[44] SUSSKIND, Richard E. *Tomorrow's lawyers*, s. 268.

BROWNSWORD, R.: LAW 3.0: RULES, REGULATION, AND TECHNOLOGY[1]

JAN TOMÍŠEK[2]

BROWNSWORD, R.: Law 3.0: Rules, Regulation, and Technology. Abingdon: Routledge, 2021, 130 s. ISBN 978-0-367-51640-6

Kniha Law 3.0 upozorňuje na skutečnost, že naše chování je čím dál častěji na místo pravidel omezováno technologickými opatřeními (ať už jde o architekturu letištních hal nebo nastavení webových platforem). Tato opatření navrhuje zahrnout do šíře práva jako společenské, vědní a pedagogické disciplíny a předkládá také možný přístup k hodnocení jejich legitimity a regulaci technologií obecně.

Podle autora lze v právu rozlišit tři samostatné diskurzy či nastavení mysli – Právo 1.0, Právo 2.0 a Právo 3.0. Právo 1.0 je charakteristické aplikací „pravidel, standardů a obecných principů na konkrétní skutkové situace“.[3] Právo 2.0 se vyznačuje formulací nových pravidel a regulatorních rámců, které slouží konkrétním účelům regulace.[4] Právo 3.0 je podobně instrumentalistické, ale vedle norem jako pravidel chování systematicky uplatňuje k dosahování sledovaných účelů také technologická opatření.[5]

[1] Tento článek vznikl v rámci projektu "Právo a technologie XI“, MUNI/A/1293/2022.

[2] Mgr. et Mgr. Ing. Jan Tomíšek je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity a partnerem v advokátní kanceláři ROWAN LEGAL, kontaktní e-mail: jantomisek@gmail.com.

[3] BROWNSWORD, Roger. Law 3.0: *Rules, Regulation, and Technology*. Abingdon: Routledge, 2020. s. 2. Všechny citace z této knihy byly přeloženy autorem této recenze.

[4] Viz tamtéž, s. 3.

[5] Viz tamtéž.

Autor poukazuje na to, že Právo 1.0 bylo narušeno novými technologiemi, které vedly k otázkám, zda jsou aktuální pravidla přiměřená svému účelu, ať už z důvodu nefunkčnosti nebo úplné absence pravidla pro danou situaci.[6] Právo 2.0 pak bylo narušeno dostupností čím dál širší palety technologií, které lze uplatnit k usměrňování lidského chování nenormativním způsobem.[7] V Právu 3.0 je tak právo jako normativní systém pouze jedním prvkem regulatorního prostředí.[8]

Klíčové je upozornění autora, že technologická opatření omezují naši „praktickou svobodu", tedy rozsah možných jednání v konkrétní situaci.[9] Proto je důležité zabývat se jejich legitimitou stejně jako v případě právních norem. Za tímto účelem autor rozčleňuje odpovědnost regulátorů do tří kategorií – odpovědnost za zachování základních předpokladů lidské existence (*commons*),[10] odpovědnost za respektování základních hodnot určitého společenství[11] a odpovědnost za přijatelné vyvažování zájmů.[12] Soulad s těmito odpovědnostmi by měl být klíčový při použití jakékoli nové technologie v praxi regulovaných subjektů (tj. jakožto objektu regulace) stejně jako při použití technického opatření jako nástroje regulace.[13]

Samotný soulad s těmito požadavky není podle autora dostatečný k tomu, abychom mohli uzavřít, že konkrétní technologické opatření naplňuje požadavky vlády práva. Stejně jako právní pravidla by mělo být přijímáno v souladu s konstitutivními pravidly daného společenství. Na druhou stranu takto přijatá opatření by měla být respektována jejich adresáty.[14] Dalšími požadavky můžou být podrobení opatření veřejné debatě, vratnost opatření, respektování limitů vzešlých z této debaty nebo právo na

[6] Viz tamtéž, s. 16.

[7] Viz tamtéž, s. 29.

[8] Viz tamtéž, s. 51.

[9] Viz tamtéž, s. 65.

[10] Viz tamtéž, s. 72.

[11] Viz tamtéž, s. 74.

[12] Viz tamtéž, s. 75.

[13] Viz tamtéž, s. 76.

[14] Tento požadavek je relevantní tam kde existuje možnost technické opatření obejít. Viz tamtéž, s. 81.

zásah člověka.[15] Zde však autor upozorňuje, že požadavek na zásah člověka se může v praxi vyprázdnit, protože může být poměrně nízká pravděpodobnost, že člověk změní výsledek aplikace technologie, pokud v ní má důvěru. Stejně tak může být nedostatečné spoléhat se na adresáty opatření, že toto své právo uplatní. Vhodnější se proto zdá být průběžná validace výsledků technologického opatření.[16]

Autor dále navrhuje, že novým technologiím by se měly věnovat dedikované a nezávislé instituce, a to jak na národní, tak na mezinárodní úrovni,[17] a navrhuje rozšířit výuku práva na Práva 3.0,[18] aby absolventi právnických fakult byli adekvátně vybaveni pro realitu, která nás obklopuje a ve které hrají technologie nezastupitelnou roli.

Kniha je stručná a čtivá, protože čtenářsky přívětivou formou shrnuje myšlenky vyjádřené ve dřívějších rozsáhlejších akademických publikacích autora.[19] Její první polovina je především popisná, vysvětluje pojmy Práva 1.0, Práva 2.0 a Práva 3.0 a jejich vztahy. Druhá polovina knihy pak předkládá hlavní návrhy autora.

Na jednu stranu lze říci, že řada východisek, které autor shrnuje v první polovině knihy, není nijak objevná. Je jasné, že naše chování v praxi ovlivňují nenormativní faktory utvářené člověkem, resp. formované regulátory – např. ekonomické nástroje, které se běžně v regulaci používají.

Na druhou stranu diskuze, kterou autor otevírá, a problémy, na které poukazuje, jsou v současné době významné, protože technologická opatření hrají v regulaci našeho chování čím dál větší roli. Proto je na místě pracovat s nimi v právu systematicky a zkoumat jejich legitimitu. Význam této diskuze podtrhuje rozvoj technologií, jako je generativní umělá inteligence, která má velký potenciál použití pro regulaci.

---

[15] Viz tamtéž, s. 82 a násl.

[16] Viz tamtéž, s. 91 a násl.

[17] Viz tamtéž, s. 95 a násl.

[18] Viz tamtéž, s. 103 a násl.

[19] Viz tamtéž, s. 6. s odkazem na BROWNSWORD, Roger. *Law, technology and society: reimagining the regulatory environment.* Abingdon: Routledge, 2019. a BROWNSWORD, Roger. Law Schools for Lawyers, Citizens, and People. In: *The Law School-Global Issues, Local Questions*. Abingdon: Routledge, 2019. s. 26–40.

Do jisté míry může být problematická úvaha autora o třech kategoriích odpovědností regulátorů, kdy se jeho pojetí základních předpokladů lidské existence zdá být významně formováno euroatlantickým pohledem na svět a nemusí být zcela funkční v jiných kulturách, které jsou méně antropocentrické.[20] Na druhou stranu, pokud se ztotožníme s myšlenkou Pavla Holländera, že základním účelem práva je zachování lidského společenství a jeho členů,[21] pak by odpovědnost regulátorů za zachování základních předpokladů lidské existence mělo být možné najít jako společný jmenovatel napříč společenstvími a kulturami.

Za důležité považuji upozornění autora, že přemíra technologických opatření omezujících naši praktickou svobodu může vést k morálnímu vyprázdnění. Jednoduše řečeno skutečnost, že člověk jedná morálně (v souladu s hodnotami svého společenství a s přiměřeným respektem k zájmům ostatních) ze svého vnitřního rozhodnutí, nikoli z důvodu, že díky technologickým opatřením je takové jednání jediné možné, má svou vlastní hodnotu. Jinými slovy, že bez nutnosti činit morální rozhodnutí může tato naše schopnost degradovat.[22]

Celkově považuji knihu za velmi zdařilou. Některé předkládané myšlenky, jako např. vytvoření speciálního mezinárodního orgánu pro regulaci technologií se mohou zdát jako ambiciózní v míře hraničící s naivitou. Současně některých témat se kniha pouze lehce dotýká – příkladem jsou technické prostředky ochrany (DRM),[23] které jsou dle mého názoru dobrým příkladem technologického opatření s problematickou legitimitou.[24] Přesto kniha stručně shrnuje komplexní téma, srozumitelným způsobem otevírá velmi důležitou diskuzi a předkládá do ní konkrétní návrhy.

---

[20] Viz POLČÁK, Radim. Internet a proměny práva. Praha: Auditorium, 2012. s. 300 a 301.

[21] Viz HOLLÄNDER, Pavel. *Filosofie práva*. Praha: Aleš Čeněk, 2012. s. 81.

[22] Viz BROWNSWORD, Roger. Law 3.0: *Rules, Regulation, and Technology*. Abingdon: Routledge, 2020. s. 74.

[23] Viz § 43 zákona č. 121/2000 Sb., autorský zákon, ve znění pozdějších předpisů, a BROWNSWORD, Roger. Law 3.0: *Rules, Regulation, and Technology*. Abingdon: Routledge, 2020. s. 79.

[24] Viz např. MYŠKA, Matěj. The true story of DRM. *Masaryk University Journal of Law and Technology*, 2009, roč. 3. č. 2, s. 267–278.

https://doi.org/10.5817/RPT2023-1-5

JAK REGULOVAT COOKIES V NAŘÍZENÍ EPRIVACY[1]

JAN TOMÍŠEK[2]

ABSTRAKT

Cílem tohoto článku je představit návrh, jak by připravované nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích (tzv. nařízení ePrivacy) mělo upravovat použití cookies a podobných technologií. Současná směrnice 2002/58/ES řeší rizika spojená s použitím cookies a podobných technologií především požadavkem na informovaný souhlas uživatele. Toto řešení však klade nepřiměřený důraz na kontrolu ze strany uživatele, kterou však není v možnostech uživatele při běžném používání internetu efektivně vykonávat. Výsledkem je tak snížená úroveň ochrany soukromí uživatele před sledováním a současně komplikace pro stránky nabízející bezplatný obsah, financovaný pomocí cílené reklamy. Článek proto popisuje, jak fungují cookies a podobné technologie, co přinese blokace tzv. cookies třetích stran v nejrozšířenějších prohlížečích, jaká je historie právní úpravy soukromí v elektronických komunikacích, jaká je platná právní úprava použití cookies a podobných technologií a jak se tato úprava vyvíjela v různých verzích návrhu nařízení ePrivacy. Následně představuje návrh, jak by podle použití cookies a podobných technologií mělo být v nařízení ePrivacy upraveno de lege ferenda.

[1] Tento článek vznikl v rámci projektu "Právo a technologie XI“, MUNI/A/1293/2022.

[2] Mgr. et Mgr. Ing. Jan Tomíšek je doktorandem na Ústavu práva a technologií Právnické fakulty Masarykovy univerzity a partnerem v advokátní kanceláři ROWAN LEGAL, kontaktní e-mail: jantomisek@gmail.com. Autor by rád poděkoval Matěji Myškovi, Jakubu Míškovi, Valdanu Rámišovi, Františku Nonnemannovi a dvěma anonymním recenzentům za jejich podnětné připomínky k tomuto článku. Veškeré chyby jdou výhradně na vrub autora.

KLÍČOVÁ SLOVA

Cookies, soukromí, osobní údaje, GDPR, ePrivacy

ABSTRACT

The aim of this article is to present a proposal on how the forthcoming Regulation of the European Parliament and of the Council on respect for privacy and the protection of personal data in electronic communications (ePrivacy Regulation) should regulate the use of cookies and similar technologies. The current Directive 2002/58/EC addresses the risks associated with the use of cookies and similar technologies primarily by requiring the informed consent of the user. However, this solution places undue emphasis on user control, which is not effectively within the user's ability to exercise in the normal course of internet use. The result is a reduced level of protection of the user's privacy from tracking and, at the same time, complications for sites offering free content financed by targeted advertising. The article therefore describes how cookies and similar technologies work, what blocking third-party cookies in the most widely used browsers will bring, the history of the legal regulation of privacy in electronic communications, what the current legal regulation of the use of cookies and similar technologies is, and how this regulation has evolved in the different versions of the draft ePrivacy Directive. It then presents a de lege ferenda proposal for how the use of cookies and similar technologies should be regulated in the ePrivacy Regulation.

KEY WORDS

Cookies; Privacy; Personal Data; GDPR; ePrivacy

1. ÚVOD

Použití cookies a podobných technologií je v právu Evropské unie řešeno především právní úpravou soukromí v elektronických komunikacích.[3] Návrh nové podoby této právní úpravy, tzv. nařízení ePrivacy, představila Ev-

[3] Viz směrnici 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).

ropská komise v lednu 2017.[4] Ani po 5 letech však nedošlo k jejímu přijetí a konec legislativního procesu zatím není v dohledu, jak je blíže objasněno v tomto článku. To otevírá prostor k hlubšímu zamyšlení, jak by nová právní úprava měla regulovat použití cookies a podobných technologií.

Cookies a podobné technologie v rámci webových stránek lze (vedle řady jiných účelů) využít ke sledování uživatelů ve smyslu sběru údajů o jejich chování.[5] Tyto údaje pak lze využít k odvozování osobnostních a dalších charakteristik uživatelů – profilování.[6] Informace z profilu uživatele lze pak využít pro cílení reklamy.[7] Důsledkem tohoto sledování mohou být diskriminace,[8] manipulace[9] a odrazující efekty (*chilling effects*).[10]

---

[4] Viz návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) COM/2017/010 final – 2017/03 (COD) (dále jen „návrh Komise“).

[5] Viz BARTH, Adam. HTTP State Management Mechanism - Request for Comments. RFC 6265. In: *Internet Engineering Task Force* [online]. 2011 [cit. 20. 7. 2022], s. 4. LIU, Peng; CHAO, Wang. *Computational Advertising: Market and Technologies for Internet Commercial Monetization*. Boca Raton: CRC Press, 2020, s. 120.

[6] 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 ve svém čl. 4 bod 4 definuje profilování jako jakoukoli formu „automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu“.

[7] Viz LIU, Peng; CHAO, Wang. *Computational Advertising: Market and Technologies for Internet Commercial Monetization*, s. 120.

[8] Viz ANGWIN, Julia, PARRIS, Terry. Facebook Lets Advertisers Exclude Users by Race. In: *ProPublica* [online]. 28. 10. 2016 [cit. 6. 3. 2022]. Dostupné z: https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race. SPEICHER, Till et al. Potential for Discrimination in Online Targeted Advertising. In: *Conference on Fairness, Accountability and Transparency*: *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* [online]. PMLR, 2018 [cit. 6. 3. 2022], s. 9, 10.

[9] Viz např. CALO, Ryan. Digital market manipulation. *George Washington Law Review* [online]. 2013, roč. 82, č. 4 [cit. 12. 2. 2023], s. 996. CRAIN, Matthew, NADLER, Anthony. Political Manipulation and Internet Advertising Infrastructure. *Journal of Information Policy* [online]. 2019, roč. 9 [cit. 10. 9. 2022], s. 374.

[10] Viz RICHARDS, Neil. *Intellectual privacy: rethinking civil liberties in the digital age*. Oxford: Oxford University Press, 2015, s. 101.

Současná směrnice 2002/58/ES řeší rizika spojená s použitím cookies a podobných technologií především požadavkem na informovaný souhlas uživatele.[11] Souhlas je však v kontextu webových stránek problematickým nástrojem ochrany soukromí. Podstatou požadavku na souhlas je snaha o dosažení kontroly uživatele nad nakládáním s informacemi o jeho osobě.[12] To je však v kontextu množství webových stránek a mobilních aplikací, které s takovými informacemi pracují a se kterými uživatel běžně interaguje, neproveditelné.[13] Poznatky z behaviorální ekonomie ukazují, že uživatelé kontrolu nejsou v tomto měřítku schopni efektivně vykonávat.[14] Důsledkem je zahlcení uživatelů žádostmi o souhlas téměř na každé webové stránce, kterou navštíví. Žádosti o souhlas jsou pro uživatele obtěžující, přitom nezvyšují povědomí uživatelů o rizicích, která jsou s použitím cookies a podobných technologií spojena – naopak často vedou k mechanickému udělení souhlasu.[15]

Cílem tohoto článku je představit návrh, jak by použití cookies a podobných technologií mělo být v nařízení ePrivacy upraveno, aby tyto problémy institutu souhlasu byly alespoň částečně překonány. Návrh spočívá ve vyloučení použití specifického druhu cookies (tzv. vlastních cookies)

[11] Viz čl. 5 odst. 3 směrnice 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).

[12] Viz RICHARDS, Neil M., HARTZOG, Woodrow. Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review* [online]. 2016, roč. 19, č. 3, [cit. 30. 1. 2021], s. 444.

[13] Slovy Woodrowa Hartzoga, kontrola není „bezedná studna". Srov. HARTZOG, Woodrow. *Privacy's blueprint*. Cambridge, Massachusetts: Harvard University Press, 2018, s. 63.

[14] Viz CAROLAN, Eoin, CASTILLO-MAYEN, M. Rosario. Why More User Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws. *Virginia Journal of Law & Technology*. 2014, roč. 19, č. 2, s. 362. COFONE, Ignacio N. The way the cookie crumbles: online tracking meets behavioural economics. *International Journal of Law and Information Technology* [online]. 2017, roč. 25, č. 1 [cit. 2. 2. 2022], s. 51. DOUGHERTY, Christie. Every Breath You Take, Every Move You Make, Facebook's Watching You: A Behavioral Economic Analysis of the US California Consumer Privacy Act and EU ePrivacy Regulation. *Northeastern University Law Review* [online]. 2020, roč. 12, č. 2 [cit. 2. 2. 2023], s. 638.

[15] Viz KULYK, Oksana et al. Has the GDPR hype affected users' reaction to cookie disclaimers? *Journal of Cybersecurity* [online]. 2020, roč. 6, č. 1 [cit. 2. 2. 2022], s. 4. Dále viz COFONE, Ignacio N. *The way the cookie crumbles: online tracking meets behavioural economics*, s. 44. CRANOR, Lorrie Faith. Cookie monster. *Communications of the ACM* [online]. 2022, roč. 65, č. 7 [cit. 2. 2. 2022], s. 32.

a podobných technologií a dále technologií nahrazujících tzv. cookies třetích stran z působnosti právní úpravy ochrany soukromí v elektronických komunikacích a ponechání jejich použití pouze v režimu GDPR, s doplněním povinností pro tvůrce webových prohlížečů o povinnost cookies třetích stran a podobné technologie blokovat ve výchozím nastavení těchto prohlížečů.

Článek proto popisuje, jak cookies a podobné technologie fungují a co přinese blokace cookies třetích stran v nejrozšířenějších prohlížečích. Dále popisuje historii právní úpravy soukromí v elektronických komunikacích a platnou právní úpravu použití cookies a podobných technologií. Následně popisuje vývoj textu nařízení ePrivacy a představuje výše nastíněný návrh. Závěr článku shrnuje provedené úvahy.

2. COOKIES A PODOBNÉ TECHNOLOGIE

Cookies jsou krátké textové řetězce, které může webová stránka uložit do webového prohlížeče uživatele.[16] Při dalším požadavku na zobrazení webové stránky internetový prohlížeč ověří, jestli má pro tuto webovou stránku uložené nějaké cookies, a pokud ano, zašle je na server jako součást hlavičky požadavku.[17] Vedle hodnoty lze cookies nastavit i další parametry. Jedním z nich je platnost (exspirace), která určuje dobu, po kterou bude od svého uložení příslušná cookie zasílána spolu s požadavky na stránky z dané domény.[18]

Cookies jsou z hlediska uložení ve webovém prohlížeči a zpřístupnění webovým stránkám vázány na doménu.[19] Pokud tedy byla cookie do prohlí-

[16] Viz BARTH, Adam. *HTTP State Management Mechanism - Request for Comments* [online]. Konkrétně může webový server do hlavičky odpovědi na požadavek zaslání obsahu konkrétní webové stránky vložit pole Set-Cookie, které může obsahovat páry klíč–hodnota, například „Set-Cookie: PHPSESSID = r2t5uvjq435r4q7ib3vtdjq120; language = cs“. Na základě tohoto pokynu si internetový prohlížeč uloží cookie „PHPSESSID“ s hodnotou „r2t5uvjq435r4q7ib3vtdjq120“ a cookie „language“ s hodnotou „cs“.

[17] Viz BARTH, Adam. *HTTP State Management Mechanism - Request for Comments* [online]. Ve výše popsaném příkladu tak součástí hlavičky požadavku na zobrazení další stránky ze stejné domény bude také pole „Cookie: PHPSESSID = r2t5uvjq435r4q7ib3vtdjq120; language = cs“.

[18] Viz tamtéž.

[19] Viz tamtéž.

žeče uložena v rámci přístupu k webové stránce na doméně „priklad.cz“, odešle se pouze v rámci požadavků na webové stránky ze stejné domény (např. „priklad.cz/ukázka“) nebo z jejích subdomén (např. „dobry.priklad.cz“).[20]

Cookies slouží primárně k zajištění stavové komunikace v rámci *World Wide Webu*. Komunikační protokol HTTP, který je využíván pro přenos webových stránek ze serveru do webového prohlížeče, je totiž tzv. bezstavový,[21] což znamená, že mezi jednotlivými požadavky na zobrazení webové stránky není v rámci HTTP protokolu přenášena žádná informace (tzv. stav).

Cookies umožňují mezi jednotlivými zobrazeními webové stránky přenášet např. preference uživatele, jako je jazyková verze webové stránky, kterou si uživatel zvolil (pokud stránka umožňuje výběr jazyka). Současně cookies umožňují také na straně serveru udržovat mezi návštěvami webové stránky tzv. sezení (*sesssion*) nesoucí stav komunikace. Toto udržování stavu se realizuje tak, že se do cookie zapíše unikátní identifikátor daného sezení (*session ID*), který je pak při následujících požadavcích zaslán příslušné webové stránce. Ta podle něj rozpozná, že určitý požadavek navazuje na požadavky již dříve realizované.[22]

Vedle zajištění stavové komunikace jako nástroje k zajištění funkcionality webové stránky však cookies mohou sloužit mnoha dalším účelům. Identifikace uživatele mezi jednotlivými přístupy je užitečná i pro měření návštěvnosti určité webové stránky a analýzu chování jejích návštěvníků – díky cookies je možné vedle počtu zobrazení jednotlivých stránek sledovat počet návštěvníků, kteří si zobrazili více stránek, sledovat opakované návštěvy (pokud je cookie nastavena delší platnost než do ukončení běhu in-

[20] Při přístupu na webovou stránku na adrese „jiny-priklad.cz“ tak tyto cookies z domény „priklad.cz“ na server odeslány nebudou.

[21] Viz BARTH, Adam. *HTTP State Management Mechanism - Request for Comments* [online].

[22] Viz tamtéž. Například, že stránku s určitým zbožím v internetovém obchodě požaduje internetový prohlížeč uživatele, který v předchozím spojení vložil jiné zboží do svého košíku – webová stránka tak může např. zobrazit uživateli indikátor, že už má nějaké zboží v košíku.

ternetového prohlížeče) a zkoumat, jak uživatelé web používají (v jakém pořadí stránky zobrazují, pomocí kterých odkazů se přesouvají, apod.).[23]

Možnosti použití cookies jsou dále rozšířeny tím, jak jsou dnes webové stránky po technické stránce obvykle strukturovány. V počátcích *World Wide Webu* byla přenosová rychlost a propustnost připojení k internetu nízká a bylo žádoucí, aby se na základě jediného HTTP požadavku načetla celá webová stránka. V současnosti jsou však přenosová rychlost a propustnost běžného připojení k internetu výrazně vyšší a před úsporou počtu požadavků má přednost bohatost obsahu a interaktivita webové stránky. Z toho důvodu se do webové stránky vkládá řada dalších prvků, které se načítají samostatnými požadavky. Nejjednodušším příkladem jsou obrázky, které jsou do webové stránky vloženy tak, že v kódu webové stránky je obsažena zvláštní značka, která pro internetový prohlížeč znamená pokyn, aby si ze stanovené adresy pomocí protokolu HTTP vyžádal obrázek a vložil ho do zobrazované webové stránky. Obdobně lze do webové stránky vkládat styly, které upravují její vizuální aspekty, nebo skripty, což jsou spustitelné počítačové programy. Takto vkládaných položek jsou dnes v rámci webové stránky běžně desítky.

Vkládání obsahu přitom není omezeno pouze na doménu, ze které se načítá příslušná webová stránka – např. webová stránka „priklad.cz“ může obsahovat značku dávající internetovému prohlížeči pokyn k vložení obrázku z adresy „databaze-obrazku.cz/priklad.png“. Jelikož je vkládaný obsah získáván opět pomocí protokolu HTTP, doména, ze které je obsah získáván, může v rámci požadavku na zaslání obsahu číst a v rámci odpovědi zapisovat cookies ve webovém prohlížeči uživatele. Ve výše uvedeném příkladu tedy webový server na adrese „databaze-obrazku.cz“ může z internetového prohlížeče číst, resp. do něj zapisovat cookies, i když uživatel aktuálně prohlíží webovou stránku na doméně „priklad.cz“.

[23] Viz BARTH, Adam. *HTTP State Management Mechanism - Request for Comments* [online]. LIU, Peng; CHAO, Wang. *Computational Advertising: Market and Technologies for Internet Commercial Monetization*, s. 120; ZHENG, Guangzhi; PELTSVERGER, Svetlana. Web analytics overview. In: *Encyclopedia of Information Science and Technology, Third Edition* [cit. 6. 2. 2023]. IGI Global, 2015 [cit. 6. 2. 2023], s. 3.

Cookies vložené z domény, na které se nachází webová stránka, již uživatel aktuálně prohlíží, se označují jako vlastní cookies (cookies první strany, *first-party cookies*). Cookies vložené z jiných domén se v daném kontextu označují jako cookies třetích stran (*third-party cookies*).[24] Ve výše uvedeném příkladu tedy cookies z domény „priklad.cz" budou vlastní cookies, cookies z domény „databaze-obrazku.cz" budou cookies třetí strany. Stále však platí, že cookies jsou ukládány a zpřístupňovány odděleně, server na adrese „databaze-obrazku.cz" tedy obdrží pouze cookies nastavené z této domény, nikoli cookies, které zapsal server s adresou „priklad.cz".

Podobně jako cookies lze ke sledování chování uživatelů použít i další technologie. Podstatou části z nich je ukládání dat do webového prohlížeče uživatele, jiné pracují s údaji, které lze získat z koncového zařízení a vypovídají o jeho hardwaru či softwaru.[25] Ukládání do webového prohlížeče využívají *ETags*, které fungují na bázi vyrovnávací paměti (*cache)* webového prohlížeče. Do této paměti se ukládají prvky webové stránky, aby nebylo třeba je opakovaně načítat při její další návštěvě. Těmto ukládaným prvkům jsou přidělovány identifikátory, které může webová stránka měnit. To lze využít k uložení jedinečného identifikátoru, podobně jako se ukládá do cookie.[26]

Standard pro kódování webových stránek HTML5 přinesl novou funkcionalitu prohlížeče označovanou webové úložiště (*web storage)*. Podobně jako cookies umožňuje ukládání párů klíč–hodnota, kapacita úložiště je však výrazně větší (5 MB na každou webovou stránku oproti 4kB na jednu cookie). Webové úložiště se dělí na dvě části – úložiště sezení (*session storage*), které

[24] Viz Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies. In: *Evropská komise* [online]. 7. 6. 2012, s. 5. [cit. 23. 1. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf (dále jen „WP194")

[25] Viz HOOFNAGLE, Chris Jay et al. Behavioral advertising: The offer you can't refuse. *Harvard Law & Policy Review*. 2012, roč. 6, s. 286.

[26] Viz HINTERNESCH, Nicolas. No Cookies, No Problem — Using ETags For User Tracking. In: *Medium* [online]. 17. 5. 2021 [cit. 18. 1. 2023]. Dostupné z: https://levelup.gitconnected.com/no-cookies-no-problem-using-etags-for-user-tracking-3e745544176b HOOFNAGLE, Chris Jay et al. *Behavioral advertising: The offer you can't refuse*, s. 281.

se vymaže po zavření záložky v prohlížeči, a místní úložiště, které nemá žádnou exspiraci (chová se tedy jako cookies bez nastavené doby exspirace).[27]

Spíše za historickou technologii lze považovat Flash cookies spojené se zásuvným modulem do webových prohlížečů označovaným Flash.[28] Tyto Flash cookies byly historicky využívány také pro obnovení cookies, které uživatel ze svého prohlížeče vymazal.[29]

Údaje o softwaru nebo hardwaru koncového zařízení využívá technika označovaná jako *device fingerprinting* nebo *browser fingerprinting*.[30] Webové stránky mají pro své fungování přístup k rozsáhlým informacím o webovém prohlížeči uživatele a jeho zařízení, jako jsou typ a verze prohlížeče, typ a verze operačního systému nebo rozlišení obrazovky. Tyto údaje jsou pro zařízení uživatele do jisté míry unikátní, a mohou tak vytvářet jeho unikátní „otisk" použitelný pro sledování.[31] Webové prohlížeče mají také dynamické funkcionality, které mohou být ovládány prostřednictvím skriptů vložených do webových stránek, a chování těchto funkcionalit se může na různých zařízeních a v různých prohlížečích i v různých verzích stejného prohlížeče lišit.[32] Využití údajů, které o sobě zařízení aktivně vysílá, lze

---

[27] Viz HOOFNAGLE, Chris Jay et al. *Behavioral advertising: The offer you can't refuse,* s. 283. HTML Web Storage API In: *W3 schools* [online]. [cit. 18. 1. 2023]. Dostupné z: https://www.w3schools.com/html/html5_webstorage.asp

[28] Viz HOOFNAGLE, Chris Jay et al. *Behavioral advertising: The offer you can't refuse*, s. 282.

[29] Viz HOOFNAGLE, Chris Jay et al. *Behavioral advertising: The offer you can't refuse*, s. 283.

[30] Do češtiny lze název přeložit jako snímání otisků zařízení, resp. prohlížeče. Viz CAO, Yinzhi, LI, Song, WIJMANS, Erik. (Cross-)Browser Fingerprinting via OS and Hardware Level Features. In: *Network and Distributed System Security Symposium*: *Proceedings 2017 Network and Distributed System Security Symposium* [online]. San Diego, CA: Internet Society, 2017, [cit. 28. 10. 2022], s. 1. HOOFNAGLE, Chris Jay et al. *Behavioral advertising: The offer you can't refuse*, s. 285. Viz také Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29. Stanovisko č. 9/2014 k uplatňování směrnice 2002/58/ES na otisky zařízení. In: *Evropská komise* [online]. 25. 11. 2014, s. 3. [cit. 1. 2. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf (dále jen „WP224")

[31] K přehledu relevantních údajů viz WP224, s. 5.

[32] CAO, Yinzhi; LI, Song; WIJMANS, Erik. (Cross-)Browser Fingerprinting via OS and Hardware Level Features. s. 2.

označit jako pasivní fingerprinting, využití údajů, které je třeba získat aktivně pomocí skriptu, pak jako aktivní fingerprinting.[33]

Jednou z takových funkcionalit je tzv. *HTML canvas* (plátno) – funkcionalita určená ke kreslení grafických prvků na obrazovky zařízení, například pro animace, herní grafiku nebo vizualizaci dat. HTML canvas lze použít pro vykreslení konkrétního obrázku mimo oblast viditelnou uživateli prohlížeče a následné zkoumání vykresleného obrázku (např. jeho rozměrů a dalších vlastností). Protože existují drobné rozdíly ve způsobu vykreslování obrázku v různých prohlížečích a na různých zařízeních, poskytuje zkoumání údaje, které lze rovněž využít k vytvoření otisku konkrétního prohlížeče.[34] Podle studie Acara a kol. z roku 2014 ze 100 000 nejnavštěvovanějších webových stránek na internetu podle portálu Alexa obsahovalo 5,5 % skripty pro snímání otisků HTML canvas.[35]

3. KONEC COOKIES TŘETÍCH STRAN

Protože cookies (zejména cookies třetích stran) lze využít ke sledování chování uživatele, obsahují některé moderní prohlížeče funkcionality, které toto sledování a uložení nebo čtení cookies v některých případech blokují.[36] V srpnu roku 2019 oznámil Google v tomto směru zahájení iniciativy nazvané *Privacy Sandbox*. Cílem této inciativy je vytvoření sady otevřených standardů, které posílí ochranu soukromí na webu.[37]

---

[33] Viz MAYER, Jonathan R., MITCHELL, John C. Third-party web tracking: Policy and technology. In: 2012 *IEEE symposium on security and privacy* [online]. IEEE, 2012 [cit. 27. 5. 2023]. s. 421.

[34] Viz KONIK, James. How Does Canvas Fingerprinting Work? In: *Fingerprint* [online]. 11. 7. 2021 [cit. 28. 10. 2022]. Dostupné z: https://fingerprint.com/blog/canvas-fingerprinting/

[35] Viz ACAR, Gunes, et al. The web never forgets: Persistent tracking mechanisms in the wild. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* [online]. 2014. [cit. 12. 2. 2023], s. 678.

[36] Viz Interactive Advertising Bureau. A Guide to the Post Third-Party Cookie Era. In: *Interactive Advertising Bureau* [online]. Březen 2022, s. 18. [cit. 31. 1. 2023]. Dostupné z: https://iabeurope.eu/wp-content/uploads/2022/03/IAB-Europe-Guide-to-a-Post-Third-Party-Cookie-Era-March-2022.pptx.pdf

[37] Viz SCHUH, Justin. Building a more private web. In: *Google* [online]. 22. 8. 2019 [cit. 26. 2. 2022]. Dostupné z: https://blog.google/products/chrome/building-a-more-private-web/

Google tak nejspíše reagoval na dřívější kroky zejména ze strany Apple, nadace Mozilla vyvíjející internetový prohlížeč Firefox a také na některé úvahy ze strany Microsoftu.[38] Apple ve svém internetovém prohlížeči Safari od roku 2017 uplatňuje opatření proti sběru údajů o chování uživatele.[39] Podobná opatření v červnu 2019 oznámila nadace Mozilla[40] a Microsoft je ve stejnou dobu přidal v experimentálním režimu do prohlížeče Edge.[41] Význam oznámení tohoto kroku ze strany Googlu je dán tím, že jeho webový prohlížeč Chrome je nejrozšířenějším prohlížečem na světě.[42]

Inciativa *Privacy Sandbox* ve své prvotní verzi neobsahovala záměr blokovat cookies třetích stran. Google toto pojetí odůvodňoval tak, že rozsáhlé blokování cookies by poškodilo zájmy uživatelů podporováním použití technik, jako je fingerprinting, a dále tím, že blokování cookies bez náhradního řešení, jak zajistit zobrazování relevantních (personalizovaných) reklam, by poškodilo financování médií a webových služeb.[43] Zdrženlivý přístup Googlu k blokování cookies třetích stran není překvapivý, když jeho příjmy pochází především z internetové reklamy.[44]

---

[38] Viz LEE, Timothy B. Google defends tracking cookies—some experts aren't buying it. In: *Ars Technica* [online]. 26. 8. 2019 [cit. 26. 2. 2022]. Dostupné z: https://arstechnica.com/tech-policy/2019/08/why-some-experts-are-skeptical-of-googles-new-web-privacy-strategy/

[39] Viz WILANDER, John. Intelligent Tracking Prevention. In: *WebKit* [online]. 5. 6. 2017 [cit. 26. 2. 2022]. Dostupné z: https://webkit.org/blog/7675/intelligent-tracking-prevention/

[40] Viz CAMP, Dave. Firefox Now Available with Enhanced Tracking Protection by Default Plus Updates to Facebook Container, Firefox Monitor and Lockwise In: *The Mozilla Blog* [online].]. 4. 6. 2019 [cit. 26. 2. 2022]. Dostupné z: https://blog.mozilla.org/en/products/firefox/firefox-now-available-with-enhanced-tracking-protection-by-default/

[41] Viz BRINKMANN, Martin. A look at Microsoft Edge's Tracking Prevention feature.. In: *gHacks Technology News* [online]. 28. 6. 2019 [cit. 26. 2. 2022]. Dostupné z: https://www.ghacks.net/2019/06/28/a-look-at-microsoft-edges-tracking-prevention-feature/

[42] Podle statistik za leden roku 2022 byl tržní podíl prohlížeče Google Chrome 64,68 %. Z hlediska velikosti podílu za ním následovaly prohlížeče Safari (18,29 %) a Microsoft Edge (4,23 %). Srov. Browser Market Share Worldwide. In: *StatCounter Global Stats* [online]. 31. 1. 2023 [cit. 31. 1. 2023]. Dostupné z: https://gs.statcounter.com/browser-market-share

[43] Viz SCHUH, Justin. Building a more private web: A path towards making third party cookies obsolete. In: *Chromium Blog* [online]. 14. 1. 2020 [cit. 30. 5. 2023]. Dostupné z: https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html

[44] Viz LEE, Timothy B. Google defends tracking cookies—some experts aren't buying it. In: *Ars Technica* [online]. 26. 8. 2019 [cit. 26. 2. 2022]. Dostupné z: https://arstechnica.com/tech-policy/2019/08/why-some-experts-are-skeptical-of-googles-new-web-privacy-strategy/

Přesto v lednu roku 2020 Google oznámil, že přistoupí k blokování cookies třetích stran v prohlížeči Google Chrome. Změnu postoje odůvodnil tím, že po diskuzi s webovou komunitou nabyl přesvědčení, že nástroje iniciativy *Privacy Sandbox* dokážou zajistit fungující web využívající financování z reklam a nahradit cookies třetích stran. V tomto okamžiku společnost avizovala záměr ukončit podporu cookies třetích stran v prohlížeči Chrome do dvou let.[45]

Inciativa *Privacy Sandbox* obsahuje celou sadu nástrojů pro nahrazení cookies třetích stran v oblastech, jako je cílení nebo měření výkonnosti reklamy. Jako klíčovou náhradu cookies třetích stran pro účely cílené internetové reklamy společnost Google původně navrhovala technologii *Federated Learning of Cohorts* (FLoC)[46] založenou na zařazování uživatelů do skupin podle jejich aktivity na internetu (sdružování uživatelů, kteří prochází podobný obsah). V rámci této technologie měl internetový prohlížeč uživatele zpracovat údaje o webových stránkách, které uživatel v poslední době procházel, a na základě matematického modelování přidělit uživateli identifikátor „kohorty" uživatelů, kteří v poslední době procházeli podobnou skladbu webových stránek. Modelování mělo být založené na technice strojového učení označované jako sdružené učení (*federated learning*), která umožňuje souběžné zlepšování modelů v jednotlivých prohlížečích, aniž by údaje o aktivitách jednotlivého uživatele musely jeho prohlížeč opustit. Identifikátor kohorty měl pak následně být z prohlížeče předáván webovým stránkám inzerentů, aby věděli, na jaké kohorty mají své reklamy cílit, a médiím, aby mohla podle preferencí zvolených inzerenty zobrazit uživateli z určité kohorty cílenou reklamu.[47] Ochranu uživatelů měla zajistit především minimální velikost kohorty, kdy by centrální administrátor systému

[45] Viz SCHUH, Justin. Building a more private web: A path towards making third party cookies obsolete [online].

[46] Název je zřejmě slovní hříčkou – anglické slovo *flock* lze přeložit jako hejno či (v tomto kontextu poněkud pejorativněji) stádo.

[47] Viz DUTTON, Sam. FLoC. In: *Chrome Developers* [online]. 18. 5. 2021 [cit. 6. 3. 2022]. Dostupné z: https://developer.chrome.com/docs/privacy-sandbox/floc/

zajišťoval, aby nebyl předáván identifikátor takové kohorty, která zahrnuje nízký počet osob (méně než tisíce).[48]

Tato technologie se stala terčem kritiky s ohledem na úroveň ochrany, kterou měla poskytnout uživatelům, a také z pohledu ochrany hospodářské soutěže. Z pohledu ochrany uživatelů byl kritizován potenciál identifikátoru kohorty usnadnit fingerprinting – v případě zařazení uživatele pomocí identifikátoru do kohorty o velikosti několik tisíc uživatelů by mohla být identifikace jednotlivce na základě jiných atributů jeho prohlížeče a zařízení výrazně jednodušší.[49] Dále bylo kritizováno riziko odhalení informací napříč kontexty – webové stránky, disponující komplexnější identitou uživatele (např. takové služby, do kterých se uživatel přihlašuje e-mailovou adresou), by mohly pomocí identifikátoru kohorty odvodit o uživateli dodatečné údaje, pokud by dokázaly zpětně odvodit vlastnosti dané kohorty.[50] Kohorty by také přitom mohly vymezovat skupiny uživatelů se specifickými vlastnostmi, jako příslušníky národnostních menšin apod. Tato vlastnost kohort by také mohla otevírat cestu ke zneužití identifikátoru kohorty pro účely diskriminace.[51]

Z pohledu hospodářské soutěže pak koncept vyvolal kritiku, že ze společnosti Google vytváří nezbytného prostředníka pro jakékoli cílení reklamy ve vztahu k uživatelům prohlížeče Google Chrome. To vedlo k zahrnutí inciativy Privacy Sandbox mezi tvrzená porušení soutěžního práva v rámci řízení vedeného generálními advokáty 15 států USA proti společnosti Google.[52] Vyšetřování této iniciativy zahájil také britský dozorový úřad pro oblast hospodářské soutěže *Competition and Markets Authority* (dále jen „CMA“).

---

[48] Viz CYPHERS, Bennett. Google's FLoC Is a Terrible Idea. In: *Electronic Frontier Foundation* [online]. 3. 3. 2021 [cit. 6. 3. 2022]. Dostupné z: https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea

[49] Viz tamtéž.

[50] Viz tamtéž.

[51] Viz tamtéž.

[52] Viz ROBERTSON, Adi. Google antitrust suit takes aim at Chrome's Privacy Sandbox. In: *The Verge* [online]. 16. 3. 2021 [cit. 6. 3. 2022]. Dostupné z: https://www.theverge.com/2021/3/16/22333848/google-antitrust-lawsuit-texas-complaint-chrome-privacy

Po více než roce vyšetřování a jednání přijal v únoru roku 2022 CMA závazky společnosti Google. Ta se mimo jiné zavázala, že podporu cookies třetích stran neukončí dříve, než CMA potvrdí, že jeho obavy z narušení hospodářské soutěže byly dostatečně ošetřeny.[53] Dle aktuálního harmonogramu je ukončení podpory plánováno od poloviny roku 2024,[54] zda se tento termín nebude posouvat, však zatím není jasné. Společnost Apple v prohlížeči Safari mezitím již k úplnému blokování cookies třetích stran přistoupila.[55]

V mezičase přitom společnost Google ukončila testování FLoC a tuto technologii opustila.[56] V lednu 2022 zveřejnila podrobnosti technologie Topics API, která má pro účely cílené reklamy nahradit cookies třetích stran namísto FLoC.[57] Podstatou technologie Topics API je přiřazení tematických štítků webovým stránkám, určení nejvýznamnějších tematických štítků pro konkrétního uživatele na základě jeho nedávné historie procházení webových stránek a zpřístupnění těchto štítků webovým stránkám skrze programové rozhraní (API) internetového prohlížeče.[58]

V rámci tohoto konceptu přitom společnost Google plánuje, že seznam dostupných štítků bude předem stanovený a omezený tak, aby nezahrnoval citlivé kategorie, jako např. zdraví či etnickou příslušnost. Přiřazení štítku webové stránce bude probíhat na základě části URL adresy (části před určením domény vyššího řádu, tzv. *hostname*, tj. např. „priklad“ u domény „priklad.cz“) pomocí strojového učení s využitím modelu předem vloženého do internetového prohlížeče. Rozhraní prohlížeče pak poskytne webové

[53] Viz Competition and Markets Authority. CMA to keep ‘close eye’ on Google as it secures final Privacy Sandbox commitments. In: *GOV.UK* [online]. [cit. 26. 2. 2022]. Dostupné z: https://www.gov.uk/government/news/cma-to-keep-close-eye-on-google-as-it-secures-final-privacy-sandbox-commitments

[54] Viz *How We’re Protecting Your Online Privacy* [online].

[55] Viz WILANDER, John. Full Third-Party Cookie Blocking and More. In: *WebKit* [online]. 24. 3. 2020 [cit. 26. 2. 2022]. Dostupné z: https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/

[56] Viz *How We’re Protecting Your Online Privacy* [online].

[57] Viz DUTTON, Sam. The Topics API. In: *Chrome Developers* [online]. 25. 1. 2022 [cit. 6. 3. 2022]. Dostupné z: https://developer.chrome.com/docs/privacy-sandbox/topics/

[58] Viz tamtéž.

stránce tři nejčastější tematické štítky pro daného uživatele, každé za jeden ze tří předcházejících týdnů.[59]

Tematické štítky si budou moci na webové stránce vyžádat i skripty třetích stran, obecně však platí, že štítek obdrží pouze taková stránka nebo skript, které se s daným štítkem pro daného uživatele již setkaly. Pokud je tedy jedním z tematických štítků za poslední období pro daného uživatele „sport“, pak jej skript reklamní sítě vložený do webu „priklad.cz“ z domény „reklamni-sit.cz“ obdrží pouze v případě, že byl v minulosti skript z domény „reklamni-sit.cz“ načten do prohlížeče tohoto uživatele na jiném webu, kterému internetový prohlížeč přiřadil štítek „sport“, například na sportovním zpravodajském serveru nebo internetovém obchodu se sportovním vybavením. Toto opatření by mělo bránit tomu, aby pomocí tematických štítků webové stránky odvozovaly o uživatelích více informací, než mohou aktuálně odvodit pomocí cookies třetích stran.[60]

Vedle konceptu Topics API představil Google v lednu 2022 také koncept technologie FLEDGE umožňující cílení na uživatele, kteří navštívili určitou internetovou stránku.[61] Podstatou této technologie je provádění reklamních aukcí nikoli v systému reklamní burzy,[62] ale přímo ve webovém prohlížeči uživatele. Technologie by měla být používána tak, že pokud uživatel navštíví webovou stránku a její provozovatel chce takovému uživateli později zobrazit cílenou reklamu související s touto návštěvou, zapíše do internetového prohlížeče uživatele skutečnost, že uživatel spadá do zájmové skupiny definované tímto provozovatelem webové stránky.[63]

Následně při návštěvě webové stránky zobrazující reklamu by měl provozovatel takové webové stránky mít možnost zahájit v zařízení uživatele aukci, pro kterou by poskytl data o potenciálních účastnících (inze-

[59] Viz tamtéž.

[60] Viz tamtéž.

[61] Viz DUTTON, Sam, LEE, Kevin K. FLEDGE. In: *Chrome Developers* [online]. 27. 1. 2021 [cit. 22. 1. 2023]. Dostupné z: https://developer.chrome.com/docs/privacy-sandbox/fledge/. K významu zkratky srov. Intent to Experiment: First "Locally-Executed Decision over Groups" Experiment (FLEDGE) In: *Google Groups* [online]. 25. 3. 2022 [cit. 22. 1. 2023]. Dostupné z: https://groups.google.com/a/chromium.org/g/blink-dev/c/0VmMSsDWsFg

[62] Viz blíže část 7.2 .

[63] Viz DUTTON, Sam, LEE, Kevin K. *FLEDGE* [online].

rentech) a zájmových skupinách, kterým tito inzerenti mají zájem zobrazit reklamu. Prohlížeč uživatele by pak oslovil ty inzerenty, jejichž zájmová skupina je v prohlížeči již zapsána, a podle jejich nabídek vyhodnotil vítěznou nabídku v aukci a zobrazil uživateli reklamu příslušného inzerenta.[64]

Vedle snah o nahrazení cookies třetích stran méně invazivními technologiemi zahrnuje inciativa *Privacy Sandbox* také další technologie, které by měly zabránit sledování chování uživatelů pomocí fingerprintingu. Jednou z nich je *Privacy Budget*, jejíž podstatou je sledování objemu informací, které si konkrétní webová stránka vyžaduje o internetovém prohlížeči a zařízení uživatele, a stanovení maximálního stropu pro objem poskytnutých informací tak, aby z těchto informací nebylo možné sestavit unikátní otisk zařízení.[65] Harmonogram jejího nasazení však Google zatím neuvádí.[66]

4. VÝVOJ PRÁVNÍ ÚPRAVY

Právní úprava ochrany soukromí v elektronických komunikacích má v evropském právu dlouhou historii. První směrnice upravující tuto oblast byla přijata v roce 1997 jako součást tzv. prvního telekomunikačního balíčku.[67] Tato směrnice ještě neobsahovala právní úpravu cookies, resp. ochrany koncového zařízení uživatele služeb elektronických komunikací.

V roce 2000 byla zahájena příprava nového legislativního rámce, později označovaného jako druhý telekomunikační balíček, jehož součástí se stala i současná směrnice 2002/58/ES.[68] Ta ve svém čl. 5 odst. 3 upravuje uchovávání informací a získávání přístupu k již uchovávaným informacím

[64] Viz tamtéž.

[65] Vit LASSEY, Brad. Combating Fingerprinting with a Privacy Budget. In: *GitHub* [online]. 25. 2. 2022 [cit. 6. 3. 2022]. Dostupné z: https://github.com/mikewest/privacy-budget WHITE, Alexandra. Privacy Budget. In: *Chrome Developers* [online]. 4. 3. 2022 [cit. 28. 10. 2022]. Dostupné z: https://developer.chrome.com/docs/privacy-sandbox/privacy-budget/

[66] Viz *How We're Protecting Your Online Privacy* [online].

[67] Viz směrnici Evropského parlamentu a Rady 97/66/ES ze dne 15. prosince 1997 o zpracování osobních údajů a ochraně soukromí v odvětví telekomunikací. Viz též PAPAKONSTANTINOU, Vagelis; DE HERT, Paul. The Amended EU Law on ePrivacy and Electronic Communications after Its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights. *John Marshall Journal of Computer and Information Law* [online]. 2011, roč. 29, č. 1, [cit. 2. 2. 2023], s. 38.

v koncovém zařízení účastníka nebo uživatele služeb elektronických komunikací. Návrh směrnice z pera Evropské komise však tuto právní úpravu neobsahoval[69] – poprvé se objevila až v návrhu vzešlém z prvního čtení v Evropském parlamentu.[70] Evropský parlament přitom navrhl úpravu, která pro uchovávání informací a získávání přístupu k již uchovávaným informacím v koncovém zařízení účastníka nebo uživatele služeb elektronických komunikací (jako jsou například cookies) vyžadovala „předchozí výslovný souhlas".[71]

Tento návrh se setkal se silnou negativní reakcí organizací zastupujících reklamní sektor a podnikatele obecně.[72] Zřejmě s ohledem na tuto opozici Rada Evropské unie ve své společné pozici nahradila požadavek na souhlas požadavkem na informování a poskytnutí možnosti uchovávání a získávání přístupu odmítnout.[73] Tento protinávrh se nakonec promítl i do schváleného znění čl. 5 odst. 3 směrnice, které bylo následující:

> *Členské státy zajistí, aby užívání sítí elektronických komunikací k uchovávání informací nebo získávání přístupu k informacím uchovávaným v koncovém zařízení účastníka nebo uživatele bylo povoleno pouze za podmínky, že dotčený účastník či uživatel byl jasně a úplně informován v souladu se směrnicí 95/46/ES, mimo jiné o úče-*

---

[68] Viz PAPAKONSTANTINOU, Vagelis; DE HERT, Paul. *The Amended EU Law on ePrivacy and Electronic Communications after Its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights*, s. 38.

[69] Viz návrh směrnice Evropského parlamentu a Rady o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací KOM/2000/0385 final – COD 2000/0189.

[70] Viz návrh směrnice Evropského parlamentu a Rady o zpracovávání osobních údajů a ochraně soukromí v odvětví elektronických komunikací KOM(2000) 385 final – C5-0439/2000 * 2000/0189(COD)), pozměňovací návrh 26.

[71] Tamtéž.

[72] Viz KOSTA, Eleni. Peeking into the cookie jar: the European approach towards the regulation of cookies. *International Journal of Law and Information Technology* [online]. 2013, roč. 21, č. 4 [cit. 11. 1. 2023], s. 387. MERCADO KIERKEGAARD, Sylvia. How the cookies (almost) crumbled: Privacy & lobbyism. *Computer Law & Security Review* [online]. 2005, roč. 21, č. 4 [cit. 11. 1. 2023].

[73] Viz společnou pozici (ES) č. 26/2002 přijatou Radou dne 28. ledna 2002 s ohledem na přijetí směrnice 2002/ES Evropského parlamentu a Rady ze dne 22. prosince 2002 o změně směrnice Evropského parlamentu a Rady (ES) č. …/…. … o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, (2002/C 113 E/03).

> *lech zpracování, a že je mu správcem údajů nabídnuto právo odmítnout takové zpracování. To nebrání technickému ukládání nebo takovému přístupu, jehož jediným účelem je provedení nebo usnadnění přenosu sdělení prostřednictvím sítí elektronických komunikací nebo, je-li to nezbytně nutné pro poskytování služeb informační společnosti, které si účastník nebo uživatel výslovně vyžádal.*[74]

Do českého právního řádu bylo ustanovení transponováno s účinností od 1. 5. 2005 prostřednictvím § 89 odst. 3 zákona č. 127/2005 Sb., o elektronických komunikacích (dále jen „ZEK“).

Další vývoj právní úpravy ovlivnil případ hudebního vydavatelství Sony/BMG. Některá hudební CD tohoto vydavatelství musela být na počítači přehrávána pomocí zvláštního softwarového přehrávače, který byl obsažen přímo na daném CD. V roce 2005 expert na bezpečnost Mark Russinovich odhalil, že při přehrávání příslušných CD nedojde na počítači pouze ke spuštění tohoto přehrávače, ale také k instalaci softwaru eXtended Copy Protection (XCP) společnosti First 4 Internet.[75]

Tento software sloužil jako technický prostředek ochrany autorských práv (nástroj pro tzv. *Digital Rights Management*, zkráceně DRM). Jeho cílem bylo omezit počet kopií hudebních CD, které bude možné pořídit, a zabránit tak jejich neoprávněnému rozmnožování. Software se však instaloval skrytě po vložení CD do počítače, bez upozornění uživatele (tomu bylo k akceptaci předloženo pouze licenční ujednání k vestavěnému hudebnímu přehrávači, které tento software nezmiňovalo), nastavoval sám pro sebe zvýšená oprávnění a kvůli nevhodnému návrhu zvyšoval zranitelnost počítače proti malwaru. Současně k němu nebyl poskytován žádný nástroj pro odinstalaci.[76] Následně bylo odhaleno, že jiná CD Sony/BMG obsahují podobný nástroj MediaMax-3, který však trpěl velmi podobnými nedo-

[74] Přestože tento text a jeho pozdější verze pracují se spojením „účastník nebo uživatel“ a návrh nařízení ePrivacy s pojmem „koncový uživatel“, pro zjednodušení v dalším výkladu používám pouze pojem uživatel ve stejném významu.

[75] Viz RUSSINOVICH, Mark. Sony, Rootkits and Digital Rights Management Gone Too Far In: *Mark's Blog* [online]. 17. 3. 2015 [cit. 11. 1. 2023]. Dostupné z: https://web.archive.org/web/20150317040653/http://blogs.technet.com/b/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx

statky.[77] Jednání společnosti Sony/BMG přitom bylo mimo působnost původního znění čl. 5. odst. 3 směrnice 2002/58/ES – nejednalo se totiž o přístup ke koncovému zařízení v souvislosti s užíváním služby elektronických komunikací.

V roce 2007 Evropská komise jako součást třetího telekomunikačního balíčku představila návrh směrnice novelizující směrnici 2002/58/ES.[78] Součástí tohoto návrhu byla také úprava čl. 5 odst. 3 tak, aby působnost ustanovení nebyla vázána na služby elektronických komunikací.[79] Teprve v rámci jednání v Evropském parlamentu byla do návrhu novely doplněna úprava požadující souhlas k uchovávání informací a získávání přístupu k již uchovávaným informacím v koncovém zařízení.[80] V rámci prvního čtení v Evropském parlamentu byl tento návrh doprovozen formulací „se zohledněním toho, že nastavení prohlížeče představuje předchozí souhlas".[81]

---

[76] Viz SunnComm MediaMax Security Vulnerability FAQ. In: *Electronic Frontier Foundation* [online]. 19. 7. 2007 [cit. 11. 1. 2023]. Dostupné z: https://www.eff.org/pages/sunncomm-mediamax-security-vulnerability-faq

[77] Viz KOSTA, Eleni. *Peeking into the cookie jar: the European approach towards the regulation of cookies*, s. 384.

[78] Viz návrh směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci v oblasti ochrany spotřebitele {SEK(2007) 1472} {SEK(2007) 1473} /* KOM/2007/0698 final – COD 2007/0248 */.

[79] Viz tamtéž.

[80] Viz legislativní usnesení Evropského parlamentu ze dne 24. září 2008 o návrhu směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci v oblasti ochrany spotřebitele (KOM(2007)0698 – C6-0420/2007 – 2007/0248(COD)).

[81] Viz tamtéž.

Po odmítnutí ze strany Evropské komise[82] byl ve druhém čtení v Evropském parlamentu opět navržen souhlasový režim, avšak bez tohoto dovětku.[83]

Jak Evropská komise, tak Rada Evropské unie následně bez zvláštního odůvodnění návrh Evropského parlamentu na souhlasový režim přijaly[84] a novela byla vydána jako směrnice 2009/136/ES. Novelizovaný čl. 5 odst. 3 zní následovně:

> *Členské státy zajistí, aby uchovávání informací nebo získávání přístupu k již uchovávaným informacím bylo v koncovém zařízení účastníka nebo uživatele povoleno pouze pod podmínkou, že dotčený účastník či uživatel poskytl svůj souhlas poté, co mu byly poskytnuty jasné a úplné informace v souladu se směrnicí 95/46/ES, mimo jiné o účelu zpracování. To nebrání technickému ukládání nebo takovému přístupu, jehož jediným účelem je provedení přenosu sdělení prostřednictvím sítě elektronických komunikací, nebo je-li to nezbytně nutné k tomu, aby mohl poskytovatel služeb informační společnosti poskytovat služby, které si účastník nebo uživatel výslovně vyžádal.*

---

[82] Viz pozměněný návrh směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci v oblasti ochrany spotřebitele ze dne 6. 11. 2008, KOM/2008/0723 final - COD 2007/0248.

[83] Viz legislativní usnesení Evropského parlamentu ze dne 6. května 2009 ke společnému postoji Rady ohledně přijetí směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele (16497/1/2008 – C6-0068/2009 – 2007/0248(COD)).

[84] Viz stanovisko Komise podle čl. 251 odst. 2 třetího pododstavce písm. c) Smlouvy o ES ke změnám navrženým Evropským parlamentem týkajícím se společného postoje Rady v souvislosti s návrhem směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele, kterým/kterou se mění návrh Komise podle čl. 250 odst. 2 Smlouvy o ES ze dne 29. 7. 2009, KOM/2009/0421 final – COD 2007/0248.Viz též KOSTA, Eleni. op. cit., s. 390.

Za zmínku stojí také to, že ještě před finálním schválením směrnice Evropským parlamentem a Radou vydalo 13 členských států (nezahrnujících Českou republiku) stanovisko, že článek 5 odst. 3 není míněn jako změna stávajícího požadavku, kdy může být souhlas vykonán jako právo odmítnout cookies nebo podobné technologie používané pro legitimní účely.[85] V tomto stanovisku se opírají o bod 66 odůvodnění směrnice 2009/136/ES, který se vztahuje k uchovávání informací a získávání přístupu k již uchovávaným informacím v koncovém zařízení, nehovoří však překvapivě o souhlasu, ale o právu takové činnosti odmítnout.[86]

Poněkud překvapivá byla také reakce České republiky na směrnici 2009/136/ES. Tato směrnice byla sice do ZEK transponována zákonem č. 468/2011 Sb.,[87] § 89 odst. 3 však tímto zákonem novelizován nebyl.[88] Ke korektní transpozici tak došlo až zákonem č. 374/2021 Sb. s účinností od 1. 1. 2022.

5. PLATNÁ PRÁVNÍ ÚPRAVA

Platná právní úprava uchovávání informací a získávání přístupu k již uchovávaným informacím v koncovém zařízení je obsažena v § 89 odst. 3 ZEK, který stanoví:

---

[85] Viz Dodatek k poznámce „I/A“ Přijetí návrhu směrnice Evropského parlamentu a Rady (ES) č. 1308/2006 Rady, kterou se mění směrnice 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací, 2002/19/ES o přístupu a propojení k sítím a službám elektronických komunikací a 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací (LA + S) (třetí čtení) ze dne 18. 11. 2009, 2007/0247 (COD), 15864/09 ADD 1 REV 1, změněno Opravou dodatku k poznámce „I/A“ Přijetí návrhu směrnice Evropského parlamentu a Rady (ES) č. 1308/2006 Rady, kterou se mění směrnice 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací, 2002/19/ES o přístupu a propojení k sítím a službám elektronických komunikací a 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací (LA + S) (třetí čtení) ze dne 19. 11. 2009, 2007/0247 (COD), 15864/09 ADD 1 REV 1 COR 1.

[86] Viz tamtéž.

[87] Viz důvodovou zprávu k zákonu č. 468/2011 Sb.

[88] K chybné transpozici čl. 5 odst. 3 viz MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie* [online]. 2014, roč. 5, č. 9 [cit. 23. 1. 2023], s. 60. TOMÍŠEK, Jan. Cookies a GDPR. *Právní rozhledy* [online]. 2018, roč. 26, č. 20 [cit. 6. 2. 2023], s. 688.

> *Každý, kdo hodlá používat nebo používá sítě elektronických komunikací k ukládání údajů nebo k získávání přístupu k údajům uloženým v koncových zařízeních účastníků nebo uživatelů, získá od těchto účastníků nebo uživatelů předem prokazatelný souhlas s rozsahem a účelem jejich zpracování. Tato povinnost neplatí pro technické ukládání nebo přístup výhradně pro potřeby přenosu zprávy prostřednictvím sítě elektronických komunikací nebo je-li to nezbytné pro potřeby poskytování služby informační společnosti, která je výslovně vyžádána účastníkem nebo uživatelem.*

Z pohledu cookies a podobných technologií umožňujících ukládání údajů v zařízení uživatele, jak jsou ETrackers a webové úložiště, tato úprava znamená požadavek na získání souhlasu s ukládáním cookies do koncového zařízení a jejich následným čtením, vyjma případů, kdy jsou tyto cookies nebo podobné technologie nezbytné k fungování webové stránky, např. košíku v internetovém obchodě.[89]

Aplikace právní úpravy na techniky využívající údaje o zařízení uživatele (fingerprinting) je méně jasná. Dle stanoviska Pracovní skupiny pro ochranu osobních údajů zřízené podle článku 29 (dále jen „WP29“)[90] se čl. 5 odst. 3 směrnice 2002/58/ES na tyto techniky vztahuje „[j]e-li otisk vytvořen uchováváním informací nebo získáním přístupu k informacím uchovávaným v koncovém zařízení uživatele.“[91] Stanovisko bohužel neobjasňuje, které údaje se z pohledu Pracovní skupiny získávají přístupem k informacím uchovávaným v koncovém zařízení uživatele a které nikoli.

Domnívám se, že tuto otázku je třeba posuzovat ve světle bodu 24 odůvodnění směrnice 2002/58/ES, který uvádí, že koncové zařízení je součástí soukromí uživatele, v anglickém znění součástí jeho privátní sféry (*private sphere)*. Bylo by podle mě příliš extenzivní dovozovat, že součástí této

[89] K tomu, jaké cookies lze považovat za nezbytné a jaké nikoli, viz WP194, s. 6. Pro shrnutí a diskuzi viz TOMÍŠEK, Jan. *Cookies a GDPR*, s. 691. Viz také KOSTA, Eleni. *Peeking into the cookie jar: the European approach towards the regulation of cookies*, s. 393.

[90] WP29 byla orgánem, který sdružoval jednotlivé dozorové úřady členských států podle právní úpravy předcházející GDPR, tedy podle 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.

privátní sféry jsou rovněž údaje, které o sobě zařízení aktivně vysílá v hlavičce požadavku na získání webové stránky v rámci protokolu HTTP.[92] Naopak součástí této privátní sféry jsou podle mého názoru údaje, které musí být zjišťovány pomocí skriptu spuštěného na koncovém zařízení. Tyto údaje nejsou sice v úzkém slova smyslu uchovávány v koncovém zařízení podobně, jako jsou strukturovaně uchovávány např. cookies nebo údaje ve webovém úložišti, jsou však jako atributy v zařízení uloženy, proto je mohou spuštěné skripty zjišťovat. Současně jak uvádí WP29, pojem přístup k údajům uloženým v koncovém zařízení se nevztahuje pouze na údaje, které do zařízení uložila konkrétní webová stránka , ale i na údaje dříve uložené.[93] Dovozuji tedy, že se čl. 5 odst. 3 neaplikuje na pasivní fingerprinting, ale pouze na fingerprinting aktivní.

---

[91] Viz WP224, s. 7. Tento závěr potvrzuje rovněž Prohlášení Evropského sboru pro ochranu osobních údajů k revizi nařízení o soukromí a elektronických komunikacích a jeho dopad na ochranu jednotlivců s ohledem na soukromí a důvěrnost jejich komunikací, které uvádí, že „nejen cookies, ale každá sledovací technologie již podléhá souhlasu uživatele nebo podléhá některé z výjimek uvedených v ePrivacy směrnici“ (viz Evropský sbor pro ochranu osobních údajů. Prohlášení Evropského sboru pro ochranu osobních údajů o revizi nařízení o soukromí a elektronických komunikacích a jejím dopadu na ochranu fyzických osob v souvislosti se soukromím a důvěrným charakterem jejich komunikace. In: *European Data Protection Board*. [online]. 5. 5. 2018 [cit. 16. 7. 2018]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_cs_0.pdf), a také návrh Doporučení k zpracovaní cookies a obdobných prostředků sledovaní od 25. května 2018 vydané Úřadem pro ochranu osobních údajů, které v bodě 2 hovoří o „používání cookies, počítačových souborů, které mimo jiné umožňují jednoznačně rozpoznat přístroj, a jiných obdobných prostředků používaných k rozlišení koncových zařízení uživatelů (jedná se například o otisky zařízení, angl. device fingerprinting).“ Viz Úřad pro ochranu osobních údajů. Doporučení k zpracování cookies a obdobných prostředků sledování od 25. května 2018. In: *Úřad pro ochranu osobních údajů* [online]. 25. 6. 2020. [cit. 1. 2. 2023]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=42915

[92] Jde o údaje o internetovém prohlížeči a operačním systému uživatele, včetně jejich verze, obsažené v poli *User-Agent*. Viz Internet Engineering Task Force. Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content [online]. červen 2014. Červen 2014 [cit. 1. 2. 2023]. In: *Data Tracker*. Dostupné z: https://datatracker.ietf.org/doc/html/rfc7231#section-5, čl. 5.1. Toto pole může mít například pro zařízení Apple iPhone a internetový prohlížeč Safari tvar „Mozilla/5.0 (iPhone; CPU iPhone OS 12_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0 Mobile/15E148 Safari/604.1“ nebo pro počítač s operačním systémem Microsoft Windows 10 a internetovým prohlížečem Chrome „Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36“.

[93] Viz WP224, s. 8.

Samotný požadavek na souhlas je pak třeba vykládat v souladu s požadavky na souhlas stanovené GDPR – směrnice 2002/58/ES ve svém čl. 2 písm. f) stanoví, že „souhlas uživatele či účastníka odpovídá souhlasu subjektu údajů podle směrnice 95/46/ES“, která byla zrušena a nahrazena GDPR. GDPR ve svém článku 94 odst. 2 pak stanoví, že odkazy na směrnici 95/46/ES se považují za odkazy na GDPR.[94] To znamená, že souhlas musí být v souladu s čl. 4 bodem 11 GDPR „svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů“.

Podrobnostem získávání souhlasu se věnují stanoviska řady dozorových úřadů členských států EU.[95] Svobodnost souhlasu v kontextu cookies znamená především, že souhlas nemůže být vynucován znemožněním přístupu k webové stránce či mobilní aplikaci při jeho neudělení (tzv. *cookie walls*

[94] Ke vztahu směrnice 2002/58/ES a GDPR blíže viz Evropský sbor pro ochranu osobních údajů. Stanovisko č. 5/2019 ke vzájemnému působení mezi směrnicí o soukromí a elektronických komunikacích a obecným nařízením o ochraně osobních údajů (GDPR), zejména pokud jde o příslušnost, úkoly a pravomoci úřadů pro ochranu údajů. In: *European Data Protection Board* [online]. 12. 3. 2019. [cit. 1. 2. 2023]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_cs.pdf ETTELDORF, Christina. EDPB on the Interplay between the ePrivacy Directive and the GDPR Reports: European Union. *European Data Protection Law Review* [online]. 2019, roč. 5, č. 2 [cit. 2. 2. 2023].

[95] Například viz Commission nationale de l'informatique et des libertés. Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs ». In: *Commission nationale de l'informatique et des libertés* [online]. [cit. 1. 2. 2023]. Str. 7. Dostupné z: https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf. Information Commissioner's Office. How do we comply with the cookie rules? In: *Information Commissioner's Office* [online]. [cit. 1. 2. 2023]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/. Na další stanoviska odkazuje Spolek pro ochranu osobních údajů. Viz Stanovisko Spolku pro ochranu osobních údajů k právní úpravě cookies v České republice od začátku roku 2022. In: *Spolek pro ochranu osobních údajů* [online]. 15. 12. 2021. [cit. 1. 2. 2023]. Dostupné z: https://www.ochranaudaju.cz/wp-content/uploads/2021/12/Stanovisko_cookies_2021_final.pdf. S politováním je třeba konstatovat, že mezi úřady, které ke cookies vydaly stanovisko, se neřadí český Úřad pro ochranu osobních údajů, který pouze v roce 2018 vydal návrh svého doporučení k veřejné konzultaci, finální stanovisko však vydáno nebylo. Viz Úřad pro ochranu osobních údajů. Doporučení k zpracování cookies a obdobných prostředků sledování od 25. května 2018 [online]. Ke kritice doporučení viz TOMÍŠEK, Jan. *Cookies a GDPR*.

nebo *tracking walls*).[96] Konkrétnost se promítá do požadavku na uvedení účelů, ke kterým budou cookies použity, přičemž uživatel musí mít možnost rozhodovat o udělení či neudělení souhlasu k jednotlivým účelům.[97] Informovanost souhlasu pak znamená zejména povinnost uvedení informací o totožnosti subjektu žádajícího souhlas, rozsahu a účelech zpracování a o právu souhlas kdykoliv odvolat.[98] Ve vztahu ke cookies je významná informace o době exspirace cookies[99] a třetích stranách, které případně budou cookies na základě souhlasu do zařízení uživatele ukládat, resp. je číst.[100] Požadavek na jednoznačnost projevu vůle vylučuje udělen

[96] Viz Stanovisko Spolku pro ochranu osobních údajů k právní úpravě cookies v České republice od začátku roku 2022 [online], s. 3; Evropský sbor pro ochranu osobních údajů. Pokyny č. 05/2020 k souhlasu podle nařízení 2016/679 ze dne 4. května 2020. In: *European Data Protection Board* [online]. 4. 5. 2020. [cit. 1. 2. 2023]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=47474t. Dále viz VEALE, Michael; BORGESIUS, Frederik Zuiderveen. Adtech and real-time bidding under European data protection law. *German Law Journal* [online]. 2022, roč. 23, č. 2, [cit. 6. 2. 2023] s. 236.

[97] Viz Stanovisko Spolku pro ochranu osobních údajů k právní úpravě cookies v České republice od začátku roku 2022 [online], s. 3 a 5. Dále viz VEALE, Michael; BORGESIUS, Frederik Zuiderveen. *Adtech and real-time bidding under European data protection law*, s. 236.

[98] Viz bod 42 odůvodnění GDPR.

[99] Viz rozsudek SDEU (velkého senátu) ze dne 1. října 2019 ve věci C-673/17, Planet49, bod 75.

[100] Blíže k informační povinnosti viz také Evropský sbor pro ochranu osobních údajů. Pokyny č. 8/2020 k cílení na uživatele sociálních médií ze dne 13. dubna 2021. In: *European Data Protection Board* [online]. 13. 4. 2021. [cit. 1. 2. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2021- 11/edpb_guidelines_082020_on_the_c_cs_0.pdf. Bod 72 a násl. Dále viz VEALE, Michael; BORGESIUS, Frederik Zuiderveen. *Adtech and real-time bidding under European data protection law*, s. 236.

souhlasu např. prostým pokračováním v prohlížení webové stránky.[101] Při sběru souhlasu je také třeba se vyhnout klamavým praktikám.[102]

6. NAŘÍZENÍ EPRIVACY

Návrh nařízení ePrivacy představila Evropská komise v lednu 2017.[103] Příslušný výbor Evropského parlamentu k němu v říjnu 2017 schválil řadu pozměňovacích návrhů, které se staly oficiální pozicí Evropského parlamentu pro jednání s Evropskou komisí a Radou Evropské unie.[104] Souběžně probíhaly diskuze v Radě,[105] které v únoru 2021 vyústily ve společnou pozici Rady pro jednání s Evropským parlamentem.[106]

Ochraně informací uchovávaných v koncových zařízeních uživatelů a souvisejících s těmito zařízeními ve vztahu ke cookies se návrh Evropské komise věnuje v čl. 8 odst. 1. Čl. 10 pak stanovuje požadavky na nastavení webových prohlížečů týkající se cookies a podobných technologií.[107]

Působnost čl. 8 odst. 1 je vztažena k „využití funkcí koncového zařízení pro zpracování a uchovávání, jakož i shromažďování informací z kon-

[101] Podle SDEU GDPR „výslovně vylučuje považovat za souhlas ‚[m]lčení, předem zaškrtnutá políčka nebo nečinnost'". Viz rozsudek SDEU ze dne 1. října 2019 ve věci C-673/17 (Planet49), bod 62. Dále viz Spolek pro ochranu osobních údajů. op.cit. s. 4. VEALE, Michael; BORGESIUS, Frederik Zuiderveen. *Adtech and real-time bidding under European data protection law*, s. 236. Úvahu o „udělení souhlasu jednoznačnou akcí uživatele na webu, např. kliknutím na libovolný odkaz, pokud je uživatel předem poučen (např. v informační liště), že taková akce se považuje za souhlas, a je mu dána možnost souhlas neudělit (např. vypnutím příslušné funkce zahrnující zpracování osobních údajů v nastavení stránky předtím, než je příslušné zpracování osobních údajů zahájeno)" vyjádřenou v TOMÍŠEK, Jan. Cookies a GDPR. *Právní rozhledy*. 2018, roč. 26, č. 20, s. 693. lze ve světle stanovisek dozorových úřadů považovat za překonanou. Pro historickou perspektivu viz BORGESIUS, Frederik J. Zuiderveen. *Personal data processing for behavioural targeting: which legal basis?* [online]. 2015, roč. 5, č. 3, [cit. 1. 2. 2023]., s. 170.

[102] Evropský sbor pro ochranu osobních údajů. Report of the work undertaken by the Cookie Banner Taskforce, Adopted on 17 January 2023. In: *European Data Protection Board* [online]. 17. 1. 2023. [cit. 1. 2. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf

[103] Viz návrh Komise.

[104] LAURISTIN, Marju. Zpráva o návrhu nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES. A8-0324/2017. In: *European Parliament* [online]. 20. 10. 2017 [cit. 11. leden 2023]. Dostupné z: https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html (dále jen „pozice Evropského parlamentu").

cových zařízení koncových uživatelů, včetně informací o softwaru a hardwaru, jinými subjekty, než jsou dotčení koncoví uživatelé“. Z této formulace oproti čl. 5 odst. 3 směrnice 2002/58/ES jednoznačně plyne, že se právní úprava vztahuje nejen na technologie spočívající v ukládání dat do webového prohlížeče uživatele jako cookies nebo webové úložiště, ale také techniky pracující s údaji, které lze z koncového zařízení získat a vypovídají o jeho hardwaru či softwaru, jako je fingerprinting. Současně jsem však toho názoru, že stejně jako čl. 5 odst. 3 směrnice 2002/58/ES se úprava čl. 8 odst. 1 nevztahuje na pasivní fingerprinting, tj. na použití údajů, které o sobě zařízení aktivně vysílá, jako jsou údaje z hlaviček požadavků protokolu HTTP.[108]

Tituly k využití funkcí koncového zařízení pro zpracování a uchovávání, jakož i shromažďování informací z koncových zařízení uživatelů, včetně informací o softwaru a hardwaru, jinými subjekty, než jsou dotčení uživatelé, jsou shodně se současnou úpravou technická nezbytnost dle písmen a)

[105] Pro shrnutí vývoje v různých fázích viz např. Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Progress report. 2017/0003(COD), 13106/20. In: *EUR-Lex* [online]. 23. 11. 2020 [cit. 27. 5. 2023]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-13106-2020-INIT/en/pdf Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). 2017/0003(COD), 5008/2. In: *EUR-Lex* [online]. 5. 1. 2021 [cit. 27. 5. 2023]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf Pro přehled všech verzí viz návrh Úřad pro publikace Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). 2017/0003(COD), 52017PC0010. In: *EUR-Lex* [online]. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52017PC0010

[106] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Mandate for negotiations with EP. 2017/0003(COD), 6087/21. In: *EUR-Lex* [online]. 10. 2. 2021 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT (dále jen „pozice Rady“).

[107] Viz návrh Komise.

a c) a souhlas uživatele dle písmene b). Doplněno bylo pouze písmeno d) umožňující tyto činnosti ve vztahu k „měření návštěvnosti internetových stránek, za předpokladu, že toto měření je prováděno poskytovatelem služby informační společnosti požadované koncovým uživatelem“.[109]

Novinkou v návrhu je především uložení povinností tvůrcům internetových prohlížečů v čl. 10. Tyto povinnosti však byly navrženy poměrně mírně – příslušný software by pouze musel „nabízet možnost zabránit třetím stranám v uchovávání informací v koncovém zařízení koncového uživatele nebo ve zpracovávání informací, které jsou v tomto zařízení již uchovávané“ (tj. možnost blokovat cookies a podobné technologie), a při instalaci informovat koncového uživatele o možnostech nastavení ochrany soukromí a k tomu, aby mohla instalace pokračovat, vyžadovat souhlas koncového uživatele s nastavením.[110]

Pozice Evropského parlamentu oproti návrhu Komise zúžila formulaci titulů pro přístup k zařízení koncového uživatele předložených Komisí (např. požadavkem na „striktní“ technickou nezbytnost nebo požadavkem na „určitý souhlas“).[111] Dále rozpracovala podmínky pro uplatnění titulu měření návštěvnosti webu a doplnila nové tituly bezpečnostních aktualizací softwaru a nezbytného přístupu zaměstnavatele k pracovnímu zařízení.[112] Doplněno rovněž bylo ustanovení specificky zakazující *cookie walls* bránící v přístupu k webové stránce při neudělení souhlasu.[113]

---

[108] Na pasivní fingerprinting lze aplikovat čl. 8 odst. 2 návrhu Komise, který se vztahuje na „[s]hromažďování informací vysílaných koncovým zařízením za účelem umožnění připojení tohoto zařízení k jinému zařízení“. Dle písmene b) tohoto ustanovení však lze takový fingerprinting realizovat, pokud „je zobrazeno jasné a nápadné oznámení informující alespoň o způsobech shromažďování, jeho účelu a osobě, která je za ně odpovědná, a podávající další informace požadované podle článku 13 nařízení (EU) 2016/679, pokud jsou shromažďovány osobní údaje, jakož i o případných opatřeních, která může koncový uživatel koncového zařízení učinit, aby shromažďování minimalizoval nebo zastavil“ a současně za podmínky použití vhodných technických a organizačních opatření podle čl. 32 GDPR.

[109] Viz čl. 8 odst. 1 návrhu Komise. Překlad autor.

[110] Viz čl. 10 odst. 1 a 2 návrhu Komise.

[111] Viz pozměňovací návrhy č. 84 až 88 pozice Evropského parlamentu.

[112] Viz pozměňovací návrhy č. 89 až 91 tamtéž. Úpravu měření návštěvnosti doplňuje rovněž pozměňovací návrh č. 99 tamtéž.

[113] Viz pozměňovací návrh č. 92 tamtéž.

Významně byly v pozici Evropského parlamentu přepracovány povinnosti tvůrců internetových prohlížečů. Nově by internetové prohlížeče musely ve výchozím nastavení blokovat cookies a podobné technologie s výjimkou takových, které jsou technicky nezbytné, při instalaci uživateli nabídnout možnost toto výchozí nastavení odsouhlasit nebo změnit, nabídnout též možnost rozhodnout o blokaci cookies a podobných technologií pro měření návštěvnosti a nabízet možnost udělení určitého souhlasu nastavením prohlížeče.[114]

Pro účely tohoto určitého souhlasu má uživatel být před prvním použitím prohlížeče informován o možnosti nastavit souhlasy pro každou webovou stránku samostatně a tato možnost nastavení má být neustále snadno dostupná.[115] Toto individuální nastavení by zřejmě měla mít možnost iniciovat i jednotlivá webová stránka.[116] Tato nastavení souhlasů a námitek proti zpracování ve smyslu čl. 21 GDPR by se současně měla promítnout do technicky specifikovaných signálů odesílaných webovým stránkám. Tyto signály by pak měly být pro příslušné webové stránky závazné.[117] Pozice Evropského parlamentu také rozšiřuje požadavek na souhlas na pasivní fingerprinting, pokud slouží jiným než technickým nebo statistickým účelům.[118]

Souběžné diskuze v Radě Evropské unie byly komplikované – trvaly více než 4 roky a ve vztahu k článku 8 a souvisejícím bodům odůvodnění při nich vzniklo nejméně 12 různých verzí návrhu obsahujících dílčí změny.[119] V úvodu diskuzí vyjádřily některé členské státy potřebu nalézt vyvážené řešení reagující na problém „souhlasového vyčerpání“ (*consent fatigue*), tedy

[114] Viz pozměňovací návrhy č. 106 až 109 tamtéž.

[115] Viz pozměňovací návrh č. 110 tamtéž.

[116] Viz pozměňovací návrh č. 116 tamtéž.

[117] Viz pozměňovací návrhy č. 103 a 111 až 115 tamtéž.

[118] Viz pozměňovací návrhy č. 95 až 99 tamtéž.

[119] Viz Úřad pro publikace Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). 2017/0003(COD), 52017PC0010. In: *EUR-Lex* [online]. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52017PC0010.

přetížení uživatelů četnými požadavky na souhlas.[120] Významným tématem diskuzí byly také technické a ekonomické vlastnosti ekosystému internetové reklamy.[121]

K prvním změnám v návrhu začalo docházet v průběhu estonského předsednictví během podzimu 2017. Článek 9 upravující souhlasy byl z důvodu obecnosti přesunut do kapitoly I jako článek 4a[122] – tato změna přetrvala až do finální pozice Rady.[123] Podobně jako v Evropském parlamentu bylo navrženo doplnění titulu pro aktualizace softwaru,[124] následně také pro lokalizaci volajícího v případě nouzového volání.[125]

[120] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Discussion on possible compromise solutions. 2017/0003(COD), 5934/19. In: *EUR-Lex* [online]. 4. 2. 2019, s. 3. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5934_2019_INIT

[121] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Presidency note. 2017/0003 (COD), 10866/17. In: *EUR-Lex* [online]. 3. 7. 2017, s. 4. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10866_2017_INIT

[122] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003 (COD), 11995/17. In: *EUR-Lex* [online]. 8. 9. 2017, čl. 4a. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11995_2017_INIT

[123] Viz pozice Rady, čl. 4a.

[124] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003 (COD), 11995/17. čl. 8.

[125] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency. 2017/0003 (COD), 15333/17. In: *EUR-Lex* [online]. 5. 12. 2017, čl. 8. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15333_2017_INIT

Přestože v říjnu 2017 schválil svůj návrh Evropský parlament, do návrhů diskutovaných v Radě se viditelným způsobem nepromítl,[126] předmětem diskuze však byla mimo jiné otázka, zda by prohlížeče měly umožňovat udělení souhlasu pro konkrétní webové stránky.[127] K diskuzi byla také předložena možnost zahrnout do textu titul pro přístup ke koncovému zařízení v podobě oprávněného zájmu.[128] Ani jeden z těchto návrhů se v danou chvíli nepromítl do diskutovaného textu,[129] předmětem diskuze se však stala otázka *cookie walls a* do bodu 21 odůvodnění byla doplněna věta deklarující, že přijetí cookies může být podmínkou přístupu k webové stránce.[130]

Problematika souhlasu jako podmínky přístupu pak byla v rámci odůvodnění postupně rozpracovávána i v dalších verzích návrhu.[131] Nejprve byla textace formulována tak, že souhlas může být vyžadován pro přístup k obsahu poskytovanému bez přímé platby, pokud je uživateli současně nabídnuta ekvivalentní možnost, jak k obsahu přistupovat bez udělení souhlasu.[132] V návrhu rakouského předsednictví Rady pak byla tato formulace doplněna deklarací, že použití cookies může být nezbytné v případě webové

[126] Viz tamtéž. Pouze zmínka o zařízeních zaměstnavatele se později promítla do bodu 20a odůvodnění návrhu viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Discussion on possible compromise solutions. 2017/0003(COD), 5934/19. s. 4.

[127] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper 2017/0003(COD), 5165/18. In: *EUR-Lex* [online]. 11. 1. 2018, s. 22. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5165_2018_INIT

[128] Viz tamtéž, s. 21.

[129] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion. 2017/0003(COD), 7207/18. In: *EUR-Lex* [online]. 22. 3. 2018, čl. 8 a 10. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7207_2018_INIT

[130] Viz tamtéž, bod 21 odůvodnění.

stránky, která je převážně financována z reklamy, pokud je uživatel vhodným způsobem informován o účelech použití cookies a toto užití přijal,[133] toto doplnění však bylo finským předsednictvím vypuštěno.[134]

Současně byl po diskuzi vypuštěn celý čl. 10 upravující funkcionality webových prohlížečů, a to s ohledem na obavy o dopady na zátěž pro prohlížeče a aplikace, otázky hospodářské soutěže a také schopnosti tohoto ustanovení řešit problém „souhlasového vyčerpání" (*consent fatigue*).[135] Ma-

[131] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency. 2017/0003(COD), 10975/18. In: *EUR-Lex* [online]. 10. 7. 2018 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10975_2018_INIT bod odůvodnění 20. Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003(COD), 13256/18. In: *EUR-Lex* [online]. 19. 10. 2018 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13256_2018_INIT bod odůvodnění 21. Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Discussion on possible compromise solutions. 2017/0003(COD), 5934/19. s. 3.

[132] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003(COD), 10975/18. bod odůvodnění 20.

[133] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003(COD), 13256/18. bod odůvodnění 21. Tato formulace se zdá být vnitřně rozporná, protože odkazuje z hlediska titulu pro přístup k zařízení jak na nezbytnost pro poskytování služby, tak na souhlas.

[134] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). 2017/0003(COD), 11291/19. In: *EUR-Lex* [online]. 26. 7. 2019, bod 21 odůvodnění. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11291_2019_INIT

terie byla v pozdější verzi částečně doplněna do bodu 21a odůvodnění návrhu.[136]

Za významný považuji návrh chorvatského předsednictví, který v návaznosti na dřívější diskuze[137] do čl. 8 vkládá jako právní titul pro přístup ke koncovému zařízení oprávněný zájem.[138] Navržená formulace byla obdobná čl. 6 odst. 1 písm. f) GDPR – přístup ke koncovému zařízení by byl možný, pokud by to bylo nezbytné pro účely oprávněných zájmů poskytovatele, s výjimkou případů, kdy by nad takovým zájmem převažovaly zájmy nebo základní práva a svobody koncového uživatele.[139] Návrh byl doplněn ustanovením stanovícím domněnku, že zájmy koncového uživatele převažují nad zájmy poskytovatele služby mj. v případě, kdy poskytovatel služby shromažďuje nebo zpracovává informace za účelem profilování uživatele.[140] Vedle toho byl doprovozen zákazem takto získané informace v neanonymizované podobě sdílet s jinými subjekty, vyjma zpracovatelů zavázaných podle čl. 28 GDPR. Podmínkou jeho využití bylo také předchozí posouzení vlivu zamýšlené činnosti na důvěrnost komunikací a soukromí koncových uživatelů podle čl. 35 GDPR, informování uživatele o zamýšleném přístupu a jeho právu tento přístup odmítnout a přijetí přiměřených technických a organizačních opatření.[141]

---

[135] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 017/0003(COD), 10975/18. s. 3

[136] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Discussion on possible compromise solutions 2017/0003(COD), 5934/19. s. 3.

[137] Viz tamtéž, s. 21.

[138] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017/0003(COD), 5979/20. čl. 8 odst. 1 písm. g) a odst. 1a.

[139] Viz tamtéž, čl. 8 odst. 1 písm. g).

[140] Viz tamtéž.

[141] Viz tamtéž, čl. 8 odst. 1a a bod odůvodnění 21b.

Tento návrh byl podroben diskuzi v Radě, přičemž z podkladu německého předsednictví, které následovalo po předsednictví chorvatském, vyplývá obava, že by tento přístup „výrazně usnadnil instalaci softwaru, který je často považován za hlavní vstupní bránu pro škodlivý software.“[142] Německé předsednictví proto navrhlo buď zachovat chorvatský návrh a diskutovat, jak zajistit bezpečnost koncových zařízení, nebo se vrátit k předchozí textaci finského předsednictví, která oprávněný zájem jako titul pro přístup ke koncovému zařízení nepřipouštěla.[143] Druhý navrhovaný přístup v Radě převládl a oprávněný zájem byl jako titul nakonec z textace vypuštěn.[144]

Ve finálním znění pozice Rady se tak samotný čl. 8 odst. 1 od původní textace navržené Evropskou komisí liší výčtem titulů pro přístup ke koncovému zařízení, ne však koncepčně.[145] Zpřesněn je titul pro měření návštěvnosti[146] a doplněn titul pro zajištění bezpečnosti služby informační společnosti, předcházení podvodům a detekci technických chyb,[147] titul pro bezpečnostní aktualizace softwaru[148] a titul pro přístup k zařízení v případě nouzového volání.[149] Dále je doplněno nové ustanovení upravující okolnosti, které by měly být zohledněny při posuzování, zda je zpracování informací získaných ze zařízení koncového uživatele k jiným účelům slučitelné s původním účelem, pro který byly informace získány, a podmínky ta-

[142] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulati-on on Privacy and Electronic Communications) – Presidency discussion paper 2017/0003(COD), 9243/20. In: *EUR-Lex* [online]. 6. 6. 2020, s. 6, překlad autor. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9243_2020_INIT

[143] Viz tamtéž.

[144] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulati-on on Privacy and Electronic Communications). 2017/0003(COD), 9931/20. In: *EUR-Lex* [online]. 4. 11. 2020, s. 4 a čl. 8. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9931_2020_INIT

[145] Viz pozici Rady.

[146] Viz čl. 8 odst. 1 písm. d a bod 21a odůvodnění pozice Rady.

[147] Viz tamtéž, čl. 8 odst. 1 písm. da).

[148] Viz tamtéž, čl. 8 odst. 1 písm. e) a bod 21b odůvodnění.

[149] Viz tamtéž, čl. 8 odst. 1 písm. f).

kového dalších zpracování vč. zákazu sdílet takové informace s jinými subjekty než zpracovateli zavázanými podle čl. 28 GDPR nebo v anonymizované podobě.[150] Do čl. 8 odst. 2 pak byl podobně jako v pozici Evropského parlamentu doplněn požadavek na souhlas s pasivním fingerprintingem, pokud slouží jiným než statistickým účelům.[151]

Významné změny se dotýkají odůvodnění návrhu a čl. 9 a 10. V bodu odůvodnění 20aaaa bylo doplněno, že přístup k webové stránce bez přímé úhrady může být podmíněn souhlasem s ukládáním a čtením cookies, aniž by uživatel byl zbaven svobodné volby, a to za předpokladu, že jsou uživateli poskytovány srozumitelné informace o používání cookies a může si volit mezi variantou služby s udělením souhlasu a ekvivalentní nabídkou, která udělení souhlasu nevyžaduje.[152] Toto pravidlo přitom nemá být možné aplikovat v případě významné nerovnováhy mezi koncovým uživatelem a poskytovatelem služby, například u služeb veřejných institucí a poskytovatelů služeb v dominantním postavení na trhu.[153] Současně však bod 21aa odůvodnění uvádí, že použití cookies může být nezbytné v případě webové stránky, která je převážně financována z reklamy, pokud je uživatel vhodným způsobem informován o účelech použití cookies a toto užití přijal.[154]

Články 9 a 10 pak byly přetvořeny do čl. 4a, který však z hlediska požadavků na funkce webových prohlížečů obsahuje minimum z původního návrhu Evropské komise. V článku je tak pouze stanoveno, že souhlas je možné vyjádřit pomocí internetového prohlížeče.[155] Nově je přitom doplněno, že takto udělený souhlas má převážit nad nastavením softwaru, a pokud je uživatelem udělen pro konkrétní službu, má být okamžitě promítnut.[156]

Materie původního čl. 10 je pak přesunuta do bodu 20a odůvodnění, který uvádí, že koncoví uživatelé čelí častým žádostem o souhlas s použitím

[150] Viz tamtéž, čl. 8 odst. 1 písm. g) až i).

[151] Viz tamtéž, čl. 8 odst. 2.

[152] Viz tamtéž, bod 20aaaa odůvodnění.

[153] Viz tamtéž.

[154] Viz tamtéž, bod 21aa odůvodnění.

[155] Viz tamtéž, čl. 4a odst. 2.

[156] Viz tamtéž, čl. 4a odst. 2aa.

cookies, což může vést k přetížení koncových uživatelů a k tomu, že žádosti o souhlas nečtou, a to může v důsledku vést ke snížení úrovně poskytované ochrany. Proto by bylo užitečné, aby určitý a informovaný souhlas k jednomu či více účelům bylo možné vyjádřit pomocí nastavení internetového prohlížeče, například formou seznamu poskytovatelů, jimž bude použití cookies určitých typů dovoleno. Odůvodnění vyzývá tvůrce internetových prohlížečů k vytvoření takových možností, nejde však o právně závaznou povinnost. Vedle toho odůvodnění doplňuje, že „přímo vyjádřený" souhlas (patrně je tím myšlen souhlas ve vztahu ke konkrétní webové stránce) by měl mít vždy přednost.[157]

Návrh tedy prodělal v průběhu jednání v Radě významný vývoj, a to směrem odlišným, než se ubírá návrh Evropského parlamentu, který klade důraz na souhlas koncového uživatele a jeho povinnou a komplexní implementaci na úrovni nastavení webových prohlížečů. S ohledem na tuto rozdílnost vyjednávacích pozic Evropského parlamentu a Rady lze očekávat dlouhou diskuzi v rámci trialogu a také je namístě diskutovat, jaké řešení úpravy přístupu ke koncovému zařízení by bylo *de lege ferenda* nejvhodnější.

7. POŽADAVKY NA NOVOU PRÁVNÍ ÚPRAVU

Pro účely diskuze je vhodné shrnout, že platná právní úprava pro ukládání a čtení cookies a použití podobných technologií včetně použití údajů o koncovém zařízení vyžaduje ve většině případů souhlas – ten není třeba pouze pro cookies a podobné technologie nezbytné k fungování příslušné webové stránky. Souhlas musí splňovat požadavky GDPR, tedy být svobodný, konkrétní, informovaný a mít formu jednoznačného projevu vůle.

Návrh nařízení ePrivacy tento základní požadavek zachovává. Výslovně rozšiřuje působnost právní úpravy na využití funkcí koncového zařízení pro zpracování dat na shromažďování informací z koncových zařízení.[158] Jak ve znění předloženém Evropskou komisí, tak v rámci pozic Evropského parlamentu a Rady pak zavádí některé další úzce vymezené výjimky z poža-

[157] Viz tamtéž, bod 20a odůvodnění.

[158] Viz čl. 8 odst. 1 a bod 20 odůvodnění návrhu Komise.

davku na souhlas – z pohledu cookies je relevantní zejména výjimka pro měření návštěvnosti webových stránek.[159]

Evropský parlament a Rada se však významně rozchází v přístupu k udělování souhlasu. Evropský parlament klade důraz na svobodnost souhlasu (vč. zákazu cookie walls),[160] možnost udělování velmi specifických souhlasů prostřednictvím nastavení internetového prohlížeče[161] a povinnost webových stránek příslušné signály internetového prohlížeče respektovat.[162] Naopak Rada připouští, že pro přístup k webové stránce poskytované bezplatně může být souhlas s použitím cookies za definovaných podmínek vyžadován[163] a navrhuje, aby poskytnutí možnosti udělovat souhlasy prostřednictvím nastavení webového prohlížeče bylo pro tvůrce těchto prohlížečů dobrovolné.[164]

Tato rozdílnost pozic ukazuje na dva hlavní problémy, se kterými by se nová právní úprava měla vyrovnat. Na jedné straně je to problematika přetížení uživatelů žádostmi o souhlas. Na druhé straně pak potřeba zajistit přiměřené podmínky pro realizaci cílené reklamy, která je zdrojem financování pro některé webové stránky, které nabízejí uživatelům obsah či služby zdarma.

Současně je potřeba vnímat, že právní úprava čtení a ukládání cookies a použití podobných technologií jako součást právní úpravy soukromí v elektronických komunikacích je nástrojem ochrany práva na soukromí, které je základním právem chráněným čl. 7 odst. 1 a čl. 10 odst. 2 a 3 Listiny základních práva a svobod,[165] čl. 7 Listiny základních práv Evropské unie a čl. 8 Úmluvy o ochraně lidských práv a základních svobod Rady Evropy.[166] Toto pojetí vyplývá z bodů 1, 4, 5, 6 a 24 odůvodnění směrnice

[159] Viz přehled v části 6. výše.

[160] Viz pozměňovací návrh č. 92 pozice Evropského parlamentu.

[161] Viz pozměňovací návrhy č. 106 až 109 tamtéž.

[162] Viz pozměňovací návrhy č. 103 a 111 až 115 tamtéž.

[163] Viz bod 20aaaa odůvodnění pozice Rady.

[164] Viz bod 20a odůvodnění pozice Rady.

[165] Viz ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů.

2002/58/ES, bodu 66 odůvodnění směrnice 2009/136/ES a z bodů 1 a 20 odůvodnění návrhu nařízení ePrivacy.

Nová právní úprava čtení a ukládání cookies a použití podobných technologií by tedy měla snížit zátěž uživatelů četnými žádostmi o souhlas, vytvořit přiměřené podmínky pro realizaci cílené reklamy jako zdroje financování pro některé webové stránky, a přitom zachovat nebo zvýšit úroveň ochrany soukromí jednotlivců v tomto kontextu.

7.1 PŘETÍŽENÍ ŽÁDOSTMI O SOUHLAS

Problém přetížení uživatelů četnými žádostmi o souhlas s použitím cookies je dle mého názoru spojen s přístupem k ochraně soukromí jako kontrole nad informacemi.[167] Ten vychází z historického pojetí soukromí jako práva jednotlivce „rozhodovat o tom, v jakém rozsahu budou jeho myšlenky a pocity komunikovány jiným,“[168] které v roce 1890 formulovali Warren a Brandeis a které se promítá se do pojetí soukromí řady moderních autorů, jako je Westin,[169] Moore[170] nebo Clarke.[171]

Přístup nastavený v roce 1890 však neobstojí tváří v tvář současným technologiím. Množství webových stránek, které pracují s informacemi relevantními pro soukromí uživatele a které běžný uživatel může za jediný den navštívit, je tak vysoké, že kvalifikované vykonání kontroly nad nakládáním s takovými informacemi (typicky rozhodnutí o udělení či neudělení souhlasu) není reálné.

Takové kvalifikované rozhodnutí by zpravidla vyžadovalo posouzení podrobných podmínek ochrany soukromí všech takových webových stránek.

---

[166] Viz sdělení č. 209/1992 Sb. federálního ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.

[167] Viz RICHARDS, Neil M.; HARTZOG, Woodrow. *Taking Trust Seriously in Privacy Law*, s. 444.

[168] Viz WARREN, Samuel D.; BRANDEIS, Louis D. Right to privacy. *Harvard Law Review* [online]. 1890, roč. 4, č. 5 [cit. 6. 2. 2023], s. 198.

[169] Viz WESTIN, A. *Privacy and Freedom*. New York: Ig Publishing, 2018, s. 24.

[170] Viz MOORE, Adam D. *Privacy rights: Moral and legal foundations*. Pennsylvania: Penn State Press, 2010, s.16.

[171] Viz CLARKE, R. Introduction to Dataveillance and Information Privacy, and Definitions of Terms In: *Roger Clarke's Web-Site* [online]. 24. 7. 2016 [cit. 3. 8. 2021]. Dostupné z: http://www.rogerclarke.com/DV/Intro.html#Priv.

Podle výzkumu z roku 2008 by přitom průměrný Američan musel strávit v průměru 201 hodin tím, aby si rychle prošel všechny zásady ochrany soukromí, se kterými se za rok setká.[172] Domnívám se, že v současnosti by počet hodin byl výrazně vyšší s ohledem na intenzivnější používání internetu i vzhledem k tomu, že s rostoucími požadavky na transparentnost[173] rozsah těchto zásad spíše vzrostl.

Podle studie z roku 2020 zkoumající pět nejčastěji používaných nástrojů pro shromažďování souhlasů na 10 000 nejnavštěvovanějších webových stránkách ve Velké Británii byl medián počtu třetích stran uvedených v souhlasovém dialogu 315. Text popisující tyto třetí strany měl v průměru 7985 slov, což by znamenalo, že čtenář čtoucí 250 slov za minutu na každé webové stránce stráví průměrně více než 31 minut čtením o třetích stranách, na které se vztahuje souhlas, o který byl požádán.[174]

I při prostudování všech příslušných zásad a informací by přitom uživatel nejspíše čelil informační asymetrii, protože procesy zpracování dat navazující na použití cookies a podobných technologií jsou zpravidla komplexní a zásady ochrany soukromí tak nemohou obsahovat veškeré informace, které o nich má provozovatel webové stránky k dispozici.[175] S komplexností těchto procesů je také spojena komplexnost předkládaných voleb. Souhlas s použitím cookies a podobných technologií musí splňovat požadavky GDPR, proto se musí žádost o souhlas vztahovat ke všem účelům zpracování a uživatel musí mít možnost o účelech rozhodovat jednot-

[172] Viz MCDONALD, Aleecia M.; CRANOR, Lorrie Faith. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* [online]. 2008, roč. 4, č. 3 [cit. 6. 3. 2022], s. 565.

[173] Zejména viz čl. 12 GDPR.

[174] Viz NOUWENS, Midas et al. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* [online]. New York, NY, USA: Association for Computing Machinery, 2020, [cit. 2. 2. 2023]. s. 4 a 6.

[175] Viz ACQUISTI, Alessandro et al. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys* [online]. 2017, roč. 50, č. 3 [cit. 2. 2. 2023] s. 4. CAROLAN, Eoin CASTILLO-MAYEN, M. Rosario. *Why More User Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws*, s. 380. COFONE, Ignacio N. *The way the cookie crumbles: online tracking meets behavioural economics*, s. 51.

livě.[176] Ohledně jedné webové stránky tak nestačí učinit jedno rozhodnutí, ale je třeba takových rozhodnutí několik (jakkoli se nakonec mohou projevit jedinou akcí směřující k udělení souhlasu pro všechny účely).[177]

Zpracování takového množství informací naráží na kognitivní limity uživatele – behaviorální ekonomie v tomto směru používá pojem limitovaná racionalita.[178] Rozhodnutí v tomto směru jsou také ovlivňována zkresleními v úsudku a chování, které mohou vést k rozhodnutím, jež nejsou v souladu se skutečnými preferencemi uživatele.[179] K tomu mohou vést také úmyslné či neúmyslné manipulace ze strany provozovatelů webových stránek, kteří mají tendenci směřovat uživatele k volbě, která je pro provozovatele výhodnější (typicky udělení souhlasu), např. zvýrazněním příslušných tlačítek.[180]

Praktická implementace žádostí webových stránek o souhlas tak nevede k vyšší informovanosti uživatelů o cookies nebo podobných technologií nebo větší motivaci informace získávat.[181] Naopak tyto žádosti mohou v uživatelích vyvolávat (ne nutně podložený) pocit lepší ochrany soukromí

[176] Viz bod 43 odůvodnění GDPR. Dále viz Spolek pro ochranu osobních údajů. op. cit., s. 5.

[177] Nemluvě o případech, kdy provozovatel webové stránky proaktivně umožňuje rozhodování o jednotlivých třetích stranách, jak to například vyžaduje standard IAB TCF 2.0. Viz Interactive advertising bureau. IAB Europe Transparency & Consent Framework Policies. In: *Interactive advertising bureau* [online]. 21. 6. 2022 [cit. 22. 1. 2023]. Dostupné z: https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/ příloha B, část C, bod c.iii. V takových případech mohou být voleb desítky.

[178] Viz ACQUISTI, Alessandro et al. *Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online,* s. 5.

[179] Viz ACQUISTI, Alessandro et al. *Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online* s. 6. ; DOUGHERTY, Christie. *Every Breath You Take, Every Move You Make, Facebook's Watching You: A Behavioral Economic Analysis of the US California Consumer Privacy Act and EU ePrivacy Regulation*, s. 640.

[180] Viz UTZ, Christine et al. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* [online]. New York, NY, USA: Association for Computing Machinery, 2019, [cit. 2. 1. 2022] s. 976. noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints. In: *noyb* [online]. 31. 5. 202 [cit. 24. 1. 2023]. Dostupné z: https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints. Obdobně viz Evropský sbor pro ochranu osobních údajů. Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them Version 1.0 Adopted on 14 March 2022. In: European Data Protection Board [online]. 14. 3. 2022 [cit. 1. 2. 2023] Dostupné z: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

a motivovat je k rozsáhlejšímu sdílení informací.[182] Současně uživatelé považují žádosti často za obtěžující.[183]

Jak tedy správně uvádí citovaný bod 20a odůvodnění návrhu nařízení ePrivacy ve znění pozice Rady Evropské unie, uživatelé internetu čelí častým žádostem o souhlas s použitím cookies, což může vést k přetížení koncových uživatelů a k tomu, že žádosti o souhlas nečtou,[184] a to může v důsledku vést ke snížení úrovně poskytované ochrany.

Řešením tohoto problému je snížení důrazu na kontrolu uživatele jako prostředku ochrany jeho soukromí. Aby toto snížení důrazu na kontrolu však současně neznamenalo snížení úrovně poskytované ochrany, je třeba najít alternativní řešení, které tuto ochranu zajistí. Východiskem dle mého názoru může být přístup k ochraně soukromí založený na důvěře, přebírající prvky z práva fiduciárních vztahů.[185]

Jak poznamenává von Lewinski, právní úprava ochrany osobních údajů je soubor pravidel, který upravuje asymetrii vznikající při zpracování

---

[181] Viz COFONE, Ignacio N. *The way the cookie crumbles: online tracking meets behavioural economics,* s. 51.

[182] Viz CAROLAN, Eoin; CASTILLO-MAYEN, M. Rosario. Why More User Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws. *Virginia Journal of Law & Technology*. 2014, roč. 19, č. 2, s. 378.

[183] Viz KULYK, Oksana et al. Has the GDPR hype affected users' reaction to cookie disclaimers? *Journal of Cybersecurity* [online]. 2020, roč. 6, č. 1, [cit. 1. 2. 2023], s. 4. Dále viz COFONE, Ignacio N. *The way the cookie crumbles: online tracking meets behavioural economics,* s. 32.

[184] Viz KULYK, Oksana et al. tamtéž., s. 11.

[185] Viz RICHARDS, Neil M.; HARTZOG, Woodrow. *Taking Trust Seriously in Privacy Law*, s. 458. Samotná myšlenka přenesení poznatků z oblasti fiduciárních vztahů do oblasti ochrany soukromí byla poprvé formulována Jackem Balkinem. Viz BALKIN, Jack M. Information Fiduciaries in the Digital Age. In: *Balkinization.* [online] 5. 3. 2014 [cit. 3. 1. 2022]. Dostupné z: https://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html_BALKIN, Jack M. Information fiduciaries and the first amendment. *UC Davis Law Review* [online]. 2015, roč. 49, č. 4 [cit. 12. 2. 2023]. K této myšlence viz ZITTRAIN, Jonathan. How to Exercise the Power You Didn't Ask For. *Harvard Business Review* [online]. 19. 9. 2018 [cit. 30. 10. 2022]. Ke kritice viz KHAN, Lina M.; POZEN, David E. A skeptical view of information fiduciaries. *Harvard Law Review* [online]. 2019, roč. 133, č. 2 [cit. 2. 2. 2023], s. 516. K diskuzi z českého prostředí viz TOMÍŠEK, Jan. Souhlasy s cookies a přístupy k ochraně osobních údajů. *Právník* [online]. 2022, roč. 161, č. 6 [cit. 6. 2. 2023], s. 571 a násl.

osobních údajů.[186] Tuto asymetrii lze podle mého názoru vyvážit nejen tím, že se slabší straně poskytne určitá kontrola nad zpracováním (přístup založený na kontrole), ale také tak, že se omezí jednání dominantní strany tak, aby se snížilo riziko, že zneužije svého postavení nebo bude jednat nedbale na úkor slabší strany. Domnívám se tedy, že nová právní úprava čtení a ukládání cookies a použití podobných technologií by měla namísto kontroly uložit subjektům, které činnosti provádí, takové povinnosti, které zajistí, že v souvislosti s těmito činnostmi nebudou jednat na úkor uživatele.

7.2 FINANCOVÁNÍ BEZPLATNÉHO OBSAHU A SLUŽEB

Problém financování webových stránek nabízejících bezplatný obsah a služby je podobně komplexní jako problém kontroly uživatele. Komentáře reprezentantů reklamního průmyslu budí dojem, že bez možnosti podmiňovat přístup k obsahu souhlasem s cookies se evropský mediální prostor zhroutí.[187] Takový pohled by byl patrně zjednodušující, na druhou stranu nelze podceňovat význam cílené reklamy pro financování médií a dalšího bezplatného obsahu.[188] Nezávislá média jsou přitom důležitá pro demokracii.[189] Z toho důvodu je namístě vést diskuzi, jak umožnit realizaci internetové reklamy způsobem, který by představoval zásah do práva na soukromí

[186] Viz VON LEWINSKI, Kai. Geschichte des Datenschutzrechts von 1600 bis 1977. In: *Freiheit-Sicherheit-Öffentlichkeit*. Heidelberg: Nomos Verlagsgesellschaft mbH & Co. KG, 2009, s. 200.

[187] Viz Interactive advertising bureau. ePrivacy Regulation. In: *Interactive advertising bureau* [online]. [cit. 20. 1. 2023]. Dostupné z: https://iabeurope.eu/proposed-eprivacy-regulation/. Podobně viz HÄRTING, Niko, GÖSSLING, Patrick. Study on the Impact of the Proposed Draft of the ePrivacy Regulation. *Computer Law Review International* [online]. 2018, roč. 19, č. 1 [cit. 20. 1. 2023].

[188] Viz Online platforms and digital advertising. In *Competition and Markets Authority*. [online]. 1. 7. 2020. Dostupné z: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf, s. 6. Evropská komise. Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers. In: *Evropská komise* [online]. 30. 1. 203 [cit. 2. 2. 2023]. Dostupné z: https://op.europa.eu/en/publication-detail/-/publication/8b950a43-a141-11ed-b508-01aa75ed71a1/language-en s. 97.

[189] Viz MCNAIR, Brian. Journalism and Democracy. In: *Journalism and Democracy* [online]. New York: Routledge, 2009, [cit. 20. 1. 2023], s. 248.

v rozsahu proporcionálním k přínosu pro právo na svobodu projevu, právo na přístup k informacím a demokratický právní stát jako veřejný statek.

Současný ekosystém internetové reklamy je ve velké míře založen na sdílení osobních údajů.[190] Tyto osobní údaje jsou sbírány jak inzerenty (např. internetovými obchody), tak provozovateli webových stránek zobrazujícími reklamu (např. online médii), resp. provozovatelé webových stránek zobrazujících reklamu umožňují tato data sbírat třetím stranám, jako jsou platformy poptávky (DSP),[191] platformy nabídky (SSP)[192] a platformy pro správu dat (DMP).[193] Tyto subjekty údaje sbírají, ukládají a budují z nich profil uživatele,[194] který využívají k tomu, aby se v reálném čase rozhodovali, jak je pro ně atraktivní zobrazení reklamy v konkrétní ploše na konkrétní webové stránce, kterou uživatel aktuálně prohlíží.[195] Současně si tyto subjekty údaje sdílí.[196]

---

[190] Ke zdůvodnění, proč jsou sdílená data osobními údaji viz Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29. Stanovisko 2/2010 k internetové reklamě zaměřené na chování. In: *Evropská komise* [online]. 22. 6. 2010. [cit. 2. 2. 2023] Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_cs.pdf s. 9. Dále srov. VEALE, Michael; BORGESIUS, Frederik Zuiderveen. *Adtech and real-time bidding under European data protection law*, s. 233; Z BORGESIUS, Frederik J. Zuiderveen. Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer Law & Security Review* [online]. 2016, roč. 32, č. 2, [cit. 2. 2. 2023] s. 270.

[191] Srov. LIU, Peng; CHAO, Wang. *Computational Advertising: Market and Technologies for Internet Commercial Monetization,* s. 106.

[192] Viz LIU, Peng; CHAO, Wang. *Computational Advertising: Market and Technologies for Internet Commercial Monetization*, s. 96, 345. YUAN, Shuai et al. Internet Advertising: An Interplay among Advertisers, Online Publishers, Ad Exchanges and Web Uses. In: *arXiv* [online]. 2. 7. 2012 [cit. 18. 11. 2022], s. 7.

[193] Viz LIU, Peng; CHAO, Wang. *Computational Advertising: Market and Technologies for Internet Commercial Monetization*, s. 96, 124.

[194] Ve smyslu čl. 4 bod 4 GDPR.

[195] Viz LIU, Peng; CHAO, Wang. tamtéž, s. 18. YUAN, Shuai; WANG, Jun; ZHAO, Xiaoxue. Real-time bidding for online advertising: measurement and analysis. In: *Proceedings of the Seventh International Workshop on Data Mining for Online Advertising* [online]. 2013 [cit. 18. 11. 2022], s. 3.

[196] Viz LIU, Peng; CHAO, Wang. tamtéž s. 124. YUAN, Shuai et al. *Internet Advertising: An Interplay among Advertisers, Online Publishers, Ad Exchanges and Web Users* [online], s. 7.

Subjekty v tomto ekosystému legitimizují svoji činnost složitě konstruovanými souhlasy.[197] Podrobná diskuze platnosti těchto souhlasů z pohledu GDPR přesahuje rámec tohoto článku.[198] I kdybychom však předpokládali, že tyto souhlasy jsou platné, nelze ignorovat zásady ochrany osobních údajů stanovené v čl. 5 GDPR.[199] Jednou z těchto zásad je zásada korektnosti zpracování osobních údajů (v anglickém znění *fairness)*, která vchází z čl. 8 Listiny základních práv Evropské unie a která vyžaduje, „aby nebyly osobní údaje zpracovány způsobem, který je pro subjekt údajů neoprávněně škodlivý, nezákonně diskriminační, neočekávaný nebo zavádějící".[200] Klíčovými prvky korektnosti jsou mimo jiné očekávání, interakce, zákaz diskriminace a zákaz vykořisťování.[201]

---

[197] Viz Interactive advertising bureau. IAB Europe Transparency & Consent Framework Policies [online], příloha B, část C.

[198] Analýzu v tomto směru předkládají VEALE, Michael, BORGESIUS, Frederik Zuiderveen. *Adtech and real-time bidding under European data protection law*, s. 243.

[199] Tyto zásady mohou být porušeny, a to bez nutnosti porušení některého dalšího ustanovení GDPR. Viz Evropský sbor pro ochranu osobních údajů. Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR) Adopted on 5 December 2022. In: *European Data Protection Board* [online]. 5. 12. 2022, bod 223. [31. 1. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2023-01/edpb_binding_decision_202204_ie_sa_meta_instagramservice_redacted_en.pdf s odkazem na Evropský sbor pro ochranu osobních údajů. Závazné rozhodnutí 1/2021 ve věci sporu ohledně návrhu rozhodnutí irského dozorového úřadu týkajícího se společnosti WhatsApp Ireland podle čl. 65 odst. 1 písm. a) obecného nařízení o ochraně osobních údajů. In: *European Data Protection Board* [online]. 28. 7. 2021, bod 191. [31. 1. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2022-03/edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_cs.pdf

[200] Viz Evropský sbor pro ochranu osobních údajů. Pokyny 4/2019 k článku 25 Záměrná a standardní ochrana osobních údajů Verze 2.0 Přijato dne 20. října 2020. In: *European Data Protection Board.* [online]. 20. 10. 2020, bod 69. [cit. 31. 1. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_cs.pdf Též viz Evropský sbor pro ochranu osobních údajů. Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR) Adopted on 5 December 2022 [online], bod 226.

[201] Viz Evropský sbor pro ochranu osobních údajů. Pokyny 4/2019 k článku 25 Záměrná a standardní ochrana osobních údajů Verze 2.0 [online], bod 70. Též viz Evropský sbor pro ochranu osobních údajů. Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR) Adopted on 5 December 2022 [online], bod 227.

Výše popsaná struktura ekosystému internetové reklamy je vzdálená chápání běžných uživatelů internetu.[202] Lze tedy těžko dovozovat, že toky jejich osobních údajů v této struktuře jsou v souladu s jejich rozumným očekáváním. Důsledkem je to, že uživatelé neznají jednotlivé subjekty zapojené do tohoto systému a jejich postavení a nejsou schopni vykonávat vůči nim svá práva – chybí tedy element interakce. Systémy internetové reklamy také umožňují diskriminující praktiky[203] a využití zranitelnosti uživatelů pro manipulaci.[204]

Tyto dílčí rozpory podle mého názoru znamenají, že zpracování osobních údajů ve stávající struktuře ekosystému internetové reklamy představuje ze strany zapojených správců osobních údajů porušení zásady korektnosti. Při důsledné revizi ze strany dozorových úřadů v oblasti ochrany osobních údajů by tedy stávající struktura ekosystému internetové reklamy neměla obstát.

Navzdory řadě podaných stížností[205] je jediným dostupným rozhodnutím dozorového úřadu v této souvislosti rozhodnutí belgického dozorového úřadu z února 2022,[206] které se však vztahuje zejména k rámci pro souhlasy

---

[202] Viz SMIT, Edith G., VAN NOORT, Guda, VOORVELD, Hilde A. M. Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior* [online]. 2014, roč. 32, s. 21. Viz též vyjádření vedoucí britského dozorového úřadu Elizabeth Denham Information Commissioner's Office ICO calls on Google and other companies to eliminate existing privacy risks posed by adtech industry [online]. 29. 11. 2021 [cit. 23. 1. 2023]. Dostupné z: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/11/ico-calls-on-google-and-other-companies-to-eliminate-existing-privacy-risks-posed-by-adtech-industry/

[203] Viz např. ANGWIN, Julia, PARRIS, Terry. Facebook Lets Advertisers Exclude Users by Race [online]. SPEICHER, Till et al. Potential for Discrimination in Online Targeted Advertising [online], s. 9, 10.

[204] Viz např. CALO, Ryan. *Digital market manipulation*, s 996. CRAIN, Matthew, NADLER, Anthony. *Political Manipulation and Internet Advertising Infrastructure*, s. 374.

[205] Viz RYAN, Johnny. Regulatory complaint concerning massive, web-wide data breach by Google and other "ad tech" companies under Europe's GDPR. In: brave [online] 12. 9. 2018 [cit. 23. 1. 2023]. Dostupné z: https://brave.com/adtech-data-breach-complaint/ RYAN, Johnny. Update on GDPR complaint (RTB ad auctions). In: *brave* [online] 28. 1. 2019 [cit. 23. 1. 2023]. Dostupné z: https://brave.com/update-rtb-ad-auction-gdpr/

[206] Autorité de protection des données. *The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR* [online]. [cit. 23. leden 1. 2023]. Dostupné z: https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr

IAB TCF a nakládání s daty při předávání souhlasů udělovaných pomocí tohoto rámce, nikoli samotnému zpracování osobních údajů v systémech internetové reklamy a nezabývá se aplikací zásady korektnosti.[207] Nedávné odvážné rozhodnutí Evropského sboru pro ochranu osobních údajů (dále jen „EDPB“) ve věci služby Instagram[208] však naznačuje, že bychom se v dohledné době mohli dočkat důslednějšího zásahu dozorových úřadů proti ekosystému internetové reklamy. Takový zásah by pak patrně vedl k podstatné transformaci celého ekosystému.

Současně je třeba vnímat, že ekosystém internetové reklamy prodělává významnou transformaci spojenou s výše popsanou postupně končící podporou cookies třetích stran ve webových prohlížečích.[209] Společnosti jako Google, který je zároveň významným hráčem na poli internetové reklamy, na tento trend reagují snahou nalézt technologie, které zmenší zásah do soukromí spojený s použitím cookies třetích stran, ale zachovají stávající obchodní modely a strukturu ekosystému internetové reklamy.[210]

Tyto trendy jdou ruku v ruce, je však otázkou, jak by je měla reflektovat právní úprava přístupu ke koncovému zařízení. Na jednu stranu je patrné, že podpora cookies třetích stran v nejvýznamnějších internetových prohlížečích nebude mít dlouhý život a právní úprava, která by směřovala k jejich povinné blokaci, by tedy neměla pro ekosystém internetové reklamy znamenat podstatnější zásah. Na druhou stranu o dopadech technologií, které je mají nahradit, jako je Topics API a FLEDGE, na ochranu sou-

[207] Tamtéž.

[208] Interactive Advertising Bureau. A Guide to the Post Third-Party Cookie Era [online], s. 17 a násl. Podrobně viz část 3. tohoto článku.

[209] Interactive Advertising Bureau. A Guide to the Post Third-Party Cookie Era [online], s. 17 a násl. Podrobně viz část 3. tohoto článku.

[210] Viz části 3. tohoto článku. Některé open source alternativy uvádí CINAR, Naim; ATEŞ, Sezgin. Data Privacy in Digital Advertising: Towards a Post Third-Party Cookie Era [online]. *SSRN Scholarly Paper*. 24. 2. 2022 [cit. 4. 1. 2023]. Viz též Evropská komise. Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers. In: *Evropská komise* [online]. 30. 1. 2023, s. 177 a násl. [cit. 2. 2. 2023]. Dostupné z: https://op.europa.eu/en/publication-detail/-/publication/8b950a43-a141-11ed-b508-01aa75ed71a1/language-en Změna také může mít dopady z pohledu hospodářské soutěže v podobě posílení dominantního postavení některých subjektů, diskuze těchto dopadů přesahuje záběr tohoto článku.

kromí a jejich současném přínosu pro webové stránky s bezplatným obsahem financovaným z reklamy zatím nemáme jednoznačná data.[211]

Přístup právní úpravy k těmto technologiím by tedy měl být opatrný – je namístě, aby poskytoval vyšší míru flexibility, avšak pouze po důsledném zvážení a přezkoumání konkrétní technologie a se zachováním přiměřené míry kontroly ze strany uživatele.

7.3 OCHRANA SOUKROMÍ

Otázku zajištění stejné nebo vyšší úrovně ochrany soukromí je podle mého názoru třeba vykládat ve světle již citovaných bodů odůvodnění právních předpisů chránících soukromí v elektronických komunikacích a ve světle jejich vývoje.

Bod 24 odůvodnění směrnice 2002/58/ES hovoří o špionážním softwaru (*spyware*), webových štěnicích (*web bugs*), skrytých identifikátorech a jiných podobných nástrojích, které mohou pronikat do koncového zařízení uživatele bez jeho vědomí s cílem získat přístup k informacím, uchovávat skryté informace nebo sledovat činnost uživatele. Bod 66 odůvodnění směrnice 2009/136/ES o softwaru, který tajně sleduje činnost uživatele nebo podvrací provoz koncového zařízení uživatele ve prospěch třetí strany (*spyware*), a virech.[212]

Návrh nařízení ePrivacy v podobě předložené Evropskou komisí jde v tomto směru dále a v bodu 20 odůvodnění hovoří ve stejném kontextu o špionážním softwaru (*spyware*), webových štěnicích (*web bugs*), skrytých identifikátorech, sledovacích cookies a jiných podobných nežádoucích ná-

[211] Ke kritice viz GUY, Amy. Early design review for the Topics API #726. Komentář uživatele rhiaro z 12. 1. 2023. In: github [online]. 12. 1. 2023 [cit. 30. 1. 2023]. Dostupné z: https://github.com/w3ctag/design-reviews/issues/726#issuecomment-1379908459

[212] Bod 25 odůvodnění směrnice 2002/58/ES pak zdůrazňuje, že informování o cookies je „obzvláště důležité v případě, kdy uživatelé odlišní od původního uživatele mají přístup ke koncovému zařízení, a tudíž i k veškerým údajům uchovávaným v takovém zařízení, které obsahují i citlivé informace o soukromí," a proto požaduje, aby informace a právo odmítnout byly „poskytnuty jednorázově pro použití různých nástrojů, které mohou být instalovány do koncového zařízení uživatele v průběhu téhož připojení, jakož i pro další použití těchto nástrojů v průběhu následných připojení." Jakkoli je však tento záměr legitimní, stopy v zařízení uživatele zanechávají i technicky nezbytné cookies, které jsou z nastaveného režimu vyňaty.

strojích pro sledování, které mohou pronikat do koncového zařízení koncového uživatele.

Z toho lze dovodit, že právní úprava soukromí v elektronických komunikacích sleduje v rámci ochrany práva na soukromí při přístupu ke koncovému zařízení uživatele dva dílčí cíle – ochranu bezpečnosti koncového zařízení a ochranu uživatele před skrytým či neoprávněným sledováním.

Ochrana bezpečnosti koncového zařízení v tomto kontextu znamená jednak ochranu před instalací softwaru, který může být považován za malware, ale také instalací softwaru či nastavení, které mohou otevírat cestu kompromitaci koncového zařízení jiným způsobem, přičemž hranice mezi těmito dvěma skupinami může být neostrá. Cíl je ilustrován případem Sony/BMG. Software této společnosti měnil nastavení počítače takovým způsobem, který usnadňoval proniknutí malwaru do počítače, a sám byl tak později některými antivirovými programy klasifikován jako malware.

Ochrana před skrytým nebo neoprávněným sledováním se pak vztahuje jednak k softwaru, který může uživatele sledovat (*spyware*), ale také ke sledování pomocí cookies a podobných technologií. Ani v jednom případě přitom nemá ochrana formu absolutního zákazu použití těchto technologií, protože v některých případech je může uživatel do svého zařízení instalovat vědomě a cíleně.

Oba tyto cíle považuji za legitimní a stále aktuální a právní úprava ochrany soukromí v elektronických komunikacích by měla i v budoucnu směřovat k jejich plnění.

7.4 DÍLČÍ ZÁVĚR

Ve světle výše provedené diskuze by nová právní úprava přístupu ke koncovému zařízení uživatele měla ve vztahu ke cookies a podobným technologiím méně spoléhat na kontrolu ze strany koncového uživatele. Současně by však měla umožnit rozumnou míru kontroly uživatele nad novými technologiemi, které by v budoucnu měly nahradit cookies třetích stran, protože o jejich dopadech na soukromí zatím nemáme přesvědčivá data. Konečně by měla zachovat nebo zvýšit úroveň ochrany bezpečnosti koncové-

ho zařízení a ochrany uživatele před skrytým nebo neoprávněným sledováním.

8. MOŽNÉ PŘÍSTUPY K NOVÉ PRÁVNÍ ÚPRAVĚ

K realizaci výše zmíněných cílů lze podle mého názoru přistoupit třemi základními způsoby – definováním titulů, resp. výjimek pro různé scénáře použití cookies, definicí jednoho obecného titulu s určitou formou korektivu nebo kombinací těchto způsobů.

První přístup byl zvolen v návrhu nařízení ePrivacy z pera Evropské komise, a nakonec převládl i v konečné pozici Rady. Ilustruje ho nově definovaný titul pro použití cookies k měření návštěvnosti,[213] který byl košatě rozpracován Evropským parlamentem[214] i Radou.[215] Problém tohoto přístupu je jeho kazuistický charakter. Existuje řada dalších scénářů použití cookies a podobných technologií, které jsou vůči soukromí uživatele minimálně invazivní (nepředstavují skryté či neoprávněné sledování, jemuž má právní úprava zabránit), současně se však nevejdou pod základní titul technické nezbytnosti. Jde například o technické cookies spojené s některými prvky dodatečné funkcionality webové stránky, jako je přehrávání videí nebo chatovací okna.[216]

Ukázkou druhého přístupu je návrh chorvatského předsednictví doplnit mezi tituly oprávněný zájem s dodatečnými podmínkami.[217] Těmito bylo provedení balančního testu – poměřování zájmu provozovatele webové stránky a zájmů a základních práv uživatele – a splnění dalších podmínek, jako je posouzení dopadů na soukromí, informování uživatele a zabezpe-

[213] Viz čl. 8 odst. 1 návrhu Komise.

[214] Viz pozměňovací návrhy č. 89 a 99 pozice Evropského parlamentu.

[215] Viz čl. 8 odst. 1 písm. d) a bod 21a odůvodnění pozice Rady.

[216] Blíže viz příklad v části 9.3 níže.

[217] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017/0003(COD), 5979/20. In: *EUR-Lex* [online]. 21. 2. 2020, čl. 8 odst. 1 písm. g) a odst. 1a. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5979_2020_INIT

čení.[218] Problémem tohoto přístupu je aplikovatelnost navrhovaného širokého titulu i mimo oblast použití cookies a podobných technologií. Vedle minimálně invazivních scénářů ukládání a čtení cookies by tak tento titul mohl legitimizovat, nebo být zneužit k legitimizaci invazivních praktik, jako je instalace sledovacího softwaru nebo softwaru ohrožujícího bezpečnost koncového zařízení, kterým má právní úprava ochrany koncového zařízení zabránit.[219]

Kombinace těchto přístupů může podle mého názoru spočívat ve stanovení obecného titulu, resp. výjimky,[220] která by se však vztahovala pouze na použití vlastních cookies (tj. těch cookies, které do zařízení ukládá webová stránka, kterou uživatel prohlíží, nikoli jiná webová stránka), podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení a dále technologií nahrazujících cookies třetích stran, u těchto nových technologií však pouze v rozsahu, v jakém jejich konkrétní specifikace budou schváleny EDPB. Korektivem této výjimky by pak podle mého názoru mohla být aplikace GDPR na procesy, které do působnosti výjimky spadnou. Jak bude dále vysvětleno, tuto aplikaci není třeba zvláště uzákoňovat, protože plyne z působnosti GDPR.

Tento přístup podle mého názoru nejlépe naplňuje vytyčené cíle. Vyloučení vlastních cookies, podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení a vybraných technologií nahrazujících cookies třetích stran by znamenalo posun od důrazu na kontrolu v podobě souhlasu, jak jej regulují pravidla přístupu ke koncovému zařízení, k flexibilnějšímu režimu GDPR, ve kterém lze zpracování osobních údajů opřít o různé právní základy podle čl. 6 odst. 1.

---

[218] Viz tamtéž, čl. 8 odst. 1a a bod 21b odůvodnění.

[219] V tomto směru sdílím výše citovanou obavu německého předsednictví. Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulati-on on Privacy and Electronic Communications) – Presidency discussion paper 2017/0003(COD), 9243/20. In: *EUR-Lex* [online]. 6. 6. 2020, s. 6. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9243_2020_INIT

[220] K diskuzi variant titulu a výjimky viz část 9.6 .

Flexibilnější režim by zároveň znamenal otevření cesty pro realizaci cílené reklamy, pokud bude založena na vybraných technologiích nahrazujících cookies stran, u jejichž technické specifikace EDPB dospěje k závěru, že jejich dopady na soukromí jsou dostatečně malé.

Z hlediska ochrany bezpečnosti koncového zařízení by takové řešení nepředstavovalo žádný ústupek, protože by se neaplikovalo na spustitelný software ani na změny konfigurace koncového zařízení. Z hlediska ochrany před skrytým nebo neoprávněným sledováním by se rovněž nejednalo o ústupek, protože tyto činnosti by byly dále regulovány GDPR, ze kterého plyne požadavek na právní titul a řadu konkrétních opatření k zajištění ochrany práv dotčené fyzické osoby.

Ochrana před skrytým nebo neoprávněným sledováním by naopak mohla být posílena, pokud by se zvolený přístup promítl do povinností tvůrců webových prohlížečů. Výše byla popsána rizika spojená s předáváním dat ve stávající podobě ekosystému internetové reklamy. Toto předávání je primárně založeno na využití cookies třetích stran. Některé webové prohlížeče ukládání a čtení cookies třetích stran ve výchozím nastavení blokují již nyní. Jiné tuto funkcionalitu připravují.[221] Tento postupný trend založený na dobrovolnosti však patrně v dohledné době nezajistí, aby veškerý software, který uživatelé k procházení webu v Evropské unii používají, cookies třetích stran ve výchozím nastavení blokoval. Tvůrcům webových prohlížečů by proto měla být uložena povinnost k takovému výchozímu blokování.

Tato povinnost blokace ve výchozím nastavení by se mohla vztahovat i na technologie nahrazující cookies třetích stran, a to včetně těch, u nichž bude technická specifikace schválena EDPB. U těchto vybraných technologií by však bylo namístě, aby toto výchozí nastavení uživatel při prvním spuštění webového prohlížeče odsouhlasil, resp. dostal možnost jej změnit a tyto technologie povolit. Takové řešení by zachovávalo vysokou míru ochrany před skrytým či neoprávněným sledováním a také přiměřenou míru kontroly uživatele.

[221] Blíže viz část 3.

Zároveň webové prohlížeče mohou pro ochranu uživatelů udělat i více než blokovat cookies třetích stran. Jak ukazuje současná praxe popsaná v části 3. , prohlížeče mohou obsahovat technologie, které aktivně brání sledování uživatelů jinými technikami, jako je fingerprinting. Tyto techniky budou umožňovat sledování uživatelů, i když budou cookies třetích stran ve webových prohlížečích blokovány, proto je namístě uložit tvůrcům webových prohlížečů povinnost přijmout technická opatření, která tomuto sledování budou bránit.

Pokud by tvůrcům webových prohlížečů byla uložena povinnost ve výchozím nastavení blokovat cookies třetích stran a současně přijmout opatření odpovídající stavu techniky, která budou bránit skrytému nebo neoprávněnému sledování uživatele, šlo by dle mého názoru o významné posílení ochrany uživatele před skrytým nebo neoprávněným sledováním. Takové opatření by přitom nezvyšovalo nároky na kontrolu ze strany uživatelů a nijak neomezovalo limitované formy internetové reklamy.

9. ROZBOR A ZHODNOCENÍ NAVRŽENÉHO ŘEŠENÍ

9.1 APLIKACE GDPR

Výše předložený návrh výjimky, která by se však vztahovala na použití vlastních cookies a podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení, vychází z předpokladu, že na použití těchto technologií, které může představovat zásah do soukromí ve smyslu neoprávněného nebo skrytého sledování, se aplikuje GDPR, které nepřiměřenému zásahu do soukromí brání.

GDPR se aplikuje na zcela nebo částečně automatizované zpracování osobních údajů.[222] Osobními údaji se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě.[223] Identifikovatelnou fyzickou osobou se pak rozumí fyzická osoba, kterou lze přímo či nepřímo identifikovat.[224] Fyzickou osobu lze „považovat za ‚identifikovanou', jestliže je ve

[222] Viz čl. 2 odst. 1 GDPR. Také na neautomatizované zpracování těch osobních údajů, které jsou obsaženy v evidenci nebo do ní mají být zařazeny. Viz tamtéž.

[223] Viz čl. 4 bod 1 GDPR.

[224] Viz tamtéž.

skupině osob ‚odlišena' ode všech ostatních příslušníků této skupiny."[225] Identifikovatelná je tehdy, pokud ji lze odlišit od všech ostatních příslušníků této skupiny,[226] tedy pokud dostupné informace umožňují na konkrétního člověka „zaostřit".[227]

Leens rozlišuje čtyři formy identifikace – vyhledání (pomocí identifikátoru v registru či tabulce), rozpoznání (pomocí znaků, jako je fyzický vzhled), klasifikaci (označení jednotlivce jako příslušníka určité skupiny) a identifikaci sezení (sledování jednotlivce během interakce).[228] Purtova k této klasifikaci přidává pátou formu – cílení, tedy „výběr jednotlivce ze skupiny jako objektu pozornosti nebo zacházení v určitém časovém okamžiku".[229]

S výjimkou klasifikace všechny tyto formy identifikace přestavují identifikaci ve smyslu GDPR.[230] Ve vztahu k cílení tento závěr plyne zejména z bodu 26 odůvodnění GDPR, který výslovně hovoří o tom, že možnost výběru vyčleněním (*singling out*) je třeba brát v úvahu jako způsob identifikace. Tento přístup zaujímá také judikatura.[231] Přitom pokud výběr jednotlivce ze skupiny jako objektu pozornosti považujeme za formu identifikace ve smyslu GDPR, pak jakákoli forma sledování (včetně sledování skrytého

[225] Viz Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 4/2007 k pojmu osobní údaje In: *Evropská komise* [online]. 20. 6. 2007, s. 12. [cit. 2. 2. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_cs.pdf

[226] Viz tamtéž.

[227] Viz tamtéž, s. 13.

[228] Viz LEENES, Ronald E. Do They Know Me? Decomposing Identifiability *University of Ottawa Law and Technology Journal* [online]. 2007, roč. 4, č. 1-2 [cit. 6. 1. 2023], s. 146 a násl.

[229] Viz PURTOVA, Nadezhda. From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law* [online]. 2022, roč. 12, č. 3 [cit. 2. 2. 2023], s. 170.

[230] Viz PURTOVA, Nadezhda. *From knowing by name to targeting: the meaning of identification under the GDPR*, s. 177.

[231] Viz rozsudek Court of Appeal (Civil Division) ze dne 27. 3. 2015, A2/2014/0403, [2015] EWCA Civ 311, bod 114 a násl. Pro rozbor viz PURTOVA, Nadezhda. *From knowing by name to targeting: the meaning of identification under the GDPR,* s. 176. BORGESIUS, Frederik J. Zuiderveen. *Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation,* s. 267.

nebo neoprávněného) představuje zpracování informací o fyzické osobě, která je v tomto smyslu identifikovatelná.[232]

Z hlediska ochrany soukromí uživatele by tento závěr nemusel být dostatečný ve vztahu k vymáhaní právní úpravy v případě softwaru, jako např. spyware. U něj totiž může být obtížné určit, která osoba v konkrétním případě určila účel a prostředky sledování jako formy zpracování osobních údajů a která je tedy správcem osobních údajů ve smyslu GDPR,[233] který je za zpracování osobních údajů odpovědný. Proto je namístě v případě softwaru regulovat samotný akt jeho uložení do koncového zařízení. V případě použití vlastních cookies a podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení a využití údajů, které koncové zařízení vysílá, však tato nejasnost odpadá.

Cookies a podobné technologie jsou vždy uloženy ve vztahu ke konkrétní doméně a určení webové stránky, resp. provozovatele webové stránky, která je do koncového zařízení uložila, je snadnější než určení původce určitého softwaru.[234] Požadavek na souhlas ve vztahu k některým scénářům použití vlastních cookies a podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení tak podle mého názoru nepřináší pro soukromí uživatelů žádnou dodatečnou ochranu. K té postačí ponechat tyto činnosti v působnosti GDPR, do které v případě sledování uživatele spadají.

Ochrana poskytovaná GDPR je přitom komplexnější než ochrana poskytovaná právní úpravou přístupu ke koncovému zařízení. Vedle požadavku na právní titul ke zpracování osobních údajů jako činnosti zahrnující použití cookies a podobných technologií nebo využití údajů, které koncové zařízení vysílá,[235] se na jednu stranu jako ochranný „deštník“ uplatní základní

[232] Např. Nadezhda Purtova uvádí, že identifikace ve smyslu GDPR zahrnuje „také spornější, ale stále populárnější případy tzv. přechodného zpracování údajů, které se k subjektům údajů vztahuje pouze v krátkém okamžiku interakce s technologií, jako … inteligentní kamerový dohled.“ Viz PURTOVA, Nadezhda. *From knowing by name to targeting: the meaning of identification under the GDPR,* s. 181. Překlad autor.

[233] Viz čl. 4 bod 7 GDPR.

[234] Viz blíže část 2.

[235] Viz čl. 6 odst. 1 GDPR.

zásady zpracování osobních údajů uvedené v čl. 5 GDPR a na druhou stranu řada konkrétních práv dotčených fyzických osob (subjektů údajů ve smyslu čl. 4 bod 1 GDPR)[236] a povinností subjektu vykonávajícího danou činnost (správce osobních údajů ve smyslu čl. 4 bod 7 GDPR).[237]

Současně je však právní úprava v GDPR flexibilnější a kontrola subjektu údajů v ní není jediným nástrojem ochrany. Kontrola hraje v GDPR významnou roli – to je patrné jak z bodu 7 odůvodnění GDPR,[238] tak z katalogu právních základů pro zpracování osobních údajů (kde je na prvním místě uveden souhlas)[239] nebo z úpravy práv dotčených fyzických osob.[240] Zpracování osobních údajů je však možné opřít o jiné právní tituly, než je souhlas subjektu údajů, a tedy je možné zpracování legitimizovat, aniž by nad ním musela dotčená fyzická osoba předem vykonat kontrolu (v podobě udělení souhlasu). Pro použití cookies a podobných technologií je relevantní zejména právní základ oprávněného zájmu správce osobních údajů nebo třetí osoby.[241]

Oprávněný zájem lze jako právní základ uplatnit v případě, kdy je zpracování osobních údajů nezbytné pro realizaci oprávněného zájmu správce osobních údajů nebo třetí osoby a tento zájem převažuje nad zájmy a právy a svobodami dotčené osoby (subjektu údajů).[242] Tyto tři podmínky – existence oprávněného zájmu správce nebo třetí osoby, nezbytnost zpracování pro realizaci tohoto zájmu a převaha zájmu nad právy a svobodami subjektu údajů – musí být splněny kumulativně.[243]

---

[236] Viz kapitolu III GDPR.

[237] Viz kapitolu IV GDPR.

[238] Ten výslovně uvádí: „Fyzické osoby by měly mít možnost kontrolovat své vlastní osobní údaje."

[239] Viz čl. 6 odst. 1 GDPR.

[240] Viz kapitolu III GDPR.

[241] Viz čl. 6 odst. 1 písm. f) GDPR.

[242] Viz tamtéž.

[243] Viz KAMARA, Irene, DE HERT, Paul. Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach [online]. 8. 8. 2018 [cit. 8. 1. 2023], s. 11. Viz také Rozsudek SDEU (druhého senátu) ze dne 4. 5. 2017 ve věci C-13/16, Rïgas satiksme, bod 28.

Oprávněný zájem správce nebo třetí osoby nemusí být zájmem, který vyplývá z právního předpisu. Může jít o jakýkoli zájem, který právu neodporuje, včetně zájmu komerčního.[244] Podmínka nezbytnosti bude naplněna, pokud je zpracování cestou k naplnění posuzovaného oprávněného zájmu správce, která je nejméně invazivní k zájmům a právům subjektu údajů.[245] Porovnání oprávněného zájmu správce nebo třetí osoby a zájmů a základních práv a svobod subjektu údajů je nejkomplexnější podmínkou. Hraje v něm roli povaha oprávněného zájmu na jedné straně a velikost zásahu do zájmů a základních práv a svobod subjektu údajů na straně druhé. Tu určuje zejména rozsah zpracovávaných osobních údajů, jejich povaha, způsob zpracování a doba zpracování. Význam má také postavení správce osobních údajů a subjektu údajů, resp. jejich vztah.[246] Podle bodu 47 odůvodnění GDPR je významným faktorem také to, „zda subjekt údajů může v okamžiku a v kontextu shromažďování osobních údajů důvodně očekávat, že ke zpracování pro tento účel může dojít".[247] Roli hrají rovněž dodatečné záruky přijaté správcem k ochraně zájmů a základních práv subjektu údajů, jako např. dodatečné omezení rozsahu údajů, dodatečné informování nebo dodatečné zabezpečení.[248]

Příkladem zpracování, které zahrnuje použití cookies a mohlo by se opírat o oprávněný zájem, je měření návštěvnosti a sledování chování uživatelů za účelem optimalizace fungování webové stránky, pro které návrh nařízení ePrivacy (ve všech jeho podobách) obsahuje zvláštní titul. Zjištění,

[244] Viz KAMARA, Irene; DE HERT, Paul. *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach*, s. 13. Obdobně viz Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES. In: *Evropská komise* [online]. 9. 4. 2014, s. 25. [cit. 2. 2. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf (dále jen „WP217")

[245] Viz KAMARA, Irene, DE HERT, Paul. *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach,* s. 14. Obdobně viz WP127, s. 29.

[246] Viz KAMARA, Irene, DE HERT, Paul. *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach,* s. 14. Obdobně viz WP17, s. 33.

[247] Viz KAMARA, Irene, DE HERT, Paul. KAMARA, Irene; DE HERT, Paul. *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach,* s. 16.

[248] Viz WP217, s. 42.

jak uživatelé používají webovou stránku, a její následná úprava za účelem snadnějšího používání pro uživatele, příp. lepšího dosahování obchodních nebo jiných cílů provozovatele webové stránky (např. většího počtu dokončených objednávek v internetovém obchodě), je zájmem, který neodporuje svou podstatou unijnímu právu ani právu České republiky. Tento zájem není možné realizovat bez údajů o tom, jak uživatelé webovou stránku používají – např. v jakém kroku zadávání objednávky nejčastěji proces nedokončí a na jaké narážejí překážky. Diskutabilní je pouze rozsah údajů, který je k realizaci tohoto zájmu nezbytný.

Pro účely měření návštěvnosti a sledování chování uživatelů za účelem optimalizace fungování webové stránky lze sbírat údaje s různou mírou podrobnosti, od počtu návštěv jednotlivé webové stránky,[249] až po podrobný záznam pohybů kurzoru uživatele na stránce, který lze rekonstruovat prakticky do podoby videozáznamu.[250] Za nezbytný rozsah zpracování lze dle mého názoru zpravidla považovat zpracování údajů na úrovni interakce uživatele s webovou stránkou (doba setrvání na stránce, stránka, ze které uživatel přišel, stránka, na kterou odešel) a s jejími jednotlivými prvky, např. počty kliknutí, způsoby vyplňování formulářových polí apod. Naopak sběr údajů v podrobnosti umožňující rekonstrukci v podstatě odpovídající videozáznamu průchodu webovou stránkou bych zpravidla za nezbytný nepovažoval (při vyšším počtu návštěv webové stránky by takové údaje patrně bylo problematické vůbec smysluplně využít). Míra nezbytnosti však bude záležet na okolnostech konkrétního případu.

Rozsah zpracovávaných údajů také významně ovlivňuje poměřování zájmu provozovatele webové stránky se zájmy a základními právy a svobodami subjektu údajů – s rostoucím rozsahem údajů totiž roste velikost zásahu do těchto zájmů, práv a svobod, zejména práva na soukromí. Ve výše popsaném případě zpracování údajů na úrovni interakce uživatele s jednotlivými prvky webové stránky bych zásah považoval za přiměřený a zájem provozovatele webové stránky by dle mého názoru nad zájmy subjektu

[249] Viz ZHENG, Guangzhi, PELTSVERGER, Svetlana. *Web analytics overview* [online].

[250] Viz What Are Session Recordings (Session Replays) + How to Use Them In: *hotjar* [online]. [cit. 23. 1. 2023]. Dostupné z: https://www.hotjar.com/session-recordings/

údajů převažoval, mj. proto, že takové zpracování lze podle mého názoru ze strany uživatele předvídat. Naopak v případě zpracování údajů v podrobnosti umožňující rekonstrukci v podstatě odpovídající videozáznamu bych zásah zejména do práva na soukromí považoval za nepřiměřený, mimo jiné s ohledem na nízkou předvídatelnost takového zpracování.[251]

Předpokladem závěru o přiměřenosti zásahu a převaze zájmu správce by ve výše popsaném případě byla podle mého názoru implementace minimální sady vhodných (a dnes běžných) záruk, jako např. nastavení vhodně krátké doby uchování s následnou agregací a anonymizací dat, neukládání IP adres uživatelů (které by umožňovaly údaje ve spojení se záznamy, např. poskytovatele služeb elektronických komunikací spojit s uživatelem identifikovaným občanským jménem, příjmením a dalšími údaji)[252] nebo neukládání údajů, které uživatelé zadávají do formulářů (a které mohou zahrnovat jejich e-mailové adresy, občanská jména a příjmení a další údaje usnadňující identifikaci ve smyslu vyhledání či rozpoznání).[253]

Pro svou flexibilitu byl oprávněný zájem jako právní titul některými autory kritizován jako úniková cesta, kterou lze legitimizovat zpracování, která jsou na újmu subjektu údajů,[254] a pro subjektivní prvek v poměřování zájmů správce a subjektu údajů.[255] Tato volnost je zmírněna tím, že v souladu

[251] Nikoli však za tak zásadní, aby takové zpracování odporovalo zásadě férovosti zpracování ve smyslu čl. 5 odst. 1 písm. a) GDPR. Bylo by tedy možné jej podle mého názoru opřít o vhodně nastavený souhlas uživatelů webové stránky, pokud by byl prezentován např. vybranému náhodnému vzorku uživatelů, od kterých by byl sebrán rozumně zpracovatelný objem dat.

[252] Viz rozsudek SDEU (druhého senátu) ze dne 19. 10. 2016 ve věci C-582/14, Breyer, bod 47.

[253] Jako příklad lze uvést např. šifrování, ať už při přepravě nebo statické, pseudonymizaci, nebo fyzické, organizační a smluvní opatření. Viz např. Google. IP masking in Universal Analytics. In: Analytics Hepl [online]. Nedatováno [cit. 12.2. 2023]. Dostupné z: https://support.google.com/analytics/answer/2763052?hl=en&ref_topic=2919631

[254] Viz FERRETTI, Federico. Data Protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights? In: *Common Law Market Review* 2014, r. 51, č. 3, s. 843–868, citováno podle KAMARA, Irene, DE HERT, Paul. *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach,* s. 9.

se zásadou odpovědnosti, zavedenou GDPR,[256] musí správce být schopen svůj oprávněný zájem prokázat. Současně, jak bylo uvedeno výše, bod 47 odůvodnění GDPR blíže specifikuje, jak posuzovat vztah oprávněného zájmu správce a zájmů a základních práv a svobod subjektu údajů.

Na výše navržené řešení se současně podle mého neuplatní výhrada německého předsednictví, že by zavedení oprávněného zájmu do právní úpravy přístupu ke koncovému zařízení výrazně usnadnilo „instalaci softwaru, který je často považován za hlavní vstupní bránu pro škodlivý software.“[257] Oprávněný zájem by totiž jako titul nebylo možné aplikovat na jakýkoli přístup ke koncovému zařízení (např. na instalaci jakéhokoli softwaru), ale pouze na činnosti ukládání a čtení vlastních cookies, použití podobných technologií a využití údajů vysílaných koncovým zařízením, se kterými toto riziko spojeno není.

Řešení by tedy bylo možné konstruovat jako výjimku z aplikace právní úpravy přístupu ke koncovému zařízení na použití vlastních cookies a podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení a na použití technologií nahrazujících cookies třetích stran. Tyto činnosti by zůstaly v působnosti GDPR, které poskytuje robustní ochranu základním právům a současně větší flexibilitu. Tato flexibilita by se projevila mimo jiné možností aplikovat na výše uvedené činnosti právní základ nezbytnosti zpracování pro oprávněný zájem správce nebo třetí osoby, avšak pouze na tyto vymezené činnosti, nikoli na libovolný přístup ke koncovému zařízení (např. instalaci softwaru).

Takové řešení by podle mého názoru odpovídalo také lidskoprávním základům GDPR a nařízení ePrivacy. Cílem GDPR a obecně práva na ochranu osobních údajů ve smyslu čl. 8 Listiny základních práv Evropské unie je

---

[255] BALBONI, Paolo et al. Legitimate interest of the data controller New data protection paradigm: legitimacy grounded on appropriate protection. *International Data Privacy Law* [online]. 2013, roč. 3, č. 4 [cit. 2. 2. 2023], s. 253.

[256] Viz čl. 5 odst. 2 GDPR.

[257] Viz návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) – Presidency discussion paper ze dne 6. 6. 2020, 2017/0003(COD), 9243/20 s. 6.

chránit základní práva před zásahy v důsledku zpracování osobních údajů.[258] Cílem nařízení ePrivacy je především ochrana soukromí, jak bylo popsáno v části 7.3 . Jakkoli vlastní cookies a podobné technologie lze použít způsobem zasahujícím do soukromí, toto riziko je výrazně nižší než u jiných výše diskutovaných scénářů přístupu ke koncovému zařízení uživatele (např. skryté instalaci softwaru) a vzniká vždy v souvislosti se zpracováním osobních údajů. Právní úprava ochrany osobních údajů je tedy pro případ použití vlastních cookies a podobných technologií přiléhavější.

9.2 ROZSAH VÝJIMKY

Výše navržené řešení předpokládá, že by z působnosti právní úpravy přístupu ke koncovému zařízení bylo vyňato použití vlastních cookies (tj. těch cookies, které do zařízení ukládá webová stránka, kterou uživatel prohlíží, nikoli jiná webová stránka) a podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení, a to s argumentem, že na tyto činnosti se v relevantním rozsahu aplikuje GDPR.

Tento závěr by patrně bylo možné učinit i ve vztahu k širšímu rozsahu technologií, které lze použít pro sledování uživatele, zejména ve vztahu ke cookies třetích stran, které rovněž nelze použít např. k instalaci softwaru do koncového zařízení, a tak narušení jeho bezpečnosti, ale pouze k narušení soukromí ve smyslu sledování uživatele. Tato redukce z veškerých cookies na vlastní cookies je však navržena záměrně. Cookies třetích stran jsou totiž klíčovým pilířem současného ekosystému internetové reklamy, protože umožňují sdílení identifikace uživatele (ve smyslu identifikace zařízení, resp. webového prohlížeče pro účely sledování a cílení, nikoli identifikace

[258] Srov. GELLERT, Raphaël. *The Risk-Based Approach to Data Protection*. Oxford: Oxford University Press, 2020, s. 18. s odkazem na BENNETT, Colin J. *Regulating privacy: Data protection and public policy in Europe and the United States*. Ithaca: Cornell University Press, 1992, s. 33. Viz též recitál 10 GDPR a GELLERT, Raphaël; GUTWIRTH, Serge. The legal construction of privacy and data protection. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5, s. 529. [cit. 30. 5. 2023]. Jakkoli lze dle Gellerta a Gutwirtha z judikatury SDEU dovodit i výklad konstruující právo na ochranu osobních údajů jako autonomní základní právo, tento přístup by podle mého názoru vedl k velmi formální aplikaci tohoto práva a není podle mě správný.

ve smyslu např. občanského jména či příjmení).[259] Toto sdílení přitom považuji za klíčový prvek zásahů do soukromí, které jsou se současnou podobou ekosystému internetové reklamy spojeny.[260] Vynětí těchto cookies pouze do flexibilnějšího režimu GDPR bych proto považoval za nežádoucí. Ze stejného důvodu navrhuji, aby tvůrci webových prohlížečů měli povinnost cookies třetích stran ve výchozím nastavení blokovat.

Otázkou k diskuzi je, zda mírnější režim pro vlastní cookies a výchozí blokace pouze cookies třetích stran je pro ochranu soukromí uživatelů dostatečným řešením. Vedle aspektu subjektu ukládajícího cookies (vlastní cookies oproti cookies třetích stran) mají cookies také časové atributy – jejich platnost může být omezena na dobu do zavření okna webového prohlížeče, resp. konkrétní záložky (tzv. *session cookies*, cookies sezení) nebo na dobu delší.[261] Podobně webové úložiště má část, která se vymaže po zavření okna webového prohlížeče, resp. konkrétní záložky (úložiště sezení), a část sloužící jako trvalé úložiště (místní úložiště).[262] Potenciál použití krátkodobě uchovávaných dat jako cookies sezení a dat v úložišti sezení pro sledování uživatele je přitom výrazně omezenější, protože neumožňuje spojit údaje o chování při dvou různých návštěvách webové stránky, které odděluje zavření okna webového prohlížeče, resp. konkrétní záložky.

Tyto cookies by přitom nemusely být ve výchozím nastavení blokovány absolutně. Namísto toho by se k nim mohly webové prohlížeče chovat tak, jak se chovají prohlížeče mimo mobilní zařízení k požadavkům na otevření nového okna prohlížeče (tzv. vyskakovacího okna, *pop-up window*) – tedy tak, že by uložení jiných dat, než dat platných po dobu sezení zablokovaly, avšak s upozorněním pro uživatele, že k blokaci došlo, aby uživatel mohl blokaci a uložení údaje povolit. Alternativně by nemusely webové prohlížeče uložení jiných dat než dat platných po dobu sezení automaticky blokovat, ale vyžadovat k jejich uložení souhlas, o který by si webová stránka

[259] Ostatně z tohoto důvodu je řada webových prohlížečů ve výchozím nastavení blokuje nebo zamýšlí blokovat.

[260] Blíže viz část 7.2 .

[261] Viz COFONE, Ignacio N. *The way the cookie crumbles: online tracking meets behavioural economics,* s. 39.

[262] Viz část 2.

mohla požádat přes rozhraní prohlížeče a musel by přes toto rozhraní být udělen.

Ani jedno z těchto řešení by však dle mého názoru nebylo v souladu s výše shrnutými požadavky na ošetření použití cookies a podobných technologií v právní úpravě přístupu ke koncovému zařízení. Je třeba si uvědomit, že data (zejména cookies) s platností delší, než je doba sezení, jsou nutná pro řadu legitimních účelů, jako je zapamatování nastavení webové stránky (např. preferovaného jazyka stránky nebo preferované měny v internetovém obchodě), zapamatování přihlášení apod.[263]

Současně by toto řešení zvýšilo požadavky na kontrolu koncového uživatele, který by musel v legitimních případech uložení data s platností delší, než je doba sezení, aktivně povolovat, nebo u veškerých těchto uložení rozhodovat o souhlasu, přičemž takovým žádostem by mohl čelit téměř na každé webové stránce s ambicí cílit na něj reklamu.

Otázkou také je, zda by se mírnější režim měl vztahovat na technologie nahrazující cookies třetích stran, jako je Topics API a FLEDGE.[264] S ohledem na diskuzi v části 7.2 se domnívám, že s těmito technologiemi nelze zacházet stejně jako s vlastními cookies a podobnými technologiemi, protože jejich dopady na ochranu soukromí a vnímání ze strany uživatelů nejsou dostatečně prozkoumané. Na druhou stranu s ohledem na zachování otevřených cest pro budoucí financování webových stránek nabízejících bezplatný obsah a také prevenci přetížení uživatelů budoucími žádostmi o souhlas by bylo vhodné aplikovat požadavek na kontrolu vůči těmto technologiím v mírnější formě.

Tato mírnější forma kontroly by mohla mít podobu vynětí těchto technologií z požadavku na souhlas spolu s jejich výchozí blokací ve webovém prohlížeči a povinností webového prohlížeče při prvním použití předložit uživateli toto nastavení k odsouhlasení. Tento režim by se však měl vztahovat pouze na takové technologie, jejichž technickou specifikaci posoudí EDPB a schválí ji s ohledem na minimální zásah do soukromí, který tyto technologie vytváří.

[263] Viz WP194, s. 6.

[264] Blíže viz část 3.

Je otázkou, na kolik lze takové řešení považovat za mírnější oproti současné úpravě. Je však třeba vzít v úvahu, že dopady jednotlivých technologií pro ochranu soukromí zatím nejsou některými odborníky hodnoceny jako dostatečné zlepšení oproti aktuálnímu stavu.[265] Současně návrh vychází z předpokladu, že tyto technologie bude možné využít bez zpracování osobních údajů, tj. bez nutnosti získávat souhlas se zpracováním osobních údajů podle GDPR – tento předpoklad může být naplněn u některých technologií, ne však nutně všech.[266]

Za téma pro další zkoumání a případnou diskuzi tedy považuji otázku, zda vedle kladného posouzení technologií EDPB ještě vyžadovat jejich výchozí blokaci a následně odsouhlasení jejich použití uživatelem, případně zda dovolit webovým stránkám podmiňovat přístup k bezplatnému obsahu povolením použití těchto technologií (pozitivně hodnocených EDPB). Tento přístup by uživatele nezbavil možnosti rozhodovat o použití těchto technologií. Současně by se však rozsah kontroly snížil na proveditelnou úroveň a zachoval vysokou míru ochrany soukromí (s ohledem na výchozí nastavení blokující tyto technologie). Na druhou stranu by však mohl znamenat překážku pro financování webových stránek pomocí cílené reklamy a obecně nepřiměřené opatření vzhledem k rizikům pro ochranu soukromí, které by tyto schválené technologie představovaly. Na druhou stranu rezignace na požadavek souhlasu může představovat příliš velký zásah do autonomie uživatele jako aspektu práva na soukromí.[267]

---

[265] Viz výhrady Mozilla Foundation, společnosti Apple a pracovní skupiny World Wide Web Consortium pro architekturu webu (W3C TAG). Request for Position: Topics API #622. In: github [online]. 17. 3. 2022 [cit. 28. 5. 2023]. Dostupné z: https://github.com/mozilla/standards-positions/issues/622 komentář uživatele martinthomson z 6. 1. 2023. The Topics API #111. In: github [online]. 20. 12. 2022 [cit. 28. 5. 2023]. Dostupné z: https://github.com/WebKit/standards-positions/issues/111 komentář uživatele annevk z 20. 12. 2022. Early design review for the Topics API #726. In: github [online]. 25. 3. 2023 [cit. 28. 5. 2023]. Dostupné z: https://github.com/w3ctag/design-reviews/issues/726#issuecomment-1379908459 komentář uživatele rhiaro z 12. 1. 2023.

[266] Viz blíže rozbor v části 9.4 .

[267] K autonomii jako složce soukromí viz GELLERT, Raphaël; GUTWIRTH, Serge. *The legal construction of privacy and data protection*. s. 524. Britský ICO požaduje volbu uživatele jako jeden z atributů technologií nahrazujících cookies třetích stran. Viz Information Commissioner's Office. Data protection and privacy expectations for online advertising proposals. s. 43.

Za vhodné proto považuji vázat výjimku na veškeré použití vlastních cookies a podobných technologií spočívajících v ukládání dat do koncového zařízení bez ohledu na dobu platnosti těchto dat a také na použití technologií nahrazujících cookies třetích stran s omezenými dopady na soukromí. K další diskuzi je případná povinnost pro tvůrce internetových prohlížečů blokovat ve výchozím nastavení cookies třetích stran (nikoli jiné druhy cookies) a také technologie nahrazující cookies třetích stran s omezenými dopady na soukromí (s povinností toto dílčí nastavení koncovému uživateli při prvním použití předložit ke schválení či úpravě).

9.3 APLIKACE V SOUČASNÉ PRAXI

V souvislosti s výše předloženým návrhem je také vhodné popsat, jak by se patrně propsal do fungování webových stránek pohledem současného stavu techniky (tj. bez aplikace technologií nahrazujících cookies třetích stran), a to v porovnání se současnou právní úpravou a navrženými podobami nařízení ePrivacy. V současnosti se uživatelé na většině webových stránek setkají se žádostí o souhlas s použitím cookies – liší se především jeho komplexnost a forma. Podkladem pro rozdílnou komplexnost souhlasu je většinou různá míra komplexnosti použití cookies.

Běžná firemní webová prezentace (např. prezentace výrobního podniku či advokátní kanceláře) používá vlastní cookies především pro analýzu chování uživatelů za účelem hodnocení a zlepšování webové prezentace, resp. odvozování obecných trendů. Podle současné právní úpravy je k takovému použití cookies potřeba souhlas. Při případné aplikaci na nařízení ePrivacy jak ve znění návrhu Evropské komise, tak ve znění pozic Evropského parlamentu a Rady by tento souhlas nebyl nezbytný, pokud by analýza nepřekračovala rozsah a splňovala podmínky, které se v různých zněních liší.[268]

Ve znění návrhu Evropské komise by mohla situaci ovlivnit volba zabránit třetím stranám v uchovávání informací v koncovém zařízení, kterou by musel webový prohlížeč při instalaci uživateli nabídnout.[269] Protože by

[268] Viz část 6.

[269] Viz čl. 10 odst. 1 a 2 návrhu Komise.

však tato volba znamenala blokaci všech cookies, tedy volbu s vyznamným negativním dopadem na fungování řady webových stránek, patrně by nešlo o volbu příliš často využívanou.

Znění navržené Evropským parlamentem by změnilo mechanismus udělování souhlasu. Ten by na úrovni jednotlivé webové stránky mělo jít udělit v nastavení prohlížeče. To by se pak mělo promítnout do signálů zasílaných webové stránce, které by se pro tuto stránku staly závaznými. To by v praxi nejspíše znamenalo, že již implementované standardy signálů jako Do Not Track[270] by se staly pro webové stránky závaznými, současně by to však patrně vyžadovalo vývoj zcela nových webových standardů pro udělování souhlasů a vyjadřování námitek, což by byla patrně časově velmi náročná procedura. Pozice Evropského parlamentu sice v jednom pozměňovacím návrhu uvádí, že by některé technologie měly být schvalovány EDPB,[271] ve vztahu k závazným signálům však není taková procedura specificky upravena.

Pozici Rady je ve vztahu k udělování souhlasu nastavením prohlížeče složité interpretovat – pozice sice obsahuje povinnost tento způsob udělování souhlasu umožnit,[272] není však jasné, zda ustanovení cílí na souhlas obecný, či určitý souhlas pro konkrétní webovou stránku. Obecný souhlas by patrně neobstál vůči požadavkům na souhlas popsaným v části 5.

V případě aplikace řešení, které navrhuji, by souhlas rovněž nebyl nezbytný, pokud by analýzu bylo možné opřít o nezbytnost pro oprávněný zájem provozovatele webové stránky – tedy pokud by nepředstavovala nepřiměřený zásah do zájmů a základních práv (zejména práva na soukromí) a při implementaci vhodných záruk. Současně by nebyla vyloučena komplexnější analýza chování na základě souhlasu, pokud by (např. svým rozsahem) neodporovala zásadě férovosti.[273]

---

[270] Viz KAMARA, Irene, KOSTA, Eleni. Do Not Track initiatives: regaining the lost user control. *International Data Privacy Law* [online]. 2016, roč. 6, č. 4 [cit. 2. 2. 2023].

[271] Viz pozměňovací návrh č. 166 pozice Evropského parlamentu.

[272] Viz čl. 4a odst. 2 pozice Rady.

[273] Viz příklad v části 9.3 .

Komplexnější webová aplikace (např. internetový obchod) nebo komplexnější, spotřebitelsky orientovaná webová prezentace (např. webová prezentace banky či pojišťovny) obvykle využívá cookies pro širší paletu účelů. Zpravidla na ní probíhá výše popsaná analýza chování, pro kterou platí závěry uvedené výše. Dále taková webová stránka zpravidla používá vlastní cookies, cookies třetích stran a podobné technologie pro některé dodatečné funkcionality, jako jsou chatovací okna, přehrávání videí, zapamatování preferencí apod.

Při aplikaci současné právní úpravy je třeba u každé takové cookie nebo podobné technologie zvažovat, nakolik je nezbytná „pro potřeby přenosu zprávy prostřednictvím sítě elektronických komunikací nebo je-li to nezbytné pro potřeby poskytování služby informační společnosti, která je výslovně vyžádána účastníkem nebo uživatelem“.[274] Např. u chatovacích oken a přehrávání videí je toto posouzení problematické a často vede k závěru, že příslušná cookie nezbytná není a může být uložena pouze buď na základě aktivace příslušného prvku (kliknutí na video), nebo na základě souhlasu uživatele.

Ve znění pozice Evropského parlamentu by také musely být ve výchozím nastavení blokovány veškeré cookies vyjma takových, které jsou technicky nezbytné, přičemž uživatel by měl mít při instalaci prohlížeče možnost toto nastavení odsouhlasit nebo změnit.[275] V tomto směru není jasné, jak by měl webový prohlížeč rozpoznat, které cookies jsou pro fungování webové stránky technicky nezbytné – tuto informaci v sobě cookies a další ukládaná data nenesou. Bylo by tedy třeba upravit minimálně internetový protokol HTTP upravující cookies a standard HTML5 definující webové úložiště, aby tato informace byla přenášena, resp. ukládána. Webový prohlížeč by pak musel spoléhat na to, že webová stránka pravdivě označí, které cookies jsou pro ni technicky nezbytné, což by se v praxi nemuselo vždy dít.[276]

[274] Viz § 89 odst. 3 ZEK. Blíže viz WP194.

[275] Pozměňovací návrhy č. 106 až 109 tamtéž.

[276] Nezisková organizace noyb zjistila u 21 % zkoumaných webových stránek, že za nezbytné označují cookies, které pro fungování webové stránky nezbytné nejsou. Viz noyb aims to end “cookie banner terror” and issues more than 500 GDPR complaints [online].

Při aplikaci mnou navrhovaného řešení by pro tyto účely zpravidla nebyl vyžadován souhlas uživatele – ve většině případů by u použití dané technologie bylo možné dovodit nezbytnost pro oprávněný zájem provozovatele webové stránky a převahu nad zájmy a právy uživatele (s ohledem na minimální zásah do těchto práv). Příslušné prvky by však bylo třeba technicky upravit tak, aby nevyužívaly cookies třetích stran, které by byly ve výchozím nastavení ve webových prohlížečích blokovány. Tato změna však bude patrně nutná již v souvislosti s tím, že ve většině webových prohlížečů budou cookies třetích stran ve výchozím nastavení blokovány dobrovolně.

Taková komplexnější webová aplikace či prezentace také často využívá cookies třetích stran pro cílení reklamy provozovatele webové stránky na webových stránkách třetích stran (např. výše popsaný retargeting, tj. zobrazení reklamy na dříve prohlíženou webovou stránku či konkrétní produkt nebo službu).[277] Podle současné právní úpravy je k tomuto použití potřeba souhlas. Tento požadavek zachovává i návrh nařízení ePrivacy ve všech jeho navrhovaných zněních. Mezi těmito zněními by se výše popsaným způsobem odlišoval možný mechanismus udělování souhlasu nastavením prohlížeče a míra blokace cookies ve výchozím nastavení.

V případě aplikace řešení, které navrhuji, by toto cílení nebylo možné s ohledem na výchozí blokaci cookies třetích stran. V souvislosti s dobrovolnou blokací cookies třetích stran ve výchozím nastavení většiny webových prohlížečů by byl dopad podobný, může jej však změnit aplikace nových technologií, diskutovaná níže v části 9.4 . Provozovatel webové stránky by byl motivován případně využít schválené technologie nahrazující cookies třetích stran, pokud by takové retargeting umožňovaly.

[277] Retargeting se běžně projevuje tak, že uživatele na různých webových stránkách, jako jsou např. zpravodajské portály, „pronásleduje“ reklama na zboží nebo službu, které si nedávno prohlížel např. v internetovém obchodě. Blíže viz LAMBRECHT, Anja, TUCKER, Catherine. When does retargeting work? Information specificity in online advertising. *Journal of Marketing research* [online]. 2013, roč. 50, č. 5, s. 562. [cit. 2. 2. 2023], s. 561–576. Dostupné z SagePub: https://journals.sagepub.com/doi/pdf/10.1509/jmr.11.0503

Specifické je použití cookies na webových stránkách, které nabízejí bezplatný obsah nebo služby financované z cílené reklamy.[278] Tyto webové stránky zpravidla do zařízení uživatele pomocí vložených skriptů ukládají desítky cookies různých třetích stran, jako jsou reklamní sítě a burzy a dodavatelé platforem nabídky. K tomu je podle současné právní úpravy potřeba souhlas, přičemž podle standardů aplikovaných v reklamním ekosystému musí mít tento souhlas definovanou strukturu podle účelů, ale také podle třetích stan.[279] Výsledný dialog žádosti o souhlas je tak zpravidla vysoce komplexní, přinejmenším v druhé vrstvě a dalších vrstvách (tj. po kliknutí na tlačítko umožňující podrobnější nastavení).

Podle nařízení ePrivacy by byl požadavek na souhlas zachován, s komplexními dialogy bychom se proto patrně setkávali i nadále. Podle návrhu Evropské komise a pozice Evropského parlamentu by se však opět výše popsaným způsobem odlišoval možný mechanismus udělování souhlasu nastavením prohlížeče a míra blokace cookies ve výchozím nastavení.

Podle návrhu Rady by příslušná webová stránka mohla udělením souhlasu podmiňovat přístup k obsahu, pokud by zároveň nabízela alternativní přístup bez požadavku na souhlas (např. placený přístup k jednotlivému článku nebo předplatné).[280] To by v praxi znamenalo zachování komplexních souhlasových dialogů, avšak proměněných do podoby cookie walls – bez udělení komplexního souhlasu by tedy nebylo možné k obsahu přistoupit.

Řešení, které navrhuji, by znamenalo pro tyto webové stránky podobné omezení jako návrh Komise a pozice Evropského parlamentu s ohledem na výchozí blokaci cookies třetích stran. Bylo by tak motivací pro provozovatele webových stránek k implementaci schválených technologií nahrazujících cookies třetích stran, které by představovaly menší zásah do sou-

[278] Pro účely tohoto příkladu odhlížím od výhrad k reálnosti a udržitelnosti takového řešení diskutovaných v části 7.2 .

[279] Viz Interactive Advertising Bureau. IAB Europe Transparency & Consent Framework Policies [online], příloha B, část C, bod c.iii.

[280] Tamtéž bod 20aaaa odůvodnění.

kromí,[281] popř. k přechodu na jiné formy cílení reklamy, které nevyžadují sledování uživatele, jako je kontextová reklama.[282]

Relevantní je také diskutovat dopad mnou navrhovaného řešení na webové stránky, které by cíleně obcházely (či již dnes obcházejí) blokaci cookies třetích stran za účelem sledování uživatele (ať už pro potřeby cílené reklamy nebo z jiných důvodů). Blokaci cookies třetích stran lze obcházet pomocí technik, jako je fingerprinting, nebo například technickým prezentováním cookies třetích stran jako vlastních cookies.[283]

Současná právní úprava na aktivní fingerprinting aplikuje požadavek souhlasu, jakkoli úprava v tomto směru není výslovná.[284] Stejně tak cookies třetích stran vydávané za cookies vlastní podléhají režimu souhlasu, pokud nejsou technicky nezbytné pro fungování webové stránky (což je nepravděpodobná varianta). Nařízení ePrivacy z pera Komise explicitně rozšiřuje působnost požadavku na souhlas i na aktivní fingerprinting, návrhy Parlamentu a Rady tuto působnost rozšiřují i na fingerprinting pasivní.[285] Podle návrhu Evropské komise a pozice Evropského parlamentu by pak byly některé druhy cookies, vč. vlastních cookies, ve výchozím nastavení webového prohlížeče blokovány (s nutností odsouhlasení nebo změny tohoto úvodního nastavení uživatelem).[286]

Specifická opatření, která by sama o sobě bránila sledování v případě, kdy webová stránka právní předpis poruší a provede např. fingerprinting bez souhlasu, návrh nařízení ePrivacy v žádném znění neobsahuje. Je pouze otázkou, jak by se na fingerprinting měl aplikovat požadavek Evropské-

[281] Blíže viz rozbor v částech 3. a 9.4 .

[282] Viz ZHANG, Kaifu, KATONA, Zsolt. Contextual advertising. *Marketing Science* [online]. 2012, roč. 31, č. 6 [cit. 6. 2. 2023]. K dalším alternativám viz VEALE, Michael; BORGESIUS, Frederik Zuiderveen. *Adtech and real-time bidding under European data protection law*, s. 239.

[283] Tato technika se označuje CNAME cloaking a není na internetu neobvyklá. Viz REN, Tongwei et al. An Analysis of First-Party Cookie Exfiltration due to CNAME Redirections. In: *Workshop on Measurements, Attacks, and Defenses for the Web*: *Proceedings 2021 Workshop on Measurements, Attacks, and Defenses for the Web* [online]. Virtual: Internet Society, 2021, [cit. 4. 1. 2023]. s. 3, 10.

[284] Blíže viz rozbor v části 5.

[285] Blíže viz část 6.

[286] Viz diskuzi v části 9.3 .

ho parlamentu ve výchozím nastavení prohlížeče blokovat ukládání a čtení údajů z koncového zařízení, které není technicky nezbytné. Pokud by tento požadavek byl vykládán jako povinnost blokovat fingerprinting, pak by s ohledem na kategorickou formulaci povinnost nemusela být pro tvůrce webových prohlížečů splnitelná, protože jednoznačně rozpoznat, kdy je čtení údajů o zařízení technicky nezbytné a kdy nikoli, je obtížné.

Mnou navrhované řešení zachovává výše uvedené požadavky na souhlas s fingerprintingem.[287] Ve vztahu ke cookies třetích stran vydávaných za vlastní cookies nestanoví požadavek na souhlas, je však otázkou, zda by takové jednání nešlo kvalifikovat jako obcházení zákona ze strany provozovatele webové stránky. V každém případě by však fingerprintingu i technikám jako vydávání cookies třetích stran za vlastní měla v právní úpravě dle mého návrhu bránit opatření přijatá na úrovni internetového prohlížeče. Internetové prohlížeče jsou obecně ve vhodném postavení, aby bránily soukromí uživatelů před neoprávněným sledováním.[288] Bez využití funkcionalit webového prohlížeče totiž nemůže webová stránka uživatele sledovat. Opatření implementovaná prohlížečem jsou méně náročná pro uživatele – snižují nároky na kontrolu z jeho strany. Internetových prohlížečů, resp. jejich tvůrců, je také výrazně méně než provozovatelů webových stránek, což usnadňuje vymáhání.[289] Současně řadu opatření v tomto směru již internetové prohlížeče implementují.[290]

Aplikace řešení, které navrhuji, na fungování webových stránek pohledem současného stavu techniky ukazuje, že by v praxi přineslo menší počet žádostí o souhlas (nebo alespoň jejich menší komplexnost). Současně by ře-

[287] Resp. požadavku na souhlas s pasivním fingerprintingem podle čl. 8 odst. 2 pozice Parlamentu a pozice Rady se navržené řešení nijak nedotýká. Přesto jsem skeptický ohledně vymahatelnosti tohoto požadavku, protože zda webová stránka provádí pasivní fingerprinting nelze zpravidla zjistit jinak než zkoumáním softwaru používaného k jejímu provozu. Viz MAYER, Jonathan R., MITCHELL, John C. *Third-party web tracking: Policy and technology*, s. 421.

[288] Viz COFONE, Ignacio N. *The way the cookie crumbles: online tracking meets behavioural economics*, s. 56.

[289] Viz tamtéž.

[290] Pro přehled existujících technologií implementovaných ve webových prohlížečích viz Interactive Advertising Bureau. A Guide to the Post Third-Party Cookie Era [online], s. 18. [cit. 30. 5. 2023].

šení nezvětšilo možný rozsah zásahů do soukromí uživatelů, ale naopak zvýšilo úroveň jeho ochrany prostřednictvím opatření ve webových prohlížečích, která by nevyžadovala kontrolu ze strany uživatele.

9.4 APLIKACE NA TECHNOLOGIE NAHRAZUJÍCÍ COOKIES TŘETÍCH STRAN

Relevantní je také popsat, jak by se řešení, které navrhuji, aplikovalo na technologie, které mají nahradit cookies třetích stran, a to opět v porovnání se současnou právní úpravou a navrženými podobami nařízení ePrivacy.

Technologie Topics API, popsaná v části 3. , z pohledu právní úpravy spočívá ve čtení údajů z koncového zařízení. Nejde přitom o informace aktivně ukládané webovou stránkou, ale informace generované samotným webovým prohlížečem. Z pohledu přístupu ke koncovému zařízení se tak do jisté míry podobá fingerprintingu, jakkoli fingerprinting spíše pracuje se statickými vlastnostmi zařízení a prohlížeče, nikoli generovanými údaji. Právní důsledky jsou přesto stejné – použití technologie Topics API ze strany webové stránky by podle platné právní úpravy podléhalo souhlasu, stejně tak podle návrhu nařízení ePrivacy. Podle návrhu nařízení ePrivacy ve znění návrhů Evropské komise a Evropského parlamentu by zřejmě mělo být použití technologie Topics API předmětem volby uživatele, resp. by mělo být ve výchozím nastavení blokováno.

Z hlediska GDPR je status Topics API nejednoznačný. Na jednu stranu lze argumentovat, že použití této technologie neposkytuje žádný (byť pseudonymní) identifikátor uživatele. Na druhou stranu Topics API poskytuje údaje pro cílení ve smyslu, který Purtova podřazuje pod identifikaci ve smyslu GDPR, a tedy pod zpracování osobních údajů. Současně údaje poskytované Topics API mohou být do značné míry unikátní.[291] Nelze tedy vyloučit, že použití Topcis API by podléhalo souhlasu podle GDPR.

Technologie FLEDGE se pak svým pojetím více blíží cookies, protože spočívá v ukládání údajů (příslušnosti k zájmové skupině) do prohlížeče uživatele. Tyto údaje nejsou následně čteny přímo webovou stránkou,

[291] Viz THOMSON, Martin. A *Privacy Analysis of Google's Topics Proposal*. In: github [online]. 6. 1. 2023 [cit. 28. 5. 2023]. Dostupné z: https://mozilla.github.io/ppa-docs/topics.pdf s. 12

webová stránka, která je chce využít, však spouští funkci internetového prohlížeče realizující příslušnou akci a zpracovávající tyto zapsané údaje. Uložení údaje o zájmové skupině do prohlížeče by podléhalo souhlasu dle současné právní úpravy i dle nařízení ePrivacy. U spuštění aukce v prohlížeči uživatele je závěr podle současné právní úpravy méně jednoznačný, domnívám se však, že s ohledem na její účel v podobě ochrany soukromé sféry uživatele by mělo i toto spuštění podléhat souhlasu, protože do této sféry zasahuje – využívá výpočetní prostředky zařízení uživatele a vede k vyslání signálů ze zařízení uživatele třetím stranám, přičemž tyto signály vypovídají o zařazení zařízení do zájmové skupiny. Návrh nařízení ePrivacy je v tomto směru explicitní a spuštění akce by podle něj souhlasu podléhalo jednoznačně. Použití FLEDGE by také, podobně jako Topics API, omezovalo výchozí nastavení prohlížeče podle návrhu nařízení ePrivacy ve znění návrhů Evropské komise a Evropského parlamentu.

Z pohledu GDPR by pak použití FLEDGE nemělo představovat zpracování osobních údajů, protože FLEDGE poskytuje webové stránce spouštějící reklamní aukci minimum informací. V podstatě by se měla jen dozvědět, jaká reklama byla zobrazena, který inzerent podal vítěznou nabídku a jakou cenu má za zobrazení zaplatit. Tyto údaje by neměly webové stránce umožňovat cílení na uživatele, které se odehrává mimo její kontrolu v zařízení uživatele.

Řešení, které navrhuji, by tak u Topics API, FLEDGE a podobných technologií (za předpokladu že by jejich použití nebylo považováno za zpracování osobních údajů) upouštělo od souhlasu na úrovni každé jednotlivé webové stránky, pokud by daná technologie odpovídala specifikaci schválené EDPB. Tyto technologie by však mohly být ve výchozím nastavení blokovány a uživateli by bylo toto nastavení mohlo být povinně předkládáno k odsouhlasení při prvním použití webového prohlížeče.[292] Rozhodující by pak bylo vnímání těchto technologií ze strany uživatelů. Pokud by se jejich

[292] Tento přístup by odpovídal doporučením ve stanovisku ICO. Viz Information Commissioner's Office. *Data protection and privacy expectations for online advertising proposals.* In: *Information Commissioner's Office* [online]. 25. 11. 2021, s. 43. [cit. 2. 2. 2023]. Dostupné z: https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pd

tvůrcům podařilo přesvědčit nejen EDPB, ale také uživatele, že tyto technologie nepředstavují významný zásah do jejich soukromí a jsou důležité pro fungování webových stránek nabízejících bezplatný obsah, uživatelé by měli jednoduchou možnost jejich fungování v prohlížeči povolit.

Alternativou by také mohlo být připuštění obdoby cookies walls ve vztahu k těmto technologiím, tj. že by webové stránky mohly podmiňovat přístup k bezplatnému obsahu povolením těchto technologií. Na rozdíl od dnešní podoby cookies walls, které vynucují povolení cookies vč. cookies třetích stran by tyto jejich obdoby vynucovaly použití výrazně méně invazivní technologie a lze zde uvažovat, že volba na straně uživatele by byla reálná a smysluplná – zda snese mírnější formu zásahu do soukromí, nebo upřednostní placený přístup k obsahu.

Dosavadní data přitom naznačují, že postoj uživatelů k cílení reklamy je spíše negativní.[293] Například poté, co Apple na svých zařízeních zavedl možnost jednoduše se rozhodnout o sledování či nesledování za účelem cílené reklamy v konkrétní mobilní aplikaci, po 4 měsících od zavedení této funkce se poměr souhlasů z celkového počtu žádostí pohyboval okolo 20 %.[294] Je tedy otázkou, jaký podíl uživatelů by příslušnou technologii ve svém webovém prohlížeči povolil. Roli by zde mohla hrát dodatečná dobrovolná opatření, která by v tomto směru mohly webové prohlížeče nabídnout, např. možnost na konkrétních webových stránkách tuto funkcionalitu zakázat apod. Na druhou stranu dostupná data nepopisují postoj uživa-

[293] Viz TUROW, J. et al. Americans Reject Tailored Advertising and Three Activities that Enable It. In: *SSRN*. [online]. 29. 9. 2009. [cit. 2. 2. 2023]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214, s. 3. V Evropě se 7 z 10 lidí obává, že by společnosti mohly využívat data k novým účelům, jako je cílená reklama, aniž by je o tom informovaly. Viz Evropská komise. Special Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union. In: *Evropská komise* [online]. červen 2011, s. 146. [cit. 2. 2. 2023]. Dostupné z: https://joinup.ec.europa.eu/sites/default/files/document/2014-12/Part%20I%20of%20Special%20Eurobarometer%20359%20-%20Attitudes%20on%20Data%20Protection%20and%20Electronic%20Identity%20in%20the%20European%20Union.pdf

[294] Viz LAZUIK, Estelle. iOS 14 Opt-in Rate - Weekly Updates Since Launch. In: *Flurry*. [online]. 25. 5. 2021. [cit. 2. 2. 2023]. Dostupné z: https://www.flurry.com/blog/ios-14-5-opt-in-rate-idfa-app-tracking-transparency-weekly/

telů k cílení v kontextu jiných protihodnot, např. bezplatnému přístupu k obsahu.[295]

9.5 SROVNÁNÍ A ZHODNOCENÍ

Z popisu aplikace navrženého řešení v praxi jsou patrné odlišnosti mezi řešením, které navrhuji, současnou právní úpravou a různými zněními nařízení ePrivacy.

Návrh Evropské komise a pozice Evropského parlamentu výrazně akcentují prvek kontroly uživatele. Ten se projevuje požadavkem na souhlas u většiny případů použití cookies a podobných technologií. Jakkoli se návrh i pozice Evropského parlamentu snaží řešit problém přetížení uživatelů požadavky na souhlas prostřednictvím nastavení webových prohlížečů, toto řešení by podle mě nebylo účinné. Sice by se díky němu pravděpodobně zjednodušil a sjednotil způsob udělování souhlasů (nešlo by o odlišné dialogy na různých webových stránkách, ale jednotný dialog v rozhraní internetového prohlížeče), s ohledem na aplikaci požadavků GDPR na tyto souhlasy by stále bylo však třeba, aby uživatel činil rozhodnutí o udělení souhlasu na úrovni jednotlivých webových stránek.

Toto řešení by tak dle mého názoru významně neposílilo ochranu soukromí uživatelů, ale pouze zmírnilo některé nedostatky současného stavu, a to za cenu podstatné zátěže pro tvůrce internetových prohlížečů, a hlavně tvůrce webových stránek, kteří by své stránky novým nastavením prohlížeče a mechanismům sběru souhlasu museli přizpůsobit.

Pozice Rady Evropské unie pak poměrně kategoricky (na úrovni odůvodnění) deklaruje, že u bezplatných služeb je možné souhlas (za stanovených podmínek) vyžadovat. Toto řešení by však dle mého názoru nesnížilo zátěž uživatelů z hlediska počtu žádostí o souhlas, pouze by snížilo jejich kontrolu skrze odepření bezprostřední možnosti souhlas odmítnout.

Jakkoli se toto řešení může zdát smysluplné u webových stránek, které uživatel navštěvuje pravidelně (např. webový zpravodajský portál, který uživatel navštěvuje denně), a má tak možnost se efektivně rozhodnout, zda

[295] Viz MAYER, Jonathan R., MITCHELL, John C. *Third-party web tracking: Policy and technology*, s. 417.

za službu „zaplatí“ svým soukromím či penězi formou předplatného, v případě jednotlivé návštěvy webové stránky už řešení funguje hůře. Pokud by si tedy uživatel např. na základě sdílení odkazu na sociální síti chtěl přečíst zpravodajský článek na webovém portálu, který běžně nenavštěvuje, stál by před volbou, zda si zaplatit předplatné ve výši nepřiměřené k přínosu přečtení jednoho článku,[296] „zaplatit“ přístup svým soukromím nebo k obsahu nepřistoupit. Jelikož první volba je ekonomicky neracionální, zbydou uživateli fakticky pouze druhá a třetí možnost, kde se však již o „skutečné možnosti volby“ (zmiňované v odůvodnění návrhu ve znění pozice Rady) dá hovořit jen obtížně.

Současně lze takto postavenou možnost volby vykládat tak, že ochrana před zásahy do soukromí má být dostupná jen pro ty, kteří jsou dostatečně finančně vybaveni pro přístup k placenému obsahu. V tomto směru se neztotožňuji s tím, že adekvátní ochrana soukromí jako základního práva by měla být „luxusem“, který si nemůže dovolit každý.

Návrh řešení, který předkládám, spočívá ve stanovení výjimky pro vlastní cookies, podobné technologie a technologie nahrazující cookies třetích stran, pokud by odpovídaly technické specifikaci schválené EDPB. Použití těchto technologií by tak zůstalo pouze v režimu GDPR. Současně by cookies třetích stran byly ve výchozím nastavení blokovány ve webovém prohlížeči.

Obdobně by mohly být blokovány technologie nahrazující cookies třetích stran, blokace by však podléhala odsouhlasení uživatele, který by mohl nastavení změnit. Pokud by použití těchto technologií nepředstavovalo zpracování osobních údajů (přičemž zde závisí na specifikaci konkrétních technologií), nebyl by pro jejich použití nutný souhlas podle GDPR na úrovni každé jednotlivé webové stránky. Řešení by pak doplňovala opatření odpovídající stavu techniky na úrovni prohlížeče, která by bránila skrytému nebo neoprávněnému sledování uživatele.

Toto řešení by podle mě odstranilo výše popsané nedostatky návrhů Evropského parlamentu a Rady. Díky vynětí vlastních cookies, podobných technologií a technologií nahrazujících cookies třetích stran z působnosti

[296] Za předpokladu, že zpravodajský portál neumožňuje přístup pouze k jednotlivému článku.

právní úpravy přístupu ke koncovému zařízení by se pravděpodobně významně snížil počet žádostí o souhlas, kterými by se museli uživatelé zabývat, nebo by se alespoň snížila komplexnost těchto žádostí. K řadě dnes běžných a málo invazivních způsobů zpracování by totiž nebyl potřeba souhlas, ale bylo by možné pro ně najít jiný právní titul podle čl. 6 odst. 1 GDPR, popř. by se GDPR na použití daných technologií neaplikovalo vůbec.

Současně by však nehrozil scénář popsaný německým předsednictvím, tedy výrazné usnadnění instalace „softwaru, který je často považován za hlavní vstupní bránu pro škodlivý software“,[297] neboť instalace jakéhokoli softwaru by stále podléhala právnímu režimu přístupu ke koncovému zařízení, tj. zpravidla požadavku na souhlas.[298]

Vedle toho by navrhovaný přístup mohl přinést větší flexibilitu ve vztahu k financování webových stránek pomocí cílení reklamy s využitím technologií nahrazujících cookies třetích stran. Je přitom k diskuzi, zda použití těchto technologií podmiňovat souhlasem uživatele na úrovni webového prohlížeče, pokud bude daná technologie pozitivně zhodnocena EDPB.

V takovém případě by použití těchto technologií nevyžadovalo souhlas uživatele na úrovni webové stránky, muselo by však být webovém prohlížeči povoleno. Odpadla by tak nutnost sbírat složitě souhlasy technikou podle pozice Evropského parlamentu. Současně by tento přístup znamenal zachování jisté míry kontroly uživatele, která by se realizovala právě skrze nastavení prohlížeče. Na druhou stranu by toto řešení nemuselo být dostatečné z hlediska flexibility pro financování webových stránek pomocí cílené reklamy, pokud by procento uživatelů, kteří by ve svém prohlížeči povolili technologie nahrazující třetích stran, bylo nízké. V takovém případě bychom se pravděpodobně vrátili k úvahám o období cookie walls v duchu pozice Rady, které by blokovaly přístup k bezplatnému obsahu pro uživatele se zakázanými technologiemi nahrazujícími cookies třetích stran. Volby vytvářené těmito obdobami cookies walls by však byly smysluplnější, pro-

[297] Viz návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) – Presidency discussion paper ze dne 6. 6. 2020, 2017/0003(COD), 9243/20, s. 6.

[298] Tím není dotčena možnost přijmout výjimky například pro bezpečnostní aktualizace.

tože potenciální zásah do soukromí by byl u technologií pozitivně hodnocených EDPB nízký.

Ať už však zvolíme variantu s výchozí blokací technologií nahrazujících cookies třetích stran, či nikoli, navrhované řešení podle mého názoru snižuje důraz na kontrolu uživatele, může zvýšit flexibilitu právní úpravy ve vztahu k omezeným formám cílené reklamy a současně zvyšuje úroveň ochrany soukromí uživatele prostřednictvím technických opatření na úrovni internetových prohlížečů.

9.6 NÁVRH ZNĚNÍ

Na základě výše provedené diskuze je namístě také formulovat, jak by navrhované řešení mělo být promítnuto do návrhu nařízení ePrivacy. V návrhu Komise je čl. 8 odst. 1 nařízení formulován jako pravidlo zakazující využití funkcí koncového zařízení pro zpracování a uchovávání, jakož i shromažďování informací z koncových zařízení, včetně informací o softwaru a hardwaru, jinými subjekty, než jsou dotčení uživatelé, s výjimkou využití pro definované důvody. Navrhované řešení nespočívá ve vymezení nového důvodu pro využití funkcí koncového zařízení, ale v úplném vyloučení některých způsobů využití funkcí koncového zařízení z působnosti výše popsaného pravidla. Z toho důvodu by podle mě nemělo být formulováno jako nové písmeno v čl. 8 odst. 1, ale jako nový odstavec čl. 8, stanovící výjimku z odst. 1.

Tato výjimka by pak měla být formulována tak, že se bude vztahovat na vlastní cookies a podobné technologie, tedy na ukládání a čtení informací z koncového zařízení v případě, že tyto informace budou uloženy tak, že je bude moci číst pouze webová stránka, která tyto informace do zařízení uložila. Výjimka by se proto neměla vztahovat na čtení informací v koncovém zařízení, které nebyly do zařízení uloženy příslušnou webovou stránkou. Výjimka by se také neměla vztahovat na počítačové programy (software) podle směrnice Evropského parlamentu a Rady 2009/24/ES ze dne 23.

dubna 2009, o právní ochraně počítačových programů.[299] Pro účely zajištění ochrany bezpečnosti koncového zařízení by také ukládané informace neměly měnit bezpečnostní nastavení koncového zařízení.

Tyto požadavky splňuje následující znění, které by mohlo být vloženo do čl. 8 jako nový odstavec 3 (s předpokladem přečíslování stávajících odst. 3 a 4):

> *Odst. 1 se nevztahuje na uchovávání informací a získávání přístupu k již uchovávaným informacím v koncovém zařízení, pokud*
>
> *1. jsou informace do koncového zařízení při poskytování služby informační společnosti vyžádané koncovým uživatelem uloženy poskytovatelem této služby,*
>
> *2. přístup k těmto informacím je omezen na poskytovatele služby informační společnosti, který tyto informace do koncového zařízení uložil,*
>
> *3. tyto informace nejsou počítačovými programy a*
>
> *4. tyto informace nemění bezpečnostní nastavení koncového zařízení.*

Ve vztahu k technologiím nahrazujícím cookies třetích stran by se výjimka měla vztahovat na technologie, jejichž technickou specifikaci schválí EDPB. Taková právní úprava by vyžadovala doplnění nařízení ePrivacy o zcela nová ustanovení upravující příslušnou kompetenci EDPB, postup schvalování technických specifikací a kritéria jejich hodnocení. Není mou ambicí předkládat zde možné komplexní znění takové úpravy,[300] pouze se domnívám, že by mělo směřovat k podrobnému posouzení příslušné technické specifikace z hlediska dopadů dané technologie na soukromí uživatelů.

Do čl. 8 by se pak výjimka mohla promítnout jako nový odstavec 4 následujícího znění.

---

[299] Směrnice 2009/24/ES pojem počítačový program nedefinuje, není tedy podle mě nutné zavádět jeho definici ani do nařízení ePrivacy, jakkoli by patrně bylo vhodné v odůvodnění nařízení uvést, že tento pojem má stejný význam jako ve směrnici 2009/24/ES.

[300] Inspirací obecně může být právní úprava technických požadavků na výroby podle nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a kterým se zrušuje nařízení (EHS) č. 339/9.

Odst. 1 se nevztahuje na využití funkcí koncového zařízení pro zpracování a uchovávání, jakož i shromažďování informací z koncových zařízení koncových uživatelů, včetně informací o softwaru a hardwaru, jinými subjekty, než jsou dotčení koncoví uživatelé, pokud k němu dochází pomocí funkcionality softwaru uváděného na trh, který umožňuje elektronické komunikace včetně získávání a prezentování informací na internetu, a tato funkcionalita odpovídá technické specifikaci schválené Evropským sborem pro ochranu osobních údajů.

Požadavky na funkcionality webových prohlížečů jsou upraveny v čl. 10 návrhu Evropské komise. Odstavce 1 a 2 popisují požadované funkcionality a způsob jejich prezentace koncovému uživateli. Tyto dva odstavce by měla nahradit právní úprava, která tvůrcům internetových prohlížečů uloží ve výchozím nastavení blokaci cookies třetích stran ve webovém prohlížeči a implementaci opatření odpovídajících stavu techniky na úrovni prohlížeče, která budou bránit skrytému nebo neoprávněnému sledování uživatele. Opatření proti sledování koncového uživatele je přitom podle mého názoru třeba formulačně vázat na koncové zařízení, protože to je úroveň, na které je webový prohlížeč schopen sledování bránit. Odstavec 1 by tak mohl znít:

Software uváděný na trh, který umožňuje elektronické komunikace včetně získávání a prezentování informací na internetu, musí ve výchozím nastavení

1. *bránit uchovávání informací a získávání přístupu k již uchovávaným informacím v koncovém zařízení, pokud přístup k těmto informacím není omezen na poskytovatele služby informační společnosti, který tyto informace do koncového zařízení uložil, a*
2. *mít aktivovaná přiměřená opatření odpovídající stavu techniky, která budou bránit skrytému nebo neoprávněnému sledování koncového zařízení.*

Pokud bychom na základě diskuze navržené výše v částech 9.4 a 9.5 dospěli k závěru, že technologie nahrazující cookies třetích stran nemají být ve výchozím nastavení webového prohlížeče blokovány, pak by písmeno a) odst. 1 mělo znít:

1) Bránit uchovávání informací a získávání přístupu k již uchovávaným informacím v koncovém zařízení, pokud přístup k těmto informacím není omezen na poskytovatele služby informační společnosti, který tyto informace do koncového zařízení uložil, a nejde o uchovávání informací nebo získávání přístupu pomocí funkcionality softwaru uváděného na trh, který umožňuje elektronické komunikace včetně získávání a prezentování informací na internetu, odpovídající technické specifikaci schválené Evropským sborem pro ochranu osobních údajů,

Odstavec 2 upravuje odsouhlasení nastavení uživatelem. To podle mého názoru může být (dle výsledků diskuze navržené v částech 9.4 a 9.5) namístě pouze ve vztahu k technologiím nahrazujícím cookies třetích stran, tedy dle výše předloženého návrhu technologií uznaných EDPB. Odstavec 2 by proto mohl znít následovně:

2) Software při prvním spuštění informuje koncového uživatele o nastavení bránícím využití funkcionalit odpovídajících technické specifikaci schválené Evropským sborem pro ochranu osobních údajů a vyžaduje souhlas koncového uživatele s tímto nastavením nebo jeho změnu.

Pokud bychom dospěli k závěru, že technologie nahrazující cookies třetích stran by neměly být ve výchozím nastavení webového prohlížeče blokovány, pak by bylo možné odst. 2 zcela vypustit a následující odstavce přečíslovat.

Odstavec 3 v čl. 10 návrhu Komise obsahuje přechodné ustanovení. Toto ustanovení ukládá v případě softwaru, který bude ke dni účinnosti nařízení již instalován, splnit požadavky podle odstavců 1 a 2 při první aktualizaci softwaru, nejpozději však do tří měsíců od účinnosti. Druhou část požadavku považuji za nesplnitelnou, protože aktualizace softwaru zpravidla není pod kontrolou jeho tvůrce (toho, kdo jej uvádí na trh), ale toho, kdo má pod kontrolou zařízení, na kterém je software instalován. Druhá část požadavku by proto měla být podle mého názoru vypuštěna se zachováním pouze požadavku na splnění povinností při první aktualizaci.

Rovněž v souvislosti s aktualizací softwaru považuji za důležité, aby uživatel byl upozorněn na nové výchozí nastavení prohlížeče a měl možnost jej změnit. Tato povinnost by proto měla být uložena tvůrcům internetových prohlížečů. Odstavec 3 by proto mohl znít následovně:

3) V případě softwaru, který byl ke dni vstupu tohoto nařízení v účinnost již instalován, musí být požadavky podle odstavce splněny při první aktualizaci softwaru. Při instalaci aktualizace software informuje koncového uživatele o výchozím nastavení podle odstavce 1 a umožní mu jeho změnu.

10. ZÁVĚR

Podle platné právní úpravy ochrany soukromí v elektronických komunikacích je pro ukládání a čtení cookies a použití podobných technologií včetně použití údajů o koncovém zařízení nezbytný souhlas uživatele. Ten není vyžadován pouze pro použití cookies a podobných technologií v rozsahu nezbytném k fungování příslušné webové stránky. Souhlas musí splňovat požadavky GDPR, tedy být svobodný, konkrétní, informovaný a mít formu jednoznačného projevu vůle.

Široce formulovaný požadavek na souhlas je projevem přístupu k ochraně soukromí založeného na kontrole a jeho důsledkem je přetížení uživatelů žádostmi o jejich souhlas. V důsledku množství a složitosti procesů využívajících cookies a s nimi související informační asymetrie, složitosti předkládaných voleb, kognitivních limitů uživatelů a manipulativních uživatelských rozhraní není ve vztahu k použití cookies a souvisejících technologií kontrola ze strany uživatele reálná. Snaha o tuto kontrolu naopak vede k frustraci uživatelů. Řešením je podle mého názoru menší důraz na kontrolu a větší důraz na preventivní povinnosti pro ty, kdo relevantní činnosti vykonávají.

Požadavky na souhlas také komplikují realizaci cílené reklamy, která často slouží k financování webových stránek nabízejících bezplatný obsah nebo služby. Jakkoli financování prostřednictvím reklamy není například ve vztahu k médiím jediným možným modelem financování, je třeba počítat s tím, že přechod k jiným modelům financování bude postupný. Proto je

z pohledu významu nezávislých médií pro demokracii žádoucí najít způsob, jak umožnit bez větších komplikací realizaci cílené reklamy ve formě, která by představovala zásah do práva na soukromí v rozsahu proporcionálním k přínosu pro právo na svobodu projevu, právo na přístup k informacím a demokratický právní stát jako veřejný statek.

Návrh nařízení ePrivacy problém přílišného důrazu na kontrolu uživatele ani problém překážek pro omezené formy cílené reklamy neodstraňuje. Pozice Evropské komise pouze zpřesňuje některé pojmy, doplňuje dílčí tituly, o které lze opřít použití cookies bez souhlasu, a přidává požadavky na nastavení souhlasů ve webových prohlížečích. Evropský parlament ve své pozici zvětšuje důraz na souhlas uživatele a zpřesňuje požadavky na možnost jeho udělování prostřednictvím webového prohlížeče, vč. povinnosti webového prohlížeče vysílat signály o nastavení souhlasů a povinnosti webových stránek tyto signály respektovat. Toto řešení sice zmírňuje některé problémy kontroly s ohledem na sjednocení mechanismu udělování souhlasu, nesnižuje však potřebu, aby uživatel rozhodoval o udělení souhlasu ve vztahu k většině webových stránek, které navštíví. Současně nepřináší žádnou flexibilitu ve vztahu k omezeným formám internetové reklamy.

Pozice Rady vypouští závazné požadavky na nastavení webového prohlížeče a umožňuje pro přístup k webové stránce poskytované bezplatně vyžadovat souhlas s použitím cookies (za definovaných podmínek). Toto řešení by sice usnadnilo realizaci cílené reklamy opřené o souhlas, ale zachovalo by stávající problém přílišného důrazu na kontrolu a do jisté míry jej prohloubilo vytvářením neopodstatněného dojmu volby u služeb, které by souhlas mohly vyžadovat.

Východisko spatřuji v zakotvení výjimky z požadavku na souhlas pro použití vlastních cookies (tj. těch cookies, které do zařízení ukládá webová stránka, kterou uživatel prohlíží, nikoli jiná webová stránka), podobných technologií spočívajících v ukládání dat do koncového zařízení nebo jejich čtení a technologií nahrazujících cookies třetích stran. Ve vztahu k technologiím nahrazujícím cookies třetích stran by se tato úprava měla vztahovat pouze na technologie odpovídající technické specifikaci schválené EDPB.

Tato úprava by pak měla být doplněna povinností webových prohlížečů ve výchozím nastavení blokovat cookies třetích stran vč. technologií, které je nahrazují, a přijmout opatření odpovídající stavu techniky, která budou bránit skrytému nebo neoprávněnému sledování uživatele. Nastavení výchozí blokace schválených technologií nahrazujících cookies třetích stran by mělo být uživateli při prvním použití webového prohlížeče předloženo ke schválení.

Pokud by vlastní cookies, podobné technologie spočívající v ukládání dat do koncového zařízení a technologie nahrazující cookies třetích stran nepodléhaly požadavku na souhlas podle právní úpravy přístupu ke koncovému zařízení, jejich použití pro sledování uživatele by i nadále podléhalo GDPR.

Cílem právní úpravy přístupu ke koncovému zařízení je zajištění ochrany před skrytým nebo neoprávněným sledováním uživatele – společně s udržením bezpečnosti koncového zařízení, kterou však cookies a podobné technologie nemohou narušit. GDPR se vztahuje na zpracování informací o fyzické osobě, která je identifikovaná nebo kterou lze přímo či nepřímo identifikovat. Identifikací lze rozumět mimo jiné cílení na danou osobu ve smyslu výběru jednotlivce ze skupiny jako objektu pozornosti (výběr vyčleněním, singling out), tedy i použití cookies a podobných technologií za účelem sledování uživatele.

Právní úprava GDPR je na jednu stranu flexibilnější v rovině právního základu použití cookies a podobných technologií, kterým by nemusel být pouze souhlas nebo jiný úzce definovaný titul, a na druhou stranu poskytuje komplexnější ochranu zahrnující základní zásady zpracování osobních údajů, práva subjektu údajů a povinnosti správce osobních údajů.

Pokud by použití vlastních cookies a podobných technologií podléhalo pouze GDPR, v řadě situací v praxi by odpadla nutnost získávat souhlas uživatele k použití cookies, které nejsou technicky nezbytné k fungování webové stránky, ale zásah do soukromí jimi vyvolaný je minimální. Návrh nařízení ePrivacy v tomto směru zavádí titul pro úzce vymezené způsoby měření návštěvnosti webové stránky, existují však další případy, kdy přísný režim souhlasu není namístě.

Jestliže by z požadavku na souhlas na úrovni každé webové stránky bylo vyňato také použití technologií nahrazujících cookies třetích stran, v rozsahu, v jakém by tyto technologie byly pro minimální zásah do soukromí schváleny EDPB, pak by právní úprava poskytovala také větší flexibilitu pro omezenou formu cílené reklamy jako zdroje financování obsahu, který je na internetu poskytován bezplatně. Je přitom k diskuzi, zda by, s ohledem na zachování přiměřené míry kontroly uživatele, měly být tyto technologie ve výchozím nastavení webového prohlížeče blokovány a toto nastavení mělo být uživateli předloženo ke schválení nebo úpravě.

V případě, že by současně ve webových prohlížečích byly ve výchozím nastavení blokovány cookies třetích stran a byla zavedena opatření odpovídající stavu techniky, která by bránila skrytému nebo neoprávněnému sledování uživatele, uživatel by byl chráněn proti stávajícím formám invazivní cílené reklamy založené na sledování a sdílení osobních údajů pomocí cookies třetích stran. Chráněn by byl také proti technikám, které se snaží blokaci cookies třetích stran obejít, jako je vydávání cookies třetích stran za vlastní a fingerprinting. Toto pojetí právní úpravy by odpovídalo trendu, který již nyní nastavují nejrozšířenější webové prohlížeče.

Výše popsané řešení by tak podle mého názoru oproti současné právní úpravě i návrhu nařízení ePrivacy snížilo důraz na kontrolu uživatele, umožnilo flexibilnější použití omezených forem cílené reklamy a přitom zvýšilo úroveň ochrany soukromí uživatelů před skrytým nebo neoprávněným sledováním.

11. POUŽITÉ PRAMENY

[1] ACAR, Gunes, et al. The web never forgets: Persistent tracking mechanisms in the wild. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security [online]. 2014 [cit. 12. 2. 2023], s. 674-689. Dostupné z ACM Digital Library: https://dl.acm.org/doi/abs/10.1145/2660267.2660347

[2] ACQUISTI, Alessandro et al. Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys* [online]. 2017, roč. 50, č. 3, s. 44:1-44:41. ISSN 0360-0300. [cit. 2. 2. 2023]. Dostupné z: DOI:10.1145/3054926

[3] ANGWIN, Julia, PARRIS, Terry. Facebook Lets Advertisers Exclude Users by Race. *ProPublica* [online] 28. 10. 2016 [cit. 6. 3. 2022]. Dostupné z: https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race

[4] BALBONI, Paolo et al. Legitimate interest of the data controller New data protection paradigm: legitimacy grounded on appropriate protection. *International Data Privacy Law* [online]. 2013, roč. 3, č. 4, s. 244–261. ISSN 2044-3994. [cit. 2. 2. 2023]. Dostupné z: DOI:10.1093/idpl/ipt019

[5] BALKIN, Jack M. Information Fiduciaries in the Digital Age. In: *Balkinization.* [online] 5. 3. 2014 [cit. 3. 1. 2022]. Dostupné z: https://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html

[6] BALKIN, Jack M. Information fiduciaries and the first amendment. *UC Davis Law Review* [online]. 2015, roč. 49, č. 4 [cit. 12. 2. 2023], s. 1183. Dostupné z: https://openyls.law.yale.edu/bitstream/handle/20.500.13051/4692/49_U.C._Davis_Law_Review_1183_2016_.pdf?sequence=2

[7] BARTH, Adam. *HTTP State Management Mechanism* [online]. Request for Comments RFC 6265. B.m.: Internet Engineering Task Force 2011 [cit. 20. 7. 2022]. Dostupné z: DOI:10.17487/RFC6265

[8] BENNETT, Colin J. *Regulating privacy: Data protection and public policy in Europe and the United States*. Ithaca: Cornell University Press, 1992, s. 33.

[9] BORGESIUS, Frederik J. Zuiderveen. Personal data processing for behavioural targeting: which legal basis? *International Data Privacy Law* [online]. 2015, roč. 5, č. 3, s. 163–176. ISSN 2044-3994. [cit. 2. 2. 2023]. Dostupné z: doi:10.1093/idpl/ipv011

[10] BORGESIUS, Frederik J. Zuiderveen. Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer Law & Security Review* [online]. 2016, roč. 32, č. 2, s. 256–271. ISSN 0267-3649. [cit. 2. 2. 2023]. Dostupné z: doi:10.1016/j.clsr.2015.12.013

[11] BRINKMANN, Martin. A look at Microsoft Edge's Tracking Prevention feature - gHacks Tech News. In: *gHacks Technology News* [online] 5. 6. 2017. [cit. 26. 2. 2022]. Dostupné z: https://www.ghacks.net/2019/06/28/a-look-at-microsoft-edges-tracking-prevention-feature/

[12] CALO, Ryan. Digital market manipulation. *George Washington Law Review* [online]. 2013, roč. 82, č. 4 [cit. 12. 2. 2023], s. 995-1051. Dostupné z HeinOnline: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/gwlr82&section=34&casa_token=oY9YY-cEQUoAAAAAA:1EOMhftCNdkJvbtLXxrwB6X5-eRQXEcSMvUbPKvKCJVf1ta-LiG33fb3rckI-MlflvR2MbcBETw

[13] CAMP, Dave. Firefox Now Available with Enhanced Tracking Protection by Default Plus Updates to Facebook Container, Firefox Monitor and Lockwise In: *The Mozilla Blog* [online]. 4. 6. 2019 [cit. 26. 2. 2022]. Získáno z: https://blog.mozilla.org/en/products/firefox/firefox-now-available-with-enhanced-tracking-protection-by-default/

[14] CAO, Yinzhi, LI, Song, WIJMANS, Erik. (Cross-)Browser Fingerprinting via OS and Hardware Level Features. In: *Network and Distributed System Security Symposium*: *Proceedings 2017 Network and Distributed System Security Symposium* [online]. San Diego, CA: Internet Society, 2017 [cit. 28. 10. 2022]. ISBN 978-1-891562-46-4. Dostupné z: DOI:10.14722/ndss.2017.23152

[15] CAROLAN, Eoin, CASTILLO-MAYEN, M. Rosario. Why More User Control Does Not Mean More User Privacy: An Empirical (and Counter-Intuitive) Assessment of European E-Privacy Laws. *Virginia Journal of Law & Technology* [online]. 2014, roč. 19, č. 2 [cit. 28. 10. 2022], s. 324–388. Dostupné z HeinOnline: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/vjolt19&section=6&casa_token=5uomoDkHG_MAAAAA:81N49Z1dJlF_mRM66PAf-KX6bPIlVhCSzc553AzMgr-MU4DYWwtw0J0--phzTGIkm2IApkBKKfg

[16] CINAR, Naim, ATEŞ, Sezgin. Data Privacy in Digital Advertising: Towards a Post Third-Party Cookie Era. *SSRN Scholarly Paper* [online]. 24. 2. 2022. [cit. 4. 1. 2023]. Dostupné z: DOI:10.2139/ssrn.4041963

[17] CLARKE, Roger. Introduction to Dataveillance and Information Privacy, and Definitions of Terms [online] 24. 7. 2016 [cit. 3. 8. 2021]. Dostupné z: http://www.rogerclarke.com/DV/Intro.html#Priv

[18] COFONE, Ignacio N. The way the cookie crumbles: online tracking meets behavioural economics. *International Journal of Law and Information Technology* [online]. 2017, roč. 25, č. 1 [cit. 2. 2. 2023], s. 38–62. ISSN 0967-0769. Dostupné z: DOI:10.1093/ijlit/eaw013

[19] CRAIN, Matthew, NADLER, Anthony. Political Manipulation and Internet Advertising Infrastructure. *Journal of Information Policy* [online]. 2019, roč. 9 [cit. 10. 9. 2022], s. 370–410. ISSN 2381-5892. Dostupné z: DOI:10.5325/jinfopoli.9.2019.0370

[20] CRANOR, Lorrie Faith. Cookie monster. *Communications of the ACM* [online]. 2022, roč. 65, č. 7 [cit. 2. 2. 2023], s. 30–32. ISSN 0001-0782. Dostupné z: doi:10.1145/3538639

[21] CYPHERS, Bennett. Google's FLoC Is a Terrible Idea. *Electronic Frontier Foundation* [online] 3. 3. 2021 [cit. 6. 3. 2022]. Dostupné z: https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea

[22] DOUGHERTY, Christie. Every Breath You Take, Every Move You Make, Facebook's Watching You: A Behavioral Economic Analysis of the US California Consumer Privacy Act and EU ePrivacy Regulation. *Northeastern University Law Review* [online]. 2020, roč. 12, č. 2 [cit. 2. 2. 2023], s. 629–659. Dostupné z HeinOnline: https://heinonline.org/HOL/Page?handle=hein.journals/norester12&div=23&g_sent=1&casa_token=

[23] DUTTON, Sam, LEE, Kevin K. FLEDGE. In: *Chrome Developers* [online] 27. 1. 2021 [cit. 22. 1. 2023]. Získáno z: https://developer.chrome.com/docs/privacy-sandbox/fledge/

[24] DUTTON, Sam. FLoC. In: *Chrome Developers* [online] 18. 5. 2021 [cit. 6. 3. 2022]. Dostupné z: https://developer.chrome.com/docs/privacy-sandbox/floc/

[25] DUTTON, Sam. The Topics API. In: *Chrome Developers.* [online] 25. 1. 2022 [cit. 6. 3. 2022]. Dostupné z: https://developer.chrome.com/docs/privacy-sandbox/topics/

[26] ETTELDORF, Christina. EDPB on the Interplay between the ePrivacy Directive and the GDPR. *European Data Protection Law Review* [online]. 2019, roč. 5, č. 2 [cit. 2. 2. 2023], s. 224–231. Dostupné z HeinOnline: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/edpl5&section=37

[27] GELLERT, Raphaël; GUTWIRTH, Serge. The legal construction of privacy and data protection. *Computer Law & Security Review* [online]. 2013, roč. 29, č. 5, s. 522-530. Dostupné ze ScienceDirect: https://www.sciencedirect.com/science/article/abs/pii/S0267364913001325

[28] GELLERT, Raphaël. *The Risk-Based Approach to Data Protection*. Oxford: Oxford University Press, 2020.

[29] GUY, Amy. Early design review for the Topics API #726. Komentář uživatele rhiaro z 12. 1. 2023. In: github [online]. 12. 1. 2023 [cit. 30. 1. 2023]. Dostupné z: https://github.com/w3ctag/design-reviews/issues/726#issuecomment-1379908459

[30] HÄRTING, Niko, GÖSSLING, Patrick. Study on the Impact of the Proposed Draft of the ePrivacy Regulation. *Computer Law Review International* [online]. 2018, roč. 19, č. 1 [cit. 20. 1. 2023], s. 6–11. ISSN 2194-4164. Dostupné z: DOI:10.9785/cri-2018-190103

[31] HARTZOG, Woodrow. *Privacy's blueprint*. Cambridge, Massachusetts: Harvard University Press, 2018.

[32] HINTERNESCH, Nicolas. No Cookies, No Problem — Using ETags For User Tracking. *Medium* [online] 2. 7. 2020 [cit. 18. 1. 2023]. Dostupné z: https://levelup.gitconnected.com/no-cookies-no-problem-using-etags-for-user-tracking-3e745544176b

[33] HOOFNAGLE, Chris Jay et al. Behavioral advertising: The offer you can't refuse. *Harvard Law & Policy Review*. 2012, roč. 6, s. 273.

[34] JENSEN, Paul. Intent to Experiment: First „Locally-Executed Decision over Groups" Experiment (FLEDGE) In: *Google Groups*. [online] 25. 3. 2022 [cit. 22. 1. 2023]. Dostupné z: https://groups.google.com/a/chromium.org/g/blink-dev/c/0VmMSsDWsFg

[35] KAMARA, Irene, DE HERT, Paul. Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach. *SSRN Scholarly Paper* [online]. 8. 8. 2018 [cit. 8. 1. 2023]. Dostupné z: DOI:10.2139/ssrn.3228369

[36] KAMARA, Irene, KOSTA, Eleni. Do Not Track initiatives: regaining the lost user control. *International Data Privacy Law* [online]. 2016, roč. 6, č. 4 [cit. 2. 2. 2023], s. 276–290. ISSN 2044-3994. Dostupné z: DOI:10.1093/idpl/ipw019

[37] KHAN, Lina M.; POZEN, David E. A skeptical view of information fiduciaries. *Harvard Law Review* [online]. 2019, roč. 133, č. 2 [cit. 2. 2. 2023], s. 497-541. Dostupné z JSTOR: https://www.jstor.org/stable/pdf/26868033.pdf

[38] KONIK, James. How Does Canvas Fingerprinting Work – In: *Fingerprint* [online] 11. 6. 2021 [cit. 28. 10. 2022]. Dostupné z: https://fingerprint.com/blog/canvas-fingerprinting/

[39] KOSTA, Eleni. Peeking into the cookie jar: the European approach towards the regulation of cookies. *International Journal of Law and Information Technology* [online]. 2013, roč. 21, č. 4 [cit. 11. 1. 2023], s. 380–406. ISSN 0967-0769. Dostupné z: DOI:10.1093/ijlit/eat011

[40] KULYK, Oksana et al. Has the GDPR hype affected users' reaction to cookie disclaimers? *Journal of Cybersecurity* [online]. 2020, roč. 6, č. 1 [cit. 2. 2. 2023], s. 1-14. ISSN 2057-2085. Dostupné z: DOI:10.1093/cybsec/tyaa022

[41] LAMBRECHT, Anja, TUCKER, Catherine. When does retargeting work? Information specificity in online advertising. *Journal of Marketing research* [online]. 2013, roč. 50, č. 5 [cit. 2. 2. 2023], s. 561–576. Dostupné z SagePub: https://journals.sagepub.com/doi/pdf/10.1509/jmr.11.0503

[42] LASSEY, Brad. Combating Fingerprinting with a Privacy Budget. In*: github.* [online]. 25. 2. 2022 [cit. 6. 3. 2022]. Dostupné z: https://github.com/bslassey/privacy-budget

[43] LAURISTIN, Marju. REPORT on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), A8-0324/2017.In: *European Parliament.* [online] 20. 10. 2017 [cit. 11. 1. 2023]. Dostupné z: https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html

[44] LAZUIK, Estelle. iOS 14 Opt-in Rate - Weekly Updates Since Launch. In: *Flurry.* [online]. 25. 5. 2021. [cit. 2. 2. 2023]. Dostupné z: https://www.flurry.com/blog/ios-14-5-opt-in-rate-idfa-app-tracking-transparency-weekly/

[45] LEE, Timothy B. Google defends tracking cookies—some experts aren't buying it. In: *Ars Technica* [online] 26. 8.2019. [cit. 26. 2. 2022]. Dostupné z: https://arstechnica.com/tech-policy/2019/08/why-some-experts-are-skeptical-of-googles-new-web-privacy-strategy/

[46] LEENES, Ronald E. Do They Know Me? Decomposing Identifiability *University of Ottawa Law and Technology Journal* [online]. 2007, roč. 4, č. 1-2 [cit. 6. 1. 2023], s. 135-161. Dostupné z: https://research.tilburguniversity.edu/files/1310856/Leenes_Do_they_know_me_110216_publishers_immediately.pdf

[47] MAYER, Jonathan R., MITCHELL, John C. Third-party web tracking: Policy and technology. In: 2012 *IEEE symposium on security and privacy* [online]. IEEE, 2012 [cit. 27. 5. 2023]. s. 413-427. Dostupné z: https://ieeexplore.ieee.org/abstract/document/6234427

[48] VON LEWINSKI, Kai. Geschichte des Datenschutzrechts von 1600 bis 1977. In: *Freiheit-Sicherheit-Öffentlichkeit*. Heidelberg: Nomos Verlagsgesellschaft mbH & Co. KG, 2009, s. 196–220.

[49] LIU, Peng; CHAO, Wang. *Computational Advertising: Market and Technologies for Internet Commercial Monetization*. Boca Raton: CRC Press, 2020.

[50] MCDONALD, Aleecia M., CRANOR, Lorrie Faith. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* [online]. 2008, roč. 4, č. 3 [cit. 6. 3. 2022], s. 543. Dostupné z HeinOnline: https://heinonline.org/HOL/Page?handle=hein.journals/isjlpsoc4&div=27&g_sent=1&casa_token=

[51] MCNAIR, Brian. Journalism and Democracy. In: *Journalism and Democracy* [online]. New York: Routledge, 2009, s. 257–269 [cit. 20. 1. 2023]. ISBN 978-0-203-87768-5. Dostupné z: doi:10.4324/9780203877685-27

[52] MERCADO KIERKEGAARD, Sylvia. How the cookies (almost) crumbled: Privacy & lobbyism. *Computer Law & Security Review* [online]. 2005, roč. 21, č. 4 [cit. 2. 2. 2023], s. 310–322. ISSN 0267-3649. Dostupné z: doi:10.1016/j.clsr.2005.06.002

[53] MÍŠEK, Jakub. Souhlas se zpracováním osobních údajů za časů Internetu. *Revue pro právo a technologie* [online]. 2014, roč. 5, č. 9 [cit. 23. 1. 2023], s. 3–74. Dostupné z: https://journals.muni.cz/revue/article/view/5017

[54] MOORE, Adam D. *Privacy rights: Moral and legal foundations*. Pennsylvania: Penn State Press, 2010.

[55] NOUWENS, Midas et al. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In: *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* [online]. New York, NY, USA: Association for Computing Machinery, 2020, s. 1–13 [cit. 2. 2. 2023]. ISBN 978-1-4503-6708-0. Dostupné z: https://doi.org/10.1145/3313831.3376321

[56] PAPAKONSTANTINOU, Vagelis, DE HERT, Paul. The Amended EU Law on ePrivacy and Electronic Communications after Its 2011 Implementation; New Rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights. *John Marshall Journal of Computer and Information Law* [online]. 2011, roč. 29, č. 1 [cit. 2. 2. 2023], s. 29–75. ISSN 1078-4128. Dostupné z HeinOnline: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jmjcila29&section=5

[57] PURTOVA, Nadezhda. From knowing by name to targeting: the meaning of identification under the GDPR. *International Data Privacy Law* [online]. 2022, roč. 12, č. 3 [cit. 2. 2. 2023], s. 163–183. ISSN 2044-3994. [cit. 2. 2. 2023]. Dostupné z: doi:10.1093/idpl/ipac013

[58] REN, Tongwei et al. An Analysis of First-Party Cookie Exfiltration due to CNAME Redirections. In: *Workshop on Measurements, Attacks, and Defenses for the Web*: *Proceedings 2021 Workshop on Measurements, Attacks, and Defenses for the Web* [online]. Virtual: Internet Society, 2021 [cit. 4. 1. 2023]. ISBN 978-1-891562-67-9. Dostupné z: doi:10.14722/madweb.2021.23018

[59] RICHARDS, Neil. *Intellectual privacy: rethinking civil liberties in the digital age*. Oxford, UK: Oxford University Press, 2015, 220 s. ISBN 978-0-19-994614-3.

[60] RICHARDS, Neil M., HARTZOG, Woodrow. Taking Trust Seriously in Privacy Law. *Stanford Technology Law Review* [online]. 2016, roč. 19, č. 3, [cit. 30. 1. 2021], s. 431-472. Dostupné z HeinOnline: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/stantlr19&section=19

[61] ROBERTSON, Adi. Google antitrust suit takes aim at Chrome's Privacy Sandbox. In: *The Verge.* [online] 16. 3. 2021 [cit. 6. 3. 2022]. Dostupné z: https://www.theverge.com/2021/3/16/22333848/google-antitrust-lawsuit-texas-complaint-chrome-privacy

[62] RUSSINOVICH, Mark. Sony, Rootkits and Digital Rights Management Gone Too Far. In: *Mark's Blog* [online] 31. 10. 2015 [cit. 11. 1. 2023]. Dostupné z: https://web.archive.org/web/20150317040653/http://blogs.technet.com/b/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx

[63] RYAN, Johnny. Regulatory complaint concerning massive, web-wide data breach by Google and other "ad tech" companies under Europe's GDPR. In: brave [online] 12. 9. 2018 [cit. 23. 1. 2023]. Dostupné z: https://brave.com/adtech-data-breach-complaint/

[64] RYAN, Johnny. Update on GDPR complaint (RTB ad auctions). In: *brave* [online] 28. 1. 2019 [cit. 23. 1. 2023]. Dostupné z: https://brave.com/update-rtb-ad-auction-gdpr/

[65] RYAN, Johnny. ICCL sues DPC over failure to act on massive Google data breach. In: *Irish Council for Civil Liberties.* [online] 15. 3. 2022 [cit. 23. 1. 2023]. Dostupné z: https://www.iccl.ie/news/iccl-sues-dpc-over-failure-to-act-on-massive-google-data-breach/

[66] SCHUH, Justin. Building a more private web: A path towards making third party cookies obsolete. In: *Chromium Blog*[online]. 14. 1. 2020 [cit. 7. 8. 2021]. Dostupné z: https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html

[67] SCHUH, Justin. Building a more private web. In: *Google* [online] 22. 8. 2019 [cit. 26. 2 2022]. Dostupné z: https://blog.google/products/chrome/building-a-more-private-web/

[68] SMIT, Edith G., VAN NOORT, Guda, VOORVELD, Hilde A. M. Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior* [online]. 2014, roč. 32, s. 15–22. ISSN 0747-5632. [cit. 2. 2. 2023]. Dostupné z: doi:10.1016/j.chb.2013.11.008

[69] SPEICHER, Till et al. Potential for Discrimination in Online Targeted Advertising. In: *Conference on Fairness, Accountability and Transparency*: *Proceedings of the 1st Conference on Fairness, Accountability and Transparency* [online]. PMLR, 2018 [cit. 6. 3. 2022], s. 5–19. Dostupné z: https://proceedings.mlr.press/v81/speicher18a.html

[70] THOMSON, Martin. A *Privacy Analysis of Google's Topics Proposal*. In: github [online]. 6. 1. 2023 [cit. 28. 5. 2023]. Dostupné z: https://mozilla.github.io/ppa-docs/topics.pdf s. 12.

[71] TOMÍŠEK, Jan. Cookies a GDPR. *Právní rozhledy* [online]. 2018, roč. 26, č. 20 [cit. 6. 2. 2023], s. 687–696. Dostupné z beck-online: https://www.beck-online.cz/bo/chapterview-document.seam?documentId=nrptembrhbpxa4s7giyf6427gy4do

[72] TOMÍŠEK, Jan. Souhlasy s cookies a přístupy k ochraně osobních údajů [online]. *Právník*. 2022, roč. 161, č. 6 [cit. 6. 2. 2023], s. 561–577. Dostupné z: https://www.ilaw.cas.cz/casopisy-a-knihy/casopisy/casopis-pravnik/archiv/2022/2022-06.html?a=3686

[73] TUROW, J. et al. Americans Reject Tailored Advertising and Three Activities that Enable It. In: *SSRN* [online]. 29. 9. 2009 [cit. 2. 2. 2023]. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214.

[74] UTZ, Christine et al. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In: *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* [online]. New York, NY, USA: Association for Computing Machinery, 2019, s. 973–990 [cit. 2. 1. 2022]. CCS '19. ISBN 978-1-4503-6747-9. Dostupné z: doi:10.1145/3319535.3354212

[75] VEALE, Michael, BORGESIUS, Frederik J. Zuiderveen. Adtech and real-time bidding under European data protection law. *German Law Journal* [online]. 2022, roč. 23, č. 2 [cit. 6. 2. 2023], s. 226–256. Dostupné z: https://www.cambridge.org/core/journals/german-law-journal/article/adtech-and-realtime-bidding-under-european-data-protection-law/017F027B4E78EBCAE1DCBC1E12B93B9D

[76] WARREN, Samuel D., BRANDEIS, Louis D. Right to privacy. *Harvard Law Review* [online]. 1890, roč. 4, č. 5 [cit. 6. 2. 2023], s. 193–220. Dostupné z JSTOR: https://www.jstor.org/stable/1321160

[77] WHITE, Alexandra. Privacy Budget. In: *Chrome Developers* [online] 4. 3. 2022. [cit. 28. 10. 2022]. Dostupné z: https://developer.chrome.com/docs/privacy-sandbox/privacy-budget/

[78] WILANDER, John. Intelligent Tracking Prevention. In: *WebKit* [online]. 5. 6. 2017 [cit. 26. únor 2022]. Dostupné z: https://webkit.org/blog/7675/intelligent-tracking-prevention/

[79] WILANDER, John. Full Third-Party Cookie Blocking and More. In: *WebKit* [online]. 2020. [cit. 26. 2. 2022]. Dostupné z: https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/

[80] YUAN, Shuai et al. Internet Advertising: An Interplay among Advertisers, Online Publishers, Ad Exchanges and Web Users. In: *arXiv* [online]. 2. 7. 2012 [cit. 18. 11. 2022]. Dostupné z: http://arxiv.org/abs/1206.1754

[81] YUAN, Shuai, WANG, Jun; ZHAO, Xiaoxue. Real-time bidding for online advertising: measurement and analysis. In: *Proceedings of the Seventh International Workshop on Data Mining for Online Advertising* [online]. 2013 [cit. 18. 11. 2022], s. 1–8. Dostupné z ACM Digital Library: https://dl.acm.org/doi/abs/10.1145/2501040.2501980

[82] ZHANG, Kaifu, KATONA, Zsolt. Contextual advertising. *Marketing Science* [online]. 2012, roč. 31, č. 6 [cit. 6. 2. 2023], s. 980–994. Dostupné z: https://pubsonline.informs.org/doi/abs/10.1287/mksc.1120.0740

[83] ZHENG, Guangzhi, PELTSVERGER, Svetlana. Web analytics overview. In: *Encyclopedia of Information Science and Technology, Third Edition* [online]. IGI Global, 2015 [cit. 6. 2. 2023], s. 7674–7683. Dostupné z: https://www.igi-global.com/chapter/web-analytics-overview/112470

[84] ZITTRAIN, Jonathan. How to Exercise the Power You Didn't Ask For. *Harvard Business Review* [online]. 19. 9. 2018 [cit. 30. 10. 2022]. ISSN 0017-8012. Dostupné z: https://hbr.org/2018/09/how-to-exercise-the-power-you-didnt-ask-for

[85] Autorité de protection des données. The BE DPA to restore order to the online advertising industry: IAB Europe held responsible for a mechanism that infringes the GDPR In: *Autorité de protection des données* [online] 2. 2. 2022 [cit. 23. 1. 2023]. Dostupné z: https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr

[86] Competition and Markets Authority. Online platforms and digital advertising. In *Competition and Markets Authority*. [online]. 1. 7. 2020. Dostupné z: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf

[87] Competition and Markets Authority. CMA to keep 'close eye' on Google as it secures final Privacy Sandbox commitments. In: *GOV.UK*. [online] 11. 2. 2022 [cit. 26. 2. 2022]. Dostupné z: https://www.gov.uk/government/news/cma-to-keep-close-eye-on-google-as-it-secures-final-privacy-sandbox-commitments

[88] Early design review for the Topics API #726. 25. 3. 2023 [cit. 28. 5. 2023]. Dostupné z: https://github.com/w3ctag/design-reviews/issues/726#issuecomment-1379908459

[89] Electronic Frontier Foundation. SunnComm MediaMax Security Vulnerability FAQ. In: *Electronic Frontier Foundation* [online]. 19. 7. 2007 [cit. 11. 1. 2023]. Dostupné z: https://www.eff.org/pages/sunncomm-mediamax-security-vulnerability-faq

[90] Evropská komise. Special Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union. In: *Evropská komise*. [online]. Červen 2011 [cit. 2. 2. 2023]. Dostupné z: https://joinup.ec.europa.eu/sites/default/files/document/2014-12/Part%20I%20of%20Special%20Eurobarometer%20359%20-%20Attitudes%20on%20Data%20Protection%20and%20Electronic%20Identity%20in%20the%20European%20Union.pdf

[91] Evropská komise. Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers. In: *Evropská komise* [online]. 30. 1. 203 [cit. 2. 2. 2023]. Dostupné z: https://op.europa.eu/en/publication-detail/-/publication/8b950a43-a141-11ed-b508-01aa75ed71a1/language-en

[92] Evropský sbor pro ochranu osobních údajů. Prohlášení Evropského sboru pro ochranu osobních údajů o revizi nařízení o soukromí a elektronických komunikacích a jejím dopadu na ochranu fyzických osob v souvislosti se soukromím a důvěrným charakterem jejich komunikace. In: *European Data Protection Board*. [online]. 5. 5. 2018 [cit. 16. 7. 2018]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/edpb_statement_on_eprivacy_cs_0.pdf

[93] Evropský sbor pro ochranu osobních údajů. Pokyny 4/2019 k článku 25 Záměrná a standardní ochrana osobních údajů Verze 2.0 Přijato dne 20. října 2020. In: *European Data Protection Board.* [online]. 20. 10. 2020. [cit. 31. 1. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2021-04/
edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_cs.pdf

[94] Evropský sbor pro ochranu osobních údajů. Stanovisko č. 5/2019 ke vzájemnému působení mezi směrnicí o soukromí a elektronických komunikacích a obecným nařízením o ochraně osobních údajů (GDPR), zejména pokud jde o příslušnost, úkoly a pravomoci úřadů pro ochranu údajů. In: *European Data Protection Board* [online]. 12. 3. 2019. [cit. 1. 2. 2023]. Dostupné z: https://edpb.europa.eu/sites/default/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_cs.pdf

[95] Evropský sbor pro ochranu osobních údajů. Pokyny č. 8/2020 k cílení na uživatele sociálních médií ze dne 13. dubna 2021. In: *European Data Protection Board* [online]. 13. 4. 2021. [cit. 1. 2. 2023] Dostupné z: https://edpb.europa.eu/system/files/2021-11/edpb_guidelines_082020_on_the_c_cs_0.pdf

[96] Evropský sbor pro ochranu osobních údajů. Závazné rozhodnutí 1/2021 ve věci sporu ohledně návrhu rozhodnutí irského dozorového úřadu týkajícího se společnosti WhatsApp Ireland podle čl. 65 odst. 1 písm. a) obecného nařízení o ochraně osobních údajů. In: *European Data Protection Board* [online]. 28. 7. 2021 [31. 1. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2022-03/
edpb_bindingdecision_202101_ie_sa_whatsapp_redacted_cs.pdf bod 191.

[97] Evropský sbor pro ochranu osobních údajů. Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them Version 1.0 Adopted on 14 March 2022. In: European Data Protection Board [online]. 14. 3. 2022 [cit. 1. 2. 2023] Dostupné z: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf

[98] Evropský sbor pro ochranu osobních údajů. Binding Decision 4/2022 on the dispute submitted by the Irish SA on Meta Platforms Ireland Limited and its Instagram service (Art. 65 GDPR) Adopted on 5 December 2022 In: *European Data Protection Board.* [online]. 5. 12. 2022 [cit. 31. 1. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2023-01/edpb_binding_decision_202204_ie_sa_meta_instagramservice_redacted_en.pdf

[99] Evropský sbor pro ochranu osobních údajů. Report of the work undertaken by the Cookie Banner Taskforce, Adopted on 17 January 2023. In: *European Data Protection Board* [online]. 17. 1. 2023. [cit. 1. 2. 2023]. Dostupné z: https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf

[100] GlobalStats. Browser Market Share Worldwide. In: *StatCounter Global Stats* [online] nedatováno [cit. 31. 1. 2023]. Dostupné z: https://gs.statcounter.com/browser-market-share

[101] Google. How We're Protecting Your Online Privacy.In: *The Privacy Sandbox*. [online] nedatováno [cit. 18. 1. 2023]. Dostupné z: https://privacysandbox.com/open-web/

[102] Google. IP masking in Universal Analytics. In: Analytics Hepl [online]. Nedatováno [cit. 12.2. 2023]. Dostupné z: https://support.google.com/analytics/answer/2763052?hl=en&ref_topic=2919631

[103] hotjar. What Are Session Recordings (Session Replays) + How to Use Them. In: *hotjar*. [online] 31. 1. 2023 [cit. 23. 1. 2023]. Dostupné z: https://www.hotjar.com/session-recordings/

[104] Information Commissioner's Office. How do we comply with the cookie rules? In: *Information Commissioner's Office* [online]. [cit. 1. 2. 2023]. Dostupné z: https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/

[105] Information Commissioner's Office. ICO calls on Google and other companies to eliminate existing privacy risks posed by adtech industry. In: *Information Commissioner's Office*. [online] 25. 11. 2021 [cit. 23. 1. 2023]. Dostupné z: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/11/ico-calls-on-google-and-other-companies-to-eliminate-existing-privacy-risks-posed-by-adtech-industry/

[106] Information Commissioner's Office. Data protection and privacy expectations for online advertising proposals. In: *Information Commissioner's Office.* [online]. 25. 11. 2021 [cit. 2. 2. 2023]. Dostupné z: https://ico.org.uk/media/about-the-ico/documents/4019050/opinion-on-data-protection-and-privacy-expectations-for-online-advertising-proposals.pdf

[107] Interactive Advertising Bureau. ePrivacy Regulation. In: *Interactive Advertising Bureau* online]. Nedatováno. [cit. 20. 1 2023]. Získáno z: https://iabeurope.eu/proposed-eprivacy-regulation/

[108] Interactive Advertising Bureau. A Guide to the Post Third-Party Cookie Era. In: *Interactive Advertising Bureau* [online]. Březen 2022 [cit. 31. 1. 2023]. Dostupné z: https://iabeurope.eu/wp-content/uploads/2022/03/IAB-Europe-Guide-to-a-Post-Third-Party-Cookie-Era-March-2022.pptx.pdf

[109] Interactive Advertising Bureau. IAB Europe Transparency & Consent Framework Policies. In: *Interactive Advertising Bureau*. [online]. 21. 6. 2022 [cit. 22. 1. 2023]. Dostupné z: https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

[110] Internet Engineering Task Force. Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content [online]. Červen 2014. [cit. 1. 2. 2023]. In: *Data Tracker*. Dostupné z: https://datatracker.ietf.org/doc/html/rfc7231#section-5

[111] noyb. noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints In: *nyob* [online] 31. 5. 202 [cit. 24. 1. 2023]. Dostupné z: https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints

[112] Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 4/2007 k pojmu osobní údaje In: *Evropská komise* [online]. 20. 6. 2007 [cit. 2. 2. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_cs.pdf

[113] Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 4/2012 k výjimce z požadavku na souhlas s cookies. In: *Evropská komise* [online]. 7. 6. 2012 [cit. 23. 1. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_cs.pdf

[114] Pracovní skupina pro ochranu údajů zřízená podle článku 29. Stanovisko č. 6/2014 k pojmu oprávněných zájmů správce údajů podle článku 7 směrnice 95/46/ES In: *Evropská komise* [online]. 9. 4. 2014 [cit. 2. 2. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_cs.pdf

[115] Pracovní skupina pro ochranu osobních údajů zřízená podle článku 29. Stanovisko č. 9/2014 k uplatňování směrnice 2002/58/ES na otisky zařízení. In: *Evropská komise* [online]. 25. 11. 2014 [cit. 1. 2. 2023]. Dostupné z: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf

[116] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Presidency note. 2017/0003 (COD), 10866/17. In: *EUR-Lex* [online]. 3. 7. 2017 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10866_2017_INIT

[117] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003 (COD), 11995/17. In: *EUR-Lex* [online]. 8. 9. 2017 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11995_2017_INIT

[118] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency. 2017/0003 (COD), 15333/17. In: *EUR-Lex* [online]. 5. 12. 2017 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15333_2017_INIT

[119] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion paper 2017/0003(COD), 5165/18. In: *EUR-Lex* [online]. 11. 1. 2018 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5165_2018_INIT

[120] Viz Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency discussion. 2017/0003(COD), 7207/18. In: *EUR-Lex* [online]. 22. 3. 2018 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_7207_2018_INIT

[121] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 017/0003(COD), 10975/18. In: *EUR-Lex* [online]. 10. 6. 2018, [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10975_2018_INIT

[122] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003(COD), 10975/18. In: *EUR-Lex* [online]. 10. 7. 2018 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10975_2018_INIT

[123] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Examination of the Presidency text. 2017/0003(COD), 13256/18. In: *EUR-Lex* [online]. 19. 10. 2018 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_13256_2018_INIT

[124] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Discussion on possible compromise solutions 2017/0003(COD), 5934/19. In: *EUR-Lex* [online]. 4. 2. 2019 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5934_2019_INIT

[125] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). 2017/0003(COD), 11291/19. In: *EUR-Lex* [online]. 26. 7. 2019 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_11291_2019_INIT

[126] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) 2017/0003(COD), 5979/20. In: *EUR-Lex* [online]. 21. 2. 2020 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5979_2020_INIT

[127] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Progress report. 2017/0003(COD), 13106/20. In: *EUR-Lex* [online]. 23. 11. 2020 [cit. 27. 5. 2023]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-13106-2020-INIT/en/pdf

[128] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulati-on on Privacy and Electronic Communications) – Presidency discussion paper 2017/0003(COD), 9243/20. In: *EUR-Lex* [online]. 6. 6. 2020 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9243_2020_INIT

[129] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulati-on on Privacy and Electronic Communications). 2017/0003(COD), 9931/20. In: *EUR-Lex* [online]. 4. 11. 2020 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9931_2020_INIT

[130] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). 2017/0003(COD), 5008/2. In: *EUR-Lex* [online]. 5. 1. 2021 [cit. 27. 5. 2023]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-5008-2021-INIT/en/pdf

[131] Rada Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Mandate for negotiations with EP. 2017/0003(COD), 6087/21. In: *EUR-Lex* [online]. 10. 2. 2021 [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT

[132] Request for Position: Topics API #622. In: github [online]. 17. 3. 2022 [cit. 28. 5. 2023]. Dostupné z: https://github.com/mozilla/standards-positions/issues/622

[133] Spolek pro ochranu osobních údajů. Stanovisko Spolku pro ochranu osobních údajů k právní úpravě cookies v České republice od začátku roku 2022. In: *Spolek pro ochranu osobních údajů* [online]. 15. 12. 2021 [cit. 1. 2. 2023]. Dostupné z: https://www.ochranaudaju.cz/wp-content/uploads/2021/12/Stanovisko_cookies_2021_final.pdf

[134] The Topics API #111. In: github [online]. 20. 12. 2022 [cit. 28. 5. 2023]. Dostupné z: https://github.com/WebKit/standards-positions/issues/111

[135] Úřad pro ochranu osobních údajů. Doporučení k zpracování cookies a obdobných prostředků sledování od 25. května 2018. In: *Úřad pro ochranu osobních údajů* [online]. 25. 6. 2020 [cit. 6. 7. 2018]. Dostupné z: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=42915

[136] Úřad pro publikace Evropské unie. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). 2017/0003(COD), 52017PC0010. In: *EUR-Lex* [online]. [cit. 27. 5. 2023]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A52017PC0010

[137] w3schools. HTML Web Storage API. In: *w3schools.* [online] nedatováno [cit. 18. 1. 2023]. Dostupné z: https://www.w3schools.com/html/html5_webstorage.asp

---

INSTRUCTIONS FOR AUTHORS

The Review of Law and Technology is a peer-reviewed scientific journal for technological areas of law and jurisprudence.

Since 1st January 2015 the journal is listed in the List of non-impact peer-reviewed journals published in the Czech Republic and since 24th June 2015 in ERIH PLUS database.

Contributions submitted for the Topic and Discussion sections are anonymously peer-reviewed by at least two independent reviewers and the final decision on publication is the in the sole discretion of the editorial board. Review process takes approximately one month. The submissions are not subject to language proofreading.

Contributions shall be submitted through our web-based system available at https://journals.muni.cz/revue

RECOMMENDED EXTENT OF THE CONTRIBUTIONS:

Discussion:	15 – 30 standard pages
Annotation:	2 – 10 standard pages
Essays:	5 – 10 standard pages
Thesis review:	2 – 5 standard pages
Book review:	2 – 5 standard pages
Topic:	30 – 50 standard pages

(including spaces, footnotes and bibliography)

CITATIONS FORMAT

Citations shall be in accordance with the ISO 690:2011 citation standard.

Referencing examples are available in interpretations of the aforementioned citation standard (e. g. at www.ezdroje.muni.cz/prehled/zdroj.php?lang=en&id=441).

Individual sources are referenced in the text by upper index. The actual citation of the source is then contained in a footnote.

DEADLINES FOR CONTRIBUTIONS SUBMISSIONS

For the summer issue: 28th February

For the winter issue: 31st August

The Review of Law and Technology is a gold open access journal.

Contributions are included into respective electronic legal information systems operated by Wolters Kluwer ČR, a. s. (ASPI), Nakladatelství C. H. BECK, s. r. o. (beck-online.cz) and ATLAS consulting spol. s r. o. (CODEXIS).

Detailed information about the publication process, structure and format of the contributions, the review process and copyright are available in the "For authors" section at https://journals.muni.cz/revue/about/submissions. Further information is available upon request addressed to editorial staff (contact e-mail: revue@law.muni.cz).

REVIEW OF LAW AND TECHNOLOGY

VOLUME 14 | YEAR 2023 | NUMBER 27

Review of Law and Technology
Peer-reviewed scientific journal for technological areas of law and jurisprudence, listed in the List of non-impact peer-reviewed journals published in the Czech Republic and ERIH PLUS database.
Only the contributions submitted for the Discussion and Topic sections are peer-reviewed.
Published bi-annually. This issue was published on 30th June 2023.
ISSN 1804-5383 (Print), ISSN 1805-2797 (Online), Ev. nr. MK ČR E 19707
Published by: Masaryk University, Žerotínovo nám. 9, 601 77 Brno, Czech Republic, ID-Nr. 00216224
Editor-in-chief and contact person: JUDr. Ing. František Kasl, Ph.D., Institute of Law and Technology, Faculty of Law, Masaryk University, Veveří 70, 611 80 Brno, Czech Republic, tel: +420 549 49 5545, contact e-mail: frantisek.kasl@muni.cz | revue@law.muni.cz | https://journals.muni.cz/revue
Deputy editor-in-chief: Mgr. Anna Blechová
Editorial Staff: JUDr. Mgr. Jakub Harašta, Ph.D., JUDr. MgA. Jakub Míšek, Ph.D.
Editor: Martin Erlebach
Editorial Board: prof. JUDr. Radim Polčák, Ph.D. (honorary chairman), JUDr. Zuzana Adamová, Ph.D., prof. JUDr. Michael Bogdan, B.A., LL.M., jur. dr. (Lund), JUDr. Marie Brejchová, LL.M., JUDr. Jiří Čermák, prof. JUDr. Bc. Tomáš Gřivna, Ph.D., doc. JUDr. Josef Kotásek, Ph.D., JUDr. Bc. Zdeněk Kučera, Ph.D., Mgr. Ing. Zbyněk Loebl, LL.M., JUDr. Ján Matejka, Ph.D., prof. RNDr. Václav Matyáš,M.Sc., Ph.D., doc. JUDr. Matěj Myška, Ph.D., Mgr. Antonín Panák, LL.M., Mgr. Bc. Adam Ptašnik, Ph.D., JUDr. Danuše Spáčilová, JUDr. Eduard Szattler, Ph.D., JUDr. Tomáš Ščerba, Ph.D.
Layout: Mgr. Martin Loučka, doc. JUDr. Matěj Myška, Ph.D.
Print: POINT CZ, s.r.o., Milady Horákové 20, 602 00 Brno
The publication of this issue of the Review of Law and Technology was funded by the project „Právo a technologie XI", MUNI/A/1293/2022.

MUNI LAW

Ústav práva a technologií

Rádi bychom Vás pozvali také na následující akce konané v druhé polovině roku 2023:

Konference Lidé, zdravotnictví a právo

XIII. ročník akce zaměřené na zdravotnické právo pořádané ve spolupráci Všeobecné zdravotní pojišťovny České republiky a Masarykovy univerzity v Brně se uskuteční ve dnech 14. a 15. září 2023 v areálu univerzitního kampusu Masarykovy univerzity, Kamenice 5, Brno.
Více informací na: https://www.vzpkonference.cz/konference-2023/

Legal challenges of disruptive technology. From AI to Quantum

Tento mezinárodní workshop věnovaný novým technologiím spolupořádaný Ústavem práva a technologií Právnické fakulty Masarykovy univerzity se bude konat 27.-28. října v polské Varšavě.
Příspěvky jsou přijímány do 31. července.
Více informací na: https://www.kozminski.edu.pl/en/international-scientific--workshop-i-legal-challenges-disruptive-technologies

Mezinárodní konference Cyberspace

Již XXI. ročník tradiční podzimní akce pořádané Ústavem práva a technologií Právnické fakulty Masarykovy univerzity společně s Fakultou sociálních studií Masarykovy univerzity a European Academy of Law and ICT se uskuteční ve dnech 24. a 25. listopadu 2023 v prostorách Právnické fakulty Masarykovy univerzity, Veveří 158/70, Brno.
Příspěvky jsou přijímány do 31. července.
Více informací na: https://cyberspace.muni.cz/

Diskuze

Anotace

Essays

Recenze závěrečných prací

Recenze

Téma

MUNI PRESS