zborník

Bratislavské právnické fórum 2024
PRÁVO A TECHNOLÓGIE V 21. STOROČÍ OPTIKOU EURÓPSKEHO PRÁVA

Bratislava legal forum 2024
LAW AND TECHNOLOGY IN THE 21ST CENTURY THROUGH THE LENS OF EUROPEAN LAW

Dražová, Ťažká (zost.)

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

Zborník

Bratislavské právnické fórum 2024
Právo a technológie v 21. storočí optikou európskeho práva

zborník príspevkov z medzinárodnej vedeckej konferencie
„Bratislavské právnické fórum 2024"
ktorá sa konala 17. – 19. septembra 2024
na Právnickej fakulte Univerzity Komenského v Bratislave

Bratislava legal forum 2024
Law and technology in the 21st century through the lens of European law

collection of papers from the international scientific conference
„Bratislava legal forum 2024"
which was held on 17. – 19. september 2024
at the Faculty of law, Comenius University in Bratislava

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

2024

Bratislavské právnické fórum 2024 : právo a technológie v 21. storočí optikou európskeho práva / Petra Dražová, Veronika Ťažká (zost.). Bratislava : Právnická fakulta Univerzity Komenského v Bratislave, 2024. 150 s. ISBN 978-80-7160-728-1.

Zostavovatelia: Petra Dražová, Veronika Ťažká

Návrh obálky: Jozef Andraško

Všetky príspevky prešli dvojitým anonymným recenzným konaním.

1. vydanie
Právnická fakulta Univerzity Komenského v Bratislave
2024

ISBN (e-verzia) 978-80-7160-728-1

Spoluorganizátori 10. ročníka konferencie Bratislavské právnické fórum

MINISTERSTVO ZAHRANIČNÝCH VECÍ A EURÓPSKYCH ZÁLEŽITOSTÍ SLOVENSKEJ REPUBLIKY

MINISTERSTVO SPRAVODLIVOSTI SLOVENSKEJ REPUBLIKY

NAJVYŠŠÍ SÚD SLOVENSKEJ REPUBLIKY

SLOVENSKÁ ADVOKÁTSKA KOMORA

Konferencia sa uskutočnila s finančnou podporou

Visegrad Fund

CENTRAL EUROPEAN FOUNDATION

CEF

Obsah

NARIADENIE EP A RADY EÚ 2024/1938 O NORMÁCH KVALITY PRE LÁTKY ĽUDSKÉHO PÔVODU URČENÉ PRE HUMÁNNE POUŽITIE A ZRUŠENÍ SMERNÍC 2002/98/ES A 2004/23/ES A JEHO MOŽNÝ DOPAD NA REGULATÓRNY RÁMEC 3D BIOTLAČE.

EP AND EU COUNCIL REGULATION 2024/1938 ON QUALITY STANDARDS FOR SUBSTANCES OF HUMAN ORIGIN INTENDED FOR HUMANE USE AND REPEAL OF DIRECTIVES 2002/98/EC AND 2004/23/EC AND ITS POSSIBLE IMPACT ON THE REGULATORY FRAMEWORK OF 3D BIOPRINTING

Dominika Zábavská[1]

Abstrakt: Jedným z následkov technologického pokroku dosiahnutého počas 4-tej priemyselnej revolúcie je aj nárast interdisciplinárnej implementácie technológií. To však okrem zjavných benefitov prináša aj výzvy, medzi ktoré nepochybne patrí aj vágny legislatívny rámec novovznikajúcich odvetví. Za účelom stanovenia regulačného rámca využívania technológie 3D biotlače, je tak potrebné skúmať právnu úpravu prijatú vo všetkých aspektoch, ktorých sa biotlač dotýka.
Cieľom autora príspevku tak bude skúmať novú prijatú právnu úpravu na úrovní EÚ a jej možný dopad na regulačný rámec 3D biotlače v právnom prostredí Slovenskej republiky ako členského štátu Európskej únie.

Kľúčové slová: 4-tá priemyselná revolúcia, biotlač, biomedicínsky výskum, tkanivové inžinierstvo, regulačný rámec

Abstract: One of the consequences of the technological progress achieved during the 4th industrial revolution is the increase in the interdisciplinary implementation of technologies. However, in addition to the obvious benefits, this also brings challenges, which undoubtedly include the vague legislative framework of emerging industries. In order to determine the regulatory framework for the use of 3D bioprinting technology, it is therefore necessary to examine the legislation adopted in all aspects that bioprinting touches.

[1] Univerzita Pavla Jozefa Šafárika v Košiciach, Právnická fakulta, Katedra obchodného a hospodárskeho práva

The goal of the author of the paper will be to examine the new legal regulation adopted at the EU level and its possible impact on the regulatory framework of 3D bioprinting in the legal environment of the Slovak Republic as a member state of the European Union.

Key words: 4th industrial revolution, bioprinting, biomedical research, tissue engineering, regulatory framework

Úvod

Rámec EÚ pre bezpečnosť a kvalitu látok ľudského pôvodu pred prijatím nariadenia Európskeho parlamentu a Rady EÚ č. 2024/1938 o normách kvality pre látky ľudského pôvodu určené pre humánne použitie pozostával najmä z 3 hlavných smerníc a to smernici o krvi[2] (ktorá sa nariadením ruší), smernici o tkanivách a bunkách[3] (ktorá sa nariadením ruší) a smernici o orgánoch[4].
V každej z týchto smerníc boli ustavonujúce normy bezpečnosti a kvality pre všetky kroky od darovania a odberu z tela darcu, cez testovanie, spracovanie, skladovanie a distribúciu až po prípadné použitie na tele pacientov.
Nová právna regulácia na úrovni Európskej únie v podobe Nariadenia sa vzťahuje na krv, tkanivá a bunky a je prepojená so smernicou o orgánoch, najmä pokiaľ ide o užšiu spoluprácu medzi príslušnými orgánmi členských štátov pre krv, tkanivá, bunky a orgány, a pre požiadavky týkajúce sa vigilancie.
Ak možno krv, tkanivá a bunky použiť pri výrobe zdravotníckych výrobkov, ktoré sú regulované inými právnymi predpismi Únie, alebo ako ich vstupnú a východiskovú surovinu, rámec pre látky ľudského pôvodu sa uplatňuje na prvé činnosti v reťazci (*darovanie, odber, testovanie*), zatiaľ čo tieto neskoršie činnosti (*výroba, skladovanie, distribúcia atď.*) sú regulované inými vhodnými legislatívnymi rámcami (napr. legislatívnym rámcom pre lieky vrátane liekov na inovatívnu liečbu alebo zdravotnícke pomôcky[5]). V praxi sú však zavedené určité mechanizmy na zabezpečenie súladu medzi právnymi predpismi o krvi, tkanivách a bunkách

[2] Smernica Európskeho parlamentu a Rady 2002/98/ES z 27. januára 2003, ktorou sa stanovujú normy kvality a bezpečnosti pre odber, skúšanie, spracovanie, uskladňovanie a distribúciu ľudskej krvi a zložiek krvi a ktorou sa mení a dopĺňa smernica 2001/83/ES

[3] Smernica 2004/23/es Európskeho parlamentu a Rady z 31. marca 2004 ustanovujúca normy kvality a bezpečnosti pri darovaní, odoberaní, testovaní, spracovávaní, konzervovaní, skladovaní a distribúcii ľudských tkanív a buniek

[4] Smernica Európskeho parlamentu a Rady 2010/53/EÚ zo 7. júla 2010 o normách kvality a bezpečnosti ľudských orgánov určených na transplantáciu

[5] pozri Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach, zmene smernice 2001/83/ES, nariadenia (ES) č. 178/2002 a nariadenia (ES) č. 1223/2009 a o zrušení smerníc Rady 90/385/EHS a 93/42/EHS

a predmetnými priľahlými rámcami, pričom nové Nariadenie má potenciál práve spoluprácu medzi týmito priľahlými rámcami posilniť[6].
V tomto príspevku, tak bude cieľom autorky skúmať novú prijatú právnu úpravu na úrovní EÚ a jej možný dopad na regulačný rámec 3D biotlače v právnom prostredí Slovenskej republiky ako členského štátu Európskej únie, a to využitím metód faktickej analýzy a syntézy skúmania právneho rámca biomedicínskeho výskumu a 3D biotlače v prostredí Slovenskej republiky ako členského štátu Európskej únie.

Nariadenie EP a Rady EÚ 2024/1938 o normách kvality pre látky ľudského pôvodu určené pre humánne použitie a zrušení smerníc 2002/98/ES a 2004/23/ES

Európska komisia prijala 14. júla 2022 návrh zákona na revíziu existujúcich pravidiel, čo bolo možné považovať za záverečný stavebný kameň širšej revízie rámca pre krv, tkanivá a bunky.
Znenie Nariadenia EP a Rady EÚ 2024/1938 o normách kvality pre látky ľudského pôvodu určené pre humánne použitie a zrušení smerníc 2002/98/ES a 2004/23/ES (ďalej ako „ *Nariadenie*“) Európsky parlament formálne schválil 24. apríla 2024 a Rada 27. mája. 2024, pričom Nariadenie bolo spoluzákonodarcami podpísané 13. júna 2024 a 17. júla 2024 uverejnené v úradnom vestníku.
Cieľom nového Nariadenia je zlepšiť bezpečnosť a kvalitu krvi, tkanív a buniek používaných v zdravotníctve. Zahŕňa širokú škálu činností od registrácie a testovania darcov, odberu a spracovania až po aplikáciu na ľudí a monitorovanie klinických výsledkov látok ľudského pôvodu.
Nariadenie stanovuje opatrenia, ktoré stanovujú vysoké štandardy kvality a bezpečnosti pre všetky látky ľudského pôvodu určené na použitie u ľudí a pre činnosti súvisiace s týmito látkami. Zabezpečuje vysokú úroveň ochrany ľudského zdravia, najmä pre darcov, príjemcov a potomkov z medicínsky asistovanej reprodukcie, a to aj posilnením kontinuity dodávok kritických látok ľudského pôvodu[7].
Ako sme už vyššie uviedli, Nariadenie ruší predchádzajúci rámec týkajúci sa bezpečnosti činností od darcovstva až po humánne použitie – smernicu 2002/98/ES (známu aj ako smernica o krvi) a smernicu 2004/83/ES (známu aj ako smernica o tkanivách a bunkách). Hodnotenie uskutočnené v súvislosti s týmito právnymi predpismi ukázalo, že sa už nezaoberajú najnovším vedeckým a technickým stavom

[6] Návrh Nariadenia Európskeho parlamentu a Rady o normách kvality a bezpečnosti pre látky ľudského pôvodu určené na humánne použitie a o zrušení smerníc 2002/98/ES a 2004/23/ES – Dôvodová správa

[7] SPRÁVA A9-0250/2023 o návrhu nariadenia Európskeho parlamentu a Rady o normách kvality a bezpečnosti pre látky ľudského pôvodu určené na humánne použitie a o zrušení smerníc 2002/98/ES a 2004/23/ES

a vyžadujú si aktualizáciu, pričom pandémia COVID-19 ešte viac zdôraznila niektoré z týchto nedostatkov[6].
Nariadenie definuje látku ľudského pôvodu ako „akúkoľvek látku získanú z ľudského tela, či už obsahuje bunky alebo nie, a či sú tieto bunky živé alebo nie, vrátane prípravkov látky ľudského pôvodu, ktoré sú výsledkom spracovania takejto látky"[8] a vzťahuje na používanie látok ľudského pôvodu v liekoch, pokrokových terapiách, východiskových materiáloch na výrobu skúšaných liekov a pri transplantáciách kmeňových buniek pri rakovine krvi a iných stavoch[9].
Zároveň považujeme za potrebné uviesť, že v rámci farmaceutickej stratégie pre Európu prebieha hodnotenie a revízia farmaceutického právneho rámca. Nové Nariadenie tak má potenciál byť zároveň podkladom pre predmetnú revíziu, najmä pokiaľ ide o regulačné vymedzenie medzi sektorom krvi, tkanív a buniek a farmaceutickým sektorom[6].

Ciele nariadenia EP A RADY EÚ 2024/1938

Cieľom Nariadenia je najmä posilniť existujúci právny rámec a zároveň zvýšiť jeho flexibilitu, aby bolo možné držať krok s vedeckým a technologickým pokrokom.
Zároveň je cieľom zaistenie bezpečnosti a kvality pre pacientov liečených liečebnými postupmi s látkami ľudského pôvodu a na ich plnú ochranu pred rizikami, spojenými s látkami ľudského pôvodu, ktorým sa dá predísť.
Medzi ciele patrí aj zaistenie bezpečnosti a kvality pre darcov látok ľudského pôvodu a pre deti narodené z darovaných vajíčok, spermií alebo embryí a posilnenie a umožnenie harmonizácie postupov dohľadu medzi členskými štátmi.
Ďalšími nemenej dôležitými cieľmi novej legislatívnej úpravy sú uľahčenie vývoja bezpečných a účinných inovatívnych liečebných postupov s látkami ľudského pôvodu, zlepšenie odolnosti tohto sektoru a zmiernenie rizika nedostatku látok[10].
Ciele zaistenia bezpečnosti a kvality pre pacientov aj darcov, sú úzko prepojené, keďže oba zahŕňajú stanovenie technických požiadaviek na bezpečnosť a kvalitu za účelom efektívnejšej ochrany ochrany občanov EÚ. Aj napriek skutočnosti, že EÚ nemá mandát priamo zasahovať do riadenia dodávok, spoľahlivé monitorovanie a nahlasovanie nedostatku látok by členským štátom pomohlo odhaliť náhle poklesy v dodávkach látok ľudského pôvodu, trendy smerujúce k nedostatku alebo závislosti

[8] Článok 3 bod 1 Nariadenia EP a Rady EÚ 2024/1938 o normách kvality pre látky ľudského pôvodu určené pre humánne použitie a zrušení smerníc 2002/98/ES a 2004/23/ES
[9] Článok 2 Nariadenia EP a Rady EÚ 2024/1938 o normách kvality pre látky ľudského pôvodu určené pre humánne použitie a zrušení smerníc 2002/98/ES a 2004/23/ES
[10] Tlačová správa Rady Európskej únie z 27.05.2024, dostupné na: https://www.consilium.europa.eu/sk/press/press-releases/2024/05/27/council-adopts-new-rules-on-substances-of-human-origin/

od iných členských štátov alebo tretích krajín a pomohlo by im prijať vhodné zmierňujúce opatrenia[6].
Nariadenie ustanovuje tzv. „Princíp dobrovoľného a bezplatného darcovstva" tzn. darcovstvo by malo byť zásadne dobrovoľné a bezplatné. Je však potrebné poukázať na skutočnosť, že aj napriek zásade, v zmysle ktorej darcovia nemajú byť finančne motivovaní k darcovstvu, paradoxne všetky formy kompenzácie alebo úhrady, vrátane pevných platieb žijúcim darcom, sú stále prijateľné, ak sa uskutočňujú v súlade s vnútroštátnymi právnymi predpismi[6].
Cieľom Nariadenia je zároveň zvýšiť harmonizáciu a uľahčiť cezhraničné výmeny a prístup k látkam ľudského pôvodu prostredníctvom zriadenia koordinačnej rady látok ľudského pôvodu na úrovni EÚ na podporu členských štátov pri vykonávaní Nariadenia.
Je potrebné poukázať taktiež na skutočnosť, že prijaté Nariadenie rozširuje rozsah látok ľudského pôvodu tak, aby zahŕňal ľudské materské mlieko a črevnú mikroflóru. Zameriava sa tak aj na budúcnosť právnych predpisov EÚ tým, že zahŕňa ďalšie látky ľudského pôvodu, ktoré sa môžu v budúcnosti aplikovať na ľudí, a umožňuje flexibilnejšie budúce aktualizácie[10]. Nariadenie uľahčí inováciu prostredníctvom spoločného postupu EÚ na hodnotenie a povoľovanie nových prípravkov látok ľudského pôvodu, úmerne k súvisiacim rizikám. Zároveň sa v Nariadení stanovujú aj ďalšie požiadavky na povoľovanie a kontrolu zariadení, ktoré takéto látky spracúvajú, skladujú, prepúšťajú, dovážajú a vyvážajú. Novotou je aj tzv: "systém rýchleho varovania", ktorého cieľom je riešiť vážne reakcie a incidenty postihujúce príjemcov alebo darcov, pričom sa členské štáty vyzývajú, aby vytvorili národné núdzové plány, ktoré budú zahŕňať opatrenia na riešenie kritického nedostatku.

3D biotlač

3D biotlač je proces integrácie živých buniek s biomateriálmi, ktorý umožňuje riadené ukladanie buniek/bioatramentu po vrstvách a vyznačuje sa hierarchickými štrukturálnymi vlastnosťami, so zachovanou životaschopnosťou buniek v 3D priestore na vytvorenie komplexných, mnohostranných tkanív. Základom 3D biotlače je prienik technológií tkanivového inžinierstva, syntetickej biológie, mikro/nanofabrikácie a výroba biomateriálov na biospracovanie[11].
Pochybnosti o reálnej možnosti implementácie 3D biotlače boli rozptýlené preukázanými úspechmi využitia technológie biotlače tkanív a orgánov v rámci rapídneho vývoja a výskumu v tejto oblasti. Vypracovaním základných techník

[11] ZÁBAVSKÁ, Dominika; HLUBEŇOVÁ, Jana., HUDÁK, Radovan., Právne a etické aspekty 3D biotlače. Online. In: Proceedings of the Trendy v biomedicínském inženýrství 2023. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, s. 234-241, ISBN 978-80-214-6173-4

a metód bolo zároveň prekonaných množstvo obmedzení na samotnú implementáciu technológie, pričom táto technológia už bola použitá na riešenie problémov v transplantológii, regeneratívnej medicíne a dokonca aj v oblasti asistovanej reprodukcie.
Hlavnou výzvou 3D biotlače v tkanivovom inžinierstve a regeneratívnej medicíne je výroba funkčných tkanív a orgánov na kompenzáciu obmedzeného počtu darcov transplantátov[12]. Uvedená výzva je však zároveň aj evidentným prísľubom, nakoľko technológie biotlače predstavujúca možnosť riešenia problému nedostatku orgánov a tkanív na transplantáciu vie priniesť aj pridanú hodnotu v podobe tzn."personalizovanej medicíny" keďže sa "vyrábaný orgán" koncipuje na mieru príjemcu[11].

Nariadenie EP a Rady EÚ 2024/1938 a jeho možný dopad na 3D biotlač

Technológia 3D biotlače využíva najmä integráciu živých buniek s biomateriálmi t.z. stavebnou jednotkou biotlače je látka ľudského pôvodu – živá bunka. S ohľadom na uvedené je tak nepochybné, že regulácia procesu a technológie 3D biotlače priamo podlieha právnej úprave manipulácie s látkami ľudského pôvodu.
Odsek 6 recitálu Nariadenia[13] uvádza dôvod prijatia Nariadenia, ktorým je aj vymedzenie spoločných noriem pre krv, tkanivá a bunky na vysokej úrovni zlúčené do jedného právneho aktu, so zohľadnením osobitných vlastností každého typu látky, pri zachovaní rovnakej úrovne právnej ochrany pre všetky typy látok ľudského pôvodu a to harmonizáciou postupov dohľadu nad manipuláciou s látkami ľudského pôvodu.
Jedným z markantných dopadov Nariadenia, je podľa názoru autorky, priame rozšírenie definície látok ľudského pôvodu tak, aby zahŕňala ľudské materské mlieko a črevnú mikroflóru[14]. Uvedená skutočnosť má význam najmä pri ochrane darcov a príjemcov predmetných látok, nakoľko sa na nich budú vzťahovať rovnaké podmienky ako pre príjemcov a darcov ostatných látok ľudského pôvodu. Zároveň sa tým rozšíria aj možnosti využívania predmetných látok vo výskume technológie 3D biotlače a možnosti nadobúdania rozšírených látok v rámci cezhraničnej spolupráce,

[12] FRIDRICH BALOGOVÁ, Alena, TREBUŇOVÁ, Marianna, RAJŤÚKOVÁ Viktória, HUDÁK, Radovan, Fresh method: 3D Bioprinting as a new appriach for tissue and organ regeneration. In: Acta Tecnologia – International Scientific Journal about Trchnologies, Vol. 7, 2021, Issue: 3, s. 79-82 ISSN: 2453-675X

[13] Odsek 6 recitálu Nariadenia EP a Rady EÚ 2024/1938 o normách kvality pre látky ľudského pôvodu určené pre humánne použitie a zrušení smerníc 2002/98/ES a 2004/23/ES
[14] Odsek 7 recitálu Nariadenia EP a Rady EÚ 2024/1938 o normách kvality pre látky ľudského pôvodu určené pre humánne použitie a zrušení smerníc 2002/98/ES a 2004/23/ES

čo pri aktuálnej neúplnej právnej úprave zakotvenej v transponovaných smerniciach možné nie je[15].

Ďalším z možných dopadov Nariadenia na oblasť 3D biotlače je nepochybne jeho cieľ uľahčenia cezhraničnej výmeny a prístupu k látkam ľudského pôvodu. Možnosť cezhraničnej výmeny a prístupu k látkam ľudského pôvodu je tak, ako aj pre iné oblasti závislé na variabilite vzoriek potrebných k výskumu, pre vývoj oblasti biotlače kruciálny, keďže vyššia variabilita vzoriek stavebného materiálu zabezpečí možnosť zvýšiť rozsah výskumu a nesústrediť sa tak výlučne na lokálne zdroje a vzorky[16].

V súvislosti s uľahčením cezhraničnej výmeny a prístupu k látkam ľudského pôvodu je taktiež potrebné poukázať na zriadenie platformy EÚ pre látky ľudského pôvodu, ktorej úlohou je najmä podpora cezhraničnej výmeny informácií spojených s látkami ľudského pôvodu na úrovni EÚ[17].

Pre potreby tohto príspevku považuje autorka za potrebné zároveň poukázať na skutočnosť, že nakoľko akákoľvek procedúra s využitím látok ľudského pôvodu prostredníctvom technológie 3D biotlače nie je momentálne v EÚ schválenou liečebnou procedúrou, ide tak toho času stále o procedúry v rovine biomedicínskeho výskumu. Efektívnemu vývoju a následnej možnosti začlenenia technológie 3D biotlače ako schváleného liečebného postupu (cieľu uľahčenia vývoja inovatívnych liečebných postupov s látkami ľudského pôvodu a to konkrétne liečebných postupov prostredníctvom technológie 3D biotlače) má však potenciál dopomôcť práve podpora cezhraničnej výmeny látok aj informácii spojených s látkami ľudského pôvodu a harmonizácia kvality vzoriek zakotvená v Nariadení.

Poskytnutím rámca pre cezhraničnú spoluprácu, ktorý vychádza zo spoločného súboru pravidiel, v podobe úpravy nakladania s látkami ľudského pôvodu vo forme Nariadenia s priamym účinkom a všeobecnou platnosťou, majú prijaté opatrenia predpoklady byť účinnými riešeniami interdiciplinárnych otázok, do ktorých proces technológie 3D biotlače a jeho možné začlenenie do regeneratívnej medicíny s určitosťou patrí.

Do doby účinnosti Nariadenia je nakladanie s látkami ľudského pôvodu upravené v smerniciach, ktorých transpozícia do právnych poriadkov členských štátov môže znamenať rozdiely v právnej úprave členských štátov EÚ. Zavedením noriem kvality a bezpečnosti látok ľudského pôvodu v Nariadení, sa tak pre všetkých občanov EÚ

---

[15] pozri VERBEKE, Frederick, JANSSENS, Yorick, WYNENDAELE, Evelien et al.Faecal microbiota transplantation: a regulatory hurdle?. BMC Gastroenterol 17, 128 (2017), https://doi.org/10.1186/s12876-017-0687-5

[16] pozri článok 26, 47 a 51 Nariadenia EP a Rady EÚ 2024/1938 o normách kvality pre látky ľudského pôvodu určené pre humánne použitie a zrušení smerníc 2002/98/ES a 2004/23/ES

[17] Článok 73 Nariadenia EP a Rady EÚ 2024/1938 o normách kvality pre látky ľudského pôvodu určené pre humánne použitie a zrušení smerníc 2002/98/ES a 2004/23/ES

zvýši prístup k bezpečnejším liečebným postupom s posilnením zásady právnej istoty a ochrany oprávnených očakávaní občana EÚ v prípade nutnosti cezhraničného poskytovania liečebného postupu (a/alebo experimentálneho liečebného postupu) zaručeného rovnakými normami pre všetky členské štáty.

Záver

Cieľom príspevku bolo preskúmať novú prijatú právnu úpravu na úrovni Európskej únie v podobe Nariadenia, a jej možný dopad na regulačný rámec 3D biotlače, v právnom prostredí Slovenskej republiky ako členského štátu EÚ. Preskúmaním návrhu Nariadenia, jeho dôvodovej správy a znenia Nariadenia, bolo možné poukázať na ciele, ktoré mal zákonodarca v úmysle pri prijímaní nového regulačného rámca a špecifiká, ktoré sa nepochybne budú vzťahovať aj na oblasť 3D biotlače, ktorá je vďaka rapídnemu technologickému pokroku dosiahnutého počas 4-tej priemyselnej revolúcie technológiou s veľkým prísľubom využitia v regeneratívnej medicíne.

Zoznam použitej literatúry

1. FRIDRICH BALOGOVÁ, Alena, TREBUŇOVÁ, Marianna, RAJŤÚKOVÁ Viktória, HUDÁK, Radovan, Fresh method: 3D Bioprinting as a new appriach for tissue and organ regeneration. In: Acta Tecnologia – International Scientific Journal about Technologies, Vol. 7, 2021, Issue: 3, s. 79-82 ISSN: 2453-675X
2. VERBEKE, Frederick, JANSSENS, Yorick, WYNENDAELE, Evelien et al., Faecal microbiota transplantation: a regulatory hurdle?, BMC Gastroenterol 17, 128 (2017). https://doi.org/10.1186/s12876-017-0687-5
3. ZÁBAVSKÁ, Dominika; HLUBEŇOVÁ, Jana., HUDÁK, Radovan., Právne a etické aspekty 3D biotlače. Online. In: Proceedings of the Trendy v biomedicínském inženýrství 2023. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, s. 234-241, ISBN 978-80-214-6173-4
4. Nariadenie Európskeho parlamentu a Rady 2024/1938 o normách kvality pre látky ľudského pôvodu určené pre humánne použitie a zrušení smerníc 2002/98/ES a 2004/23/ES
5. Nariadenie Európskeho parlamentu a Rady 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach, zmene smernice 2001/83/ES, nariadenia (ES) č. 178/2002 a nariadenia (ES) č. 1223/2009 a o zrušení smerníc Rady 90/385/EHS a 93/42/EHS
6. Návrh Nariadenia Európskeho parlamentu a Rady o normách kvality a bezpečnosti pre látky ľudského pôvodu určené na humánne použitie a o zrušení smerníc 2002/98/ES a 2004/23/ES

7. Smernica 2004/23/es Európskeho parlamentu a Rady z 31. marca 2004 ustanovujúca normy kvality a bezpečnosti pri darovaní, odoberaní, testovaní, spracovávaní, konzervovaní, skladovaní a distribúcii ľudských tkanív a buniek
8. Smernica Európskeho parlamentu a Rady 2002/98/ES z 27. januára 2003, ktorou sa stanovujú normy kvality a bezpečnosti pre odber, skúšanie, spracovanie, uskladňovanie a distribúciu ľudskej krvi a zložiek krvi a ktorou sa mení a dopĺňa smernica 2001/83/ES
9. Smernica Európskeho parlamentu a Rady 2010/53/EÚ zo 7. júla 2010 o normách kvality a bezpečnosti ľudských orgánov určených na transplantáciu
10. SPRÁVA A9-0250/2023 o návrhu nariadenia Európskeho parlamentu a Rady o normách kvality a bezpečnosti pre látky ľudského pôvodu určené na humánne použitie a o zrušení smerníc 2002/98/ES a 2004/23/ES
11. Tlačová správa Rady Európskej únie z 27.05.2024, dostupné na: https://www.consilium.europa.eu/sk/press/press-releases/2024/05/27/council-adopts-new-rules-on-substances-of-human-origin/

Kontaktné údaje

JUDr. Dominika Zábavská, MBA
dominika.zabavska@gmail.com
Univerzita Pavla Jozefa Šafárika v Košiciach, Právnická fakulta, Katedra obchodného a hospodárskeho práva

BRUSELSKÝ EFEKT A REGULÁCIA UMELEJ INTELIGENCIE: GLOBÁLNE DÔSLEDKY EURÓPSKYCH NORIEM [1]

ARTIFICIAL INTELLIGENCE REGULATION AND THE BRUSSELS EFFECT: GLOBAL IMPLICATIONS OF EUROPEAN STANDARDS

Jana Zigo[2]

Abstract: The European Union significantly influences global rules and regulations, also known as the Brussels effect, which can be encountered more often. Therefore, it is necessary to consider the impact of adopted European legislation on countries outside of the EU. In this context, it is necessary to examine what effect European regulation has on other jurisdictions and what standards it sets for foreign entities operating within the EU. This paper focuses on the analysis of this phenomenon, especially in the context of the adopted regulation of artificial intelligence - the EU AI Act, as it can be assumed that these regulations will, in a certain way, affect the functioning of foreign companies within the EU and may also have an impact on the further development of AI regulation in other countries. As part of that paper, we also partially examine different approaches to regulating artificial intelligence within China and the possible consequences for innovation, trade and international cooperation.

Key words: EU. AI. Brussels effect. Regulation.

Introduction

It is common for the EU to influence legislation outside its territory through specific mechanisms and thus shape regulatory standards globally. One of these mechanisms is the so-called Brussels effect[3], which can be understood as a process of unilateral regulatory globalisation when the EU's regulatory standards exceed its borders and influence the behaviour of companies and legislation in other countries, either through the voluntary adoption of these rules by companies (*Brussels effect de facto*)

[1] *This article was supported by the Slovak Research Development Agency under the Contract no. APVV-23-0137 - Legal and technical aspects of cybersecurity situational awareness.*

[2] Comenius University in Bratislava , Faculty of Law, Department of Civil Law

[3] This term was introduced by prof. Anu Bradford in 2012 following the example of the California effect, *See more:* BRADFORD, A. "The Brussels Effect: How the European Union Rules the World" (2020).

or through the formal adoption of European standards into legislation other states (*Brussels effect de jure*).[4] We do not even have to go far back in history when the GDPR regulation can be mentioned as an example of the Brussels effect.[5] A strong regulatory potential can be seen within the EU, especially in digital transformation, when the EU adopted several important regulations, such as the Digital Services Act (DSA)[6], Digital Markets Act (DMA), and the debated and expected regulation of artificial intelligence in the form of the EU AI Act.[7] Given that the legal framework of the EU AI Act is the first of its kind, especially from the point of view of complexity, its potential to become a global model for the regulation of artificial intelligence is being discussed. This paper aims to analyse whether this regulation will have any global consequences in the form of the so-called *Brussels effect*. Several key questions emerged from the set aim. In the beginning, it was necessary to investigate whether there are currently indications that international companies will be willing to adapt to EU rules or whether there are indications that some countries could formalise AI regulations along the EU model. After examining the assumption of the so-called *de jure Brussels effect*, another critical question related to the main differences between EU and Chinese regulations. This paper focuses on this jurisdiction because is world power that may also have an important say in AI regulation. The EU AI Act entered into force in August 2024.[8] Following its subsequent application, we can begin to evaluate how this regulation's predicted

[4] ALMADA, M., and RADU, A. The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy. German Law Journal, 2024. pp. 1–18. [online]. Available at: https://www.cambridge.org/core/services/aop-cambridge

[5] In this case, it would be challenging to think that this regulation would not have a global impact in the form of the Brussels effect, especially given the extraterritorial spread of the GDPR regulation, when this regulation applies not only to organizations based in the EU but also to those outside EU if they process personal data of natural persons within the EU. As for the adoption of similar regulations have been adopted in various countries such as Japan, Argentina and South Korea, but even China has adopted a legal framework for personal data protection, which at least partially corresponds to the European regulation in specific points. *See more about the Brussels effect in the GDPR regulation:* GUNST, S., and DE VILLE, F. The Brussels Effect: How the GDPR Conquered Silicon Valley. European Foreign Affairs Review. 2021. Vol. 26. Issue 3, pp. 437-458. [online].Availableat:https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/26.3/EERR2021036

[6] *See more about the potential Brussels effect at DSA*: HUSOVEC, M., URBAN, J. Will the DSA have the Brussels Effect?, VerfBlog, 2024/2/21, [online]. Available at: https://verfassungsblog.de/will-the-dsa-have-the-brussels-effect/

[7] NIESTADT, M, REICHERT, J. The global reach of the EU's approach to digital transformation. 2024. EPRS. [online]. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757632/EPRS_BRI(2024)757632_EN.pdf

[8] *See more:* AI Act enters into force [online]. Available at: https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en

individual effects and impacts will be reflected in reality. In the following subsections of this paper, we focus on analysing the potential effects of this regulation, either on entities operating within the EU or other jurisdictions interested in regulating AI.

Possible impact on the subjects operating in the EU - *de facto* Brussels Effect

The *de facto Brussels effect* is when global companies adopt strict European regulations outside the European Union, mainly for economic and practical reasons. This effect is characterized by companies that want to continue to operate in the large and lucrative EU market choosing to comply with European rules in all jurisdictions to minimize the costs associated with managing different regulatory regimes in different markets.[9] In short, if a new regulation is adopted within the EU, the company has two options: to leave the EU market[10] or adapt to the new regulation.[11] Suppose it agrees to remain on the market and assimilate. In that case, it also has two options: it will differentiate its offer of goods or services for different markets when it applies different rules for different markets or globally apply European regulation. In this case, we can talk about the de facto Brussels effect. However, several conditions must be considered and fulfilled for this effect to occur.[12]

The first essential requirement is the *size and importance of the EU market.*[13] While the EU may not currently lead in AI systems[14], it remains a robust and lucrative market for global companies. Large technology companies, for instance, would not want to miss out on the opportunity to serve millions of users. Adapting to these

[9] MARKOFF, T. The First of its Kind: the EU AI Act and What it Means for the Future of AI. 2024 [online]. Available at: https://news.law.fordham.edu/jcfl/2024/04/23/the-first-of-its-kind-the-eu-ai-act-and-what-it-means-for-the-future-of-ai/

[10] Although, in most cases, global companies adapt to European regulation and implement it globally, there are companies that do not comply with these regulations (in general, concerning several regulations, not only in relation to the EU AI Act), an example is the social platform X (owned by Elon Musk), which is announcing the possibilities of exit from the EU market due the strict regulation. *For example, see more:* Elon Musk's best move in EU fight may be an eXit [online]. Available at: https://www.reuters.com/breakingviews/elon-musks-best-move-eu-fight-may-be-an-exit-2024-08-21/

[11] An example of the de facto Brussels effect is the GDPR, where technology giants such as Google and Meta (Facebook) began to apply strict data protection rules even in countries where such regulations did not formally exist.

[12] SIEGMANN, Ch. and ANDERLJUNG, M. The Brussels Effect and Artificial Intelligence: How EU regulation will impact the global AI market. 2022. p. 28 [online]. Available at: https://cdn.governance.ai/Brussels_Effect_GovAI.pdf

[13] *Ibid*. p. 19

[14] NIESTADT, M, REICHERT, J. The global reach of the EU's approach to digital transformation. 2024. EPRS. p. 5 [online]. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757632/EPRS_BRI(2024)757632_EN.pdf

strict regulations can bring significant economic benefits to companies, enabling them to continue trading in one of the world's largest markets while streamlining global operations. It is more cost-effective and less complex to implement the same standards worldwide than to create different versions of products for different markets.[15] Another key attribute is the EU's *regulatory capacity*.[16] With AI being a new technology, there is limited established knowledge on how to regulate AI systems. The EU has taken the lead in bridging this gap by developing extensive AI expertise and applying the existing product safety framework. This has given the EU a technical and institutional advantage over other jurisdictions.[17] A Brussels effect is likely if EU standards are more stringent than other jurisdictions. However, the AI Act does not create a comprehensive legal framework for all AI systems. The AI Act is a comprehensive regulation that introduces risk scaling. It categorizes AI systems based on risk and sets different regulatory requirements for them. [18] For systems not prohibited or classified as high-risk, the Act is limited to a disclosure requirement, meaning compliance with the AI Act may not be sufficient to meet stricter laws in other jurisdictions. However, the EU rules are quite strict in high-risk AI systems and systems with systemic risk. Another requirement for the Brussels effect is that regulation must be aimed at an *inelastic target*.[19] In practice, this means that the Brussels effect requires that the regulation aim be firmly tied to the regulatory regime, regardless of its characteristics. In the case of the AI Act, this can be achieved through territorial extension, which ensures that its provisions apply to any AI system whose outputs are in the EU, even if the providers or users are outside the EU. This makes it more difficult for providers operating in the EU market to avoid the regulation of the AI Act. [20]The last attribute is the so-called *indivisibility of the regulated object*.[21] The affected entities cannot create separate versions of AI systems

[15] ENGLER, A. The EU AI Act Will Have Global Impact, but a Limited Brussels Effect, Brookings. 2022. [online]. Available at: https://www.brookings.edu/research/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/

[16] *Ibid.*

[17] ALMADA M, RADU A. The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy. *German Law Journal*. Published 2024. pp. 1-18. [online]. Available at: https://www.cambridge.org/core/journals/german-law-journal/article/brussels-sideeffect-how-the-ai-act-can-reduce-the-global-reach-of-eu-policy/032C72AEC537EBB6AE96C0FD90387E3E

[18] European Commission – Shaping Europe's Digital Future, AI Act, European Commission, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework ai#:~:text=The%20AI%20act%20will%20be,%2C%20safety%2C%20and%20ethical%20principles.

[19] *See* supranote 17.

[20] FRYM, W. A Practical Guide to the Extraterritorial Reach of the AI Act. 2024. [online]. Available at: https://www.lexology.com/library/detail.aspx?g=72b8e937-9a95-4ff1-89f4-0411a345dc12

[21] ALMADA, M., and RADU, A. The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy. German Law Journal, 2024. pp. 1–18. [online]. Available at: https://www.cambridge.org/core/services/aop-cambridge-

for different markets. However, it is important to note that such indivisibility cannot, for example, be seen in the case of prohibited systems, as providers can continue to commercialize these systems in jurisdictions that allow them.[22] However, in the case of the AI Act, most AI systems, especially general AI models, require huge amounts of data and computing power, meaning that providers will likely develop systems that meet the same standards across all markets. This is mainly due to the high costs of such differentiation for different markets; as we mentioned below, creating EU-specific products is more expensive than worldwide compliance with the requirements of EU law.[23] Based on the above, it can be assumed that only market factors are unlikely to be sufficient for the global expansion of European rules. However, systems classified as high-risk are likely to form the basis for AI regulation at a global level, as they are one of the areas where the EU sets stricter rules than other jurisdictions. Even in these more stringent categories, the spread of EU standards depends on the extent to which products can be adapted and the extent to which the product safety framework addresses specific regulatory issues. Given this, the Brussels effect can be assumed to a limited extent.[24]

Possible impact on other jurisdictions - *de jure* Brussels Effect

As the introduction of this paper states, *the Brussels effect de jure* occurs when countries outside the EU adopt legislation inspired by regulations introduced in the EU, either by directly adopting these regulations or by adapting them to their own legal framework.[25] This situation may occur for various reasons and through various channels, mainly due to pressure from global companies that prefer a uniform regulatory environment and want to avoid facing different legal requirements in different jurisdictions. It can also happen due to competition in markets outside the EU and also due to the reduction of costs.[26] Another reason is that foreign jurisdictions often expect EU-like regulations to be highly quality and aligned with their regulatory goals. The Brussels effect is not solely a result of passive adoption. The EU also actively promotes the adoption of EU-like regulations, for instance,

core/content/view/032C72AEC537EBB6AE96C0FD90387E3E/S2071832223001086a.pdf/the-brussels-side-effect-how-the-ai-act-can-reduce-the-global-reach-of-eu-policy.pdf

[22] ENGLER, A. The EU AI Act Will Have Global Impact, but a Limited Brussels Effect, Brookings. 2022. [online]. Available at: https://www.brookings.edu/research/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/

[23] *See* supranote 21.

[24] SIEGMANN, Ch. and ANDERLJUNG, M. The Brussels Effect and Artificial Intelligence: How EU regulation will impact the global AI market. 2022. p. 23 [online]. Available at: https://cdn.governance.ai/Brussels_Effect_GovAI.pdf

[25] *Ibid.* p. 3

[26] *Ibid.* p. 3

through trade rules or other bilateral or multilateral agreements. This intentional promotion of EU standards further solidifies the Brussels effect. This type of Brussels effect can generally be expected, especially in jurisdictions with significant trade relations with the EU.[27]

In analysing this type of Brussels effect, it is necessary to state that other jurisdictions worldwide have also started preparing AI regulations[28]. Countries such as Canada, Japan, South Korea, the UK, Taiwan and many others have started preparing for the regulation of AI. It was within the legislation of some of these countries that the de jure Brussels effect could be seen to a large extent in the case of the GDPR[29], and to assume that European legislation will have a particular influence in this case as well. However, only after stabilising this regulatory "storm" will we probably see the real effects of European regulation on foreign jurisdictions. However, the eye has mainly focused on world powers such as China or the USA and their AI regulation, considering that China started by adopting partial regulation even before the EU. The US held the less strict position. [30] In the sense of the above, we focused specifically on China's jurisdiction as part of a narrower analysis since, just like in the case of the EU, it is the market leader whose approach to AI regulations can also have an important say. In that case, knowing this jurisdiction's primary approaches to regulations is essential. China, as regards the process of preparing the regulation itself, it is important to state at the outset that China has the lead in the regulation of this area, even if only in a partial form and not as comprehensive as the EU AI Act, and it was explicitly about the regulation of generative artificial intelligence.[31] As can be evaluated from the regulation structure, it is evident that China, unlike the EU, prefers the so-called vertical approach, which focuses on individual regulations for specific systems, while the EU maintains the horizontal approach - regulation for all AI systems. In addition to this difference, however, it is necessary to state that the EU's regulations primarily focus on the protection of privacy and the observance of

---

[27] *Ibid.* p. 5

[28] *See more*: PONOMAROV, C. Global AI Regulations Tracker: Europe, Americas & Asia-Pacific Overview. [online]. Available at: https://legalnodes.com/article/global-ai-regulations-tracker

[29] GUNST, S., and DE VILLE, F. The Brussels Effect: How the GDPR Conquered Silicon Valley. European Foreign Affairs Review. 2021. Vol. 26. Issue 3, pp. 437-458. [online]. Availableat:https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/26.3/EERR2021036

[30] SIEGMANN, Ch. and ANDERLJUNG, M. The Brussels Effect and Artificial Intelligence: How EU regulation will impact the global AI market. 2022. p. 24 [online]. Available at: https://cdn.governance.ai/Brussels_Effect_GovAI.pdf

[31]HINE, E. and FLORIDI, L. New deepfake regulations in China are a tool for social stability, but at what cost?. In Nat Mach Intell Vol. 4, (2022). pp. 608–610 [online]. Available at: https://www.researchgate.net/publication/362149296_New_deepfake_regulations_in_China_are_a_tool_for_social_stability_but_at_what_cost

fundamental rights in order to avoid the misuse of technology. For example, using social credit systems and real-time biometric identification that could compromise rights is prohibited. However, China primarily wants to focus on technological progress and economic prosperity in its regulation[32]. In China, the main emphasis is on national security and state control. Some AI systems are and will be used in China to maintain order and national security while protecting privacy, which is a much lower priority. Related to this is another significant difference in the regulation of generative artificial intelligence, where China sets much stricter rules than the EU, especially regarding deepfake technology.[33] Even though the EU and China are committed to cooperating and supporting the fair and ethical development of innovation, including AI, the approaches regarding its regulation are different and therefore, in the sense of the above, it can be concluded that the global effect of this regulation can only be expected with difficulty or into a considerably limited extent, so that we cannot speak of a *de jure Brussels effect*, such as in the case of the GDPR.[34] To outline a specific contrast, the USA can be mentioned, when in the case of the primary strategy, together with the EU[35], they share alignment with the risk-based approach and, unlike China, they jointly respect the observance and enforcement of principles in the field of trustworthy AI, but their approach is also significantly different. Their regulation is now fragmented and primarily aimed at supporting innovation, which is likely less strict regulation. Conversely, the EU prefers stricter regulations, while the US relies more on a market-oriented and more flexible approach. Therefore, it is unlikely that the US will directly adopt EU-inspired regulations. American companies will probably partially adapt their AI systems to

[32] CIHANOVÁ, J. AI regulation: the EU and China approach. In. Acta Facultatis Iuridicae Universitatis Comenianae. 43. 16. 2024. pp. 3-18 24 [online]. Available at: https://www.researchgate.net/publication/381948785_AI_REGULATION_THE_EU_AND_CHINA_APPROACH

[33] HUW, R. et al. Governing artificial intelligence in China and the European Union: Comparing aims and promoting ethical outcomes. In: The InformaTIon SocIeTy2023, VoL. 39, no. 2, pp. 79–97 [online]. Available at: https://www.tandfonline.com/doi/epdf/10.1080/01972243.2022.2124565?needAccess=true

[34] In 2021, China adopted the Personal Information Protection Law, which provides GDPR-like protections for citizens against private corporations. *For example see more:* LEPLAY, P. and LEPLAY, E., China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU? (2020). Penn State Journal of Law & International Affairs, Vol. 8, No. 1, 2020.

[35] SZCZEPAŃSKI, M. United States approach to artificial intelligence. EPRS. 2023. [online]. Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATA(2024)757605_EN.pdf

European rules to access the European market. However, this probably does not mean American laws will follow the same direction. [36]

Conclusion

Since the regulations and rules created by the European Union often exceed the EU borders, they significantly influence global legislative standards. The Brussels effect is a phenomenon that has already demonstrated its power in regulating personal data protection through the GDPR. Thus, there were assumptions that a similar scenario would be repeated with the EU AI Act. However, based on the analysis, it can be concluded that although this regulation will undoubtedly have a global impact, it will probably have only a limited Brussels effect.[37] As we indicated in the previous chapter, in the case of a de facto Brussels effect, market factors may not be sufficient to lead to the globalization of all EU standards for AI, especially for systems that do not fall into strictly regulated categories. In the case of the de jure Brussels effect, there are assumptions that other jurisdictions, if they decide to regulate artificial intelligence, will be inspired by European legislation. However, with the aim of not restricting the growth of innovation, its impact is likely to be less significant than with GDPR. As for the impact on the regulation of AI in China, no significant impact can be assumed in this case, based on the analysis of the approach to AI regulations. Even though in the past China was inspired by EU legislation when creating some of its laws, in this case, it is doubtful that there will be any effect de jure since even before the adoption of the AI Act itself, China adopted specific regulations related to AI, which are even stricter than the regulation within the EU. In the case of the USA, it can be stated that this jurisdiction focuses mainly on supporting innovations with minimal restrictions rather than strict regulations. In conclusion, we can state that the Brussels effect, in its de facto and de jure forms, is likely to show only in some parts of the EU regulatory regime. A de facto effect can be expected, especially for large technology companies with "high-risk" AI systems, as defined in the EU AI Act. These companies are likely to follow European standards globally because the costs of creating different versions of products for different markets are high. The EU AI Act can thus be particularly significant in setting global standards for trustworthy and human-oriented development and deployment of AI.

[36] SULLIVAN, M. Global AI Regulation: A Closer Look at the US, EU, and China. [online]. Available at: https://transcend.io/blog/ai-regulation

[37] ENGLER, A. The EU AI Act Will Have Global Impact, but a Limited Brussels Effect, Brookings. 2022. [online]. Available at: https://www.brookings.edu/research/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/

Zoznam použitej literatúry

1. ALMADA, M., and RADU, A. The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy. German Law Journal, 2024. pp. 1–18. [online]. [last accessed 01.10.2024] Available at: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/032C72AEC537EBB6AE96C0FD90387E3E/S2071832223001086a.pdf/the-brussels-side-effect-how-the-ai-act-can-reduce-the-global-reach-of-eu-policy.pdf
2. CIHANOVÁ, J. AI regulation: the EU and China approach. In. Acta Facultatis Iuridicae Universitatis Comenianae. 43. 16. 2024. pp. 3-18 24 [online]. [last accessed 01.10.2024] Available at: https://www.researchgate.net/publication/381948785_AI_REGULATION_THE_EU_AND_CHINA_APPROACH
3. ENGLER, A. The EU AI Act Will Have Global Impact, but a Limited Brussels Effect, Brookings. 2022. [online]. [last accessed 01.10.2024] Available at: https://www.brookings.edu/research/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/
4. European Commission – Shaping Europe's Digital Future, AI Act, European Commission, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework ai#:~:text=The%20AI%20act%20will%20be,%2C%20safety%2C%20and%20ethical%20principles.
5. FRYM, W. A Practical Guide to the Extraterritorial Reach of the AI Act. 2024. [online]. [last accessed 25.09.2024] Available at: https://www.lexology.com/library/detail.aspx?g=72b8e937-9a95-4ff1-89f4-0411a345dc12
6. GUNST, S., and DE VILLE, F. The Brussels Effect: How the GDPR Conquered Silicon Valley. European Foreign Affairs Review. 2021. Vol. 26. Issue 3, pp. 437-458. [online]. [last accessed 25.09.2024] Availableat:https://kluwerlawonline.com/journalarticle/European+Foreign+Affairs+Review/26.3/EERR2021036
7. HINE, E. and FLORIDI, L. New deepfake regulations in China are a tool for social stability, but at what cost?. In Nat Mach Intell Vol. 4, (2022). pp. 608–610 [online]. [last accessed 21.03.2024] Available at: https://www.researchgate.net/publication/362149296_New_deepfake_regulations_in_China_are_a_tool_for_social_stability_but_at_what_cost
8. HUSOVEC, M., URBAN, J. Will the DSA have the Brussels Effect?, VerfBlog, 2024/2/21, [online]. [last accessed 30.09.2024] Available at: https://verfassungsblog.de/will-the-dsa-have-the-brussels-effect/

9. HUW, R. et al. Governing artificial intelligence in China and the European Union: Comparing aims and promoting ethical outcomes. In: The InformaTIon SocIeTy2023, VoL. 39, no. 2, pp. 79–97 [online]. [last accessed 25.09.2024] Available at: https://www.tandfonline.com/doi/epdf/10.1080/01972243.2022.2124565?needAccess=true
10. MARKOFF, T. The First of its Kind: the EU AI Act and What it Means for the Future of AI. 2024 [online]. [last accessed 30.09.2024] Available at: https://news.law.fordham.edu/jcfl/2024/04/23/the-first-of-its-kind-the-eu-ai-act-and-what-it-means-for-the-future-of-ai/
11. NIESTADT, M, REICHERT, J. The global reach of the EU's approach to digital transformation. 2024. EPRS. [online]. [last accessed 25.09.2024] Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/757632/EPRS_BRI(2024)757632_EN.pdf
12. SIEGMANN, Ch. and ANDERLJUNG, M. The Brussels Effect and Artificial Intelligence: How EU regulation will impact the global AI market. 2022. p. 28 [online]. [last accessed 30.09.2024] Available at: https://cdn.governance.ai/Brussels_Effect_GovAI.pdf
13. SULLIVAN, M. Global AI Regulation: A Closer Look at the US, EU, and China. [online]. [last accessed 19.09.2024] Available at: https://transcend.io/blog/ai-regulation
14. SZCZEPAŃSKI, M. United States approach to artificial intelligence. EPRS. 2023. [online]. [last accessed 19.09.2024] Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATA(2024)757605_EN.pdf

Kontaktné údaje

Mgr. Jana Zigo, LL.M.
cihanova2@uniba.sk
Comenius University in Bratislava, Faculty of Law,
Department of Civil Law

DIGITÁLNA STRATÉGIA EÚ - PRÁVNY RÁMEC PRE INOVATÍVNU EURÓPU

EU DIGITAL STRATEGY - LEGAL FRAMEWORK FOR INNOVATIVE EUROPE

Mária Kevická[1]

Abstrakt: Digitálne technológie prinášajú so sebou veľa právnych výziev, ktoré sú zároveň právnymi príležitosťami. V rámci digitálnej stratégie EÚ: Európa pripravená na digitálny vek sa Európska únia snaží aktívne vytvoriť právny rámec, ktorý podporí inovácie a zároveň zabezpečí ochranu základných práv a slobôd a integritu digitálneho prostredia. Hlavným cieľom príspevku vedeckej konferencie je sumarizácia právneho rámca digitálnej stratégie EÚ a jeho dopadov na rôzne právne oblasti. Budeme sa zaoberať právnym rámcom, ktorý vytvára Európska únia a budeme sa snažiť identifikovať kľúčové výzvy a príležitosti pre tvorbu práva EÚ.

Kľúčové slová: Európa pripravená na digitálny vek, legislatívna záťaž, konkurencieschopnosť EÚ, správa Mario Draghi

Abstract: Digital technologies present numerous legal challenges that concurrently offer opportunities for legal development. Within the framework of the EU's Digital Strategy: A Europe fit for the digital age, the European Union has been actively creating a comprehensive and coherent legal framework to support innovation while also safeguarding fundamental rights and freedoms and the integrity of the digital environment. The primary objective of this academic conference contribution is to analyse the legal framework of the EU's Digital Strategy, identify its key elements, and assess its impact on various areas of law. We will analyse the legal tools and mechanisms employed by the EU to construct this framework and identify the primary challenges and opportunities arising from the creation and implementation of this legal framework.

Key words: A Europe fit for the digital age, Regulatory burden, EU competitiveness, Mario Draghi report

[1] Univerzita Mateja Bela v Banskej Bystrici, Právnická fakulta, Katedra medzinárodného, európskeho práva a právnej komunikácie.

Úvod

Digitálne technológie prinášajú so sebou veľa právnych výziev, ktoré sú zároveň právnymi príležitosťami. V rámci digitálnej stratégie EÚ: *Európa pripravená na digitálny vek* sa Európska únia snaží aktívne vytvoriť právny rámec, ktorý podporí inovácie a zároveň zabezpečí ochranu základných práv a slobôd a integritu digitálneho prostredia.
Hlavným cieľom príspevku vedeckej konferencie je sumarizácia právneho rámca digitálnej stratégie EÚ a snaha o identifikáciu kľúčových výziev a príležitostí pre tvorbu práva EÚ.

Digitálna transformácia Európy - základné informácie

K východiskám digitálnej transformácie Európy môžeme zaradiť predstavenie novej priemyselnej stratégie a v rámci nej myšlienku už bývalého komisára pre vnútorný trh Thierryho Bretona, ktorý **10. marca 2020** uviedol: *„Európa má najsilnejší priemysel na svete. Naše spoločnosti - veľké aj malé - nám poskytujú pracovné miesta, prosperitu a strategickú autonómiu. Riadenie ekologickej a digitálnej transformácie a vyhýbanie sa vonkajším závislostiam v novom geopolitickom kontexte si vyžaduje radikálnu zmenu, s ktorou musíme začať okamžite.* [2]".
O rok neskôr, **9.marca 2021,** Európska komisia predstavila víziu a spôsoby ako dosiahnuť digitálnu transformáciu do roku 2030. Ambiciózna vízia sa zameriava na zvýšenie digitálnych kompetencií obyvateľstva (skills), rozšírenie prístupu k vysokorýchlostnému internetu (infrastructures), podporu inovácií v podnikoch všetkých veľkostí (business) a modernizáciu verejnej správy prostredníctvom digitalizácie kľúčových služieb (government). Táto stratégia si kladie za cieľ vybudovať digitálne konkurencieschopnú a udržateľnú Európu.

Európa pripravená na digitálny vek

V zmysle stratégie Európa pripravená na digitálny vek, Európska únia predstavila svoj záujem v digitálnom veku: chrániť práva ľudí, podporovať demokraciu a zabezpečiť zodpovedné konanie všetkých aktérov, vytvoriť férové online prostredie a ochranu pred nezákonným a škodlivým obsahom, garantovať bezpečnosť a ochranu online, zabezpečiť, aby technika ľudí zjednocovala a nie rozdeľovala, aby mal každý rovnaký prístup pre všetkých, aj službám aj zručnostiam aj obsahu, aby mal každý by kontrolu nad svojimi údajmi aj vo vzťahu k štátu. Dôležitým bodom je aj udržateľnosť a zelená transformácia. Európska únia musí posilniť digitálnu nezávislosť a vytvoriť si vlastné normy.

[2] Dostupné online: https://europske.noviny.sk/2020/03/11/komisia-predstavila-novu-priemyselnu-strategiu-pre-konkurencieschopnu-zelenu-a-digitalnu-europu/ (cit. 4.10.2024).

Právne akty a dohody prijaté v rámci stratégie Európa pripravená na digitálny vek

V nadväznosti na uvedené ciele vznikli viaceré právne akty. Medzi najdôležitejšie právne akty zaraďujeme **akt o digitálnych službách**[3], ktorého obsahom je zaistenie bezpečného a zodpovedného online prostredia a **akt o digitálnych trhoch**, ktorý rieši zabezpečenie spravodlivých a otvorených digitálnych trhov[4]. Návrh týchto aktov datujeme na 15. decembra 2020.

Deň neskôr, dňa 16. decembra 2020, bola predložená nová stratégia kybernetickej bezpečnosti Európskej únie ako dôležitý prvok formovania digitálnej budúcnosti Európy. Na základe stratégie kybernetickej bezpečnosti EÚ bol dňa 15. septembra 2022 predstavený nový návrh **aktu EÚ o kybernetickej bezpečnosti** na ochranu spotrebiteľov a podnikov pred produktmi s nedostatočnými ochrannými prvkami, ktorý mal podľa predsedníčky Európskej komisie Ursuly von der Leyen zaručiť, že digitálne produkty (bez/káblové výrobky a softvér) budú bezpečnejšie. Návrh nebol prijatý. V mesiaci apríl 2023 bol predstavený návrh na cielené zmeny existujúceho aktu o kybernetickej bezpečnosti za účelom vytvorenie európskych systémov certifikácie pre spravované bezpečnostné služby. Predmetom politickej dohody zo dňa 6. marca 2024 bol **akt o kybernetickej odolnosti**, ktorý rieši požiadavky na kybernetickú bezpečnosť. Akt popri smernici NIS 2 a spolu s **aktom o kybernetickej solidarite v EÚ** (návrh Komisie zo dňa 18. apríla 2023), má vytvárať stavebné prvky pri dosahovaní cieľa stanoveného stratégiou.

V nových iniciatívach, ktoré boli predstavené 23. februára 2023, boli riešené otázky pripojiteľnosti a sieťového pokrytia a rozvoja pre 6G. Tieto iniciatívy prispeli k politickej dohode o **akte o gigabitovej infraštruktúre**[5], ktorej obsahom sú opatrenia na zjednodušenie a urýchlenie zavádzania sietí s veľmi vysokou kapacitou (optické vlákna a 5G).

Dňa 21.apríla 2021 boli prijaté nové pravidlá a opatrenia v záujme excelentnosti a dôvery v umelú inteligenciu pozostávajúce z právneho rámca umelej inteligencie

---

[3] Akt (Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES) nadobudol účinnosť 16. novembra 2022. Dostupný online: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32022R2065&qid=1727648806916 (cit. 1.10.2024).

[4] Akt (Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/1925 zo 14. septembra 2022 o súťažeschopných a spravodlivých trhoch digitálneho sektora a o zmene smerníc (EÚ) 2019/1937 a (EÚ) 2020/1828), zameraný na riadne fungovanie vnútorného trhu nastavením pravidiel pre zabezpečenie súťažeschopnosti a spravodlivosti pre trhy digitálneho sektora. Dostupný online: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=OJ:L:2022:265:TOC (cit. 2.10.2024).

[5] Aktom (Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1309 z 29. apríla o opatreniach na zníženie nákladov na zavádzanie gigabitových elektronických komunikačných sietí, ktorým sa mení nariadenie (EÚ) 2015/2120 a zrušuje smernica 2014/61/EÚ) sa harmonizujú podmienky pre rozširovanie vysokorýchlostných sietí novej generácie. Dostupné online: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=OJ:L_202401309&qid=1727894316385 (cit. 2.10.2024)

a nového koordinovaného plánu pre členské štáty. Výsledkom snahy v oblasti umelej inteligencie bolo prijatie **aktu o umelej inteligencii**[6], ktorý je zameraný na rozdelenie obmedzení podľa konceptu rizika. Dňa 29. mája 2024 Komisia zriadila Úrad pre umelú inteligenciu s cieľom posilniť vedúce postavenie EÚ v oblasti bezpečnej a dôveryhodnej umelej inteligencie. Súčasťou diskusií bol aj **balík inovačných opatrení v oblasti umelej inteligencie** na podporu start-upov a MPS v oblasti umelej inteligencie.

Ďalším dôležitým prijatým dokumentom je **Európsky akte o čipoch,** ktorého návrh bol predstavený dňa 08.februára 2022 a znamená posilnenie konkurencieschopnosti a odolnosti Európy v oblasti polovodičových technológií[7], akt nadobudol dňa 21.septembra 2023.

Významnú zmenu, v oblasti európskej dátovej stratégie, priniesol **Akt EÚ o údajoch,** ktorého návrh z 23.februára 2022 stanovil pravidlá používania a prístupu k údajom vytvorených v EÚ vo všetkých hospodárskych odvetviach[8], akt nadobudol účinnosť dňa 11. januára 2024.

Zabezpečenie prístupu k bezpečným, diverzifikovaným, cenovo dostupným a udržateľným dodávkam kritických surovín (keďže Európa vo veľkej miere závisí od dovozu z tretích krajín s monopolným postavením) upravuje **akt o kritických surovinách**[9] z 11. apríla 2024.

Akt o **interoperabilnej Európe**[10], ktorý nadobudol účinnosť dňa 11.apríla 2024, by mal prispieť k dosiahnutiu cieľa online dostupnosti kľúčových verejných služieb.

---

[6] Akt o umelej inteligencii (Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828) dostupný online https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32024R1689 (cit. 4.10.2024).

[7] Akt o čipoch (Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1781 z 13. septembra 2023, ktorým sa zriaďuje rámec opatrení na posilnenie európskeho ekosystému polovodičov a mení nariadenie (EÚ) 2021/694). Dostupný online: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=OJ:L:2023:229:TOC (cit. 2.10.2024).

[8] Dostupný online: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=OJ:L_202302854 (cit. 2.10.2024)

[9] Európsky akt o kritických surovinách (Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1252 z 11. apríla 2024, ktorým sa stanovuje rámec na zaistenie bezpečných a udržateľných dodávok kritických surovín a ktorým sa menia nariadenia (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1724 a (EÚ) 2019/1020) upriamuje pozornosť na koordinované vnútroštátne opatrenia pri zabezpečovaní bezpečných a udržateľných dodávok kritických surovín ako nástroj na udržanie fungujúceho vnútorného trhu. Dostupné online: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=OJ:L_202401252&qid=1727892417689 (cit. 2.10.2024).

[10] Akt (Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/903 z 13. marca 2024, ktorým sa stanovujú opatrenia na zabezpečenie vysokej úrovne interoperability verejného sektora v celej Únii)

V rámci témy digitálnej identity je dôležitá predbežná politická **dohoda o európskej peňaženke digitálnej identity**, potrebná pre revolúciu v oblasti digitálnej identifikácie.[11]

Konkurencieschopnosť Európy

V nadväznosti na uvedené akty a kroky a v súlade so stratégiou Posilnenia konkurencieschopnosti Európy, Európska komisia v apríli 2024 vydala vyhlásenie: *„Európa je dnes jedným z najkonkurencieschopnejších, najdynamickejších a najinovatívnejších regiónov na svete. Niekoľko posledných rokov však prinieslo niekoľko historických výziev vrátane pandémie COVID-19 a útočnej vojny Ruska proti Ukrajine. Hoci sa Európskej únii podarilo úspešne prekonať tieto krízy, vybrali si daň na našej celkovej konkurencieschopnosti."*[12] Napriek explicitnému uznaniu potreby posilnenia európskej konkurencieschopnosti zo strany Európskej komisie, v apríli 2024 Komisia paradoxne konštatovala absenciu výraznejších problémov v tejto oblasti.

Správa Enrica Letta o jednotnom trhu EÚ[13]

Enrico Letta, taliansky politik a bývalý premiér, prezident Inštitútu Jacquesa Delorsa a člen talianskej Poslaneckej snemovne, dostal v septembri 2023 od európskych inštitúcií mandát na vypracovanie správy na vysokej úrovni o budúcnosti jednotného trhu.

---

dostupný online: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=OJ:L_202400903&qid=1727894769529 (cit. 2.10.2024).

[11] V rámci stratégie Európa pripravená na digitálny vek došlo aj k zavedeniu jednotného patentového systému z 1. júna 2023, či k politickej dohode na nariadení o podpore výroby munície zo 7. júla 2023. Dňa 21.januára 2022 Komisia navrhla Európskemu parlamentu a Rade podpis vyhlásenia o digitálnych právach a zásadách - podpísané 15. decembra 2022). Dňa 11.mája 2022 bola predstavená nová Európske stratégia vytvárania lepšieho internetu pre deti a dňa 19. septembra 2022 bol Komisiou predstavený nový nástroj núdzovej pomoci pre jednotný trh (SMEI), ktorý je zameraný na zachovanie voľného pohybu tovaru, služieb a osôb v prípade núdzových situácií. Predmetom politických diskusií boli aj odporúčania opatrení na boj proti falšovaniu a lepšej ochrane práv duševného vlastníctva, prvá stratégia európskeho obranného priemyslu na úrovni EÚ a nový program obranného priemyslu, balík opatrení v oblasti pripojiteľnosti, odporúčania o kritických technologických oblastiach pre hospodársku bezpečnosť EÚ, prijatie novej stratégie pre web 4.0 a virtuálne svety, oznámenia o Európskej stratégii hospodárskej bezpečnosti, odporúčaniach o boji proti online pirátstvu v prípade športových a iných živých podujatí či boli prijaté nové pravidlá roamingu v EÚ, stratégia v oblasti manažmentu vesmírnej prevádzky.

[12] Dostupné online: https://commission.europa.eu/topics/strengthening-european-competitiveness_sk (cit. 4.10.2024).

[13] Dostupné online: https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf (cit. 4.10.2024).

V apríli 2024 Enrico Letta[14] predstavil päťbodový plán pre konkurencieschopnejšiu Európu, ktorý spočíva v nasledovných krokoch: (i) uvoľnenie väčšieho kapitálu pre európske podniky, (ii) zabezpečenie energetickej nezávislosti a lacnejšej energie, (iii) riešenie nedostatku zručností, (iv) podpora digitálnych inovácií, (v) uvoľnenie plného potenciálu obchodu a ochrana trhu EÚ a vytváranie rovnakých podmienok na celosvetovej úrovni. Hoci správa Enrica Letta zdôrazňuje potrebu posilnenia konkurencieschopnosti Európy, podobne ako Európska komisia, dospieva k záveru, že Únia nečelí významnejším problémom v tejto oblasti.

Budúcnosť európskej konkurencieschopnosti: Správa Mario Draghi

Výsledky volieb do Európskeho parlamentu 8. júna 2024 vytvorili nový politický mandát pre legislatívnu činnosť Únie v oblasti digitalizácie a konkurencieschopnosti. Stále absentuje skutočný obraz konkurencieschopnosti Európskej únie. Ten so sebou prináša až Správa, ktorú vypracoval Mario Draghi. Mario Draghi, taliansky ekonóm, bankár a politik, bývalý prezident Európskej centrálnej banky a predseda vlády Talianska, upozornil ako prvý dôrazne vo svojej **Správe o budúcnosti európskej konkurencieschopnosti** publikovanej 9. septembra 2024 (ďalej len „Správa") na to, že ***európska ekonomika nedokáže držať krok s konkurenciou - ekonomická realita starého kontinentu, základy, na ktorých stojí Európska únia sa otriasajú - EÚ čelí existenčnej výzve a ak sa nepodarí, aby bola EÚ konkurencieschopná, neexistuje dôvod jej ďalšej existencie.***[15] Pokyn na vypracovanie Správy dostal z Európskej komisie.

Rast Európskej únie sa spomalil sa podľa Maria Draghiho spomalil aj v dôsledku pandémie COVIDu 19, vojny na Ukrajine, ktorá priniesla stratu veľkého dodávateľa energie (Rusko), poklesu populácie, zle stanovených priorít, dôsledkom ktorých sú: (i) **drahé energie:** v závislosti od dôsledkov vojny v Ukrajine, cena plynu pre priemysel je v EÚ vyššia o 158 % ako v USA, (ii) **premeškanie prvej digitálnej revolúcie:** rýchly vývoj technológií a neschopnosť Európskej únie spôsobila, že Európa premeškala prvú digitálnu revolúciu, nové modely AI sú vyrábané v USA, Európa nemá veľkých hráčov v oblasti cloudu, niektoré digitálne sektory sú stratené, riešením je potreba sústredenia sa na ďalšiu vlnu technickej revolúcie a snažiť sa začleniť AI do sektoru priemyslu a MSP, (iv) **nedostatok nerastných surovín:** Európa nemá strategické suroviny a ich zásobárne sa nachádzajú v Ázii, (v) **problémy s investíciami v rámci EÚ**: rozdiel medzi USA a EU predstavuje 1,5 % HDP ročne, (vi) **pomalý rast HDP**: objem vyrobených tovarov a služieb v danej krajine, v Európe je

[15] Dostupné online: https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en#paragraph_47059 (cit. 4.10.2024).

o 30 % pomalší v porovnaní s Čínou a o 12 % pomalší v porovnaní s USA, (vii) **chýbajúce zručnosti:** Európa zaostáva v AI, čipoch, infraštruktúre, vzdelaní.
Mario Draghi v rámci svojej správy identifikoval **tri kľúčové oblasti, ktoré si vyžadujú urgentné opatrenia**: (i) zníženie inovačného rozdielu voči USA a Číne, (ii) vytvorenie koherentnej stratégie pre dosiahnutie klimatických cieľov pri súčasnom posilňovaní konkurencieschopnosti a (iii) posilnenie bezpečnostnej odolnosti EÚ a zníženie jej závislosti od tretích krajín. Tieto odporúčania predstavujú výzvu pre všetky inštitúcie Európskej únie.
Záver Správy formulovaný Mariom Draghim znie veľmi naliehavo: ***„Ak sa EÚ nestane viac konkurencieschopná, bude si musieť vybrať. Nie je možné, aby sa stala lídrom nových technológií, zároveň prebrala plnú klimatickú zodpovednosť a naďalej zastávala existujúcu sociálnu politiku. Bude musieť obetovať bohatstvo, životné prostredie alebo slobody. Koniec prokrastinácie. Je čas na akciu.*"**

Legislatíva ako jedna z bŕzd Európskej únie

Legislatívna a administratívna záťaž spôsobila, že Európska únia stala *právnikom sveta*, celý svet (najmä Čína a USA) obchoduje, len Európska únia reguluje. Na základe Správy je zrejmé, že podniky sú odrádzané od podnikania v celej EÚ z dôvodu regulácie, ktorá predstavuje bremeno. Finančné prostriedky na administratívu majú len väčšie spoločnosti, ktoré nemajú sídlo v EÚ. Spoločnosti nemajú schopnosť a motiváciu znášať náklady spojené s dodržiavaním regulácií, mladé firmy nezačínajú podnikanie v EÚ. Obmedzenia pri ukladaní a spracúvaní údajov vytvárajú vysoké náklady na dodržiavanie predpisov a bránia vytváraniu veľkých integrovaných súbor údajov (o.i. na trénovania modelov AI), čo predstavuje znevýhodnenie v porovnaní s USA, ktoré sa spolieha na súkromný sektor vytvárajúci rozsiahle súbory údajov a s Čínou, ktorá využíva centrálne štátne inštitúcie na zber a agregáciu údajov. Problémom je aj presadzovanie férovej právne správnej hospodárskej súťaže, ktorá brzdí vnútroodvetvovú spoluprácu. Na základe uvedeného je nevyhnutné zjednodušenie pravidiel podnikania v EÚ, Komisia síce rieši redukciu regulácií, ale bez väčšieho výsledku.
V zmysle štatistických údajov za obdobie 2019-2024, ktoré tvoria súčasť Správy, bolo v USA bolo prijatých 3.500 legislatívnych aktov a 2.000 rezolúcií, pričom v EÚ bolo prijatých až 13.000 legislatívnych aktov. Uvedené potvrdzuje aj úvod príspevku, ktorý obsahuje len vybrané právne akty v oblasti digitálnej stratégie, ktorá má priamy vplyv na konkurencioschopnosť oblasti technologického pokroku a vývoja.
Významným metodologickým nedostatkom pri tvorbe európskej legislatívy je absencia komplexnej analýzy nákladov a prínosov. Zatiaľ čo Európska komisia disponuje obmedzenými nástrojmi na hodnotenie dopadov navrhovaných právnych predpisov, Európsky parlament a Rada tieto nástroje systematicky nevyužívajú.

Následne členské štáty len v obmedzenej miere analyzujú dopady európskej legislatívy pri jej implementácii na národnej úrovni.
Nedostatočná analýza vplyvu legislatívy na malé a stredné podniky predstavuje významný problém v rámci európskej regulácie. Hoci malé a stredné podniky sú cieľovou skupinou väčšiny legislatívnych iniciatív Európskej komisie, len polovica z nich je podrobená dôkladnému hodnoteniu vplyvu na túto skupinu. To vedie k situácii, kedy regulácie často neúmerne zaťažujú práve malé a stredné podniky. Prieskumy potvrdzujú, že regulácie sú vnímané ako významná prekážka dlhodobých investícií v EÚ, pričom výrazné percento respondentov označilo regulácie za výrazne väčší problém v porovnaní s inými regiónmi sveta.[16]
Podľa Maria Draghiho, vnútroštátna transpozícia predstavuje ďalšiu dodatočnú záťaž. Často dochádza k rozdielnej implementácii zákonov, následnému podkopávaniu cieľov EÚ, množstvo členských štátov rozširuje požiadavky kladené EÚ, ide o efekt s názvom „***Gold plating***".
Problémy legislatívy EÚ spočívajú najmä v tom, že je vydávaných množstvo právnych predpisov, z ktorých sa mnohé ***prekrývajú a existuje medzi nimi nesúlad***. Správa uvádza, že v rámci skúmaných 13 právnych predpisov bolo nájdených 169 duplicít povinností (29 %) a 11 % úplných nezrovnalostí v povinnostiach. Najviac zaťažujúce oblasti práva sú oblasti udržateľnosti, ochrany osobných údajov a odpadovej a obalovej legislatívy.
Riešením problémov legislatívy EÚ je odstránenie legislatívy a zjednodušenie, resp. konsolidácia predpisov, pričom dôraz je potrebné klásť na odstránenie prekrývania a nezrovnalostí, vymenovanie zodpovedného nového podpredsedu Komisie, prijatie jednotnej metodiky pre EÚ, ale aj členské štáty na analýzu dopadov legislatívy, posilnenie skupiny Single Market Enforcement Taskforce (SMET), zodpovednú za skúmanie transpozícii práva a prekračovanie požiadaviek práva EÚ, zníženie povinností malých a stredných podnikov, odloženie iniciatív Komisie, ktoré majú neúmerný vplyv na malé a stredné podniky a obchod.

Záver

Úvodná sumarizácia právneho rámca Digitálnej stratégie EÚ odhaľuje komplexný a však zároveň problematický systém regulácie v rámci EÚ. Aj alebo práve vďaka intenzívnej legislatívnej činnosti sa Európska únia potýka s klesajúcou konkurencieschopnosťou. Nadmerná regulácia, nedostatočná analýza vplyvu a nekonzistentnosť právnych predpisov predstavujú hlavné prekážky pre inovácie a rast európskeho hospodárstva.

[16] V zmysle Správy Maria Draghiho: 61 % účastníkov prieskumu z 21 štátov EÚ označilo regulácie ako prekážku dlhodobého investovania v EÚ a 83 % účastníkov uvádza, že EÚ má viac právnych prekážok ako iné regióny.

Správa Maria Draghiho jednoznačne poukazuje na potrebu zásadnej reformy. Európa musí zjednodušiť legislatívu, zintenzívniť analýzu nákladov a prínosov a zamerať sa na podporu kľúčových oblastí, ako je výskum, vývoj a digitalizácia. Európska únia je preťažená reguláciami, ktoré majú negatívny vplyv na podnikanie a investície. Zvýšenie flexibility umožní EÚ sa rýchlejšie prispôsobovať meniacim sa podmienkam sveta. Uvedené však nebude možné bez intenzívnej spolupráce inštitúcií a členských štátov. Obavou ostáva aj skutočnosť, že Európska únia sa stretáva s problémami v dobe, kedy viaceré členské štáty porušujú hodnoty právneho štátu.

Zoznam použitej literatúry

Internetové zdroje:

1. www.eur-lex.europa.eu
2. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_sk
3. https://www.consilium.europa.eu/sk/policies/digital-markets-act/
4. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_sk
5. https://digital-strategy.ec.europa.eu/sk/factpages/data-act-explained
6. https://digital-strategy.ec.europa.eu/sk/policies/strategy-better-internet-kids
7. https://digital-strategy.ec.europa.eu/sk/factpages/digital-decade-2024-report-country-fact-pages
8. https://slovakia.representation.ec.europa.eu/news/sprava-o-digitalnom-desatroci-za-rok-2024-2024-07-09_sk
9. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal/green-deal-industrial-plan/european-critical-raw-materials-act_sk
10. https://digital-strategy.ec.europa.eu/sk/policies/cyber-resilience-act
11. https://digital-strategy.ec.europa.eu/sk/policies/regulatory-framework-ai
12. https://www.consilium.europa.eu/sk/press/press-releases/2024/03/04/interoperable-europe-act-council-adopts-new-law-for-more-efficient-digital-public-services-across-the-eu/
13. https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf
14. https://digital-strategy.ec.europa.eu/sk/policies/gigabit-infrastructure-act
15. https://digital-strategy.ec.europa.eu/sk/policies/ai-office
16. https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en#paragraph_47059

Kontaktné údaje
JUDr. Mária Kevická, Ph.D.
maria.kevicka@umb.sk
Univerzita Mateja Bela v Banskej Bystrici, Právnická fakulta, Katedra medzinárodného, európskeho práva a právnej komunikácie

OD PAPIERA K PIXELOM: VPLYV NARIADENIA O EURÓPSKOM PRIESTORE ZDRAVOTNÝCH ÚDAJOV NA SLOVENSKÉ ZDRAVOTNÍCTVO

FROM PAPER TO PIXELS: THE IMPACT OF THE REGULATION ON EUROPEAN HEALTH DATA SPACE ON THE SLOVAK HEALTHCARE

Soňa Sopúchová[1]

Abstrakt: Tento článok skúma predpokladaný vplyv nariadenia o Európskom priestore zdravotných údajov na slovenské zdravotníctvo, so zameraním na prechod od papierových zdravotných záznamov k plne digitálnej infraštruktúre. Táto štúdia poskytuje právnu analýzu súčasných postupov zdieľania zdravotných údajov na Slovensku a hodnotí ich súlad s navrhovaným rámcom Európskej únie. Kľúčové oblasti záujmu zahŕňajú regulačné výzvy spôsobené dualitou papierových a elektronických záznamov, dôsledky pre ochranu údajov a kybernetickú bezpečnosť. Zistenia poukazujú na potrebu, aby Slovensko prispôsobilo svoju právnu a technologickú infraštruktúru novým požiadavkám, čím by zabezpečilo súlad a ochranu práv pacientov. Autorka článok uzatvára odporúčaniami pre tvorcov politík na podporu úspešnej integrácie Slovenska do tohto vyvíjajúceho sa európskeho digitálneho zdravotného prostredia.

Kľúčové slová: európsky priestor zdravotných údajov, zdieľanie zdravotných údajov, digitálne zdravotníctvo, elektronické zdravotné záznamy

Abstract: This paper examines the anticipated impact of the European Health Data Space on the Slovak healthcare system, focusing on the transition from paper-based health records to a fully digital infrastructure. This study provides a legal analysis of Slovakia's current health data sharing practices, assessing their alignment with the proposed European Union framework. Key areas of focus include the regulatory challenges posed by the duality of paper and electronic records, the implications for data privacy and cybersecurity. The findings highlight the necessity for Slovakia to adapt its legal and technological infrastructure to meet the new requirements, ensuring both compliance and the protection of patient rights. The paper concludes with recommendations

[1] Univerzita Komenského v Bratislave, Právnická fakulta

for policymakers to support Slovakia's successful integration into this evolving European digital health environment.

Key words: european health data space, health data sharing, dgital healthcare, electornic health records

Úvod

Nedoddeliteľnou súčasťou poskytovania zdravotnej starostlivosti je zdravotná dokumentácia, ktorá je dôležitým nástrojom pri zabezpečení kontinuity starostlivosti o pacientov a efektívneho riadenia ich zdravotného stavu. V súčasnosti prechádza v rámci Slovenskej republiky vedenie zdravotnej dokumentácie významnou transformáciou, ktorá je spôsobená narastajúcou digitalizáciou a využívaním informačno-komunikačných technológií (ďalej tiež „IKT") v zdravotníctve. Európska únia na základe svojej *Stratégie pre dáta* z roku 2020 postupne zavádza rôzne opatrenia na vytvorenie sektorových európskych dátových priestorov. Jednou z najvýznamnejších iniciatív v tejto oblasti je návrh *Nariadenia o Európskom priestore zdravotných údajov* (ďalej tiež „EHDS" alebo „Navrj nariadenie pre zdravotné údaje"), ktorý predstavuje nový právny rámec pre správu a zdieľanie zdravotných údajov v celej Európskej únii (ďalej tiež „EÚ").
Cieľom príspevku je poskytnúť právnu analýzu zdieľania zdravotných údajov na úrovni EÚ a Slovenskej republiky, pričom sa zameriava na dopad návrhu Nariadenia o Európskom priestore zdravotných údajov na slovenský zdravotný systém. Príspevok skúma právne výzvy, ktoré so sebou prináša zavedenie tejto novej legislatívy, a zároveň sa sústreďuje na navrhovanie právnych opatrení (de lege ferenda), ktoré by Slovenská republika mala prijať, aby zabezpečila úspešnú integráciu do nového digitálneho zdravotného priestoru EÚ.
Pri analýze skúmanej problematiky bol aplikovaný prístup, ktorý zahŕňa právnu analýzu súčasnej slovenskej legislatívy upravujúcej zdravotnú dokumentáciu, s dôrazom na identifikovanie výziev spojených s implementáciou Nariadenia o Európskom priestore zdravotných údajov. Táto analýza zahŕňa syntézu jednotlivých právnych noriem a ich vzájomné prepojenia, s cieľom posúdiť, do akej miery je Slovenská republika pripravená na harmonizáciu s európskym právnym rámcom. Na základe týchto zistení sú navrhnuté odporúčania, ktoré sú zamerané na úpravu slovenskej legislatívy a zavedenie potrebných technických opatrení.

Zdravotná dokumentácia v Slovenskej republike

Pri poskytovaní zdravotnej starostlivosti má nezastupiteľnú úlohu zdravotná dokumentácia. Zdravotná dokumentácia je v podmienkach Slovenskej republiky legálne definovaná, a to v Zákone č. 576/2004 Z. z. o zdravotnej starostlivosti,

službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov (ďalej tiež „Zákon o zdravotnej starostlivosti") ako *„súbor údajov o zdravotnom stave osoby, o poskytnutej zdravotnej starostlivosti a o službách súvisiacich s poskytovaním zdravotnej starostlivosti tejto osobe*."[2]
Zdravotná dokumentácia je teda záznamom obsahujúcim osobné údaje pacienta v rozsahu nevyhnutnom na jeho identifikáciu a zistenie jeho anamnézy, rovnako ako informácií o ochoreniach pacienta, o priebehu a výsledkoch vyšetrenia, liečbe a o ďalších významných okolnostiach súvisiacich so zdravotným stavom pacienta a s postupom pri poskytovaní zdravotnej starostlivosti. Tento záznam má povahu písomnú, obrazovú, zvukovú, elektronickú alebo akúkoľvek inú, ktorá prichádza od úvahy. Vyskytuje sa v podobe analógovej alebo digitálnej na tomu zodpovedajúcich nosičoch[3]. *„Správne a podrobne vedená zdravotná dokumentácia je jedným z prostriedkov komunikácie medzi zdravotníckymi pracovníkmi, napomáha kontinuite zdravotnej starostlivosti, dokladuje kvalitu a rozsah poskytnutej zdravotnej starostlivosti, je nástrojom pre posilnenie právnej ochrany zdravotníckeho pracovníka v pracovno-právnych sporoch, je nástrojom posilnenia bezpečnosti poskytovanej starostlivosti a ochrany bezpečnosti pacienta, a má aj forenzný význam v prípadných medicínsko-právnych sporoch."*[4] Zdravotná dokumentácia je ako celok vedená všeobecným lekárom, iný ošetrujúci zdravotnícky pracovník ju môže viesť v rozsahu ním poskytovanej zdravotnej starostlivosti. Samotné vedenie zdravotnej dokumentácie obsahuje získavanie, zhromažďovanie a zaznamenávanie údajov, ktoré tvoria jej obsah.

Forma zdravotnej dokumentácie v Slovenskej republike

Zdravotná dokumentácia sa vedie v elektronickej zdravotnej knižke[5] v národnom zdravotníckom informačnom systéme s kvalifikovaným elektronickým podpisom zdravotníckeho pracovníka. Elektronická zdravotná knižka je súborom údajov zo zdravotnej dokumentácie osoby vedených v Národnom registri elektronických zdravotných knižiek v rozsahu ustanovenom Zákonom č. 153/2013 Z. z. o Národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov (ďalej tiež „ Zákon o NZIS"), ktorý obsahuje identifikačné údaje osoby, elektronické

[2] Ustanovenie § 2 ods. 1 Zákona o zdravotnej starostlivosti.
[3] POLICAR, Radek. Zdravotnická dokumentace v praxi. Praha: Grada Publishing, 2009, s. 224.
[4] CAPÍKOVÁ, Silvia – NOVÁKOVÁ, Mária. Zdravotná dokumentácia vo vzťahu k posudzovaniu zdravotnej spôsobilosti zamestnanca – vybrané otázky. In: Zborník príspevkov z vedeckej konferencie Zdravotná spôsobilosť zamestnancov. 2020, s. 50.
[5] Osoba pristupuje do svojej elektronickej zdravotnej knižky cez Národný portál zdravia. Kvôli bezpečnosti a ochrane elektronických zdravotných záznamov je pre identifikáciu a autentifikáciu potrebný elektronický občiansky preukaz s elektronickým čipom.

zdravotné záznamy, údaje z účtu poistenca, vlastné záznamy osoby a záznamy o prístupe, o poskytnutí údajov a každý pokus o prístup alebo o poskytnutie údajov.[6] Obsahové náležitosti, členenie, rozsah zapisovaných údajov, okruh oprávnených osôb a poskytovanie a sprístupňovanie údajov z elektronickej zdravotnej knižky sú ustanovené v osobitnom predpise, ktorým je Zákon o NZIS.
Primárnou formou vedenia zdravotnej dokumentácie je teda elektronická forma v elektronickej zdravotnej knižke okrem prípadov, kedy zákon vyžaduje[7] alebo umožňuje[8] písomnú formu[9]. Tieto rôzne možnosti výberu formy zdravotnej starostlivosti považujeme za nežiaduce.

Zdieľanie zdravotných údajov v Slovenskej republike

Zákon o zdravotnej starostlivosti v podstate nepriamo vymedzil dva druhy zdravotnej dokumentácie, a to písomnú a elektronickú. Nadpisy jednotlivých súčastí zákona totiž používajú výlučne vyjadrenie zdravotná dokumentácia a následne jednotlivé úkony s ňou súvisiace sa rozlišujú na tie, ktoré sa vykonávajú zápisom do elektronickej zdravotnej knižky a tie, ktoré súvisia s písomnou zdravotnou dokumentáciou. V zmysle toho sa rozlišuje (i) zápis do elektronickej zdravotnej knižky a (ii) zápis do písomnej zdravotnej dokumentácie. Rovnaké členenie sa aplikuje v prípade zdieľania údajov zo zdravotnej dokumentácie.
Zdravotné údaje možno zdieľať dvomi spôsobmi, a to poskytnutím zdravotných údajov zo zdravotnej dokumentácie alebo ich sprístupnením. Ako sme vyššie uviedli, tieto procesy sa odlišujú podľa toho, či ide o zdieľanie zdravotných údajov nachádzajúcich sa v zdravotnej dokumentácii vedenej v písomnej forme alebo zdravotných údajov nachádzajúcich sa v elektronickej zdravotnej knižke. To znamená, že vzniká rôznorodý spôsob zdieľania zdravotných údajov.
Poskytovanie údajov z písomnej zdravotnej dokumentácie sa týka zdravotnej dokumentácie existujúcej na základe Zákona o zdravotnej starostlivosti. Údaje sa poskytujú v rámci výpisu zo zdravotnej dokumentácie, ktorý sa skladá zo zákonom stanovených informácií.[10] Všeobecný lekár, ošetrujúci zdravotnícky pracovník

[6] Ustanovenie § 2 ods. 6 Zákona o NZIS.
[7] Ustanovenie § 20 ods. 2 Zákona o zdravotnej starostlivosti – ide napríklad o prípad, kedy je potrebný písomný informovaný súhlas alebo ide o zmenu liečebného postupu.
[8] Ustanovenie § 20 ods. 3 Zákona o zdravotnej starostlivosti – ide o dôvod hodný osobitného zreteľa.
[9] Písomnou formou má v tomto kontexte zákonodarca na mysli papierovú, resp. listinnú formu. V ďalšej časti príspevku budeme tieto výrazy používať ako synonymá.
[10] Ustanovenie § 24 ods. 1 Zákona o zdravotnej starostlivosti.

a poskytovateľ sú povinní poskytnúť na vyžiadanie výpis zo zdravotnej dokumentácie len subjektom, ktoré im taxatívne vymedzuje Zákon o zdravotnej starostlivosti.[11]

Poskytovanie údajov z elektronickej zdravotnej knižky je upravené v Zákone o NZIS, a to taxatívnym vymedzením osôb, ktorým možno údaje poskytnúť s uvedením rozsahu, ktorý je pre každý tento subjekt rôzny.[12] Údaje z elektronickej zdravotnej knižky sa poskytujú takto vymedzeným subjektom po tom, ako zdravotnícky pracovník vloží občiansky preukaz s elektronickým čipom alebo doklad o pobyte s elektronickým čipom do technického zariadenia poskytovateľa zdravotnej starostlivosti. V prípade žiadosti o poskytnutie väčšieho rozsahu, ako zákon pre ten ktorý subjekt stanovuje, zdravotnícky pracovník je oprávnený na prístup k takýmto údajom len na základe súhlasu osoby, ktorého účel získavania je zdravotnícky pracovník povinný preukázateľne odôvodniť.[13]

Sprístupňovanie údajov zo zdravotnej dokumentácie upravené v Zákone o zdravotnej starostlivosti sa týka tak dokumentácie vedenej v písomnej forme ako aj elektronickej zdravotnej knižky. Údaje zo zdravotnej dokumentácie vedenej v písomnej forme sa sprístupňujú formou nahliadania do zdravotnej dokumentácie osobám taxatívne vymenovaným.[14] V prípade, ak je určitá osoba oprávnená nahliadnuť do zdravotnej dokumentácie, má právo si robiť výpisky alebo kópie, a to v rozsahu ako osobitný predpis (Zákon o NZIS) stanovuje pre elektronické zdravotné knižky. Zákon o zdravotnej starostlivosti ďalej upravuje postup sprístupňovania údajov z elektronickej zdravotnej knižky, a to tak, že osoba je oprávnená udeliť súhlas na prístup k údajom v nej sa nachádzajúcich iným osobám v rozsahu a spôsobom, ktoré stanovuje Zákon o NZIS.[15]

Na základe uskutočnenej analýzy zdieľania zdravotných údajov v podmienkach Slovenskej republiky konštatujeme, že zdieľanie musí prebiehnúť v súlade s podmienkami stanovenými dvomi zákonmi týkajúcimi sa rozsahu údajov, spôsobu zdieľania a okruhu osôb, ktorým môžu byť údaje zdieľané. Za zaujímavosť, v tomto prípade v negatívnom zmysle slova, považujeme skutočnosť, že na sprístupňovanie údajov zo zdravotnej dokumentácie vedenej v elektronickej zdravotnej knižke sa

[11] Na základe ustanovenia § 24 ods. 2 – 4 Zákona o zdravotnej starostlivosti ide napríklad o iného ošetrujúceho zdravotníckeho pracovníka, orgán na účely sociálnej pomoci, inšpektorát práce alebo osoby oprávnené nahliadať do zdravotnej dokumentácie.

[12] Na základe ustanovenia § 5 ods. 6 Zákona o NZIS ide napríklad o ošetrujúceho lekára, zdravotníckeho pracovníka záchrannej zdravotnej služby, ošetrujúcu sestru, lekára samosprávneho kraja, znalca ustanoveného súdom a ďalšie osoby.

[13] Ustanovenie § 5 ods. 8 Zákona o NZIS.

[14] Na základe ustanovenia § 25 ods. 1 Zákona o zdravotnej starostlivosti ide napríklad o zákonného zástupcu, manžela, manželku, revízneho lekára a ďalšie osoby.

[15] Súhlas sa na základe ustanovenia § 5 ods. 11 Zákona o NZIS udeľuje cez Národný portál zdravia prostredníctvom úradného autentifikátora.

vyžaduje súhlas danej osoby, zatiaľ čo v prípade zdravotnej dokumentácie vedenej v písomnej forme to takto zákonodarca neprecizuje a potrebu súhlasu neuvádza.

Nariadenie o európskom priestore pre zdravotné údaje

Návrh nariadenia pre zdravotné údaje bol vypracovaný v roku 2022 a jeho hlavným cieľom je zabezpečiť, aby jednotlivci v Európskej únii mali v praxi väčšiu kontrolu nad svojimi elektronickými zdravotnými údajmi. Zároveň má ambíciu riešiť problémy súvisiace s prístupom a zdieľaním elektronických zdravotných údajov, ktoré sú obsiahnuté v elektronických zdravotných záznamoch. Tento dokument prináša definície viacerých nových pojmov, ktoré by mohli zlepšiť nejednotnú terminológiu tejto oblasti v členských štátoch Európskej únie. Ide o pojmy osobný eletronický zdravotný údaj, iný ako osobný elektronický zdravodný údaj, držiteľ údajov, používateľ údajov či príjemca údajov.[16]
Za jednu z najpodstatnejších vecí, ktoré Návrh nariadenia pre zdravotné údaje plánuje zaviesť do praxe, je rozlíšenie prvotného a druhotného použitia elektronických zdravotných údajov, o ktorých sa bližšie zmienime v ďalšej časti tohto príspevku. Ďalšou novinkou sú osobitné technické požiadavky a štandardy, ktoré budú musieť spĺňať všetky elektronické zdravotné záznamy v štátoch Európskej únie, ide o európsky formát na výmenu elektronických zdravotných záznamov, a to predovšetkým pre účely dosiahnutia interoperability.[17]

Prvotné používanie elektronických zdravotných údajov

Ako to aj z názvu vyplýva, pri prvotnom používaní elektronických zdravotných údajov ide *„o spracúvanie osobných elektronických zdravotných údajov na účely poskytovania služieb zdravotnej starostlivosti s cieľom posúdiť, udržať alebo obnoviť zdravotný stav fyzickej osoby, ktorej sa uvedené údaje týkajú, vrátane predpisovania, vydávania a poskytovania liekov a zdravotníckych pomôcok, ako aj na účely príslušných služieb sociálneho zabezpečenia, administratívnych služieb alebo služieb preplácania nákladov*."[18] V tomto prípade je teda dôraz kladený na práva pacienta, pretože prvotné použitie má priamy súvis s poskytovaním zdravotnej starostlivosti. Pacienti budú mať prístup k svojim elektronickým osobným zdravotným údajom a budú mať možnosť rozhodnúť sa, kto ďalší k nim bude mať prístup (ktoré subjekty iné ako zdravotnícki pracovníci). Zdravotnícki pracovníci budú mať taktiež prístup k osobným zdravotným údajom pacientov, ale pacienti ich môžu obmedziť. Návrh nariadenia pre zdravotné údaje stanovuje v tejto oblasti pomerne obšírny diapazón práv pacienta,

[16] Bližšie pozri článok 2 ods. 2 Návrhu nariadenia pre zdravotné údaje.
[17] Interoperabilita je schopnosť organizácií, ako aj softvérových aplikácií alebo zariadení od toho istého výrobcu alebo rôznych výrobcov byť v interakcii v záujme plnenia vzájomne prospešných cieľov.
[18] Článok 2 ods. 2 písm. d) Návrhu nariadenia pre zdravotné údaje.

ako napríklad spomínané právo na bezodkladný prístup k svojim elektronickým zdravotným údajom, právo získať elektronickú kópiu svojich údajov, právo evidovať vlastné elektronické zdravotné údaje, právo požadovať opravu údajov, právo na poskytnutie prístupu k zdravotným údajom príjemcovi údajov, právo obmedziť prístup k údajom pre všetkých zdravotníckych pracovníkov či právo na informácie o tom, ktorí zdravotnícki pracovníci mali prístup k ich osobným zdravotným údajom.[19] Bude zaujímavé sledovať, ako sa zákonodarca a následne prax vysporiada so zabezpečovaním uvedených práv fyzických osôb vzhľadom na to, že ide o početné množstvo práv, ktoré sa napríklad v podmienkach Slovenskej republiky a jej legislatívy, momentálne nevyskytujú.

V nadväznosti na spomínané práva fyzických osôb stanovuje Návrh nariadenia pre zdravotné údaje úpravu, podľa ktorej, ak sa údaje spracúvajú v elektronickom formáte, členské štáty zabezpečia, aby zdravotnícki pracovníci systematicky zaznamenávali relevantné zdravotné údaje patriace prinajmenšom do prioritných kategórií[20], a to v elektronickom formáte v systéme elektronických zdravotných záznamov.[21]

Druhotné používanie elektronických zdravotných údajov

Návrh nariadenia pre zdravotné údaje sa vo svojej štvrtej kapitole dotýka pomerne novej a doteraz neregulovanej oblasti v rámci zdravotníctva, ktorou je používanie zdravotných údajov pacientov na druhotné ciele. Ide o spracúvanie elektronických zdravotných údajov na účely uvedené v článku 34 Návrhu nariadenia pre zdravotné údaje napr. oficiálne štatistiky, veda, výskum, vzdelávanie či testovanie a inovácie produktov, ale aj poskytovanie personalizovanej zdravotnej starostlivosti. Použité údaje môžu v zmysle článku 2. ods. 2 písm e) zahŕňať osobné elektronické zdravotné údaje pôvodne získané v kontexte prvotného používania, ale aj elektronické zdravotné údaje získané na účely druhotného používania.

Túto činnosť sprevádza niekoľko princípov. V prvom rade ide koncipovanie povinnosti držiteľa údajov tieto údaje poskytnúť, a to vždy za predpokladu, že sú splnené zákonné požiadavky.[22] Tieto sú stanovené najmä v opise žiadosti o prístup k zdravotným údajom, napríklad podrobné vysvetlenie zamýšľaného použitia, opis požadovaných elektronických zdravotných údajov či opis plánovaných záruk na zabránenie akémukoľvek inému použitiu.[23] Ak má dôjsť k takému poskytnutiu, musí byť ďalej dodržaný princíp minimalizácie, ktorý je reflektovaný v požiadavke, aby

[19] Článok 3 Návrhu nariadenia pre zdravotné údaje.
[20] Služby zdravotnej starostlivosti poskytnuté týmito pracovníkmi fyzickým osobám.
[21] Článok 7 ods. 1 Návrhu nariadenia pre zdravotné údaje.
[22] Článok 33 ods. 1 Návrhu nariadenia pre zdravotné údaje.
[23] Článok 45 ods. 2 Návrhu nariadenia pre zdravotné údaje.

údaje boli dodané v anonymizovanom formáte a len ak nie je možné dosiahnuť požadovaný účel, tak je za súčasného splnenia ďalších podmienok povolený pseudonymizovaný formát.[24]
Ak má členský štát Európskej únie vrátane Slovenskej republiky dodržiavať povinnosť poskytovať zdravotné údaje na rôzne dalšie činnosti okrem poskytovania zdravotnej starostlivosti, tieto budú musieť byť vedené v jednom elektronickom informačnom systéme, ktorý bude mať súvis s elektronickou zdravotnou knižkou, resp. inou platformou, v ktorej budú zdravotnícki pracovníci zhromažďovať zdravotné údaje o pacientoch. Ak to prepojíme s prvotným používaním zdravotných údajov, v zmysle ktorého majú fyzické osoby právo na prístup k svojim údajom, právo na zápis vlastných údajov a na kontrolu prístupu iných subjektov, je nepochybné, že tieto dve funkcionality používania údajov by mali byť reflektované v jednom inštitúte. Týmto môže byť práve elektronická zdravotná knižka, ktorá je na základe súčasnej slovenskej legislatívy, konkrétne ustanovení § 2 ods. 1 a § 4 ods. 1 Zákona o NZIS obsahom národného registra elektronických zdravotných knižiek tvoriaceho popri iných registroch Národný zdravotnícky informačný systém.

Záver

Slovenská legislatíva síce reguluje formu zdravotnej dokumentácie primárne ako elektronickú vo forme elektronickej zdravotnej knižky, ale súčasne umožňuje výnimky vedenia zdravotnej dokumentácie vo forme papierovej zdravotnej dokumentácie, čoho dôsledkom je vznik a súbežné existovanie elektronického a papierového priestoru pre zdravotné údaje, ktorý je navyše regulovaný dvomi právnymi predpismi. To prináša rozdielnu právnu úpravu obsahu, formy a zdieľania zdravotných údajov.
V druhej časti tohto príspevku sme sa dostali k otázke, akým spôsobom môže Návrh nariadenia pre zdravotné údaje vyriešiť problém elektronickej zdravotnej dokumentácie tak, aby bola plnohodnotným prostriedkom pre poskytovanie zdravotnej starostlivosti ošetrujúcimi zdravotníckymi pracovníkmi bez ohľadu na geografické parametre, teda bez ohľadu na to, kde sa práve pacient nachádza. Podľa nášho názoru táto problematika predstavuje v súčasnosti bariéru cezhraničného poskytovania zdravotnej starostlivosti, pretože členské štáty Európskej únie majú rôzne právne úpravy tvorby a zdieľanie zdravotných záznamov, ktoré nie sú vždy v elektronickom formáte. To v praxi znamená, že ošetrujúci zdravotnícky pracovník

[24] Minimalizácia údajov je upravená v článku 44 Návrhu nariadenia pre zdravotné údaje.

v inej krajine nemá prístup k všetkým zdravotným údajom fyzickej osoby, ktorá potrebuje zdravotnú starostlivosť.[25]

Okrem uvedeného, ďalšou dôležitou oblasťou je ochrana osobných údajov, ktorá bude musieť byť robustná, a to najmä v súvislosti s druhotným využívaním zdravotných údajov. S tým súvisí otázka záruk bezpečnosti a stanovenia jasnej zodpovednosti za porušenia ochrany osobných údajov alebo ich zneužitia.

Záverom uvádzame niekoľko návrhov de lege ferenda prioritne orientovaných na Slovenskú republiku:

- zjednotenie právnej úpravy vo vzťahu k zdravotnej dokumentácii
- povinná digitálna transformácia aktivít poskytovateľov zdravotnej starostlivosti, ktorá obsahuje časový harmonogram pre postupné odstránenie písomnej zdravotnej dokumentácie
- povinné zaznamenávanie elektronických zdravotných záznamov do elektronickej zdravotnej knižky s tým, že v prípade využitia výnimky bude zdravotnícky pracovník povinný po pominutí dôvodu zakladajúceho výnimku, zaznamenať elektronický zdravotný záznam do elektronickej zdravotnej knižky
- limitácia výnimiek pre písomnú zdravotnú dokumentáciu a ich obmedzenie len na dočasné technické dôvody
- nastavenie sankčného mechanizmu pre nesúlad a nedodržiavanie povinností viesť výlučne elektronickú zdravotnú dokumentáciu vo forme elektronickej zdravotnej knižky

Zoznam použitej literatúry

1. CAPÍKOVÁ, S. – NOVÁKOVÁ, M. Zdravotná dokumentácia vo vzťahu k posudzovaniu zdravotnej spôsobilosti zamestnanca – vybrané otázky. In: Zborník príspevkov z vedeckej konferencie Zdravotná spôsobilosť zamestnancov. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, 2020.
2. HUMENÍK, I. – KOVÁČ, P. a kol. Zákon o zdravotnej starostlivosti. Komentár. Praha : C. H. Beck, 2015, 505 s. ISBN 978-80-8232-027-8
3. MILLIEU Ltd. Prehľad národných zákonov o elektronických zdravotných záznamoch v členských krajinách EÚ a ich interakcia s poskytovaním cezhraničných služieb eHealth, Brusel. 2013.
4. Návrh Nariadenia Európskeho parlamentu a Rady o Európskom priestore pre zdravotné údaje.

[25] MILLIEU. Prehľad národných zákonov o elektronických zdravotných záznamoch v členských krajinách EÚ a ich interakcia s poskytovaním cezhraničných služieb eHealth, Brusel. 2013. Dostupné na: https://health.ec.europa.eu/system/files/2019-02/laws_report_recommendations_en_0.pdf

5. Nariadenia Európskeho parlamentu a Rady (EÚ) č. 910/2014 z 23. júla 2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zrušení smernice 1999/93/ES.
6. POLICAR, R. Zdravotnická dokumentace v praxi. Praha : Grada Publishing, 2010, 224 s. ISBN 978-80-247-2358-7
7. Zákon č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov.
8. Zákon č. 153/2013 Z. z. o Národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov.

Kontaktné údaje

doc. JUDr. Soňa Sopúchová, PhD.
sona.sopuchova@flaw.uniba.sk
Univerzita Komenského v Bratislave
Právnická fakulta

DRAFT CONVENTION ON THE USE OF AUTOMATED VEHICLES IN TRAFFIC: THE ANSWER TO GLOBAL REGULATION?[1]

Jozef Andraško[2]

Abstract: This article presents an analysis of the Draft Convention on the Use of Automated Vehicles in Traffic, aimed at enhancing road safety through comprehensive legal provisions. The Convention, designed to complement existing international agreements without superseding them, addresses the deployment of automated driving systems (ADS) in road traffic. Key provisions include defining automated driving systems (ADS) and its operational domain, outlining the roles and responsibilities of automated driving providers, and setting ethical principles for the safe interaction of automated vehicles with other road users. Additionally, the Convention introduces requirements for remote management of automated vehicles and establishes guidelines for incident reporting and cyber security. Within the framework of the analysis, the author will highlight the potential drawbacks of the presented convention, as well as the unresolved questions it raises.

Key words: automated vehicles, remote management, cyber security

Introduction

Advancements in vehicle technology, which allow for some or all driving tasks to be handled by systems, are challenging traditional concepts of road traffic. The driver is no longer just the person inside the vehicle. Vehicles can also be controlled remotely. Drivers have the option to delegate driving tasks to systems, which can take full control of the vehicle. Different entities must take responsibility when driving tasks are handled by the system rather than the driver. These issues pose challenges to existing legal regulations concerning road traffic at international, European, and national levels. Regulating automated vehicles solely at the national and European levels will not achieve global harmonization, a fact recognized by the United Nations (hereinafter "UN"). To address this, the UN has initiated the creation of a new convention aimed at governing the safe deployment of automated vehicles. This

[1] This article was supported by the Slovak Research Development Agency under the Contract no. APVV-23-0137 - Legal and technical aspects of cybersecurity situational awareness.

[2] Comenius University Bratislava, Faculty of Law, Institute of Information Technology Law and Intellectual Property Law.

convention will also clarify the changing roles and responsibilities of individuals and organizations regarding these vehicles.
The goal of this contribution is not to give a comprehensive overview of the new legal framework for automated vehicles but to present a general outline of the draft convention. It emphasizes the most significant changes regarding the role of the driver and their responsibilities. Furthermore, an assessment will be conducted regarding the provisions related to ethical principles and cyber security.

Road to the Scoping Draft – Establishment of Group of Experts

In 2021, the Inland Transport Committee (hereinafter referred as "ITC")[3] approved the creation of the Group of Experts to draft a new legal framework for the use of automated vehicles (hereinafter referred as "GE.3") in both domestic and international traffic. During the fourth session of GE.3, held on 1-2 September 2022, experts from Finland, Malta, the Netherlands, Poland, Sweden, and the United Kingdom of Great Britain and Northern Ireland volunteered to initiate the drafting process. Additionally, experts from France, Germany, Greece, and Luxembourg expressed their interest in joining this effort and subsequently confirmed their participation following the session, along with Portugal. At the fifth session of GE.3, held on 12 December 2022, the **zero draft**[4] was introduced. This draft was developed through seven informal drafting meetings, conducted between September and November 2022, by a group of volunteers. The submission of the document was jointly made by Finland and the Netherlands. During the sixth session of GE.3, held on 4-5 May 2023, Informal document – "Assessment of the gaps of in the Conventions and Resolutions under the auspices of WP.1 and identification of the issues to be addressed – A scoping draft approach" (hereinafter referred as "Informal document

[3] The ITC is the is the highest policy-making body of the UN Economic Commission for Europe (UNECE) in the field of inland transport to help efficiently address global and regional needs in inland transport. The ITC has some permanent subsidiary bodies whose work is relevant for automated driving. In particular, the Working Party on Road Traffic Safety (WP.1) and the World Forum for Harmonization of Vehicle Regulations (WP.29). The Working Party on Road Traffic Safety (WP.1) is responsible for administering the international road-traffic related conventions including the 1968 Convention on Road Traffic and the 1968 Convention on Road Signs and Signals. The World Forum for Harmonization of Vehicle Regulations (WP.29) is responsible for the harmonisation of technical vehicle requirements. The GE.3 was established within the Working Party on Road Traffic Safety (WP.1).

[4] UNECE. Zero-draft - Skeleton of new international legal instrument (Convention) [on the use of automated vehicles in traffic]. Informal document No. 1, GE.3-05-01. 2 December 2022.

on Scoping Draft")[5] was submitted by the experts from Finland, Germany, Greece, Luxembourg, the Netherlands, Poland, Portugal, Sweden and the United Kingdom of Great Britain and Northern Ireland. This document includes an introduction and justification section, along with a Scoping Draft - Draft Convention on the use of automated vehicles in traffic (hereinafter referred as "Scoping Draft") designed to identify potential gaps in a practical context. Its purpose is to inform and contribute to the ongoing discourse regarding the necessity of a legal framework.[6]

The Scoping Draft – Background

Current legal regulation of road traffic at the level of international law, Geneva Convention on Road Traffic 1949 (hereinafter referred as "Geneva Convention") and Vienna Convention on Road Traffic 1968 (hereinafter referred as "Vienna Convention") do not prohibit the deployment of automated vehicles. However, their provisions are primarily centered around a human driver.

In July 2022, an amendment to the Vienna Convention came into effect, adding a new Article 34 bis and modifying Article 1 by incorporating new definitions for "automated driving system" and "dynamic control" (Article 1 (ab) and (ac)). Article 34 bis was introduced to allow automated driving, provided specific conditions are met. The amendment to the Vienna Convention was necessary for certain countries to permit trials on their roads, facilitating the development of technology and allowing for learning opportunities. However, the amendment did not set any provisions aimed at preventing inconsistencies in the regulation of automated vehicles at the national level. This absence could potentially hinder the introduction and safe use of these vehicles.[7]

The role of humans in automated vehicles differs significantly from that in conventional vehicles. There may be instances where no human is responsible for operating the vehicle. Various countries are formulating approaches to clarify the roles and responsibilities associated with automated driving. However, initial strategies are already beginning to diverge between nations.

Since road traffic rules were developed, the core responsibility has centered on the driver, who must ensure the vehicle's safe behavior in traffic. In developing the

[5] UNECE. Assessment of the gaps of in the Conventions and Resolutions under the auspices of WP.1 and identification of the issues to be addressed – A scoping draft approach. Informal document No. 2, GE.3-06-02. 02 May 2023

[6] Ibid. p. 2.

[7] These amendments came into effect on July 14, 2022. See UNECE. Report of the Global Forum for Road Traffic Safety on its eighty-first session Addendum Amendments to Article 1 and new Article 34bis. UN Doc ECE/TRANS/WP.1/173/Add.1. 14 December 2020. See also UNECE. Questions and answers regarding the new legal instrument on the use of automated vehicles in traffic. Informal document No. 2 (GE.3-05-02). 7 December 2022, p. 2 and 7.

Scoping Draft, the drafting volunteers identified key issues that the existing Geneva Convention and Vienna Convention do not address. A key consideration is whether there are any specific conditions under which the driver can delegate dynamic control to the automated driving system (hereinafter "ADS"). It becomes essential to determine how responsibility for the dynamic control of the vehicle can be attributed at any given time, especially in situations where the system is engaged. This leads to further inquiries into the role and responsibilities of the driver when the ADS is active, if indeed there is still a driver present in the vehicle. If the driver is no longer responsible for certain tasks typically attributed to them, then who should bear these responsibilities? Since the ADS does not have legal personhood, this issue raises the need to identify new entities that may assume these responsibilities. Ensuring accountability across jurisdictions is another challenge. How can we make the necessary information about these entities available across different regions to enable effective enforcement of traffic rules? Furthermore, for vehicles operating without a human driver, the question arises as to who holds responsibility for their safe operation. This evolving landscape of automated driving may also demand the definition of new concepts and terms. To support this shift, international cooperation and data sharing, particularly among relevant authorities, will be crucial for the consistent application and enforcement of traffic regulations.[8]

At the third session of GE.3, held on 16 May 2022, a summary report was presented which provided the results of a survey conducted among the Contracting Parties involved in the activities of GE.3. The survey highlighted the top three road safety risks associated with automated vehicles: the lack of clarity regarding roles and responsibilities, issues related to take-over requests and fallback user expectations during transition demands, and risks concerning the technical performance and skill of vehicle automation, mode awareness, and challenges like data protection and hacking.[9]

The Scoping Draft – Scope and Definitions

The Scoping Draft includes six chapters and 33 articles. The final chapter lists the article titles, while the text of the provisions will be developed later.

The Scoping Draft does not supersede the legal obligations established by the Geneva Convention and Viena Convention. Instead, it complements these conventions in relation to the safe deployment of automated vehicles in road traffic, with the objective of enhancing road safety.[10]

[8] Informal document on Scoping Draft, p. 4.

[9] Informal document on Scoping Draft, p. 6.

[10] Scoping Draft, Art. 1 (1).

The draft of new legal instrument aims to set legal provisions for:[11]

a) The safe deployment of automated vehicles in road traffic, in particular interaction between automated vehicles and the road users, especially vulnerable road users;
b) The changing roles and responsibilities of natural and legal persons in relation to automated vehicles.

Furthermore, the draft of new legal instrument is applicable only to vehicles that are equipped with an ADS while the ADS is engaged. When the ADS is not engaged the provisions do not apply, but the provisions of the Geneva Convention and Vienna Convention apply to their respective parties.[12]

A current example of an ADS in use is the Automated Lane Keeping System (ALKS), which is governed by UN Regulation No. 157 on Automated Lane Keeping Systems. This regulation took effect in January 2021, with an increase in the permitted speed limit to 130 km/h introduced in January 2023.[13] ALKS operates at SAE Level 3 automation.[14]

The Scoping Draft contains twelve definitions. These definitions are used in hard law[15] and soft law regulations[16] and technical standards[17] related to automated vehicles (ADS, dynamic control, automated vehicle, driver, Minimal Risk Manoeuvre, Operational Design Domain, transition demand, remote management, remote management provider, remote management agent). However, new definitions related to new concepts in the field of automated vehicles can also be found here. In particular, driver-in-readiness and automated driving provider. Driver-in-readiness means "a driver who has delegated dynamic control to the ADS, but retains responsibility for the other duties placed on a driver". Automated Driving Provider means "an entity that assumes responsibilities for the behaviour of the automated vehicle on the road when the ADS is engaged".

Ethical principles

[11] Scoping Draft, Art. 1 (2).

[12] Scoping Draft, Art. 1 (3).

[13] UNECE. Proposal for the 01 series of amendments to UN Regulation No. 157 (Automated Lane Keeping Systems). ECE/TRANS/WP.29/2022/59/Rev.1. 30 May 2022.

[14] In 2021 German Federal Motor Transport Authority (KBA) granted type approval to Mercedes-Benz's automated lane-keeping system (ALKS), known as Drive Pilot. For the issue of automation levels, see Andraško, J., Mesarčík, M. Automated Vehicles and New Transportation Services: Exploring Selected Legal Issues. In Troitiño, D. R., Kerikmäe, T., Hamuľák, O. Digital Development of the European Union An Interdisciplinary Perspective. Springer. 2024, pp. 277 – 299.

[15] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users. Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the

Article 4 of the Scoping Draft outlines general ethical principles that should guide the design, maintenance, and operation of automated vehicles. The primary obligation is to ensure that such vehicles do not endanger or obstruct traffic, cause harm to humans, or damage public or private property. Automated vehicles are required to prevent accidents whenever feasible, and in unavoidable situations, they must minimize harm. The highest priority in these circumstances is the protection of human life, both inside and outside the vehicle. Additionally, automated vehicles must pay particular attention to ensure the safety of vulnerable road users, including pedestrians, cyclists, children, the elderly, and individuals with disabilities.[18]

Automated vehicle with and without driver in the vehicle

The Scoping Draft delineates scenarios where human driver is in the vehicle and when there is no human driver in the vehicle. In the first case, when a **driver is in the vehicle** a distinction is made between two situations:

European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles. More on the issue of regulation of automated vehicles in general, see also Sever, T., Contissa, G. Automated driving regulations – where are we now? In Transportation research interdisciplinary perspectives, 2024. 24, pp. 1-19. Lundahl, J. RISE Report. Steering the Future: An Overview of Current and Upcoming Regulations in Automated Driving. Version 0.5. 2024, 37 p. Košťálová, S. The German perspective on the deployment of automated vehicles. In Acta Facultatis Iuridicae Universitatis Comenianae. Vol. 42, No. 2, 2023, pp. 121 – 137.

[16] UNECE. Resolution on the Deployment of Highly and Fully Automated Vehicles in Road Traffic. UNECE. Global Forum for Road Traffic Safety (WP.1) resolution on safety considerations for activities other than driving undertaken by drivers when automated driving systems issuing transition demands exercise dynamic control. ECE/TRANS/WP.1/2021/2/Rev.1. 29 June 2022. UNECE. Proposed Draft Resolution on Remote Driving. ECE/TRANS/WP.1/2019/2. 5 July 2019. UNECE. Informal paper on remote driving. Situations when a driver operates a vehicle from the outside of the vehicle. Informal document No.1. 14 September 2021. UNECE. Automated driving. Informal document No.1/Rev.1 (September 2021). 19 September 2022. UNECE. Automated driving Situations when a driver operates a vehicle from the outside of the
Vehicle. Informal document No. 1/Rev.2 (September 2021). 6 March 2023. UNECE. Remote management of automated vehicles. Informal document No.16. 9 March 2023.

[17] SAE J3016_202104Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles.

[18] The Scoping Draft ethical principles are not the first legislative provisions of ethical principles applicable to automated vehicles. Commission Implementing Regulation (EU) 2022/1426 on ADS provisions in connection with performance requirements for ADS express the need to protect human life. In more detail, see Annex II, point 2.1.1.1, 2.1.1.2 and point 1.1.2 letter d) of the implementing regulation in question. For ethical issues, see also Košťálová, S. Top priority: protecting life as a regulatory imperative. In Comenius odborný blog. Available https://comeniusblog.flaw.uniba.sk/2024/10/10/top-priority-protecting-life-as-a-regulatory-imperative/.

a) a person exercises all or part of the dynamic control of an automated vehicle,
b) a driver delegates dynamic control to the ADS.

When the person is exercising all or part of the dynamic control including monitoring its behaviour on the road with a view to immediate and safety-critical intervention is considered to be a driver and bear all the duties of a driver. In the case when a driver delegates dynamic control to the ADS, then, for as long as that system is engaged the driver becomes a driver-in-readiness and is responsible for the relevant duties. The entity called automated driving provider assumes responsibilities for the behaviour of the vehicle on the road.[19]

The driver-in-readiness must be prepared to assume control of the vehicle when delegating dynamic control do ADS, including by holding the necessary knowledge, skills, and driving permits as prescribed by domestic legislation. They must also maintain the physical and mental ability to drive, remain in the vehicle in a position to take over control, and refrain from performing activities that may hinder their ability to respond to a transition demand from the ADS. The driver is obligated to respond to such demands in a timely and appropriate manner. Additionally, a driver-in-readiness is responsible for all driver duties not related to the behaviour of the vehicle on the road but does not bear responsibility for the vehicle's behavior in road traffic as long as the ADS remains in control.[20]

In cases where the ADS of an automated vehicle is engaged, the responsibility for the vehicle's behavior on the road rests with the automated driving provider. The Contracting Parties are tasked with implementing mechanisms to identify automated driving providers and the individuals responsible within those entities for each vehicle equipped with an ADS.[21]

Situations involving **automated vehicle without driver in vehicle** are related to remote management according to the Scoping Draft. Remote management means "the activities required to manage one or more automated vehicles which do not require a driver in the vehicle, including beyond-line-of-sight using telecommunications".[22] Remote management can consist of measures of remote assistance and remote driving.[23]

Remote assistance in the context of ADS entails various support measures aimed at ensuring safety both inside and outside the vehicle while the ADS retains dynamic control. These measures include general vehicle status monitoring, which encompasses tracking the vehicle's location with no requirement for full situational awareness. Remote assistance also involves monitoring the interior of the vehicle,

[19] Scoping Draft, Art. 12 (1).
[20] Scoping Draft, Art. 15.
[21] Scoping Draft, Art. 17.
[22] Scoping Draft, Art. 2 (j).
[23] Scoping Draft, Art. 22 and 23.

particularly with regard to the status of passengers and cargo. It plays a role in summoning help when needed and managing technical incidents and breakdowns. Additionally, remote assistance contributes to the strategic aspects of the driving task, including instructing an ADS to perform specific manoeuvres or approve specific manoeuvres proposed by the ADS. Finally, communication with authorities, first responders, and other road users is also a key component of remote assistance.[24]
Remote driving refers to scenarios where a person, located outside the automated vehicle, exercises all or part of the dynamic control of that vehicle, including monitoring its behaviour on the road with a view to immediate and safety-critical intervention. In such instances, the person is legally recognized as the driver and bears sole responsibility for the dynamic control of the automated vehicle.[25]
The Scoping Draft also regulates the remote management provider and remote management agents. Remote management providers are entities responsible for the remote management of an automated vehicle. The Contracting Parties are obliged to establish appropriate means to identify remote management providers as well as responsible persons within the entities.[26]
Remote management agent means "a natural person performing remote management activities on behalf of the Remote Management Provider"[27].
The Scoping Draft outlines that the remote management agent will be responsible for providing remote assistance and remote driving. The remote management agent must hold appropriate training and qualifications necessary for the activities involved in remote management. Additionally, they are required to maintain the necessary physical and mental fitness during their time on duty. Furthermore, they are expected to remain attentive to communications from the vehicle and respond to road traffic incidents and situations. If a remote management agent is classified as a driver under Article 23(3), they must carefully consider the distinction between the legal obligations and responsibilities associated with remote assistance and those inherent to remote driving.[28]

Cyber security

Cyber security incidents that result in the unauthorized control of a automated vehicle can have severe and potentially fatal consequences, not only for the driver and passengers but also for other road users. Such incidents can compromise road safety, leading to property damage, personal injury, or loss of life. Therefore,

[24] Scoping Draft, Art. 23.
[25] Scoping Draft, Art. 23 (3).
[26] Scoping Draft, Art. 25 (1).
[27] Scoping Draft, Art. 2 (l) and 28.
[28] Scoping Draft, Art. 28.

addressing the cyber security concerns of automated vehicles is imperative. It is crucial to ensure that vehicles and their systems are protected against a broad range of cyber threats, thus preserving road traffic integrity. The significance of cyber security is highlighted in the Scoping Draft.[29]

The automated driving provider is required to implement appropriate measures to ensure that automated vehicles are and remain resilient to cybers security threats that could compromise the safe operation of the vehicle. Additionally, steps must be taken to minimize the impact of such threats on road traffic safety. Furthermore, the automated driving provider is obligated to inform relevant authorities and users of automated vehicles, if necessary, regarding potential cyber security threats and incidents.[30]

Obligations in the field of cyber security also apply to the remote management provider. In particular, the remote management provider is obliged to ensure adequate communications network connections and cyber security of their operations and resilience of the operation in case of any disruption to the connections.[31]

Conclusions

The Scoping Draft marks a crucial legislative step toward global harmonization in the field of automated vehicles. While amending the Vienna Convention is a significant advancement in allowing the deployment of automated vehicles, it leaves unresolved key questions. These include the changing role of the driver, the introduction of new roles such as remote drivers or remote assistants, and the responsibilities of entities overseeing control when driving tasks are performed by the system.

The Scoping Draft emphasizes that the ethical framework guiding the design, maintenance, and operation of automated vehicles must prioritize the protection of human life and the safety of vulnerable road users. It establishes a primary obligation for these vehicles to avoid endangering traffic or causing harm to individuals or property. Automated vehicles are mandated to prevent accidents wherever possible and, in cases where accidents are unavoidable, to minimize the resultant harm. The main principle is to prioritize human safety, especially for those most at risk, such as pedestrians, cyclists, children, the elderly, and individuals with disabilities.

[29] For more information on the cyber security of automated vehicles, see: Andraško, J. Cyber Security of Automated and Fully Automated Vehicles – New Legal Instruments. In Šišková, N. (ed.). Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law. Kluwer Law International. 2024, 392 p.

[30] Scoping Draft, Art. 20.

[31] Scoping Draft, Art. 26 (1) (b).

The Scoping Draft establishes separate regulatory frameworks for situations involving both human drivers and ADS. When a human driver is present, the Scoping Draft outlines two key scenarios: one in which the driver exercises dynamic control over the vehicle, and another where control is handed over to the ADS. In the first scenario, the human driver retains all responsibilities. In the second scenario, the driver is designated as a driver-in-readiness, meaning they must be prepared to intervene if necessary. However, they must meet specific qualifications and remain capable of taking control when needed. When an ADS is engaged, the automated driving provider is responsible for the vehicle's behavior on the road.

The Scoping Draft also addresses scenarios where no driver is present, highlighting the concept of remote management, which includes remote assistance and remote driving. Remote assistance involves several safety measures while the ADS maintains control. This includes monitoring the vehicle's status and communicating with authorities, first responders and other road users. In contrast, remote driving requires an individual to have complete dynamic control over the vehicle from a distance. In this case, the individual is legally recognized as the driver and is solely responsible for the vehicle's operation.

The urgency to address cyber security concerns in automated vehicles is underscored by the necessity of implementing measures against diverse cyber threats. Automated driving providers bear the responsibility of ensuring that these vehicles maintain resilience to cyber security risks that could jeopardize safe operation. This includes the obligation to mitigate the effects of such threats on overall traffic safety and to inform relevant authorities and users about any potential cyber security incidents. Additionally, remote management provider must ensure adequate communication network connections, cyber security, and operational resilience in case of any disruptions.

However, the Scoping Draft raises several unanswered questions that the contracting states will need to address when implementing the new legal instrument in the form of a convention. For instance, the Contracting Parties are required to identify automated driving providers and the individuals responsible within these organizations for each automated vehicle equipped with an ADS. In addition, they must identify remote management providers and the individuals responsible within those entities. Furthermore, Contracting Parties must specify which vehicles are under the responsibility of each remote management provider. The Scoping Draft lacks a list of entities for automated driving providers and remote management providers. Different interpretations of Contracting Parties may lead to situation that one entity being recognized as an automated driving provider or remote management provider in one state, but not in another. The Scoping Draft does not clarify whether the remote driver and remote assistance need to be located in the state where the automated vehicle is being operated.

Furthermore, from a legal point of view, attributing obligations to the automated vehicle, rather than the driver or another individual, appears to be problematic.
It is important to note that Scoping Draft will be subject to detailed scrutiny to enhance a shared understanding of the gaps in the existing conventions and the issues requiring resolution, with the aim of fostering consensus on appropriate solutions. As an initial step, this examination could be conducted through a survey engaging all GE.3 members. Following this, further steps may include validating and testing the applicability of the proposed draft across various use cases, as well as conducting consultations with industry stakeholders.[32]

List of references

1. Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users.
2. Commission Implementing Regulation (EU) 2022/1426 of 5 August 2022 laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated vehicles.
3. UNECE. Zero-draft - Skeleton of new international legal instrument (Convention) [on the use of automated vehicles in traffic]. Informal document No. 1, GE.3-05-01. 2 December 2022
4. UNECE. Assessment of the gaps of in the Conventions and Resolutions under the auspices of WP.1 and identification of the issues to be addressed – A scoping draft approach. Informal document No. 2, GE.3-06-02. 02 May 2023
5. UNECE. Report of the Global Forum for Road Traffic Safety on its eighty-first session Addendum Amendments to Article 1 and new Article 34bis. UN Doc ECE/TRANS/WP.1/173/Add.1. 14 December 2020
6. UNECE. Questions and answers regarding the new legal instrument on the use of automated vehicles in traffic. Informal document No. 2 (GE.3-05-02). 7 December 2022
7. UNECE. Proposal for the 01 series of amendments to UN Regulation No. 157 (Automated Lane Keeping Systems). ECE/TRANS/WP.29/2022/59/Rev.1. 30 May 2022.
8. UNECE. Resolution on the Deployment of Highly and Fully Automated Vehicles in Road Traffic.

[32] Informal document on Scoping Draft, p. 5.

9. UNECE. Global Forum for Road Traffic Safety (WP.1) resolution on safety considerations for activities other than driving undertaken by drivers when automated driving systems issuing transition demands exercise dynamic control. ECE/TRANS/WP.1/2021/2/Rev.1. 29 June 2022
10. UNECE. Proposed Draft Resolution on Remote Driving. ECE/TRANS/WP.1/2019/2. 5 July 2019. UNECE. Informal paper on remote driving. Situations when a driver operates a vehicle from the outside of the vehicle. Informal document No.1. 14 September 2021
11. UNECE. Automated driving. Informal document No.1/Rev.1 (September 2021). 19 September 2022. UNECE. Automated driving Situations when a driver operates a vehicle from the outside of the Vehicle. Informal document No. 1/Rev.2 (September 2021). 6 March 2023
12. UNECE. Remote management of automated vehicles. Informal document No.16. 9 March 2023
13. SAE J3016_202104Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles
14. Sever, T., Contissa, G. Automated driving regulations – where are we now? In Transportation research interdisciplinary perspectives, 2024. 24, pp. 1-19.
15. Lundahl, J. RISE Report. Steering the Future: An Overview of Current and Upcoming Regulations in Automated Driving. Version 0.5. 2024, 37 p.
16. Šišková, N. (ed.). Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law. Kluwer Law International. 2024, 392 p.
17. Troitiño, D. R., Kerikmäe, T., Hamuľák, O. Digital Development of the European Union An Interdisciplinary Perspective. Springer. 2024, pp. 277 – 299.
18. Košťálová, S. Top priority: protecting life as a regulatory imperative. In Comenius odborný blog. Available https://comeniusblog.flaw.uniba.sk/2024/10/10/top-priority-protecting-life-as-a-regulatory-imperative/.
19. Košťálová, S. The German perspective on the deployment of automated vehicles. In Acta Facultatis Iuridicae Universitatis Comenianae. Vol. 42, No. 2, 2023, pp. 121 – 137.

Contact

doc. JUDr. Jozef Andraško, PhD.
jozef.andrasko@flaw.uniba.sk
Comenius University Bratislava, Faculty of Law, Institute of Information Technology Law and Intellectual Property Law.

VÝZVY A KRITIKA EURÓPSKEJ TECHNICKEJ NORMALIZÁCIE V OBLASTI KYBERNETICKEJ BEZPEČNOSTI A MIMO NEJ[1]

CHALLENGES AND CRITICISMS OF EUROPEAN TECHNICAL STANDARDISATION IN CYBERSECURITY AND BEYOND

Michal Rampášek[2]

Abstrakt: Technická normalizácia kybernetickej bezpečnosti prináša mnohé výhody, ale zároveň predstavuje významné výzvy. Nedávna kritika poukazuje na nedostatočné začlenenie ľudských práv do tvorby noriem a marginalizáciu netechnických odborných znalostí, ako sú spoločenské vedy a etika. Vývoj európskej technickej normalizácie viedol k jej „juridifikácii", ktorá považuje technické normy za súčasť práva EÚ než len za technické usmernenia, čím sa vplyv európskych normalizačných organizácií rozšíril za hranice technickej sféry do politickej diskreácie. Tento posun si vyžaduje väčšiu kontrolu a opatrné zapojenie regulačných orgánov, aby sa zabezpečil súlad noriem s demokratickými hodnotami, ekologickými politikami a sociálnymi zásadami. Príspevok sa venuje týmto výzvam a nevyhnutnosti začleniť do procesov normalizácie širšiu účasť zainteresovaných strán a úvahy o základných právach, najmä v kontexte umelej inteligencie, kde dosiahnutie súladu presahuje rámec bezpečnosti a týka sa aj etických a právnych oblastí.

Kľúčové slová: technické normy, juridifikácia, kybernetická bezpečnosť, umlá inteligencia, ľudské práva

Abstract: Technical standardisation in cybersecurity brings many benefits, but it also poses significant challenges. Recent criticism points to the lack of integration of human rights in standards development and the marginalisation of non-technical expertise such as social sciences and ethics. The development of technical standardisation has led to its 'juridification', which see technical standards as part of EU law rather than mere technical guidelines, thus

[1] Tento článok bol vypracovaný s podporou grantu udeleného Agentúry na podporu výskumu a vývoja č. APVV-23-0137 Právne a technické aspekty situačného povedomia o kybernetickej bezpečnosti

[2] Ústav práva informačných technológií a práva duševného vlastníctva, Právnická fakulta Univerzity Komenského v Bratislave

extending the influence of European standardisation organisations beyond the technical sphere into political discretion. This shift requires greater scrutiny and careful involvement of regulators to ensure that standards are consistent with democratic values, environmental policies and social principles. This paper addresses these challenges and the need to incorporate broader stakeholder participation and fundamental rights considerations into standardisation processes, especially in the context of artificial intelligence, where compliance goes beyond safety and extends to ethical and legal areas.

Key words: technical standards, juridification, cybersecurity, artificialintelligence, humanrights

Úvod

Predpisy z oblasti kybernetickej bezpečnosti, napríklad smernica NIS2[3], návrh nariadenia CRA[4] či nariadenie AIA[5], považujú technické normy a certifikáciu za jeden z najdôležitejších prvkov pre preukazovaní súladu s požiadavkami kybernetickej bezpečnosti.

Technická normalizácia je proces vedúci k zjednoteniu podľa jednotných a presne daných noriem (štandardov, z angl. *standards*). Technická normalizácia sa môže vzťahovať na produkty, služby, procesy, materiály, subjekty a systémy manažérstva, čím poukazuje na určitú úroveň kvality, bezpečnosti a spoľahlivosti daného produktu, služieb subjektov či systémov.

Technická norma je súbor pravidiel, usmernení, technických špecifikácií alebo výsledkov činností, ktoré odzrkadľujú aktuálny stav vedy a techniky, ktorý je výsledkom konsenzu (dohody) zainteresovaných strán a podlieha systematickým previerkam jej aktuálnosti (spravidla každých päť rokov).[6] Technické normy sú teda

[3] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2), článok 21.

[4] Návrh Nariadenia Európskeho parlamentu a Rady (EÚ) 2024/... o horizontálnych požiadavkách na kybernetickú bezpečnosť výrobkov s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (Akt o kybernetickej odolnosti) v znení prijatom Európskym parlamentom 12. marca 2024, najmä článok 27 (ďalej len „návrh CRA").

[5] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii), najmä recitál 117, 121, článok 40.

[6] Zo slovenskej definície technickej normy podľa § 3 ods. 1 zákon č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov (ďalej len *„zákon o technickej normalizácii*").

kodifikovanou najlepšou praxou (z angl. *best practice*), teda dokumentom, ktorý obsahuje všeobecne uznávané technické riešenia, ktoré zároveň efektívne ošetrujú riziká.[7] Tieto typické charakteristiky technickej normy ju odlišujú nielen obsahom, ale aj procesom tvorby od legislatívneho procesu tvorby právnych predpisov. Od všeobecne záväzných právnych predpisov, nie je možné efektívne očakávať špecifické technické detaily – to je úlohou technických noriem.[8]
Normy vo všeobecnosti nie sú záväzné a ich dodržanie môže upraviť ako povinnosť iba všeobecne záväzný právny predpis. V Slovenskej republike zákon o technickej normalizácií umožňuje, aby bola STN *záväzná, hoci len nepriamo*.[9]

Európska technická normalizácia

Technickú normalizáciu v európskom priestore zastrešuje činnosť Európskeho výboru pre normalizáciu (CEN – z francúzskeho „*Comité Européen de Normalisation*") spoločne s Európskym výborom pre normalizáciu v elektrotechnike (CENELEC – z francúzskeho „*Comité Européen de Normalisation Électrotechnique*"). Je to podobne ako v Medzinárodnej organizácii pre normalizáciu (ISO), kde sú technické normy v oblasti informačnej a kybernetickej bezpečnosti vydávané spoločne s Medzinárodnou elektrotechnickou komisiou (IEC). Rovnako ako v ISO/IEC, sa aj CEN/CENELEC opiera o štruktúru technických komisií. Pre oblasť informačnej a kybernetickej bezpečnosti podstatné dve. V prvom rade je to komisia CEN-CLC/JTC 13 „Kybernetická bezpečnosť a ochrana údajov", ktorej úlohou je nielen prevziať príslušné medzinárodné normy najmä z príslušnej technickej komisie ISO/IEC, ale aj vyvinúť vlastné európske normy (EN) na podporu právnych aktov EÚ (napr. CSA, návrh CRA, DORA, AI Act, NIS2). V druhom rade, je to komisia CLC/TC 65X „Meranie, riadenie a automatizácia priemyselných procesov", ktorá je ďalším hlavným zdrojom technických noriem súvisiacich s kybernetickou bezpečnosťou operačných technológií (OT).

Harmonizované normy

Postup vypracovania harmonizovaných noriem je stanovený v nariadení (EÚ) č. 1025/2012 o európskej normalizácii (ďalej len „*nariadenie č. 1025/2012*"). Nariadenie

[7] Kompetenčné a certifikačné centrum kybernetickej bezpečnosti: *Technické normy v kyberbezpečnosti.* [online] [13.09.2024]. Dostupné na: https://cybercompetence.sk/technicke-normy-v-kyberbezpecnosti/.
[8] MAKATURA, Ivan.: *Technická normalizácia v informačnej a kybernetickej bezpečnosti*. In: Bezpečnosť v praxi [on-line]. Žilina: Poradca podnikateľa, 2024. ISSN 2729-885X. [13.9.2024]. Dostupné na: https://www.bezpecnostvpraxi.sk/odborny-clanok/technicka-normalizacia-v-informacnej-a-kybernetickej-bezpecnosti.htm.
[9] MAKATURA, Ivan.: *Technická normalizácia v informačnej a kybernetickej bezpečnosti*, porov. § 12 ods. 2 zákona o normalizácii.

č. 1025/2012 kladie dôraz na vyvážené zastúpenie záujmov za účasti všetkých relevantných zainteresovaných strán pri vypracúvaní noriem, najmä malých a stredných podnikov, spotrebiteľských organizácií a zainteresovaných strán v oblasti životného prostredia a sociálnej oblasti.[10] V európskom systéme normalizácie však ústrednú úlohu zohráva Európska Komisia (ďalej aj len „Komisia"). Jedine Komisia je oprávnená požadovať vypracovanie harmonizovanej normy s cieľom implementovať smernicu alebo nariadenie. Komisia tiež určuje obsahové kritériá, ktoré musí požadovaná harmonizovaná norma spĺňať, a stanovuje lehotu na jej prijatie.[11] Napokon Komisia nielen úzko dohliada na vypracovanie harmonizovaných technických noriem, ale poskytuje aj značné finančné prostriedky (až 35 % rozpočtu CEN).[12] A je to opäť len Komisia , ktorá rozhodne, či v *Úradnom vestníku Európskej únie* uverejní, neuverejní alebo uverejní s obmedzením odkazy na príslušnú harmonizovanú normu.[13]

Európske normy sa teda stávajú harmonizovanými vtedy, keď ich európske normalizačné organizácie oficiálne predložia Komisii a Komisia ich vyhlási v Úradnom vestníku Európskej únie, najmä preto, aby so zreteľom na právne dôsledky bol stanovený dátum, od ktorého možno zhodu s európskou legislatívou predpokladať a aby všetky hospodárske subjekty v EÚ mali rovnakú východiskovú pozíciu pri využívaní harmonizovaných noriem. Dodržiavanie harmonizovaných noriem síce nie je povinné, pre výrobky, ktoré spĺňajú tieto normy, platí predpoklad zhody so základnými požiadavkami, ktoré sa ich týkajú a sú stanovené príslušnými harmonizačnými právnymi predpismi Únie.[14] Tento právny účinok, ktorý priznáva uvedená právna úprava, predstavuje jednu z podstatných vlastností týchto noriem. Harmonizované normy sú teda jedným z hlavných prostriedkov na dosiahnutie zhody a súladu s legislatívnymi požiadavkami.

Uvedené je osobitné významné pre posudzovanie zhody s regulačnými požiadavkami pre vysokorizikové systémy AI alebo modely AI na všeobecné účely[15] ako aj pre produkty s digitálnymi prvkami.[16]

V oblasti umelej inteligencie, európske normy vypracuje CEN/CENELEC na základe vykonávacieho rozhodnutia Komisie[17], ktorá požiadala o vypracovanie nových

[10] Článok 5 a 6 nariadenia č. 1025/2012.

[11] Článok 10 ods. 1 nariadenia č. 1025/2012.

[12] Návrhy Generálnej advokátky Laila Medina z 22 júna 2023 vo veci C-588/21P Public.Resource.Org, Inc., Right to Know CLG proti Európskej komisii; Článok 15 nariadenia č. 1025/2012.

[13] Článok 11 ods. 1 písm. a) nariadenia č. 1025/2012.

[14] Recitál č. 5 nariadenia č. 1025/2012.

[15] Článok 40 ods. 1 AIA.

[16] Článok 27 ods. 1 návrhu CRA.

[17] Vykonávacie rozhodnutie Komisie z 22. mája 2023 o žiadosti o normalizáciu adresovanej Európskemu výboru pre normalizáciu a Európskemu výboru pre normalizáciu v elektrotechnike na

európskych noriem alebo európskych normalizačných produktov, ako sa uvádza v prílohe I k vykonávaciemu rozhodnutiu, a to do 30. apríla 2025.

Odvrátená strana technickej normalizácie

Napriek širokej škále výhod technickej normalizácie kybernetickej bezpečnosti existujú aj nedostatky spojené s procesom tvorby noriem. Medzi popísané nedostatky patrí aj nedostatočné začleňovanie ochrany ľudských práv do procesov tvorby noriem. Zameranie sa na technologické odborné znalosti na úkor iných súborov zručností, sťažuje akceptovanie odborníkov so vzdelaním v oblasti sociálnych vied, ľudských práv alebo etiky ako legitímnych prispievateľov.[18] Tieto zistenia viedli k odporúčaniu Vysokého komisára OSN pre ľudské práva, aby normalizačné organizácie okrem iného zaviedli primerané postupy náležitej starostlivosti v oblasti ľudských práv vrátane posudzovania skutočných a potenciálnych vplyvov na ľudské práva.[19] Mnohé normy definujú procesy a činnosti, ktoré priamo reagujú na určité obavy súvisiace s ľudskými právami. Patria sem napríklad normy, ktoré sú určené na zlepšenie ochranu súkromia prostredníctvom organizačných opatrení, ako je napríklad norma ISO/IEC o riadení rizík súvisiacich so súkromím osobitne zameraná na ujmy na súkromí fyzickej osoby (ISO/IEC 27557:2022). Ďalšie normy sú zamerané na zlepšenie prístupnosti webových stránok, digitálnych technológií a digitálnych služieb pre osoby so zdravotným postihnutím (napr. ISO/IEC 40500:2012).

Ďalšie obavy súvisia s absenciou zastúpenia niektorých zainteresovaných strán a tých, ktorých sa týka používanie produktov vrátane technológie umelej inteligencie, v normalizačných alebo certifikačných procesoch. Združenia zastupujúce záujmy spotrebiteľov, ako aj združenia zastupujúce pracovníkov alebo malé podniky nemajú oficiálne právo zúčastňovať sa na práci ISO/IEC, čo vedie k situácii, keď zástupcovia z priemyslu navrhujú tie predpisy, ktorými sa sami budú riadiť.[20]

---

podporu politiky Únie v oblasti umelej inteligencie C(2023)3215 [online] [13.9.2024]. Dostupné na: https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en.

[18] 'Relationship between human rights and technical standard-setting processes for new and emerging digital technologies and the practical application of the Guiding Principles on Business and Human Rights - Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/53/42' (18.9.2023) s. 16 [13.9.2024]. Dostupné na: https://www.ohchr.org/en/hr-bodies/hrc/regular-sessions/session53/list-reports

[19] Tamže, s. 17 .

[20] GORNET, Mélanie, MAXWELL, Winston: 'The European approach to regulating AI through technical standards' (*Internet Policy Review*, 2024 13 (3)) 14 [13.9.2024]. Dostupné na: https://hal.science/hal-04254949v2/document

Juridifikácia harmonizovaných noriem

Právny význam harmonizovaných noriem vzrástol natoľko, že predpisy nie je možné plne pochopiť bez príslušných noriem, čím sa harmonizované normy stávajú *de facto* záväznými.[21] Nedávne rozhodnutie Súdneho dvora EÚ vo veci Public.Resource.Org[22], ako aj stanovisko generálneho advokáta v tejto veci, vyvoláva otázky týkajúce sa demokratických procesov v normalizačných organizáciách. Vývoj technických noriem vstúpil do štádia, ktoré akademici označujú ako „juridifikácia"[23], keď sa normy, aj keď nie sú záväzné, považujú za súčasť práva EÚ. [24]
V rozsudku Fra.bo Súdny dvor v podstate uznal, že napriek tomu, že normalizačné a certifikačné orgány sú súkromnoprávnymi subjektmi, môžu vykonávať verejnoprávne právomoci a že aj keď sú vnútroštátne technické normy dobrovoľné (keďže hospodárske subjekty majú aspoň teoreticky alternatívne prostriedky na preukázanie súladu so základnými požiadavkami príslušných sekundárnych právnych predpisov), *de facto* môžu mať záväzné účinky.[25] Súdny dvor v kľúčovom rozsudku James Elliott rozhodol, že harmonizované normy sú vzhľadom na svoje právne účinky súčasťou práva Únie, a Súdny dvor má právo ich vykladať nakoľko majú povahu opatrení vykonávajúcich právny akt Únie. [26]

---

[21] Rozsudok Súdneho dvora (štvrtá komora) z 12. júla 2012. v prípade C-171/11 Fra.bo SpA proti Deutsche Vereinigung des Gas- und Wasserfaches eV (DVGW) – Technisch-Wissenschaftlicher Verein.

[22] Rozsudok Súdneho dvora (veľká komora) z 5. marca 2024 v prípade C-588/21 *Public.Resource.Org, Inc. and Right to Know CLG proti Európska komisia*, bod 73.

[23] SCHAPEL, Harm: 'The New Approach to the New Approach: The Juridification of Harmonised Standards in EU Law.' (2013) Maastricht Journal of European and Comparative Law, 20 (4): 521–33 [13.9.2024]. Dostupné na: https://doi.org/10.1177/1023263X1302000404.; VAN GESTEL, Rob a MICKLITZ Hans-W.: "European Integration through Standardisation: How Judicial Review Is Breaking Down the Club House of Private Standardisation Bodies" [2013] *Common Market Law Review* 145-182 [13.9.2024]. Dostupné na: https://doi.org/10.54648/cola2013007; ELIANTONIO Mariolina a COLOMBO Carlo, "Harmonized Technical Standards as Part of EU Law: Juridification with a Number of Unresolved Legitimacy Concerns?" [2017] *Maastricht Journal of European and Comparative Law*, 323-340 [13.9.2024]. Dostupné na: https://doi.org/10.1177/1023263X17709753.

[24] TOVO, Carlo: 'Judicial Review of Harmonised Standards: Changing the Paradigms of Legality and Legitimacy of Private Rulemaking Under EU Law.' (2018) Common Market Law Review, 55 (4). [13.9.2024]. Dostupné na: https://doi.org/10.54648/cola2018096 ; VOLPATO, Annalisa: 'The Legal Effects of Harmonised Standards in EU law,' (2023) REALaw.blog, [13.9.2024]. Dostupné na:https://realaw.blog/?p=2879.

[25] Rozsudok Súdneho dvora (štvrtá komora) z 12. júla 2012. v prípade C-171/11 Fra.bo SpA proti Deutsche Vereinigung des Gas- und Wasserfaches eV (DVGW) – Technisch-Wissenschaftlicher Verein. Body 27 až 32

[26] Rozsudok Súdneho dvora (tretia komora) z 27. októbra 2016 v prípade C-613/14 James Elliott Construction Limited/Irish Asphalt Limited, body 34, 40

Harmonizované normy však nie sú len prosté vykonávacie opatrenia pochádzajúce od európskych normalizačných organizácií, ale majú sa považovať za prijaté Komisiou, alebo, v každom prípade, že Komisia je zodpovedná za prijatie týchto noriem v spojení s normalizačnými organizáciami.[27]
Presné vymedzenie základných požiadaviek na normu zo strany Komisie je veľmi dôležité, aby sa zabránilo nesprávnemu výkladu zo strany európskych normalizačných organizácií, pričom úroveň podrobnosti a špecifickosť požiadaviek nie je v nariadení č. 1025/2012 nijako záväzne špecifikovaná. Komisia aj Európsky parlament vyjadrujú obavy z udeľovania nadmerných oprávnení európskym normalizačným organizáciám prostredníctvom žiadostí o vypracovanie noriem a zdôrazňujú, že normalizačné organizácie by sa mali zamerať výlučne na definovanie technických metód na dosiahnutie legislatívnych cieľov a zdržať sa zasahovania do akejkoľvek politickej diskreácie. Samotná Komisia by mala postupovať mimoriadne opatrne, aby preukázala nevyhnutnosť vypracovania noriem.[28]
Z oznámenia Komisie ďalej vyplýva, že normy sa viac ako kedykoľvek predtým nemusia týkať len technických prvkov, ale musia zahŕňať aj základné demokratické hodnoty a záujmy EÚ, ako aj ekologické a sociálne zásady. Práve normy pre kybernetickú bezpečnosť alebo odolnosť kritickej infraštruktúry v tomto smere majú strategický rozmer.[29]

Spoločné špecifikácie

Komisia tiež pripúšťa, že je potrebné presunúť ešte väčšiu kontrolu nad harmonizovanými normami z európskych normalizačných organizácií na Komisiu, keď uvádza, že s cieľom zabezpečiť zohľadnenie verejného záujmu by Komisia mala byť splnomocnená priamo vypracovať - prostredníctvom vykonávacích aktov - spoločné špecifikácie (technické dokumenty alternatívne k harmonizovaným normám vypracovaným normalizačnými organizáciami).[30]
Vzhľadom na úlohu harmonizovaných noriem v harmonizačných právnych predpisoch EÚ by spoločná špecifikácia mala byť výnimočným náhradným riešením, ktoré uľahčí povinnosť povinných osôb dodržiavať regulačné požiadavky, ak žiadosť o normalizáciu neprijala žiadna z európskych normalizačných organizácií, alebo ak príslušné harmonizované normy primerane neriešia obavy týkajúce sa základných

[27] Rovnako, návrhy Generálnej advokátky Laila Medina z 22. júna 2023 vo veci C-588/21P Public.Resource.Org, Inc., Right to Know CLG proti Európskej komisii
[28] ELIANTONIO, Mariolina a VOLPATO, Annalisa, 'The European System of Harmonised Standards. Legal Opinion for ECOS' (March 11, 2022). [13.9.2024]. Dostupné na: http://dx.doi.org/10.2139/ssrn.4055292.
[29] Oznámenie Komisie z 2 Februára 2022 (COM(2022) 31 final) 'Stratégia EÚ v oblasti normalizácie', s. 4 a 5 [13.9.2024]. Dostupné na: EUR-Lex - 52022DC0031 - EN - EUR-Lex (europa.eu).
[30] Tamže.

práv, alebo ak harmonizované normy nie sú v súlade so žiadosťou, alebo ak dôjde k oneskoreniu prijatia vhodnej harmonizovanej normy.[31]
AIA odráža tento posun tým, že poveruje Komisiu vypracovaním spoločných špecifikácií v prípadoch, keď harmonizované normy buď neexistujú, sú nedostatočné, alebo primerane neriešia obavy týkajúce sa základných práv.[32] V tejto súvislosti je potrebné si tiež uvedomiť, že AIA sa odlišuje od tradičných predpisov o bezpečnosti výrobkov tým, že sa zameriava nielen na zmiernenie bezpečnostných rizík, ale aj na ochranu základných práv pred možnými nepriaznivými účinkami. Tento prístup rozširuje uplatňovanie harmonizovaných noriem a označenia CE nad rámec fyzickej bezpečnosti a zahŕňa ochranu základných práv. Takéto rozšírenie predstavuje nové výzvy a zložitosti, pretože si vyžaduje prelínanie technických noriem s etickými a právnymi aspektmi. Zabezpečenie súladu systémov AI s týmito normami nielen zvyšuje ich bezpečnosť a spoľahlivosť, ale posilňuje aj ich etické používanie, čím sa podporuje dôvera a zodpovednosť za technológie umelej inteligencie. Tento vývoj rovnako využíva právomoc Komisie prijímať technické alebo spoločné špecifikácie, čím sa vypĺňajú medzery v prípadoch, keď európske normalizačné organizácie neprijali normu alebo keď existujúce normy primerane neriešia otázky základných práv. Je zrejmé, že tento mechanizmus vydávaním spoločných špecifikácií, môže poskytnúť flexibilitu a schopnosť reagovať, čím sa zabezpečí, že poskytovatelia systémov AI budú stále spĺňať regulačné požiadavky aj v prípade oneskorenia alebo nedostatkov v normalizácii.
Rovnako tak možno poukázať aj na požiadavky kybernetickej bezpečnosti digitálnych produktov, kde návrh CRA tiež vychádza z možnosti Komisie prijať spoločné špecifikácie na dosiahnutie súladu so základnými požiadavkami uvedenými v prílohe I pre produkty s digitálnymi prvkami, len vtedy, ak sú určité splnené podmienky.[33] Pričom návrh CRA označuje prijatie spoločných špecifikácií Komisiou, ako „výnimočné núdzové" riešenie na uľahčenie povinnosti výrobcu dosiahnuť súlad so základnými požiadavkami, keď je normalizačný proces zablokovaný alebo keď pri zavádzaní vhodných harmonizovaných noriem dochádza k oneskoreniam.[34]

Záver

Právny význam technických noriem v EÚ sa výrazne zvýšil, pretože predpisy nemožno úplne pochopiť bez ich príslušných noriem, čo robí harmonizované normy de facto záväznými. To je zrejmé v prípadoch, keď legislatíva EÚ stanovuje, že dodržiavanie harmonizovanej normy zakladá domnienku zhody so základnými

[31] Recitál č. 121 AIA
[32] Porov. článok 41 ods. 1 AIA
[33] Článok 27 ods. 2 návrhu CRA
[34] Recitál č. 84 návrhu CRA

požiadavkami tejto legislatívy. Táto situácia vyústila do snahy Komisie prebrať väčšiu mieru kontroly nad normami a zároveň im konkurovať prostredníctvom vlastných technických dokumentov - spoločných špecifikácií.
Tento posun je zrejmý najmä v AIA, kde sa Komisii ukladá úloha vypracovať spoločné špecifikácie v prípadoch, keď harmonizované normy buď neexistujú, alebo sú nedostatočné, alebo primerane neriešia otázky základných práv. Tento prístup však vyvoláva niekoľko problémov. Po prvé, chýba demokratický dohľad, keď ani po zvýšení úlohy Komisie nemajú Európsky parlament ani členské štáty právomoc vetovať tieto špecifikácie, čo oslabuje demokratickú legitimitu procesu tvorby špecifikácií. Po druhé, technické obmedzenia a obmedzené zdroje Komisie spôsobujú, že je pre ňu náročné vykonávať dôkladné preskúmanie noriem, najmä v kontexte rýchlo sa vyvíjajúcich technológií, ako je napríklad umelá inteligencia. Po tretie, pokiaľ ide o dodržiavanie základných práv, ich porušovanie je často špecifické pre daný kontext a nedá sa jednoducho vyhodnotiť len prostredníctvom technických noriem alebo spoločných špecifikácií. Takéto otázky si zvyčajne vyžadujú súdne preskúmanie.
Napriek výzvam a kritike Komisie zastávame názor, že normalizačné organizácie a technické normy sú kľúčové pri formovaní postupov najlepšej praxe v oblasti kybernetickej bezpečnosti. Poskytujú rámec pre konzistentnosť a kvalitu, čo je v kontexte nových technológií nevyhnutné. Avšak vyvíjajúca sa povaha týchto noriem a ich vplyv na základné práva si vyžadujú priebežné hodnotenie a prispôsobovanie dohľadu nad ich tvorbou.

Zoznam použitej literatúry

1. ELIANTONIO Mariolina and COLOMBO Carlo: *Harmonized Technical Standards as Part of EU Law: Juridification with a Number of Unresolved Legitimacy Concerns*? [2017] *Maastricht Journal of European and Comparative Law*, [on-line]. Dostupné na: https://doi.org/10.1177/1023263X17709753.
2. ELIANTONIO, Mariolia a VOLPATO, Annalisa: *The European System of Harmonised Standards. Legal Opinion for ECOS* (March 11, 2022). [on-line]. Dostupné na: http://dx.doi.org/10.2139/ssrn.4055292
3. GORNET, Mélanie MAXWELL, Winston: *The European approach to regulating AI through technical standards* (*Internet Policy Review*, 2024 13 (3)) 14 [on-line]. Dostupné na: https://hal.science/hal-04254949v2/document
4. MAKATURA, Ivan.: *Technická normalizácia v informačnej a kybernetickej bezpečnosti*. In: Bezpečnosť v praxi [on-line]. Žilina: Poradca podnikateľa, 2024. ISSN 2729-885X. [13.9.2024]. Dostupné na: https://www.bezpecnostvpraxi.sk/odborny-clanok/technicka-normalizacia-v-informacnej-a-kybernetickej-bezpecnosti.htm

5. Oznámenie Komisie z 2 Februára 2022 (COM(2022) 31 final) '*Stratégia EÚ v oblasti normalizácie'*, [on-line]. Dostupné na: EUR-Lex - 52022DC0031 - EN - EUR-Lex (europa.eu).
6. Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/53/42' - *Relationship between human rights and technical standard-setting processes for new and emerging digital technologies and the practical application of the Guiding Principles on Business and Human Rights*. [on-line]. Dostupné na: https://www.ohchr.org/en/hr-bodies/hrc/regular-sessions/session53/list-reports
7. SCHAPEL, Harm: *The New Approach to the New Approach: The Juridification of Harmonised Standards in EU Law.* (2013) Maastricht Journal of European and Comparative Law, 20 (4) [on-line]. Dostupné na: https://doi.org/10.1177/1023263X1302000404
8. TOVO, Carlo: *Judicial Review of Harmonised Standards: Changing the Paradigms of Legality and Legitimacy of Private Rulemaking Under EU Law*. (2018) Common Market Law Review, 55 (4). [on-line]. Dostupné na: https://doi.org/10.54648/cola2018096
9. VAN GESTEL Rob a MICKLITZ Hans-W.: *European Integration through Standardisation: How Judicial Review Is Breaking Down the Club House of Private Standardisation Bodies* [2013] *Common Market Law Review* [on-line]. Dostupné na: https://doi.org/10.54648/cola2013007
10. VOLPATO, Annalisa: *The Legal Effects of Harmonised Standards in EU law*, (2023) REALaw.blog, [on-line]. Dostupné na:https://realaw.blog/?p=2879.
11. U.K. Competition and Markets Authority, *AI Foundation Models: Initial Review* (18 September 2023) [on-line]. Dostupné na: https://www.gov.uk/government/publications/ai-foundation-models-initial-report

Kontaktné údaje

JUDr. Michal Rampášek
rampasek1@uniba.sk
Ústav práva informačných technológií a práva duševného vlastníctva Právnickej fakulty Univerzity Komenského v Bratislave

THE APPLICATION OF ARTIFICIAL INTELLIGENCE: BASIC QUESTIONS AND DILEMMAS WITH A PARTICULAR REGARD TO ADMINISTRATIVE PROCEDURES

Patyi András[1] - Pollák Kitti[1] - Fekete Orsolya[1]

Abstract: Artificial intelligence (hereinafter referred to as AI) and the application of AI are at least a well-known "phenomenon", a concept both to the professionals and to those involved in a broader sense. However, "AI" does not have a completely uniformly accepted definition. Therefore, our study first tries to approach and define AI. In the second part of the research, we analyze the regulation of AI, during which we also scrutinize the latest European Union documents, especially considering that on March 13, 2024, the European Parliament - the first in the world - adopted a comprehensive AI regulation. We are also examining the effect of this on the internal - Hungarian - law. For all of this, however, it is essential to review the Hungarian regulations regarding AI. We should underline that Article XXVI of the Fundamental Law of Hungary provides a framework specifically focusing on digitization (digital administration of affairs) and talks about the role of technical solutions and science. The application of AI undoubtedly falls within this scope. Meanwhile, several questions arise, like: does the Hungarian Fundamental Law establish the possibility or the obligation of using AI? What are the application possibilities for AI in administrative procedures? Who is responsible for the damage caused by AI in administrative procedures? Finally, the study will seek answers to these questions too.

Key words: artificial intelligence, AI regulation, administrative procedures

Introduction

Even though neither public administration nor administrative procedural law has a uniformly accepted definition of artificial intelligence (hereinafter referred to as AI), they are at least familiar to professionals and those involved in a broader sense, so we attempt to describe AI as the first step in our study. The research regarding AI is evidently multidisciplinary; our research group focused on some of the basic questions and dilemmas regarding AI from an administrative legal perspective. In the second part of the study, we examined the regulation of AI, on the one hand mentioning the latest European Union documents and on the other hand reviewing

[1] Ludovika University of Public Service

Hungarian legislation, particularly the possibility or obligation (?) of applying AI in light of the Fundamental Law of Hungary and of the administrative procedural rules. The final section of our article focuses on liability issues arising from AI.

The concept of AI

The term AI was first used by John McCharty in 1956 at the Dartmouth conference. According to him, AI is the science and technique of creating intelligent machines.[2] In 1966, Marvin Minsky defined AI as the science of creating a machine that can perform tasks that require the same intelligence as humans.[3] According to Steven Finlay, AI is a replica of human analytical and/or decision-making ability.[4] According to Klaus Mainzer, systems that can solve problems on their own are intelligent.[5]
Many authors, including Aaron Sloman, Peter Jackson, and Edit Sántáné Tóth, regard AI as a specialized subfield of computer science, which is primarily concerned with the development of intelligent computing systems, which entails the creation and implementation of computer programs designed to emulate human cognitive abilities. Furthermore, this field focuses on the nature of intelligence, striving to comprehend its underlying characteristics, as well as investigating the principles and mechanisms essential for the replication and understanding of cognitive processes.[6] AI can also be identified as technology[7] and is often associated with robots, but there is no absolute connection between them.[8] AI can perhaps be defined in the simplest way as that we created and developed AI to copy, replace, or surpass the human mind.[9] AI encompasses systems that are related to intelligent behavior by analyzing

[2] RAJARAMAN, Vaidy: John McCarthy - Father of artificial intelligence, Resonance, 2014. 19(3):198-207.
[3] MINSKY, Marvin: Computation: Finite and Infinite Machines. Prentice-Hall, United States of America, 1967.
[4] FINLAY, Steven.: Artificial Intelligence and Machine Learning for Business. Relativistic, 2017.
[5] MAINZER, Klaus.: Künstliche Intelligenz – Wann übernehmen die Maschinen?. Springer Verlag, Heidelberg, 2016.
[6] See: CZÉKMANN Zsolt – KOVÁCS László – RITÓ Evelin: Mesterséges intelligencia alkalmazásának lehetőségei az államigazgatásban. Infokommunikáció és Jog. 2020. E-különszám. See: https://szakcikkadatbazis.hu/doc/5641090
[7] STEFÁN Ibolya: A mesterséges intelligencia fogalmának polgári jogi értelmezése, Pro Futoro – A jövő nemzetékek joga, 2020. 1. 30.
[8] RUSSELL, Stuart J.–NORVIG, Peter: Mesterséges intelligencia – Modern megközelítésben. Panem, Budapest, 2005, 795.; RABUNAL, Juan Ramon – DORADO, Julian De La Calle – PAZOS SIERRA, Alejandro: Encyclopedia of artificial intelligence, IGI Global, London, 2008.
[9] MOLNÁR László: Mesterséges intelligencia a közigazgatásban in: SASVÁRI Péter (szerk.): Informatikai rendszerek a közszolgálatban I., Ludovika Egyetemi Kiadó, Budapest, 2020. 189-215.

their environment to achieve specific objectives. These systems operate with a certain degree of autonomy, enabling them to execute actions independently.[10]
The scientific literature[11] distinguishes between weak AI, strong AI, and "super AI". The weak-strong categories are compared to the so-called narrow and general AI terms. The essence of weak AI is that the capabilities of machines are partially similar to human capabilities, especially in terms of logical-mathematical-linguistic intelligence, which is employed in addressing narrowly defined problems or tasks. These systems practically act as if they are intelligent, but despite this, there is no longer any information about whether the system actually has a mind or not. Therefore, it means the ability of a computer system to perform a narrowly defined task more efficiently than a human. In contrast, strong AI signifies a higher level, since the program has human capabilities; it has its own cognitive capabilities. Strong AI has independent awareness, a significant degree of self-awareness and self-direction, can solve various complex tasks from different areas and learns to solve new problems that were not yet known during his preparation. Finally, super AI is capable of more than the human brain.
It should be noted in this context that most of the current literature deals principally with the application of weak AI, which is mainly related to the following areas: development of chatbots, machine learning and robotics.[12]
AI can be grouped from several points of view, including its implementation method and its' application. When we refer to an AI tool, we basically mean a machine learning system and an expert system.[13] Nowadays, the machine learning method is one of the most widespread. The essence of it is that the machine learns on its own and then acts accordingly, rather than following precisely defined steps by the programmer.[14] The most important machine learning methods are supervised

[10] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Coordinated Plan on Artificial Intelligence See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0795
[11] See: BOSTROM, Nick: Superintelligence: Paths, dangers, strategies. Oxford University Press, London, 2014., REVOLIDIS, Ioannis–DAHI, Alan: The Peculiar Case of the Mushroom Picking Robot: Extra-contractual Liability in Robotics. In: CORRALES, Marcelo–FENWICK, Mark–FORGÓ, Nikolaus (szerk.): Robotics, AI and the Future of Law. Springer, Singapore, 2018, 59.
[12] See: CZÉKMANN Zsolt – KOVÁCS László – RITÓ Evelin 2020.
[13] FEJES Erzsébet–FUTÓ Iván: Mesterséges intelligencia a közigazgatásban – az érdemi ügyintézés támogatása. Pénzügyi Szemle, 2021/1, 30.
[14] KOVÁCS Zoltán – GURÁLY Roland: A mesterséges intelligencia és egyéb felforgató technológiák hatásait vizsgáló munkacsoport eredményei in: KOVÁCS Zoltán (ed.) A mesterséges intelligencia és egyéb felforgató technológiák hatásainak átfogó vizsgálata, Katonai Nemzetbiztonsági Szolgálat, Budapest, 2023. 12-13.

learning, unsupervised learning, reinforcement learning and deep learning.[15] On the other hand, the expert system is practically a computer application that solves complex problems and simulates human decision-making. Its knowledge can be described with "if, then" rules.[16]

From the aforementioned AI concepts, it is evident that AI cannot be identified with digitization (which is the process of converting analog signals into digital signals).[17] The possible application of AI in administrative procedures is not the same as, nor can it be simplified to, digital administrative procedures, electronic administration, or automatic decision-making procedures, the latter of which is practically a personalized level of electronic administration.[18]

Nonetheless, the application of AI means something qualitatively different in comparison: the mechanization of human thinking, the replacement of a thinking person is happening or can happen. Moreover, going further than this, the basic question can be asked whether the person can be replaced only during the thinking process that forms the basis of the administrative decision (the formation of the administrative will) or even during the action itself (the expression of the will). This leads to (or back to) the elementary question of what is human in administrative decision-making and what (may) not be? In public administration, significantly different types of activities and forms of action are manifested, not all of which are directed outside of public administration. In these actions, the preparation of decisions and the creation of decision content rest to a varying degree on computer systems and applications. However, regardless of the type of administrative activity under consideration, each fundamentally constitutes a segment of an extensive and nearly infinite chain of decision-making and data management processes. [19]

The European Union's regulation of AI

In April 2018, the European Commission published its communication entitled Artificial Intelligence for Europe, which was the first document to deal specifically

[15] See: FEJES Erzsébet–FUTÓ Iván 2021. 30.

[16] See: FUTÓ Iván: Mesterségesintelligencia-eszközök — szakértői rendszerek — alkalmazása a közigazgatásban, Dialóg Campus Kiadó, Budapest, 2019.

[17] KARAJZ Sándor: A digitalizáció és a társadalmi innovációk összefüggései. In: KOSZTOPULOSZ Andreász – KURUCZLEKI Éva (szerk.): Társadalmi és gazdasági folyamatok elemzésének kérdései a XXI. században. Szegedi Tudományegyetem Gazdaságtudományi Kar, Szeged, 2020, 192.

[18] CSATLÓS Erzsébet: az ügyfél és a hatósági döntéshozatal a digitalizáció korában, Pro Futuro 2023/1. 74-101.

[19] See: LAPSÁNSZKY András – PATYI András – Varga Zs. András: A magyar közigazgatási jog általános tanai (második, bővített kiadás), Universitas-Győr Nonprofit kft., Győr, 2024. 233-268.

with the issue of AI.[20] Examining this communication, it becomes evident that the European Union was primarily motivated by the preservation of competitiveness in relation to one of the strategically most important technologies of our century. Meanwhile, the necessity to establish ethical frameworks aligned with European values, including the Charter of Fundamental Rights, emerged at that time.
In that same year, a high-level expert group (AI HLEG) was set up, which dealt with the issue of AI from several angles (like ethical guidelines, liability, policy and investment recommendations, and their sectoral considerations).[21] Among these, we would highlight the ethical guidelines, which analyzed in detail the criteria for a reliable AI: it must be legal, ethical and stable. In order to meet the ethical requirements, AI must respect human autonomy and fundamental rights.[22]
In April 2019, the European Commission's next communication analyzed the issue of trust in human-centered AI. [23] We would like to mention regarding this topic Virginia Dignum's approach. She does not talk about the possible appearance of some future superintelligence, but about human responsibility in connection with the currently applied AI; on the enforcement of the requirement of transparency and accountability in connection with the currently used AI technologies. Dignum emphasizes that all investigations must focus on human well-being, in accordance with social values and ethical principles, and with particular attention to the fact that AI no longer only affects the rights of the individual, but also has a significant social impact. The author underlines that AI is a development by humans, and it is our responsibility to give the "machine" a goal that we really want as an output.[24]
Regarding the European Union's approach to the issue of competitiveness versus ethical considerations, Zsolt Ződi sees a kind of shift in emphasis from encouraging innovation focusing on economic competitiveness to taking account of possible disadvantages, risks and ethical considerations. According to his point of view, the

[20] See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN However, this communication that was the starting point was followed by several others, which are not analyzed in this study.
[21] See:https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai
[22] High-level expert group on artificial intelligence: Ethics guidelines for trustworthy AI, 8 April 2019. See: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
[23] Communication from the Commission to the European Parliement, the Council, the European Economic and Social Committee and the Committee of the Regions, Building Trust in Human-Centric Artificial Intelligence Brussels, 8.4.2019 COM(2019) 168 final See: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52019DC0168
[24] DIGNUM Virginia: Responsible artificial intelligence. How to develop and use AI in a responsible way. Springer, 2019. 1-7.

EU's (compared to the USA) less pro-free market and pro-capitalism attitude and its data protection policy also play a relevant role. [25]

In February 2020, the European Commission published the White Paper on Artificial Intelligence - A European approach to excellence and trust. Two emphasized elements of the White Paper were: the ecosystem of excellence and the ecosystem of trust. The former focuses on the entire value chain involved in the development of AI. The ecosystem of trust examined the following issues like the compliance with legislation, building citizen trust, guaranteeing legal certainty for both public and private sector organizations. The goal is for " Europe to become the most attractive, secure and dynamic data-agile economy in the world".[26] It corresponds with this objective The European Data Strategy, which stressed the need to unify the fragmented European data markets. In order to achieve this goal, several legal regulations have been enacted, [27] but the document always refers to the General Data Protection Regulation as a solid legal framework,[28] which plays a fundamental role in creating digital trust. As a barrier to the spread of AI technologies, it clearly records the lack of available data in the appropriate quantity and quality. [29]

After several revisions of the draft published in 2021, on March 13, 2024, the European Parliament adopted – for the first time in the world – a comprehensive AI regulation (hereinafter referred to as: AI Act).[30] The regulation uses a technology-neutral approach and classifies AI systems into four different risk levels: unacceptable, high, limited, and minimal risk. The regulation – considering the personal rights of the individuals involved therefore – prohibits practices that are potentially relevant in the field of public administration, such as the use of emotion recognition systems in education or in the workplace; "social scoring"; a risk assessment system related to natural persons for predicting the commission of

[25] ZŐDI Zsolt: Az Európai Bizottság Mesterséges Intelligencia Kódexének tervezete. Gazdaság és jog. 2021/5. 1-3.

[26] See : WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust: https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_en?filename=commission-white-paper-artificial-intelligence-feb2020_en.pdf

[27] Like: Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union See: https://eur-lex.europa.eu/eli/reg/2018/1807/oj. etc.

[28] See: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance): https://eur-lex.europa.eu/eli/reg/2016/679/oj

[29] See: European data strategy: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

[30] GKRITSI Eliza: The long and winding road to implement the AI Act. (2024. március 14.) Euractiv. See: https://www.euractiv.com/section/digital/news/the-long-and-winding-road-to-implement-the-ai-act/ See: EU AI Act: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

crimes based solely on the evaluation of their personality or characteristics; etc.[31] Among others, biometric systems authorized under EU or international law, AI systems used for admission in the field of education, or in road traffic, or in the management and operation of water, gas, heating or electricity services, access to basic private and public services, including, for example: entitlement to health services, evaluation of emergency calls, migration and asylum etc. were classified as high risk. Several of these are in the area dominated by public administration.[32] However the use of AI for national security, military and defense purposes; or specifically and exclusively for the purpose of scientific research and development does not fall under the scope of the regulation.[33]
Correspondingly, a new body at EU-level – the AI Office – is created, and each member state delegates a member to the European Artificial Intelligence Board for a period of three years, which will assist the implementation of the legislation with advice and assistance to both the member states and the European Commission. The European Data Protection Commissioner participates in the Board's work as an observer, which also shows the close connection of AI regulation with data protection law. In addition to the above-mentioned, a scientific board and advisory forum consisting of independent experts is also established.[34]

The Hungarian regulation of AI

In the subsequent section, we analyze the current Hungarian regulations regarding AI. An initial examination reveals that the specific legislation regarding AI, in its narrow sense, is not extensive, aligning with the practices observed in other European countries. Wolswinkel sees the explanation for this – based on the data of a comparative study examining the relationship between administrative law and AI, covering data from 24 EU member states – that data protection law has a dominant role in the regulation of automatic decision-making systems and of AI too. It also indicates that the general principles of administrative law should be respected in all forms of administrative decisions, regardless of the method of decision-making.[35]

[31] Article 5 of the AI Act
[32] See: Chapter III. and Annex III of AI Act
[33] Preambule (24)-(25) of the AI Act
[34] Articles 64-69. of AI Act
[35] WOLSWINKEL Johan: Comparative study on administrative law and the use of artificial intelligence and other algorithmic systems in administrative decision-making in the member states of the Counsil of Europe. Prepared by Prof. Dr. Johan Wolswinkel Tilburg University, the Netherlands, consultant, under the supervision of the European Committee on Legal Co-operation (CDCJ). Council of Europe Publishing F-67075 Strasbourg Cedex, 2021. 6. See: https://coe.int/documents/22298481/0/CDCJ%282022%2931E+-+FINAL+6.pdf/4cb20e4b-3da9-d4d4-2da0-65c11cd16116?t=1670943260563

Finding out whether the use of AI-based applications requires special regulation is the task of jurisprudence.[36]

In the fall of 2018, the Ministry of Information and Technology initiated an AI Coalition in Hungary, involving all actors of the Hungarian AI ecosystem (like stakeholders from the university, business and government area) for the creation of the framework for the Hungarian AI developments. In 2019, an action plan was published, which included the creation of the AI Challenge, the regulation of data assets, the National Data Assets Agency, and an AI Center of Excellence. At the beginning of 2020, the Hungarian AI strategy for the period 2020-2030 was accepted,[37] which includes three layers: the foundation pillar records the elements with an economic approach (development of competence, encouraging applications, development of infrastructure, creation of regulatory and ethical frameworks); the second layer is designated specific areas for AI development such as the area of public services, health care and education. The third layer mentions specific transformative projects, such as automated administration. The goal is a data-driven service in state administration,[38] "facilitating the electronic access and digitization of public services, in which AI is one of the applicable technologies."[39]

In terms of the legal rules, primarily Act CCXXII of 2015 on the general rules on electronic administration and trust services (hereinafter referred to as: Eüsztv.)[40] and its implementing decree[41] should be mentioned, of which the former establishes the possibility of using technology based on AI, and the government decree mentions voice training, voice transcription and communication assistant services supported by AI.[42]

Act CIII of 2023 on the digital state and certain rules for the provision of digital services entered into force on July 1, 2024., which repeals the Eüsztv. from September 1, 2024. and makes digital services available in several stages in an expanding range until June 1, 2025., within the framework of the National Digital Citizenship Program. This Act mentions AI in connection with central electronic administration services in the context that AI-based technology can be used as a support service.

---

[36] See: PÉTERFALVI Attila: algoritmusok és adatvédelem. Quo vadis? In: TÖRÖK Bernát – ZŐDI Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó, Budapest, 2021. 185. and Wolswinkel 2021. 9.

[37] See: https://digitalisjoletprogram.hu/hu/kiadvanyaink

[38] See: KELÉNÉ Dr. PÉTER Éva: A Mesterséges intelligencia szerepe a közigazgatásban. Jegyző és közigazgatás. 2023/3.

[39] Hungarian AI strategy 38.

[40] See: https://njt.hu/jogszabaly/en/2015-222-00-00

[41] Government Decree 451/2016. (XII. 19.) on the Detailed rules of electronic services

[42] Paragraph (5) of Article 38 of Eüsztv.

In this regard, it should also be noted that if we identify AI as a technology,[43] it should be used in administrative procedures according to the principle of efficiency stated in Article 4 of the Act CL of 2016 on the Code of General Administrative Procedure, which states that: "The authority shall organize its activity in such a manner as to result in the least possible expense for all participants in the procedure and, without prejudice to the requirements of clarifying the facts of the case, for the procedure to be closed as expeditiously as possible with the application of advanced technologies".[44] Naturally, the fundamental right to good administration must be considered during the application of AI.[45] Meanwhile, the procedural fundamental right approach that covers the fairness of all stages of the administrative procedures does not stand alone. It is true that it is basically formulated as a state goal and not as a subjective right, but the Hungarian Fundamental Law also states among the fundamental rights the specific constitutional obligation of the application of new technical solutions and the achievements of science.[46]

Paragraph (1)- (2) of Article XXVI. of the Fundamental Law of Hungary state that: "(1) The State shall strive to use the latest technical solutions and the achievements of science to make its operation efficient, raise the standard of public services, improve the transparency of public affairs and promote equality of opportunity. (2) To further the objectives set out in paragraph (1), priority shall be given to the digital administration of affairs in Hungary; to this end, the State shall secure for everyone a unique digital identifier as provided for in an Act. The State shall process the data necessary for the digital administration of affairs in a manner and within the scope determined in a decree of the Government."

Paragraph (2) of Article XXVI. of the Fundamental Law of Hungary – which was reformulated by the 12th amendment – provides a framework specifically focusing on digitization (digital administration of affairs), while paragraph (1) of this Article, still mentions in general the role of technical solutions and science. The application of AI undoubtedly falls into this category, as it is a new kind of technical solution, that relies on the results of computer science (informatics). It is not an exaggeration to claim that the use of AI in Hungarian public administration is not an option, but a

[43] STEFÁN Ibolya 2020. 30.

[44] VARGA Zs András: Az alkotmányosság követelménye és az eljárás alapelvei in: PATYI András- VARGA Zs András (szerk.): A közigazgatási eljárásjog alapjai és alapelvei, Dialóg Campus Kiadó, Budapest, 2019. 204.

[45] HOHMANN, Balázs: A mesterséges intelligencia közigazgatási hatósági eljárásban való alkalmazhatósága a tisztességes eljáráshoz való jog tükrében in: TÖRÖK Bernát - ZŐDI Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai : Tanulmányok a mesterséges intelligencia és a jog határterületeiről, Ludovika Egyetemi Kiadó, Budapest, 2021. 403-422.

[46] See: TÖRÖK Réka: XXVI. cikk Az új műszaki megoldások, tudományos eredmények alkalmazása, in: TÖRÖK Bernát (szerk.): Alapjogi kommentár az alkotmánybírósági gyakorlat alapján, Novissima Kiadó, Budapest, 2021. 312.

constitutional obligation. Whether the issue is the efficiency of state (internal) operations, or the issue is better transparency of public affairs, or the issue is ensuring equal opportunities or raising the standard of public services (and not only digital public services), AI solutions' application – with appropriate IT testing and sufficient control – cannot be avoided. According to Paragraph (2) of Article XXVI of the Fundamental Law of Hungary the digital management of affairs takes priority. This constitutional provision does not emphasize it, but it is primarily about the management of public administrative affairs. Primarily, but not exclusively. This can be derived not only because the management of affairs related to public services could be outside of the narrow sense of public administration – and this provision specifically mentions this as one of the goals-, but also because this legal clause generally refers to matters related to the state. Therefore, neither the large branches of justice (judicial, prosecutorial) nor notarial administration can be excluded from this circle.

The Hungarian research community has started examining the public services and administrative procedures containing AI elements. These research show that the application of strong AI is not yet a reality, AI is currently mainly an efficiency-enhancing and supporting element.[47]

It must also be emphasized that the spread and successful adaptation of AI in the public and private sectors depend on several factors. One pillar is indeed the efforts of the public sector. The other pillar is the user side and its digital competencies. [48] Since 2014, the European Commission has used an index, the DESI (Digital Economy and Society Index), which measures the degree of digitization of society and economy. According to the latest report, which records the changes of the past decade, Hungary has made progress in several areas. Our weak point is the level of basic digital skills of the population and the level of digitization of businesses and

[47] See for exemple: MOLNÁR Dalma: Mesterséges intelligencia szolgálatba, az államigazgatás modernizációja. Gazdaság és Jog. 2022/5-6. 47-51., RIDEG Gergely: Mesterséges intelligencia és közigazgatás. Gondolatok a mesterséges intelligencia szabályozás kockázatalapú megközelítéséről a gyakorlatban, kihívások és lehetőségek. Közigazgatás Tudomány, 2023/2 160-173., CSATLÓS Erzsébet: Prospective implementation of ai for enhancing European (in)security: Challenges in reasoning of automated travel authorization decisions. Computer Law &Security Review. Article 105995. See: https://www.sciencedirect.com/journal/computer-law-and-security-review/vol/54/suppl/C, KESERŰ Barna Arnold: A 21. századi változások hatása a jogalkotásra. Képes-e lépést tartani a jog a változó világgal? Dialóg Campus, Budapest, 2020.

[48] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A New Skills Agenda for Europe, Working together to strengthen human capital, employability and competitiveness, COM/2016/0381 final See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0381

public services. In these areas Hungary is significantly behind the EU average.[49] We strongly believe that the development of the digital competences of the population is a fundamental criteria of the implementation of the state's goals and aspirations stated in the Fundamental Law of Hungary.

The responsibility of AI?

Numerous dilemmas emerge concerning the responsibility of AI. The primary issue regarding AI liability is its unpredictability. A critical question from the perspective of liability for damages caused by AI is: who is responsible if the operation of the AI system results in a violation of law? [50]

Article XXIV. Paragraph (2) of the Fundamental Law of Hungary states that: "Everyone shall have the right to compensation for any damage unlawfully caused to him or her by the authorities in the performance of their duties, as provided for by an Act." In the case of damage caused by public administration,[51] it is obviously not possible to refer neither to the civil servant's lack of expertise, nor to the lack of opportunities and conditions provided by the public administration authority. Consequently, the damage caused by AI applied during the administrative procedure raises questions about the form of responsibility and the exemption from liability. This is particularly pertinent in cases where there may be no link between the "behavior" of self-learning AI and the actions of the programmer or user.[52]

Another question also arises in this context: whether the law enforcer bears the responsibility during the use of AI and, if so, who is the law enforcer. Several theoretical answers can be given to this question (of course, some options are not acceptable):

a) the legislator will be the law enforcer, because AI is used when administrative decision-making is simple.; and the elements of the decision are already included in the law.

b) the administrative authority is the law enforcer, since AI makes its decision on behalf of the authority

---

[49] See: 12. 2023 Report on the state of the Digital Decade: https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade. and Public administration in the EU Member States. 2022 overview: https://op.europa.eu/en/publication-detail/-/publication/2ac606f3-d20e-11ee-b9d9-01aa75ed71a1/language-en. 44.

[50] BICSKEI Tamás: A mesterséges intelligencia közigazgatásban való felhasználásával okozott kár, KözigazgatásTudomány, 2023:1 99-114.; TÓTH András: A mesterséges intelligencia szabályozásának paradoxonja és egyes jogi vonatkozásainak alapvető kérdései, Infokommunikáció és jog, 2020. 16 : 73. 3-14.

[51] See: F. ROZSNYAI Krisztina - ISTENES Attila: Gondolatok a közigazgatási jogkörben okozott kár megtérítése iránti igény érvényesítésének új lehetőségeiről, Jogtudományi Közlöny, 2017. 559-568.

[52] BICSKEI Tamás 2020. 108.

c) AI itself is the law enforcer, because AI makes decisions without human intervention. (Meanwhile, AI does not have legal personality) [53]
d) the operator of the AI system is the law enforcer, because it is responsible for the safe operation of AI. However, if the operation of the AI was "outsourced", then establishing the responsibility of a non-Hungarian organization or business, would further complicate the issues related to this responsibility system.
e) the client is responsible in the procedures commenced upon application, because the clients' request determined the decision made by AI.
f) the client's legal representative can also be the law enforcer, if legal representation is mandatory by law. (However, this would not promote efficient administration)
g) there is no application of the law. Therefore, there is no one responsible, because the law is applied by software (=AI).[54]
We can presume that in the case when an administrative decision is made by AI, the liability for damages of the legal entity exercising public authority will be established based on the rules of the Civil Code. [55] Section 6: 548 of the Act V of 2013 on the Civil Code states that: „[t]he legal person exercising public authority shall be liable for the damage caused in the course of exercising administrative powers. If the person exercising public powers is not a legal person, the administrative organ with legal personality under the auspices of which the proceeding administrative organ operates shall be liable for the damage." In order to be released from liability, there should be an "obviously and flagrantly serious error in the application and interpretation of the law, a flagrantly unreasonable evaluation of the facts".[56] The question is whether this can be tested in the case of an AI system? However, in cases, where a data protection incident occurs during an administrative procedure, the responsibility of the data controller can be established based on the current regulations. The reason for this is the technology neutrality principle laid down in the GDPR. [57]
Finally, in this context, it should also be highlighted that in 2022 the draft of the EU Directive on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) was created.[58] The purpose of this document was to make it easier

[53] ESZTERI Dániel: A mesterséges intelligencia fejlesztésének és üzemeltetésének egyes felelősségi kérdései, Infokommunikáció és Jog, 2015. 12. évf. 2-3. sz. 47-57.
[54] See: CSEH-ZELINA, Gergely - CZÉKMANN, Zsolt - RITÓ, Evelin: Az automatikus döntéshozatal helye és szerepe a hatósági eljárásban, KözigazgatásTudomány 2022: 2 35-47.
[55] BICSKEI Tamás 2020. 108.
[56] FUGLINSZKY Ádám: Kártérítési jog, HVG-ORAC, Budapest, 2015. 524.
[57] See: PÉTERFALVI Attila - BUZÁS Péter – RÉVÉSZ Balázs (szerk.): Magyarázat a GDPR-ról, Wolters Kluwer Hungary, Budapest, 2021.
[58] See: Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496

for the injured party to enforce their rights against the offender. Certainly, the adoption of this Directive would have a great impact. However, the legislator did not adopt this Directive, and in the new AI Act, we can discover elements of "distrust" or caution, which are also related to responsibility. Where do we see this? When using systems that operate with AI, it is mandatory to employ trained supervisory persons, who will ultimately "knock out" (so-called kill switch button) the AI in the event of abnormal operation.

Conclusion

In conclusion, we propose the following recommendations concerning the integration of AI in administrative procedures: according to the definition of the AI Act, AI system is a system that can demonstrate adaptability after its introduction. [59] We recommend the establishment of an analysis group at the authorities using AI in order to monitor potential changes. This aligns with the provisions outlined in the AI Act, which also requires the creation of a regulatory test environment. [60]

Mistrust may arise during the utilization of AI. [61] To resolve this issue, we recommend that, in the cases when the administrative decisions are made by AI, clients should have the option to request the involvement of a human decision-maker as a legal remedy. We recommend creating a rule similar to the existing provision of Section 42 of the Act CL of 2016 on the Code of General Administrative Procedure, which states that: „[i]f no appeal lies against a decision made in an automated decision-making procedure or summary procedure, the party may request the authority, within five days following the communication of the decision, to reconsider his application in a full procedure." This regulation would also facilitate more accessible and effective legal remedies.

Before applying AI, we consider it absolutely necessary to develop a liability system for possible damage caused by decisions made by AI.

Ultimately, we would like to draw attention to the idea contained in the ethical guidelines published by AI HLEG: *"AI is not an end in itself, but rather a promising means to increase human flourishing, thereby enhancing individual and societal well-being and the common good, as well as bringing progress and innovation*." [62] Therefore, we strongly believe that AI could be used well, as a tool.

---

[59] Article 3 of AI Act

[60] Article 57-61 of AI Act

[61] See: Commission Report on safety and liability implications of AI, the Internet of Things and Robotics, Brussels, 19.2.2020 COM(2020)64 final, 15. https://commission.europa.eu/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en

[62] See: High-level expert group on artificial intelligence: Ethics guidelines for trustworthy AI, 8 April 2019. See: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

Bibliography:

1. BICSKEI Tamás: A mesterséges intelligencia közigazgatásban való felhasználásával okozott kár, KözigazgatásTudomány, 2023:1 99-114.
2. BOSTROM, Nick: Superintelligence: Paths, dangers, strategies. Oxford University Press, London, 2014.
3. CSATLÓS Erzsébet: az ügyfél és a hatósági döntéshozatal a digitalizáció korában, Pro Futuro 2023/1. 74-101.
4. CSATLÓS Erzsébet: Prospective implementation of ai for enhancing European (in)security: Challenges in reasoning of automated travel authorization decisions. Computer Law &Security Review. Article 105995. See: https://www.sciencedirect.com/journal/computer-law-and-security-review/vol/54/suppl/C
5. CSEH-ZELINA, Gergely - CZÉKMANN, Zsolt - RITÓ, Evelin: Az automatikus döntéshozatal helye és szerepe a hatósági eljárásban, KözigazgatásTudomány 2022: 2 35-47.
6. CZÉKMANN Zsolt – KOVÁCS László – RITÓ Evelin: Mesterséges intelligencia alkalmazásának lehetőségei az államigazgatásban. Infokommunikáció és Jog. 2020. E-különszám. See: https://szakcikkadatbazis.hu/doc/5641090
7. DIGNUM Virginia: Responsible artificial intelligence. How to develop and use AI in a responsible way. Springer, 2019.
8. ESZTERI Dániel: A mesterséges intelligencia fejlesztésének és üzemeltetésének egyes felelősségi kérdései, Infokommunikáció és Jog, 2015. 12. évf. 2-3. sz. 47-57.
9. FEJES Erzsébet–FUTÓ Iván: Mesterséges intelligencia a közigazgatásban – az érdemi ügyintézés támogatása. Pénzügyi Szemle, 2021/1, 30.
10. FINLAY, Steven.: Artificial Intelligence and Machine Learning for Business. Relativistic, 2017.
11. FUGLINSZKY Ádám: Kártérítési jog, HVG-ORAC, Budapest, 2015.
12. FUTÓ Iván: Mesterségesintelligencia-eszközök — szakértői rendszerek — alkalmazása a közigazgatásban, Dialóg Campus Kiadó, Budapest, 2019.
13. GKRITSI Eliza: The long and winding road to implement the AI Act. (2024. március 14.) Euractiv. See: https://www.euractiv.com/section/digital/news/the-long-and-winding-road-to-implement-the-ai-act/
14. HOHMANN, Balázs: A mesterséges intelligencia közigazgatási hatósági eljárásban való alkalmazhatósága a tisztességes eljáráshoz való jog tükrében in: TÖRÖK Bernát - ZŐDI Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai : Tanulmányok a mesterséges intelligencia és a jog határterületeiről, Ludovika Egyetemi Kiadó, Budapest, 2021. 403-422.

15. KARAJZ Sándor: A digitalizáció és a társadalmi innovációk összefüggései. In: KOSZTOPULOSZ Andreász – KURUCZLEKI Éva (szerk.): Társadalmi és gazdasági folyamatok elemzésének kérdései a XXI. században. Szegedi Tudományegyetem Gazdaságtudományi Kar, Szeged, 2020.
16. KELÉNÉ Dr. PÉTER Éva: A Mesterséges intelligencia szerepe a közigazgatásban. Jegyző és közigazgatás. 2023/3.
17. KESERŰ Barna Arnold: A 21. századi változások hatása a jogalkotásra. Képes-e lépést tartani a jog a változó világgal? Dialóg Campus, Budapest, 2020.
18. KOVÁCS Zoltán - GURÁLY Roland: A mesterséges intelligencia és egyéb felforgató technológiák hatásait vizsgáló munkacsoport eredményei in: KOVÁCS Zoltán (ed.) A mesterséges intelligencia és egyéb felforgató technológiák hatásainak átfogó vizsgálata, Katonai Nemzetbiztonsági Szolgálat, Budapest, 2023.
19. LAPSÁNSZKY András – PATYI András – Varga Zs. András: A magyar közigazgatási jog általános tanai (második, bővített kiadás), Universitas-Győr Nonprofit kft., Győr, 2024.
20. MAINZER, Klaus.: Künstliche Intelligenz – Wann übernehmen die Maschinen?. Springer Verlag, Heidelberg, 2016.
21. MINSKY, Marvin: Computation: Finite and Infinite Machines. Prentice-Hall, United States of America, 1967.
22. MOLNÁR Dalma: Mesterséges intelligencia szolgálatba, az államigazgatás modernizációja. Gazdaság és Jog. 2022/5-6. 47-51.
23. MOLNÁR László: Mesterséges intelligencia a közigazgatásban in: SASVÁRI Péter (szerk.): Informatikai rendszerek a közszolgálatban I., Ludovika Egyetemi Kiadó, Budapest, 2020. 189-215.
24. PÉTERFALVI Attila - BUZÁS Péter – RÉVÉSZ Balázs (szerk.): Magyarázat a GDPR-ról, Wolters Kluwer Hungary, Budapest, 2021.
25. PÉTERFALVI Attila: algoritmusok és adatvédelem. Quo vadis? In: TÖRÖK Bernát – ZŐDI Zsolt (szerk.): A mesterséges intelligencia szabályozási kihívásai. Ludovika Egyetemi Kiadó, Budapest, 2021. 185. and Wolswinkel 2021. 9.
26. RABUNAL, Juan Ramon – DORADO, Julian De La Calle – PAZOS SIERRA, Alejandro: Encyclopedia of artificial intelligence, IGI Global, London, 2008.
27. RAJARAMAN, Vaidy: John McCarthy - Father of artificial intelligence, Resonance, 2014.
28. REVOLIDIS, Ioannis–DAHI, Alan: The Peculiar Case of the Mushroom Picking Robot: Extra-contractual Liability in Robotics. In: CORRALES, Marcelo–FENWICK, Mark–FORGÓ, Nikolaus (szerk.): Robotics, AI and the Future of Law. Springer, Singapore, 2018.
29. RIDEG Gergely: Mesterséges intelligencia és közigazgatás. Gondolatok a mesterséges intelligencia szabályozás kockázatalapú megközelítéséről a

gyakorlatban, kihívások és lehetőségek. Közigazgatás Tudomány, 2023/2 160-173.
30. ROZSNYAI Krisztina - ISTENES Attila: Gondolatok a közigazgatási jogkörben okozott kár megtérítése iránti igény érvényesítésének új lehetőségeiről, Jogtudományi Közlöny, 2017. 559-568.
31. RUSSELL, Stuart J.–NORVIG, Peter: Mesterséges intelligencia – Modern megközelítésben. Panem, Budapest, 2005.
32. STEFÁN Ibolya: A mesterséges intelligencia fogalmának polgári jogi értelmezése, Pro Futoro – A jövő nemzetékek joga, 2020. 1. 30.
33. TÖRÖK Réka: XXVI. cikk Az új műszaki megoldások, tudományos eredmények alkalmazása, in: TÖRÖK Bernát (szerk.): Alapjogi kommentár az alkotmánybírósági gyakorlat alapján, Novissima Kiadó, Budapest, 2021.
34. TÓTH András: A mesterséges intelligencia szabályozásának paradoxonja és egyes jogi vonatkozásainak alapvető kérdései, Infokommunikáció és jog, 2020. 16 : 73. 3-14.
35. VARGA Zs András: Az alkotmányosság követelménye és az eljárás alapelvei in: PATYI András- VARGA Zs András (szerk.): A közigazgatási eljárásjog alapjai és alapelvei, Dialóg Campus Kiadó, Budapest, 2019.
36. WOLSWINKEL Johan: Comparative study on administrative law and the use of artificial intelligence and other algorithmic systems in administrative decision-making in the member states of the Counsil of Europe. Prepared by Prof. Dr. Johan Wolswinkel Tilburg University, the Netherlands, consultant, under the supervision of the European Committee on Legal Co-operation (CDCJ). Council of Europe Publishing F-67075 Strasbourg Cedex, 2021. 6. See: https://coe.int/documents/22298481/0/CDCJ%282022%2931E+-+FINAL+6.pdf/4cb20e4b-3da9-d4d4-2da0-65c11cd16116?t=1670943260563
37. ZŐDI Zsolt: Az Európai Bizottság Mesterséges Intelligencia Kódexének tervezete. Gazdaság és jog. 2021/5. 1-3.
38. https://digitalisjoletprogram.hu/hu/kiadvanyaink

EU documents and links:

1. EU AI Act: REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689
2. Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union See: https://eur-lex.europa.eu/eli/reg/2018/1807/oj.

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance): https://eur-lex.europa.eu/eli/reg/2016/679/oj
4. Communication from the Commission to the European Parliement, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Coordinated Plan on Artificial Intelligence See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0795
5. Communication from the Commission to the European Parliement, the Council, the European Economic and Social Committee and the Committee of the Regions, Building Trust in Human-Centric Artificial Intelligence Brussels, 8.4.2019 COM(2019) 168 final See: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52019DC0168
6. Commission Report on safety and liability implications of AI, the Internet of Things and Robotics, Brussels, 19.2.2020 COM(2020)64 final, 15 See: https://commission.europa.eu/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en
7. Communication from the Commission to the European Parliement, the Council, the European Economic and Social Committee and the Committee of the Regions, A New Skills Agenda for Europe, Working together to strengthen human capital, employability and competitiveness, COM/2016/0381 final See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0381
8. High-level expert group on artificial intelligence: Ethics guidelines for trustworthy AI, 8 April 2019. See: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
9. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) COM/2022/496 final See: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0496
10. Public administration in the EU Member States. 2022 overview: https://op.europa.eu/en/publication-detail/-/publication/2ac606f3-d20e-11ee-b9d9-01aa75ed71a1/language-en.
11. European data strategy: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en
12. 2023 Report on the state of the Digital Decade: https://digital-strategy.ec.europa.eu/en/library/2023-report-state-digital-decade.
13. WHITE PAPER On Artificial Intelligence - A European approach to excellence and trust: https://commission.europa.eu/document/download/d2ec4039-c5be-423a-

81ef-b9e44e79825b_en?filename=commission-white-paper-artificial-intelligence-feb2020_en.pdf

Hungarian legal documents:

1. Fundamental Law of Hungary
2. Act V of 2013 on the Civil Code
3. Act CCXXII of 2015 on the general rules on electronic administration and trust services
4. Act CL of 2016 on the Code of General Administrative Procedure
5. Act CIII of 2023 on the digital state and certain rules for the provision of digital services
6. Government Decree 451/2016. (XII. 19.) on the Detailed rules of electronic services

Contact information:

Prof. Dr. András PATYI,
Judge at the Hungarian Constitutional Court, Head of the Doctoral School of Public Administration Sciences, Professor at Ludovika University of Public Service
Patyi.Andras@uni-nke.hu

Kitti Pollak, Dr.
Associate Professor at Ludovika University of Public Service
Pollak.Kitti@uni-nke.hu

Orsolya Fekete, Dr.
Senior Lecturer at Ludovika University of Public Service
Fekete.Orsolya@uni-nke.hu

KEĎ UMELÁ INTELIGENCIA ROBÍ CHYBY: RESPONDEAT SUPERIOR [1]

WHEN ARTIFICIAL INTELLINGENCE MAKES MISTAKES: RESPONDEAT SUPERIOR

Zoltán Gyurász[2]

Abstrakt: Analógie sú základným prvkom právnej argumentácie, avšak už dávno sa zistilo, že analógia bez teoretického rámca je v podstate slepá. Hoci existujú presvedčivé argumenty proti používaniu právnych analógií, je zrejmé, že výklad právnych noriem bez prípustnosti analógií je nedostatočný. Bolo by preto neproduktívne neuvažovať o analógiách ako o súčasti procesu právneho uvažovania, najmä keď je potrebné prijať rozhodnutia o nových technológiách. V kontexte systémov umelej inteligencie predstavujú analógie osobitný súbor výziev, ktoré je potrebné riešiť.

Kľúčové slová: Umelá inteligencia, zodpovednosť, Respondeat superior

Abstract: Analogies are a fundamental element of legal reasoning; however, it has long been established that an analogy devoid of a theoretical framework is essentially blind. Although there are persuasive arguments against the use of legal analogies, it is evident that the interpretation of legal norms without the admissibility of analogies is insufficient. It would therefore be unproductive not to consider analogies as part of the legal reasoning process, particularly when decisions about new technologies need to be made. In the context of artificial intelligence systems, analogies present a distinctive set of challenges that must be addressed.

Key words: Artificial intelligence, responsibility, Respondeat superior

[1] Tento článok bol vypracovaný s podporou grantu udeleného Agentúry na podporu výskumu a vývoja č. APVV-23-0137 Právne a technické aspekty situačného povedomia o kybernetickej bezpečnosti.

[2] Univerzita Komenského v Bratislave, Právnická fakulta

Úvod

V období, ktoré sa vyznačovalo podriadenosťou jednotlivcov autoritám, vznikla doktrína *respondeat superior*, ktorej cieľom bolo, aby osoby v mocenskom postavení museli niesť zodpovednosť za konanie tých, ktorých sú im priamo podradení.
Význam tejto doktríny len vzrástol s rastom moderného hospodárstva, ktorého hnacou silou sú veľké korporácie, ktoré sa vo veľkej miere spoliehajú na sieť dcérskych spoločností a nezávislých dodávateľov. Príklady možno vidieť v bankovom sektore, kde sa využívajú nezávislé „call centrá", v ropnom priemysle, kde sa zamestnávajú dodávatelia vrtov, ale aj v technologickom priemysle, kde sú spotrebitelia prepojení s vývojármi aplikácií.
Príchodom systémov na báze umelej inteligencie sa dané otázky len prehlbujú. Práve z týchto dôvodov sa tento príspevok bude venovať otázke doktríny *respondeat superior* v kontexte umelej inteligencie.

Analógie v kontexte umelej inteligencie

Analógie zohrávajú dôležitú rolu v právnom uvažovaní. Používanie právneho analogického uvažovania je založené na identifikácii zjednocujúceho prvku normatívneho princípu.[3]
Dworkin tvrdí, že „analógia bez teórie je slepá"[4], je však tiež zrejmé, že použitie nepresnej alebo nevhodnej teórie môže viesť ku krátkozrakému pohľadu. Aby bolo možné dospieť k záveru na základe istej analógie, je nevyhnutné mať dobre vypracovanú teóriu a zodpovedajúci princíp, ktorý ju podporuje. To je obzvlášť dôležité, keď sa uvažuje o technologickej inovácii, ktorá nemá v našich dejinách obdobu aká je práve umelá inteligencia.
Je však náročné vytvoriť analógiu, ktorá by nebola ovplyvnená postojmi jednotlivca, ktorý ju navrhuje a hodnotí. Keďže je nevyhnutné uznať, že uplatňovanie analógií je vo svojej podstate hodnotiaci proces. Zvolená analógia bude v konečnom dôsledku informovať o formulácii požadovaných a uplatniteľných právnych pravidiel. Výber vhodnej právnej analógie je podmienený procesom uvažovania, ktorý zahŕňa

[3] Porovnaj. FULLER, *L.: legal fictions*, Stanford University press, 1967. alebo OLIVIER, P: *legal fictions, practice and legal science* 1975. alebo DEL MAR, M - TWINIG, W.: *legal fictions in theory and practice*,2015. alebo CAMPBELL,K.: *Fuller on Legal Fictions*. 1983. alebo HARMON, *L.: falling off the vine: Legal Fictions And The Doctrine of Substituted Judgment*, 100 YALE L. 1991. alebo KLERMAN, D.: *Legal Fictions as Strategic Instruments.*(UC Berkeley: Berkeley Program in Law and Economics, 2009. alebo KNAUER, N.: *Legal fictions and Juristic Truth, 2010. alebo* PALMER, *B: Legal Fictions and Red Room Wine: An Excursion into History, 38 A.B.A. J. 1953. alebo* SMITH, *P.: New Legal Fictions, 2007. alebo AVIAM SOIFER, Reviewing Legal Fictions, 1986.*
[4] DWORKIN, R.: *In Praise of Theory*, 1997.

porovnanie dostupných analógií ako aj regulačných cieľov, s ktorými súvisia.[5] Tento proces zahŕňa analýzu z povahy daného problému, ktorý bol podnetom na podniknutie tejto cesty uvažovania.[6] A práve túto úlohu môže riešiť len teória, ktorá je vybudovaná a podložená na stabilných zásadách a hodnotách.

V právnej teórií nie vždy je to tak, že najvhodnejšia a najlepšia analógia bude hneď z úvodu zrejmá. Z povahy analógií vyplýva, že bude nevyhnutne vykazovať určité nedostatky vzhľadom na to, že ide o pokus ustáliť vzťah medzi dvoma odlišnými fenoménmi alebo entitami.[7] Vyvstáva teda otázka, či tento nedostatok spôsobuje nepoužiteľnosť analógie ako celku, t. j. všeobecný princíp rovnováhy, alebo vytvára len situáciu v podobe zvládnuteľného problému.[8]

Niektorí odborníci však sú dodnes skeptickí voči analogickému uvažovaniu ako rigoróznej forme argumentácie a namiesto toho obhajujú priamejšiu analýzu právneho scenára v súlade so stanovenými hodnotami.[9] Tí však, ktorí sú proti používaniu takýchto analógií, zatiaľ nepredložili alternatívu, ktorá by bola rovnako účinná alebo intuitívna. Analogické uvažovanie sa považuje za horšiu formu rozhodovania z dôvodu jeho závislosti od predchádzajúcich právnych zásad, ktoré sú často morálne, eticky alebo aj právne pochybné. Takýto prístup spochybňuje predpoklad, že analogické uvažovanie je správnou metódou na dosiahnutie stability, správneho rozhodovania a právnej istoty.[10]

A aj keď existujú presvedčivé dôvody proti používaniu právnych analógií, skutočnosť je taká, že výklad právnych noriem bez prípustnosti analógií zostáva nedostatočná. Je nevyhnutné, aby sa právne analógie používali, bez ohľadu na to, či to teória považuje za pozitívny alebo negatívny aspekt. Bolo by preto neefektívne nebrať analógie do úvahy ako súčasť procesu právneho uvažovania, najmä keď je potrebné prijať rozhodnutia o nových technológiách.[11]

V kontexte systémov umelej inteligencie predstavujú analógie osobitný súbor výziev ktorým sa musíme venovať.

---

[5] Porovnaj. GÁHER, F.: *otvorená textúra pojmu – pôvodný zmysel a kritika*, 2018 Dostupné na:<http://www.klemens.sav.sk/fiusav/doc/filozofia/2018/8/620-635.pdf>.

[6] ANAT. L.: "AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy," Mitchell Hamline Law Review: Vol. 46: Iss. 5, Article 2. Available at: https://open.mitchellhamline.edu/mhlr/vol46/iss5/2. 2020.

[7] V dôsledku toho sa analógia nemôže považovať za presné zobrazenie predmetnej veci ale len o tú najbližšiu podobu akú dokážeme vytvoriť.

[8] Porovnaj. RAWLS.J.: *a theory of justice* s. 46–53, 1971.

[9] Ako napríklad. SCHAUER.F.: *playing by the rules: a philosophical examination of rule-based decision-making in law and in life* 1995. alebo POSNER.R.: *the problems of jurisprudence,* 1990.

[10] JOHN RAWLS. *a theory of justice* s. 46–53, 1971.

[11] Pozri. GYURÁSZ. Z.: *Modality regulácie nových technológii*. Rigorózna práca, 2021. alebo GYURÁSZ. Z: *From principles to practice: regulating artificial intelligence,* Bratislava: Právnická fakulta UK, 2020.

Zodpovednosť umelej inteligencie v kontexte „respondeat superior"

Doktrína *respondeat superior*[12] však vznikla dávno pred príchodom moderného globalizovaného sveta, keďže bola zavedené v starovekom Ríme a vznikla ako prostriedok zodpovednosti hlavy domácnosti za činy členov domácnosti, a to najmä sluhov a otrokov (*alieni iuris)*.[13] Táto téma bola predmetom mnohých diskusií v súvislosti s umelou inteligenciou, pričom bolo navrhnutých mnoho analógií, pokiaľ ide o miesto umelej inteligencie v našom právnom a sociálnom systéme.[14]

V právnej teórii na to, aby bolo možné aplikovať doktrínu *respondeat superior*, je potrebné preukázať existenciu primeraného vzťahu medzi nadriadeným a podriadeným, ako aj jasnú súvislosť medzi týmto vzťahom a správaním podriadeného, ktoré viedlo k vzniku škody.[15] Doktrínu však možno za určitých okolností uplatniť za predpokladu, že umelá inteligencia pôsobí autonómne v kritickom prostredí alebo v prostredí, ktoré má vysokú pravdepodobnosť rizika zlyhania na iné subjekty.[16]

Analýza právneho postavenia[17] umelej inteligencie a jej zodpovednosti za svoje konanie odhaľuje súvislosť medzi právnym postavením umelej inteligencie dnes a postavením otrokov ustanoveným v rímskom práve. Systém umelej inteligencie ako aj otrok nie sú považované za subjekt práva ale sú skôr jeho objektmi. Za predpokladu, že existuje paralela medzi právnym postavením umelej inteligencie a postavením otrokov v starovekom Ríme, možno tvrdiť, že pri aplikácii doktríny *respondeat superior* všetky škody spôsobené konaním umelej inteligencie by mal nahradiť jej vlastník alebo právnická osoba, za ktorú koná. V rímskom práve to znamenalo, že za delikty spáchané otrokmi bola zodpovedná hlava domácnosti.[18]

Dnes by to znamenalo, že vývojár alebo za istých okolností používateľ systému umelej inteligencie by musel prebrať zodpovednosť za konanie inteligentného systému. Uplatňovanie doktríny *respondeat superior* v kontexte systémov umelej inteligencie však komplikuje tzv. problém „čiernej skrinky". Tento koncept v podstate

---

[12] Z lat. „nech pán odpovedá"

[13] Doktrína stanovovala, že pri delikte možno voči dominovi uplatniť noxálnu žalobu, na základe ktorej musí buď zaplatiť náhradu škody, ktorá sa za takýto delikt bežne platí, alebo vydať otroka poškodenému. Pozri REBRO, K. - BLAHO. P.: *Rímske právo*. 2019

[14] Pozri. METEŇKANYČ, O. – GYURÁSZ, Z.: Priznanie práv a právnej subjektivity nonhumánnym entitám. Prípady prírodných javov a umelej inteligencie. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022,

[15] Pozri bližšie. Catholic Church Welfare Society v. Various Claimants, 2012. Dostupné na. https://www.supremecourt.uk/cases/docs/uksc-2010-0230-judgment.pdf

[16] Porovnaj. BENNETT, H.: *Principles of the law of agency*. 2013.

[17]METEŇKANYČ, O. – GYURÁSZ, Z.: Priznanie práv a právnej subjektivity nonhumánnym entitám. Prípady prírodných javov a umelej inteligencie. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022,

[18] REBRO, K. - BLAHO. P.: *Rímske právo*. 2019

popisuje problém vysvetliteľnosti rozhodnutí, ktoré urobí inteligentný systém. Porovnať by sme to mohli k Heisenbergovmu princípu neurčitosti. A teda, že síce vieme akými informáciami bol inteligentný systém „kŕmený" a vieme k akému záveru systém dospel. Avšak súčasne nám nebudú presne známe, podľa ktorých vybraných dát a ako metódou dospel systém k danému záveru. Preto ako Heisenberg tvrdil o subatomárnych časticiach aj my môžeme tvrdiť o umelej inteligencii, že *„ani minulé ani budúce správanie (...) sa nedá predpovedať s istotou*." [19]

Záver

Je čoraz viac zrejmé, že systémy na báze s umelou inteligenciou sú nenahraditeľnou súčasťou súčasnej spoločnosti, pričom tieto systémy budú v budúcnosti len a len získavať na dôležitosti. S tým, ako sa zvyšuje integrácia týchto systémov do našich domácností a priemyselných odvetví, je neodvrátiteľné, že budú spôsobovať škody. Používanie právnych analógií na určenie vhodného režimu zodpovednosti systémov na báze umelej inteligencie je bežnou metódou riešenia nových javov, a to najmä v kontexte nových technológií.

Výber vhodnej právnej analógie však nie je samostatným fenoménom, ktorý nebude mať vplyv na právny systém okolo nás. Výber vhodnej právnej analógie je ovplyvnený viacerými faktormi vrátane regulačných cieľov, ktoré sa snažíme dosiahnuť, ako aj spôsobu, akým vnímame systémy na báze umelej inteligencie ako súčasť našej spoločnosti.

Najpresnejšou analógiou na porozumenie vzťahu medzi systémami na báze umelej inteligencie a našou spoločnosťou je považovať ich za objekt, ktoré sú pod kontrolou a vedením ľudských entít. Bez ohľadu na legitímnosť rozdielnych názorov na túto právnu analógiu je režim prísnej zodpovednosti, ktorý je jej základom, vo forme *respondeat superior*, v kontexte zodpovednosti systémov na báze umelej inteligencie najvhodnejší.

Zoznam použitej literatúry

1) ANAT. L.: "AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy," Mitchell Hamline Law Review: Vol. 46: Iss. 5, Article 2. Available at: https://open.mitchellhamline.edu/mhlr/vol46/iss5/2. 2020.

[19] Pre problematiku princípu neurčitosti Pozri bližšie BAKER, J. *50 physics ideas you really need to know*. London: Quercus Publishing Plc, 2007, 112 s. K problematike čiernej skrinky pozri bližšie GUIDOTTI, R. - MONREALE, A. – PEDRESCHI, D.: The AI black box Explanation Problem. *ERCIM*, 2019, alebo ZEDNIK, C.: Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence. *Philosophy & Technology*, Springer, 2019, Dostupné na: https://link.springer.com/article/10.1007/s13347-019-00382-7

2) BAKER, J. *50 physics ideas you really need to know*. London: Quercus Publishing Plc, 2007.
3) BENNETT, H.: *Principles of the law of agency*. 2013.
4) CAMPBELL,K.: *Fuller on Legal Fictions*. 1983.
5) DEL MAR, M - TWINIG, W.: *legal fictions in theory and practice*,2015.
6) DWORKIN, R.: *In Praise of Theory*, 1997.
7) FULLER, *L.: legal fictions*, Stanford University press, 1967.
8) GÁHER, F.: *otvorená textúra pojmu* – Pôvodný Zmysel A Kritika, 2018 Dostupné na:<http://www.klemens.sav.sk/fiusav/doc/filozofia/2018/8/620-635.pdf>.
9) GUIDOTTI, R. - MONREALE, A. – PEDRESCHI, D.: The AI black box Explanation Problem. *ERCIM*, 2019,
10) GYURÁSZ. Z: *From principles to practice: regulating artificial intelligence,* Bratislava: Právnická fakulta UK, 2020.
11) GYURÁSZ. Z.: *Modality regulácie nových technológii*. Rigorózna práca, 2021.
12) HARMON, *L.: falling off the vine: Legal Fictions And The Doctrine of Substituted Judgment*, 100 YALE L. 1991.
13) KLERMAN, D.: *Legal Fictions as Strategic Instruments.*(UC Berkeley: Berkeley Program in Law and Economics, 2009.
14) KNAUER, N.: *Legal fictions and Juristic Truth, 2010.*
15) METEŇKANYČ, O. – GYURÁSZ, Z.: Priznanie práv a právnej subjektivity nonhumánnym entitám. Prípady prírodných javov a umelej inteligencie. 1. vydanie. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2022,
16) OLIVIER, P: *legal fictions*, *practice and legal science* 1975.
17) PALMER, *B: Legal Fictions and Red Room Wine: An Excursion into History, 38 A.B.A. J. 1953.*
18) POSNER.R.: *the problems of jurisprudence,* 1990.
19) REBRO, K. - BLAHO. P.: *Rímske právo*. 2019
20) SCHAUER.F.: *playing by the rules: a philosophical examination of rule-based decision-making in law and in life* 1995.
21) SMITH, *P.: New Legal Fictions, 2007. alebo AVIAM SOIFER, Reviewing Legal Fictions, 1986.*
22) ZEDNIK, C.: Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence. *Philosophy & Technology*, Springer, 2019, Dostupné na: https://link.springer.com/article/10.1007/s13347-019-00382-7
23) Catholic Church Welfare Society v. Various Claimants, 2012. Dostupné na. https://www.supremecourt.uk/cases/docs/uksc-2010-0230-judgment.pdf

Kontaktné informácie

JUDr. Zoltán Gyurász, PhD.
Univerzita Komenského v Bratislave
Právnická fakulta
Ústav práva informačných technológii a práva duševného vlastníctva

PRIENIK UMELEJ INTELIGENCIE A PRÁVA DUŠEVNÉHO VLASTNÍCTVA: VÝZVY A OČAKÁVANIA

THE INTERSECTION OF ARTIFICIAL INTELLIGENCE AND INTELLECTUAL PROPERTY LAW: CHALLENGES AND EXPECTATIONS

Martin Daňko[1]

Abstrakt: Tento článok sa zaoberá prienikom práv duševného vlastníctva a umelej inteligencie, kde sa bližšie zameriava na analýzu súčasného právneho rámca na Slovensku a v Európskej únii, ktorý je vo veci autorstva a pôvodcovstva založený na antropocentrickom prístupe. Článok analyzuje výzvy spojené s posudzovaním autorstva diel vytvorených umelou inteligenciou, ale venuje sa aj otázkam, ako sú právna subjektivita umelej inteligencie a ochrane práv predmetov duševného vlastníctva použitých pri trénovaní umelej inteligencie. V poslednej časti autor článku skúma a hodnotí stav právnej úpravy v tejto oblasti na úrovni práva Európskej únie.

Kľúčové slová: umelá inteligencia, práva duševného vlastníctva, právna subjektivita umelej inteligencie , Akt o umelej inteligencii v práve EÚ.

Abstract: This article deals with the intersection of intellectual property rights and artificial intelligence, focusing on the analysis of the current legal framework in Slovakia and the European Union, which is based on an anthropocentric approach in the matter of authorship. The article analyses the challenges related to the assessment of authorship of works created by artificial intelligence, but also addresses issues such as the legal subjectivity of artificial intelligence and the protection of the rights of intellectual property objects used in the training of artificial intelligence. In the last part of the article, the author examines and assesses the state of the law in this area at the level of European Union law.

Keywords: Artificial intelligence, Intellectual property rights, Legal personality of artificial intelligence , Artificial Intelligence Act in EU law.

[1] Univerzita Komenského v Bratislave, Právnická fakulta, Ústav práva informačných technológií a práva duševného vlastníctva

Úvod

Je právo duševného vlastníctva odkázané na tvorivosť ľudí ako živých bytostí alebo je jeho budúcnosť spätá aj s niečím neživým? Nie je potrebné dlhé zamyslenie na konkretizáciu položenej otázky. Niečo neživé v kontexte existujúcich tvorivých procesov súčasnosti je pomenovanie umelej inteligencie. Umelá inteligencia je pojem, ktorý je v súčasnosti predmetom objavovania, skúšania, ale aj využívania zo strany dotknutej verejnosti. Toto tvrdenie je možné z časti potvrdiť aj výskumom, ktorý uvádza, že „viac ako polovica ľudí (53 percent) túži po tom, aby im umelá inteligencia uľahčila každodenné fungovanie, vylepšila možnosti zábavy a celkovo zvýšila kvalitu života".[2] Očakávania vychádzajú z prezentovaného technického pokroku v oblasti umelej inteligencie. Najsignifikantnejšie je to možné pozorovať pri výsledkoch činnosti generatívnych modelov[3], ako sú ChatGPT[4] a DALL-E[5], ktoré

[2] TREND: Len 15 percent Európanov vie, ako využívať umelú inteligenciu v každodennom živote. Publikované 29.9.2024, Dostupné online na: https://www.trend.sk/spravy/len-15-percent-europanov-vie-ako-vyuzivat-umelu-inteligenciu-kazdodennom-zivote

[3] Na technickej úrovni ich možno odlišovať od tradičnejších modelov AI rôznymi spôsobmi. Sú trénované na obrovských množstvách textu a generujú jazyk ako výstup. Často sú generatívne AI modely charakterizované ich širším rozsahom a väčšou autonómiou pri extrakcii vzorov v rámci veľkých súborov údajov. NOVELLI, C., CASOLARI, F.,HACKER, P., SPEDICATO, G., FLORIDI, L.: Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity, Zverejnené 14.1.2024. Dostupné online na SSRN: https://ssrn.com/abstract=4694565 or http://dx.doi.org/10.2139/ssrn.4694565

[4] ChatGPT, vyvinutý spoločnosťou OpenAI, je prominentným príkladom modelu veľkého jazyka (LLM), ktorý využíva architektúru Generative Pre-trained Transformer (GPT). Tento model je navrhnutý tak, aby generoval ľudský text na základe vstupu, ktorý dostane. Základná technológia ChatGPT je zakorenená v architektúre transformátora, ktorá využíva mechanizmy, ako je pozornosť na spracovanie a generovanie jazyka. Mechanizmus pozornosti umožňuje modelu zvážiť význam rôznych slov vo vete, čo mu umožňuje pochopiť kontext a produkovať koherentné odpovede. XU, W., WANG, X., GUO, Q., SONG, X., ZHAO, R., ZHAO, G., ... & YANG, Y. (2023). Decomposition is all you need: single-objective to multi-objective optimization towards artificial general intelligence. Mathematics, 11(20), 4390. Dostupné online na https://doi.org/10.3390/math11204390

[5] DALL-E pracuje tak, že vezme miliardy bitov textu z internetu a preloží ich do abstrakcie, ktorú uloží na miesto v „latentnom" alebo logickom priestore. Vo vesmíre opísateľných vecí bude napríklad „pavián" „umiestnený" silnými asociáciami v blízkosti iných primátov, pravdepodobne neďaleko „Afriky", „savany" alebo „zoo". Obrázky sa tiež čítajú z internetu a sú spojené s ich popismi a transponované do rovnakých logických oblastí. Takže text a príslušné popisy obrázkov, hoci sú stále odlišné, sú umiestnené v silných asociáciách blízko seba. To umožňuje DALL-E nájsť druhy obrázkov v priestoroch označených textovou výzvou používateľa. Potom vygeneruje súbor kľúčových funkcií, ktoré môže tento obrázok obsahovať. V našom príklade "pavián v člne" by prišiel s charakteristickými znakmi paviána, napríklad farbou jeho srsti, rukami a ramenami podobnými človeku alebo psovitým tvarom jeho hlavy, ako aj s charakteristickými znakmi člna, napríklad so zakriveným okrajom člna. Potom DALL-E nasadí to, čo sa nazýva difúzny model, ktorý začína statickým šumom a potom tvaruje pixely spôsobom informovaným o latentnej reprezentácii textového popisu, čím vytvára jedinečné obrázky pri každom spustení programu. SLACK, G.: What DALL-E Reveals About Human Creativity.

priniesli zásadné otázky v tvorbe a ochrane predmetov práv duševného vlastníctva. Diela generované predmetnými modelmi sú častokrát nerozlíšiteľné od ľudskej tvorby, a preto je na mieste otázka, aký charakter z pohľadu práva majú výsledky činnosti týchto modelov. Je preto na mieste riešiť nové právne a etické výzvy, nakoľko súčasná právna úprava neposkytuje komplexné riešenie, ktoré je v týchto prípadoch však nevyhnutné.

Tento článok si dáva ambíciu analyzovať prienik umelej inteligencie a práva duševného vlastníctva, pričom základnou vedeckou hypotézou je konštatovanie, že súčasná legislatíva Európskej únie dostatočne nerieši regulačné výzvy umelej inteligencie vo vzťahu k ochrane tvorcov a pôvodcov predmetov práv duševného vlastníctva. Sekundárnou skúmanou problematikou tohto článku je hľadanie rovnováhy medzi ochranou tvorcov a pôvodcov predmetov práv duševného vlastníctva a podporou inovácií, tzn. subjektov, ktoré prostredníctvom umelej inteligencie vytvárajú nový obsah, ale aj subjektov, ktoré samotné systémy umelej inteligencie vytvárajú alebo inovujú.

Výzvy AI v oblasti práv duševného vlastníctva

Tvorba predmetov práv duševného vlastníctva je v slovenskom právnom poriadku považovaná za činnosť viazanú na fyzickú osobu. Autorom, pôvodcom vynálezu, úžitkového vzoru alebo dizajnu môže byť len fyzická osoba, nakoľko len fyzická osoba je schopná tvorivej duševnej činnosti.[6] Preto otázka a zároveň výzva pre právnu reguláciu v súvislosti s výsledkami činnosti umelej inteligencie je stanovenie subjektu práv, ktorý by mal k týmto výsledkom subjektívne práva. Podľa niektorých autorov AI predstavuje zásadnú výnimku z tohto antropologického chápania jedinej možnosti pôvodu predmetov práv duševného vlastníctva ako výsledkov tvorivej duševnej činnosti fyzickej osoby.[7] Na druhej strane neexistuje zatiaľ všeobecne akceptovaný názor, že by umelá inteligencia mohla mať právnu subjektivitu[8], a tak predmety práv

(17.1.2023) Standford University, Human -Centered Artificial Intelligence, Arts and Humanities, Neuro and Cognitive Science, Dostupné online na: https://hai.stanford.edu/news/what-dall-e-reveals-about-human-creativity

[6] GYURÁSZ, Z.: Duševné vlastníctvo vo svetle umelej inteligencie. In: ComenIUS [elektronický dokument] . – Bratislava (Slovensko) : Univerzita Komenského v Bratislave. Právnická fakulta UK. – ISSN (online) 2454-0846. – Roč. 5, č. 2 (2020), s. 6-14

[7] VISHNU. S.: Rise of Artificial Intelligence and Copyright Challenges (July 31, 2023). Osmania University Journal of IPR [OUJIPR], 1(1), pp. 86-98, Dostupné online na SSRN: https://ssrn.com/abstract=4675455

[8] MOERLAND, A.: Artificial Intelligence and Intellectual Property Law. Zverejnené 20. 5. 2022, Dostupné online na SSRN: https://ssrn.com/abstract=4203360 alebo http://dx.doi.org/10.2139/ssrn.4203360

duševného vlastníctva, ktoré by vytvorila by museli byť priradené len inému právnemu subjektu, a to bez ohľadu na to, či by išlo o fyzickú alebo právnickú osobu. Ako sme už uvádzali bližšie v slovenskom právnom poriadku autorom môže byť len fyzická osoba. Takáto právna úprava vychádza z Bernského dohovoru o ochrane literárnych a umeleckých diel z 9. septembra 1886 v znení neskorších revízií, kde prostredníctvom ochrany autorových osobnostných práv, ktorých úprava sa nachádza v článku 6bis tohto dohovoru vo forme autorstva k dielu, vieme určiť, že autorom môže byť len fyzická osoba, nakoľko len fyzická osoba môže disponovať osobnostnými právami. Otázne však ostáva, ako vnímať autorstvo k dielu vytvoreného umelou inteligenciou. Napriek pomerne náročnej otázke, je možné odpoveď na túto otázku hľadať aj inak ako len vysvetlením algoritmov a strojového učenia, vďaka ktorému umelá inteligencia dokáže vygenerovať obsah. Ako príklad nám poslúži generovanie umeleckého diela z výtvarného umenia, kde spisovateľka Lauren de Plesiss upozorňuje že originalita AI je rozpoznateľná, respektíve nerozpoznateľná umeleckým publikom. Ako príklad uviedla výstavu, ktorej publikum nedokázalo rozpoznať, či daný obraz bol vytvorený fyzickou osobou alebo umelou inteligenciou. Na predmetnej výstave sa publikum dožadovalo umelca, ktorý podľa ich presvedčenia predmetné diela vytvoril. Dôvodom pre takéto stretnutie bola zvedavosť na umelcov príbeh, ktorý podľa publika mal byť motiváciou pre vytvorenie predmetných diel. Bez príbehu nie je umenie? Za týmto príbehom je profesor Ahmed Elgammal, ktorý pôsobí na Katedre počítačovej vedy na Rutgers University, kde založil Art and AI Lab. Profesor Elgammal a jeho tím v rámci tohto vytvorili AICAN (AI Creative Adversarial Network), čo je sieť GAN, ktorá bola trénovaná na 100 000 obrazoch z piatich storočí západného umenia.[9] Generative Adversarial Networks (GAN) sú typy architektúr neurónových sietí schopné generovať nové dáta, ktoré zodpovedajú naučeným vzorcom. GAN je možné použiť na vytváranie obrázkov ľudských tvárí alebo iných objektov, na vykonávanie prekladu textu na obrázok, na prevod jedného typu obrázku na iný a na zvýšenie rozlíšenia obrázkov (super rozlíšenie) medzi inými aplikáciami. Keďže siete GAN dokážu generovať úplne nové údaje, sú na čele mnohých špičkových systémov, aplikácií a výskumu AI.[10] Rozhodnúť o tom, či umelú inteligenciu považujeme za autora, alebo niekedy v budúcnosti budeme považovať za autora je možné aj prostredníctvom filozofického prístupu. Osobitne v tomto smere je značne inšpirujúci pohľad Mackienze Caldwella, ktorý otázku autorstva a autora posudzuje podľa filozofických prístupov Locka, Hegla a Kanta. Podľa Lockovho princípu robotníci majú právo na ovocie svojej práce,

[9] PLESSIS, L.D.: What Is AI Art? A Guide on How It Works and How to Create It., Domestika (14. augusta 2022), https://www.domestika.org/en/blog/10352-what-is-ai-art-a-guide-on -ako-to-funguje-a-ako-to-vytvoriť [https://perma.cc/84YB-YDKZ]

[10] NELSON, D.: Čo je to Generative Adversarial Network (GAN)? Zverejnené 05.10.2020. Dostupné online na: https://www.unite.ai/sk/what-is-a-generative-adversarial-network-gan/

autorstvo k dielu patrí autorovi, ktorý dielo vytvoril. Hoc ako Caldwell dodáva Lockov prístup Najvyšší súd USA neprijal, nakoľko sa viac priklonil k otázke pôvodu originality. Podľa amerického vnímania ochrany autorského práva sa právo viac zameriava na ochranu výsledku tvorby autora ako ochranu procesu vzniku autorského diela. Z Lockovej teórie vlastníctva je možné ako podstatné vnímať to, že autorom je ten, kto autorské právo vytvoril. A nie len to, ale aj viac. Lockova teória práce rozšírená o intelektualistickú teóriu sa zameriava na autorov úsudok, tzn. na „intelektuálny vklad" autora, ktorý je rovnako dôležitý ako samotná kreativita diela. Kantove chápanie autorstva a autorského práva je založené na komunikácii osoby autora s verejnosťou. Táto komunikácia predstavuje podstatu existencie autorského diela, dielo nevzniká ako samostatný predmet, ktorého použitím je obohacované publikum, ale ako vyjadrenie autorových myšlienok a ochrany týchto myšlienok. V novodobom poňatí vnímania autorských práv Kant preferoval myšlienku, že akýkoľvek zásah do autorských práv je zásah len do osobnostných práv autora, nakoľko tie sú jediné, ktoré autor má, tzn. možno zasiahnuť do osobnosti autora, myšlienok autora zhmotnených v jeho diele. Caldwell Kantovu teóriu stavia do možnosti porušenia autorských práv prostredníctvom umelej inteligencie, pretože použitie existujúcich autorských diel pri trénovaní umelej inteligencie je neoprávnený zásah do osobnostných práv autorov takto použitých diel. Hegel na rozdiel od Kanta si uvedomuje podstatu a význam aj majetkových práv autora, ale všetko za účelom rozvoja osobnosti autora. Práve vlastnícke práva teda umožňujú dosiahnuť individuálnu spokojnosť prostredníctvom rozvoja osobnosti jednotlivca a ich ochrana je najlepším pokrokom vedy a umenia. Bez ochrany autorských práv aj na majetkovej úrovni by nemohlo možné autorov spravodlivo odmeniť a financovať rozvoj ich duševnej činnosti. V kombinácii s popretím morálnych práv podľa Kanta je popretie vlastníckych práv v umení AI popretím osobnostného rozvoja založeného na schopnosti a túžbe autora tvoriť. Je zaujímavé, že v prípade „náhodného autorstva" predstavuje autorské prijatie náhodného účinku akt vôle. V umení AI predstavujú vedomé voľby autora autorovu vôľu, ducha a osobnosť, ku ktorým by mali byť pripojené morálne, pracovné a osobnostné práva. Neuznanie týchto práv bráni rastu autorských práv tým, že odrádza od vytvárania nových diel. Ak sa pozrieme na tieto tri pohľady spolu, autorstvo pozostáva z komunikácie jednotlivca prostredníctvom volieb, ktoré jednotlivec robí pri vytváraní diela, a tento produkt by mal byť chránený pred nemorálnymi úpravami. Autorstvo AI teda pozostáva z práce, osobnosti a komunikácie.[11]

[11] CALDWELL, M: What Is an "Author"?-Copyright Authorship of AI Art Through a Philosophical Lens. In. Houston Law Review, Vol. 61, Issue 2, 2023, Dostupné online na: https://houstonlawreview.org/article/92132-what-is-an-author-copyright-authorship-of-ai-art-through-a-philosophical-lens

Autorská dilema? Vishnu zhrnul možnosti autorského pôvodu diel vytvorených umelou inteligenciou do viacerých variant. Prvá varianta stanovuje konštatovanie, že tvorcami diel generovaných umelou inteligenciou by mali byť jednotlivci alebo organizácie, ktoré vyvinuli algoritmy umelej inteligencie použité na vytvorenie diela. Druhá varianta sa opiera o argument, že tvorcami by mali byť jednotlivci alebo organizácie, ktoré trénovali modely umelej inteligencie, alebo jednotlivci alebo organizácie, ktoré poskytli údaje, na ktorých boli modely AI vyškolené. Tieto argumenty však nie sú bez kontroverzií. Tretia varianta vychádza z tvrdení, že skutočnými tvorcami diel generovaných umelou inteligenciou sú samotné systémy umelej inteligencie a že týmto systémom by sa mala udeliť určitá forma právnickej subjektivity alebo uznania ako nezávislých subjektov práva. Posledný prístup sa opiera o názor, že diela vytvorené umelou inteligenciou by nemali byť vôbec chránené autorským právom, pretože chýba tvorivý zámer a autorstvo, ktoré sú ústredným prvkom autorského práva.[12] Každý z argumentov má svoje hodnotové východiská a logické argumenty. Prvá varianta má logické zdôvodnenie, nakoľko sa opiera o tvorivú duševnú činnosť tých, ktorí umelú inteligenciu vytvorili. Nie je možné poprieť autorské práva autorov umelej inteligencie k nej samotnej, ale považovať ich automaticky aj za výlučných autorov/pôvodcov obsahu, ktorý takáto umelá inteligencia dokáže vygenerovať, je unáhlené a nejednoznačné. Takýmto prístupom by mohli byť predčasne eliminovaní aj iní autori a pôvodcovia, ktorí do procesu tvorby nového obsahu vstúpili. Bohužiaľ toto tvrdenie nie je možné zovšeobecniť, nakoľko som presvedčený, že každý výsledok tvorby umelej inteligencie je potrebné hodnotiť osobitne. Osobitne je potrebné zhodnotiť, či pre tvorbe nového obsahu umelou inteligenciou nedošlo k spracovaniu existujúcich diel, na ktorých sa umelá inteligentná trénovala, alebo či používateľ umelej inteligencie svojimi príkazmi nevytvoril nové dielo, nakoľko jeho príkazy by mohli byť z pohľadu autorského práva chápané ako tvorivá duševná činnosť.[13]

Konštatovať, že samotná umelá inteligencia by mala mať vlastnú právnu subjektivitu, vnímam v súčasnosti za veľmi nereálne až priam utopistické riešenie, ktoré nedokáže poňať všetky právne dopady, ktoré by toto riešenie prinieslo. Len jeden argument o nereálnosti tohto riešenia je vôľa zákonodarcu pripustiť, že umelá inteligencia je plnohodnotným subjektom práva, ktorý môže svojim konaním zakladať, meniť a rušiť právne vzťahy. Len táto požiadavka by znamenala obrovské zmeny v právnych poriadkoch, nadnesene takmer na celom svete. Museli by sa vymyslieť a následne

[12] VISHNU. S.: Rise of Artificial Intelligence and Copyright Challenges (July 31, 2023). Osmania University Journal of IPR [OUJIPR], 1(1), s. 90, Dostupné online na SSRN: https://ssrn.com/abstract=4675455

[13] HUGENHOLTZ, P., B. a QUINTAIS. J.P.: 2021. 'Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output?' IIC - International Review of Intellectual Property and Competition Law 52 (9): 1190–1216. Dostupné online na: https://doi.org/10.1007/s40319-021-01115-0

svetovo harmonizovať pravidlá pre samotný vznik, konanie, ale aj zánik tohto subjektu práva. Rozsah práv právnym poriadkom priznaných umelej inteligencii by bol vzhľadom na svoje činnosti limitovaný oproti už existujúcim subjektom práva, lebo napríklad ani v súčasnosti právnická osoba nemôže byť biologickým rodičom, a tak nemôže mať rodičovské práva a povinnosti. Znamenalo by to, že by išlo o komplexnú právnu úpravu celej existencie umelej inteligencie. Bez ohľadu na skúmanie tak právne náročných otázok existencie právnej subjektivity umelej inteligencie ako je vôľa, prejav vôle alebo posudzovanie zodpovednosti, musíme skonštatovať, že pokiaľ výskum a vývoj umelej inteligencie neprinesie nové koncepty umelej inteligencie, či v tomto smere až priam „samostatne mysliaceho robota", zákonodarcovia nebudú mať potrebu sa púšťať do tak náročných legislatívnych projektov. Súčasnosť neponúka úplné riešenia ani na otázku ochrany práv duševného vlastníctva, ktoré sú využívané pri trénovaní umelej inteligencie, čo je podľa môjho názoru vzhľadom na možný zásah do majetkových práv autorov alebo iných pôvodcov práv duševného vlastníctva aktuálnejšia otázka na riešenie.

Akt o umelej inteligencii a jeho dopady na ochranu práv duševného vlastníctva

Pri charakterizovaní právnej úpravy umelej inteligencie na úrovni práva EÚ vo forme nariadenia Európskeho Parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024,ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (ďalej aj ako „Akt o umelej inteligencii" alebo len „Akt") by sme mohli použiť pozitívne hodnotenia v kontexte pomerne rozsiahlej a komplexnej úpravy[14] právnych aspektov existencie umelej inteligencie v spoločnosti[15], no zámerom tohto článku je hodnotenie len obmedziť na tú úpravu, ktorá sa venuje prieniku umelej inteligencie a práva duševného vlastníctva.

Hneď úvodom hodnotenia tohto prieniku je potrebné povedať, že samotný Akt má verejnoprávny charakter, čo je prvý problém z pohľadu hľadania uvádzaného prieniku. Akt o umelej inteligencii nerieši otázku autorstva alebo pôvodcovstva

[14] CIHANOVÁ, J.: AI regulation : the EU and China aprproach. In. Acta Facultatis Iuridicae Universitatis Comenianae, č. 1, rok 2024, s. 5

[15] Podľa recitálu 1 Aktu o umelej inteligencii je účelom tohto nariadenia zlepšiť fungovanie vnútorného trhu stanovením jednotného právneho rámca, najmä pokiaľ ide o vývoj, uvádzanie na trh, uvádzanie do prevádzky a používanie systémov umelej inteligencie v EÚ v súlade s jej hodnotami, podporovať zavádzanie dôveryhodnej umelej inteligencie zameranej na človeka a zároveň zaistiť vysokú úroveň ochrany zdravia, bezpečnosti a základných práv zakotvených v Charte základných práv Európskej únie, vrátane ochrany demokracie, právneho štátu a životného prostredia, chrániť pred škodlivými účinkami systémov umelej inteligencie v EÚ a podporovať inovácie na jednotnom trhu.

predmetov vytvorených umelou inteligenciou,[16] ale len sa zaoberá problematikou ochrany predmetov práv duševného vlastníctva, tzn. ochrany práv autorov a pôvodcov týchto predmetov z pohľadu transparentnosti použitia týchto predmetov pri trénovaní systémov umelej inteligencie. Vytvorený právny rámec požaduje väčšiu transparentnosť od spoločností implementujúcich nástroje generatívnej umelej inteligencie, ako je napríklad ChatGPT4 a to tak, že musia zverejniť všetok použitý materiál chránený autorskými právami pri vývoji svojich systémov.[17] Z pohľadu autorských práv je potrebné spomenúť generatívnu umelú inteligenciu, ktorá vykonáva hĺbkovú analýzu textu alebo údajov (ďalej ako „TDM")[18] podľa Smernice Európskeho parlamentu a Rady (EÚ) 2019/790 zo 17. apríla 2019 o autorskom práve a právach súvisiacich s autorským právom na digitálnom jednotnom trhu a o zmene smerníc 96/9/ES a 2001/29/ES (ďalej aj ako „Smernica o jednotnom digitálnom trhu"). Táto smernica v čl. 2 ods. 2 definuje TDM ako „ akákoľvek automatizovanú analytickú techniku zameranú na analýzu textu a údajov v digitálnej forme s cieľom vytvárať informácie, okrem iného aj vzory, trendy a korelácie". Táto definícia vo svojom obsahovom rámci vymedzuje mnohé školiace aktivity potrebné na vývoj systému umelej inteligencie, najmä typu strojového učenia, vrátane generatívnych systémov umelej inteligencie. Články 3 a 4 Smernice o jednotnom digitálnom trhu následne obsahujú dve povinné výnimky súvisiace s TDM. Článok 3 poskytuje výnimku pre úkony TDM na účely vedeckého výskumu – pokrývajúceho prírodné aj humanitné vedy – výskumnými organizáciami a inštitúciami kultúrneho dedičstva, pokiaľ ide o diela/predmety, ku ktorým majú tieto organizácie zákonný prístup. Článok 4 ustanovuje výnimku pre rozmnoženiny a extrakcie legálne sprístupnených diel/predmetov ochrany na účely TDM. To má za cieľ pridať právnu istotu pre subjekty, ktoré nemusia spĺňať podmienky dočasnej a prechodnej výnimky kópie v článku 5 ods. 1 smernice 2001/29/ES Európskeho parlamentu a Rady z 22. mája 2001 o zosúladení niektorých aspektov autorských práv a s nimi súvisiacich práv v informačnej spoločnosti (ďalej ako „Smernice InfoSoc"). Táto výnimka podlieha výhrade držiteľov práv, a to aj prostredníctvom „strojovo čitateľných prostriedkov v prípade obsahu sprístupneného verejnosti online", napríklad použitím metadát a podmienok webovej stránky alebo služby. Takáto výhrada neovplyvní uplatnenie

[16] Recitál 109 Aktu o umelej inteligencii.

[17] LAYTNER, V.H.: Understanding The EU AI Act: a new era in AI Regulation In Europe, Zverejnené 10.12. 2023, Dostupné online na SSRN: https://ssrn.com/abstract=4659892 alebo http://dx.doi.org/10.2139/ssrn.4659892

[18] Smernica o jednotnom digitálnom trhu v slovenskom preklade v čl. 2 ods. 2 používa pojem „vyťažovanie textov a dát" čo považujem za doslovný preklad s anglického originálu text and data mining (TDM).

výnimky TDM na vedecké účely v článku 3 Smernice o jednotnom digitálnom trhu.[19] Novelli však vidí pri aplikácií článku 4 Smernice o jednotnom digitálnom trhu komplikácie, a to v prípadoch jej aplikácie na trénovanie systémov umelej inteligencie. In concreto článok 4 ods. 2 Smernice o jednotnom digitálnom trhu stanovuje, že rozmnoženiny a extrakcie získané podľa článku 4 odseku 1 tejto smernice sa môžu uchovávať tak dlho, ako je to potrebné na účely TDM. Problematický by bol výklad predmetného ustanovenia, ktorý by reštriktívne obmedzil použitie výnimky pre TDM len na trénovaciu fázu systémov umelej inteligencie, ktorá je oddelená od nasledovných fáz použitia samotnej umelej inteligencie, nakoľko v takom prípade by systémy umelej inteligencie museli vymazať obsah použitý počas tréningu bezprostredne po jeho použití. Dôsledkom takéhoto prístupu by bolo zamedzenie použitia vyššie uvedenej výnimky podľa článku 4 Smernice o jednotnom digitálnom trhu na validáciu alebo testovanie systémov umelej inteligencie. Novelli preto navrhuje širší výklad použitia výnimky pre TDM, tzn. je potrebné vykladať článok 4 Smernice o jednotnom digitálnom trhu tak, že predmetnú výnimku je možné použiť aj na validáciu a testovanie systémov umelej inteligencie.[20] Podporu jeho tvrdení je možné abstrahovať zo znenia recitálu 105 Aktu, kde je zdôraznené, že najmä veľké generatívne modely umelej inteligencie schopné generovať text, obrázky a iný obsah, predstavujú jedinečné inovačné príležitosti, ale aj výzvy pre umelcov, autorov a iných tvorcov a pre spôsob, akým sa ich tvorivý obsah vytvára, distribuuje, používa a spotrebúva. Na druhej strane samotný recitál 105 Aktu upozorňuje, že akékoľvek použitie obsahu chráneného autorským právom si vyžaduje povolenie príslušného nositeľa práv, pokiaľ sa neuplatňujú príslušné výnimky a obmedzenia autorského práva upravené v Smernici o jednotnom digitálnom trhu. Odôvodnenie recitálu 105 Aktu nám neposkytuje odpoveď, ako bude chránené autorské právo v prípadoch, keď nebude možné aplikovať výnimku TDM podľa Smernice o jednotnom digitálnom trhu. Respektíve, odpoveď je v súčasnosti jasne stanovená v čl. 53 od. 1 písm. c) Aktu, podľa ktorého poskytovatelia umelej inteligencie „zavedú politiku dodržiavania práva Únie v oblasti autorského práva a s ním súvisiacich práv, najmä s cieľom identifikovať a dodržiavať výslovné vyhradenie práv podľa článku 4 ods. 3 Smernice o jednotnom digitálnom trhu, a to aj prostredníctvom najmodernejších technológií". Predmetné ustanovenie neprináša nič zásadné z pohľadu ochrany autorov vo vzťahu k použitiu ich diel umelou inteligenciou.

[19] QUINTAIS, P.J.: Generative AI, Copyright and the AI Act. Kluwer Copyright. Zverejnené 9.5. 2023, Dostupné na: https://copyrightblog.kluweriplaw.com/2023/05/09/generative-ai-copyright-and-the-ai-act/

[20] NOVELLI, C., CASOLARI, F.,HACKER, P., SPEDICATO, G., FLORIDI, L.: Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity. Zverejnené 14.11. 2024, Dostupné online na SSRN: https://ssrn.com/abstract=4694565 alebo http://dx.doi.org/10.2139/ssrn.4694565

Ochrana autorských práv sa v celom Akte opiera len o existujúcu európsku úpravu, ktorá napriek značnej harmonizácii, nie je unifikovaná a je postavená na ochrane autorských práv prostredníctvom právnych predpisov jednotlivých členských štátov. Napriek tomu povinnosť poskytovateľov umelej inteligencie tak, ako je upravená v čl. 53 ods. 1 písm. d) Aktu prináša s cieľom zvýšiť transparentnosť údajov, ktoré sa používajú pri trénovaní modelov umelej inteligencie vrátane textu a údajov chránených autorským právom, povinnosť pre poskytovateľov takýchto modelov vypracovať a zverejniť dostatočne podrobné zhrnutie obsahu použitého na trénovanie modelu umelej inteligencie. Touto povinnosťou sa má zabezpečiť, aby sa stranám s oprávnenými záujmami, tzn. pôvodcom a majiteľom priemyselných práv, ako aj nositeľom autorských práv uľahčilo uplatňovanie a presadzovanie ich práv podľa práva EÚ, napríklad uvedením hlavných zbierok alebo súborov údajov, ktoré boli súčasťou trénovania modelu, ako sú veľké súkromné alebo verejné databázy alebo archívy údajov, a poskytnutím opisného vysvetlenia k iným použitým zdrojom údajov.[21]

Záver

Využívanie umelej inteligencie v spoločnosti prinieslo nové podnety pre vzdelávanie, vedu, ale aj podnikanie. Tieto podnety však následne implikujú nové právne výzvy, mimo iného aj v oblasti práva duševného vlastníctva. Tie výzvy si vyžadujú dôkladnú analýzu existujúcej právnej úpravy (bez ohľadu na to, či ide o vnútroštátnu, európsku alebo medzinárodnú) a jej aplikáciu na novovznikajúce právne vzťahy, ktorých súčasťou je umelá inteligencia. Súčasná právna úprava autorstva a pôvodcovstva predmetov priemyselných práv na Slovensku a v rámci Európskej únie sa opiera o antropocentrický prístup, v ktorom len fyzické osoby môžu byť považované za tvorcov predmetov duševného vlastníctva. Táto tradičná predstava je však čoraz viac konfrontovaná s technologickým pokrokom, najmä s výtvormi generatívnych modelov umelej inteligencie, ktoré dokážu vytvárať diela takmer nerozlíšiteľné od ľudskej tvorby.

Zásadným problémom naďalej zostáva otázka autorstva/pôvodcovstva a ochrany predmetov vytvorených umelou inteligenciou. Diskusia právnej vedy poukazuje na skutočnosť, že napriek tomu, že stanovená otázka sa vyvíja, no všeobecne akceptovaný konsenzus zatiaľ neexistuje. Umelá inteligencia sama o sebe zatiaľ nedisponuje právnou subjektivitou, čo znamená, že diela, ktoré vytvára, musia byť právne pripísané iným subjektom – či už ide o fyzické osoby, ktoré umelú inteligenciu trénovali, resp. organizácie, ktoré ju vyvinuli, alebo môže ísť aj o spoluautorstvo uvedených osôb a osôb zapojených do samotného procesu tvorby diela.

[21] Recitál 107 Aktu o umelej inteligencii

Súčasná európska legislatíva v oblasti autorského práva neprináša aplikačne jasný záver na vyššie uvádzané problémy. Prijatý Akt o umelej inteligencii rieši len otázky transparentnosti a zodpovednosti pri používaní umelej inteligencie, no priamočiaremu riešeniu otázok autorstva a pôvodcovstva predmetov vzniknutých prostredníctvom umelej inteligencie sa vyhýba. Preto je stále nejasné, do akej miery je tvorba obsahu umelej inteligencie skutočne originálna a ako sa dá chrániť pred zásahmi do autorských práv existujúcich diel.
Budúcnosť ochrany práv duševného vlastníctva v kontexte umelej inteligencie bude závisieť od toho, ako sa legislatíva vysporiada s balansovaním medzi ochranou týchto práv a podporou inovácií. Je však potrebné uviesť, že existuje skutočná výzva pre legislatívu - výzva medzi zabezpečením spravodlivej ochrany práv fyzických osôb a podpory rozvoja technológií, ktoré posúvajú hranice toho, čo považujeme za „tvorivú činnosť." Táto výzva si vyžaduje nový prístup k legislatíve, ktorý však Akt o umelej inteligencii ešte nepriniesol.

Zoznam použitej literatúry:

1. CALDWELL, M: What Is an "Author"?-Copyright Authorship of AI Art Through a Philosophical Lens. In. Houston Law Review, Vol. 61, Issue 2, 2023, Dostupné online na: https://houstonlawreview.org/article/92132-what-is-an-author-copyright-authorship-of-ai-art-through-a-philosophical-lens.
2. CIHANOVÁ, J.: AI regulation : the EU and China aprproach. In. Acta Facultatis Iuridicae Universitatis Comenianae, č. 1, rok 2024, s. 3-18.
3. GYURÁSZ, Z.: Duševné vlastníctvo vo svetle umelej inteligencie. In: ComenIUS [elektronický dokument] . – Bratislava (Slovensko) : Univerzita Komenského v Bratislave. Právnická fakulta UK. – ISSN (online) 2454-0846. – Roč. 5, č. 2 (2020), s. 6-14.
4. HUGENHOLTZ, P., B. a QUINTAIS. P.J.: 2021. 'Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output?' IIC - International Review of Intellectual Property and Competition Law 52 (9): 1190–1216. Dostupné online na: https://doi.org/10.1007/s40319-021-01115-0.
5. QUINTAIS, P.J.: Generative AI, Copyright and the AI Act. Kluwer Copyright, Zverejnené 9.5. 2023, Dostupné online na: https://copyrightblog.kluweriplaw.com/2023/05/09/generative-ai-copyright-and-the-ai-act/
6. MOERLAND, A.: Artificial Intelligence and Intellectual Property Law. Zverejnené 20. 5. 2022, Dostupné online na SSRN: https://ssrn.com/abstract=4203360 alebo http://dx.doi.org/10.2139/ssrn.4203360

7. NELSON, D.: Čo je to Generative Adversarial Network (GAN)? Zverejnené 05.10.2020, Dostupné online na: https://www.unite.ai/sk/what-is-a-generative-adversarial-network-gan/.
8. NOVELLI, C., CASOLARI, F.,HACKER, P., SPEDICATO, G., FLORIDI, L.: Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity, Zverejnené 14.1.2024. Dostupné online na SSRN: https://ssrn.com/abstract=4694565 alebo http://dx.doi.org/10.2139/ssrn.4694565
9. PLESSIS, L.D.: What Is AI Art? A Guide on How It Works and How to Create It., Domestika, Zverejnené 14. 10. 2022, https://www.domestika.org/en/blog/10352-what-is-ai-art-a-guide-on -ako-to-funguje-a-ako-to-vytvoriť [https://perma.cc/84YB-YDKZ]
10. SLACK, G.: What DALL-E Reveals About Human Creativity. (17.1.2023) Standford University, Human -Centered Artificial Intelligence, Arts and Humanities, Neuro and Cognitive Science, Dostupné online na: https://hai.stanford.edu/news/what-dall-e-reveals-about-human-creativity
11. VISHNU. S.: Rise of Artificial Intelligence and Copyright Challenges (July 31, 2023). Osmania University Journal of IPR [OUJIPR], 1(1), pp. 86-98, Zverejnené online na SSRN: https://ssrn.com/abstract=4675455
12. XU, W., WANG, X., GUO, Q., SONG, X., ZHAO, R., ZHAO, G., ... & YANG, Y. (2023). Decomposition is all you need: single-objective to multi-objective optimization towards artificial general intelligence. Mathematics, 11(20), 4390. Dostupné online na https://doi.org/10.3390/math11204390

Kontaktné údaje

doc. Mgr. Martin Daňko, PhD.
martin.danko@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta, Ústav práva informačných technológií a práva duševného vlastníctva.

BOJ PROTI ONLINE DEZINFORMÁCIÁM: ÚLOHA VŠEOBECNÉHO NARIADENIA O OCHRANE ÚDAJOV V EURÓPSKEJ ÚNII[1]

COUNTERING ONLINE DISINFORMATION: THE ROLE OF THE EUROPEAN UNION GENERAL DATA PROTECTION REGULATION

Matúš Mesarčík[2]

Abstrakt: Šírenie hybridných online hrozieb vrátane dezinformácií predstavuje významnú výzvu pre demokratické procesy a spoločenskú dôveru, čo si vyžaduje pevné regulačné rámce na ochranu údajov a kybernetickú bezpečnosť. V tomto príspevku sa skúma všeobecné nariadenie EÚ o ochrane údajov (GDPR) ako kľúčový nástroj v boji proti dezinformáciám v digitálnom prostredí. V nariadení GDPR, ktoré bolo prijaté v roku 2018, sa stanovujú prísne požiadavky na zhromažďovanie a spracúvanie osobných údajov, čím sa obmedzuje schopnosť škodlivých aktérov mikrocieliť na jednotlivcov klamlivým obsahom. V tejto štúdii sa skúma vzájomný vzťah medzi ochranou údajov a zmierňovaním dezinformácií, pričom sa zdôrazňuje, ako môžu ustanovenia nariadenia GDPR zvýšiť transparentnosť a zodpovednosť v online priestore. Prostredníctvom komplexnej analýzy týchto regulačných opatrení príspevok dokazuje, že nariadenie GDPR nielen chráni súkromie jednotlivcov, ale slúži aj ako dôležitá súčasť širšej stratégie na zachovanie demokratickej integrity a dôvery verejnosti tvárou v tvár rastúcim dezinformačným hrozbám.

Kľúčové slová: GDPR, ochrana osobných údajov, dezinformácie

Abstract: The proliferation of online hybrid threats including disinformation poses significant challenges to democratic processes and societal trust, necessitating robust regulatory frameworks on data protection and cyber-security. This paper examines the EU General Data Protection Regulation (GDPR) as a pivotal tool in combating disinformation in the digital landscape. The GDPR, enacted in 2018, establishes stringent requirements for the collection and processing of personal data, thereby limiting the ability of malicious actors to micro-target individuals with deceptive content. This study

[1] Tento článok bol vypracovaný s podporou grantu udeleného Agentúry na podporu výskumu a vývoja č. APVV-23-0137 Právne a technické aspekty situačného povedomia o kybernetickej bezpečnosti .
[2] Univerzita Komenského v Bratislave, Právnická fakulta.

explores the interplay between data protection and disinformation mitigation, highlighting how GDPR provisions can enhance transparency and accountability in the online space. Through a comprehensive analysis of these regulatory measures, the paper argues that the GDPR not only safeguards individual privacy but also serves as a critical component in the broader strategy to uphold democratic integrity and public trust in the face of rising disinformation threats.

Key words: GDPR, data protection, disinformation

Úvod

V súčasnej dobe čelí spoločnosť mnohým výzvam spojeným s rozšírením online dezinformácií, ktoré ohrozujú demokratické procesy a narúšajú dôveru verejnosti. Právo disponuje pomerne silným arzenálom nástrojom, prostredníctvom ktorých je možné s týmto negatívnym fenoménom bojovať a šírenie dezinformácií mierniť.
Tento článok sa zameriava na úlohu Všeobecného nariadenia o ochrane údajov (GDPR)[3] v boji proti týmto dezinformáciám. GDPR, prijaté v roku 2018, predstavuje zásadný nástroj na ochranu osobných údajov a zabezpečenie transparentnosti a zodpovednosti v digitálnom prostredí. Cieľom tohto článku je preskúmať, ako môže GDPR prispieť k zmierneniu dezinformácií a zabezpečiť ochranu jednotlivcov pred manipuláciou zo strany škodlivých aktérov. Analýza sa opiera o normatívny právny výskum. Prvým krokom je preskúmanie textu GDPR a jeho aplikácie na spracovanie osobných údajov v kontexte online dezinformácií. Následne sa zameriame na konkrétne mechanizmy, ktoré GDPR zavádza nielen na ochranu jednotlivcov a ich osobných údajov, ale aj v širšom – systémovejšom meradle. V prvej časti vymedzíme pôsobnosť právneho predpisu v kontexte dezinformácií. Následne analyzujeme systémové a individuálne nástroje pre boj s dezinformáciami, ktoré GDPR ponúka. Závery sú zhrnuté v poslednej časti.

Pôsobnosť GDPR a dezinformácie

Predtým, než sa pustíme do analýzy a diskusia požiadaviek GDPR relevantných pre boj s dezinformáciami online, považujeme za nevyhnutné načrtnúť základné postuláty pôsobnosti predmetného právneho predpisu v kontexte šírenia dezinformácií. Vecná pôsobnosť GDPR je upravená v článku 2 ods. 1 GDPR. Dané ustanovenie upravuje pozitívnu vecnú pôsobnosť GDPR. V zmysle dikcie predmetného článku sa GDPR aplikuje na spracúvanie osobných údajov, ktoré je

[3] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

vykonávané (i) automatizovanými prostriedkami, (ii) čiastočne automatizovanými prostriedkami alebo (iii) manuálne, ak osobné údaje tvoria súčasť informačného systému.

Samotné spracúvanie osobných údajov je definované v článku 4 bode 2 GDPR, a to demonštratívnymi výpočtom spracovateľských operácií, ktoré možno subsumovať pod definíciu spracúvania osobných údajov. V zmysle daného článku sa pod spracúvaním osobných údajov rozumie: „operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami." Automatizované šírenie dezinformácií, ktoré obsahujú osobné údaje bude spadať pod dikciu predmetného ustanovenia. Zároveň je potrebné poznamenať, že aj činnosť odporúčacích systémov, prostredníctvom ktorých sa dezinformácie šíria je založené na automatizovanom spracúvaní osobných údajov užívateľov a určitej miere profilovania. Ústredným pojmom GDPR je však definícia osobného údaju. Osobným údajom *„je akékoľvek informácia týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby."* [4] Identifikovateľná fyzická osoba je taká osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä prostredníctvom odkazu na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby. Pre otázku dezinformácií je vysoko relevantný faktor, že osobný údaj predstavuje „akúkoľvek informáciu." Z pohľadu povahy resp. kvality osobného údaju môže ísť o akékoľvek tvrdenia o konkrétnej osobe na akomkoľvek nosiči. Môže ísť o informácie objektívne alebo subjektívne. Z nášho pohľadu je kľúčové, že na to, aby informácie boli osobnými údajmi, nie je potrebné, aby boli pravdivé alebo preukázané. Legislatíva na ochranu osobných údajov takúto situáciu predpokladá a ustanovuje právo dotknutej osoby na prístup k týmto informáciám a na ich spochybnenie prostredníctvom vhodných opravných prostriedkov.[5]

Dezinformácie môžu obsahovať aj osobné údaje. Ide spravidla o situácie, ak sa šíria konkrétne nepravdivé informácie o konkrétnom jednotlivcovi. Praktickým príkladom

[4] GDPR, článok 4 bod 1.

[5] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 4/2007 on the concept of personal data*. Adopted on 20th June, 01248/07/EN.WP 136, s. 6.

je šírenie dezinformácií o zdravotníckych pracovníkoch počas pandémie COVID-19.[6] Zároveň, odporúčacie systémy na sociálnych sieťach fungujú na kreovaní profilov na základe osobných údajov. Aké nástroje a inštitúty poskytuje GDPR či už z hľadiska systémových nástrojov alebo individuálnych práv? Za systémové nástroje budeme považovať také, ktoré predstavujú horizontálne požiadavky na prevádzkovateľov prípadne sprostredkovateľov. Podľa nášho názoru z týchto systémových nástrojov je nutné diskutovať požiadavky na automatizované individuálne rozhodovanie, vykonanie posúdenia vplyvu na ochranu údajov, inštitút špecificky navrhnutej a štandardnej ochrany osobných údajov. Za individuálne možnosti nápravy pri šírení dezinformácií, ktoré obsahujú osobné údaje považujeme využitie niektorých práv dotknutej osoby a to konkrétne právo na opravu, právo na vymazanie (zabudnutie) a ďalšie práva týkajúce sa podania sťažnosti na dozorný orgán a obrany na súde.

Systémové nástroje

Automatizované individuálne rozhodovanie je pojem, s ktorým operuje GDPR na viacerých miestach. Pred tým, než sa pustíme do analýzy požiadaviek pri jeho vykonávaní, považujeme za nevyhnutné predmetný pojem charakterizovať. Za automatizované spracúvanie možno v zmysle GDPR považovať spracúvanie osobných údajov bez ľudského zásahu výlučne prostredníctvom informačných technológií.[7]

Predmetom analýzy tejto časti je článok 22 všeobecného nariadenia o ochrane údajov, ktorý upravuje automatizované individuálne rozhodovanie (ďalej aj ako „AIR"). V zmysle článku 22 ods. 1 GDPR: *„Dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú.* " Pri automatizovanom individuálnom rozhodovaní je potrebné odlišovať všeobecne rozhodnutia na základe profilovania a rozhodnutia urobené výlučne automatizovaným spracúvaním s právnymi účinkami na dotknutú osobu. O rozhodnutie na základe profilovania pôjde napríklad v prípade, ak údaje dotknutej osobe spracuje algoritmus, ktorý na základe týchto dát vydá odporúčanie ohľadom rozhodnutia; predmetné rozhodnutia už ale urobí ľudská bytosť. Rozhodnutie urobené výlučne automatizovaným spracúvaním osobných údajov vrátane profilovania, ktoré má právne účinky na dotknutú osobu, ktoré sa dotknutej

[6] ROZHLAS A TELEVÍZIA SLOVENSKA. *Verdikt v spore lekára Sabaku s hnutím Republika by mohol padnúť o necelý mesiac*. Dostupné na: https://spravy.rtvs.sk/2023/06/sudny-spor-lekara-p-sabaku-s-hnutim-republika-vrcholi-verdikt-by-mohol-padnut-o-necely-mesiac/.

[7] KUNER, CH. – BYGRAVE, L. – DOCKSEY, CH. *The EU General Data Protection Regulation (GDPR). A commentary*. Oxford: Oxford University Press, 2020, s. 121.

osoby týkajú alebo dotknutú osobu podobne významne ovplyvňujú ilustruje situácia, ak by občanovi došlo rozhodnutie o priamo od algoritmu, ktorý o ňom spracúval dáta a sám rozhodol o výsledku jeho žiadosti.[8] Článok 22 GDPR sa aplikuje iba na poslednú z ilustrovaných situácií. Usmernenie Výboru na ochranu osobných údajov,[9] zároveň potvrdzuje, že rutinná ľudská intervencia môže stále znamenať, že rozhodnutie je urobené výlučne automatizovanými prostriedkami.[10] Dôležitou časťou definície AIR v zmysle GPDR je, že rozhodnutia musí mať právny alebo podobný efekt na dotknutú osobu. Ide o pomerne komplikovanú požiadavku, ktorú je v aplikačnej praxi náročné naplniť. Právny účinok vyžaduje, aby rozhodnutie, ktoré je založené výlučne na automatizovanom spracovaní, ovplyvnilo práva, ako je sloboda združovať sa s inými, hlasovať vo voľbách alebo prijímať právne kroky. Právnym účinkom môže byť aj niečo, čo ovplyvňuje právne postavenie osoby alebo jej práva podľa zmluvy.[11] Zaujímavejším pojmom je však práve „podobne významný vplyv" ako právny efekt. Aby spracovanie údajov niekoho významne ovplyvnilo, musia byť účinky spracovania dostatočne veľké alebo dôležité. Ako príklady Výbor na ochranu osobných údajov uvádza zásadnú zmenu okolností, správania alebo volieb dotknutej osoby s dlhotrvajúcim vplyvom, v extrémnych prípadoch vedúcich k diskriminácií.[12] K totožnému výkladu dospel aj generálny advokát Súdneho dvora EÚ vo svojom názore v prípade *OQ proti Land Hessen,* ktorý je prvým prejedávaným prípadom týkajúcim sa výkladu článku 22 GDPR.[13]

Osobitne usmernenie Výboru na ochranu údajov analyzuje zobrazovanie reklamy (v širšom kontexte obsahu) užívateľom, ktoré je taktiež založené na automatickej analýze osobných údajov. Práve tento kontext je veľmi dôležitý pre šírenie dezinformácií online. Výbor uvádza, že zobrazovanie reklamy štandardne nebude spôsobovať právny alebo podobne závažný vplyv na dotknutú osobu.[14] Avšak nie je vylúčené, že pri zohľadnení určitých skutočností takýto vplyv môže zobrazovanie online reklamy mať. Pre naše účely je vhodné upriamiť pozornosť na dva faktory a to konkrétne invazívnosť procesu profilovania vrátane sledovania jednotlivcov

[8] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* Adopted on 3 October 2017. As last Revised and Adopted on 6 February, s. 9.

[9] V zmysle GDPR nahradená Výborom na ochranu údajov, pričom jeho/jej stanoviská sú relevantné pre adresátov noriem a taktiež orgány aplikujúce právo.

[10] Tamže, s. 21.

[11] ARTICLE 29 DATA PROTECTION WORKING PARTY: *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* Adopted on 3 October 2017. As last Revised and Adopted on 6 February, s. 21.

[12] Tamže.

[13] *Stanovisko Generálneho Advokáta Priit Pikamäe predneseného dňa 16.3.2023 vo veci C-634/21 OQ proti Land Hessen za účasti: SCHUFA Holding AG*, body 34 – 35.

[14] Tamže, s. 22.

v rôznych webových stránkach, zariadeniach a službách a využitie znalostí o zraniteľnosti dotknutých osôb.[15] Zobrazovanie dezinformácií môže využívať zraniteľnosť dotknutých osôb, či už z pohľadu geografickej lokalizácie alebo veku. V určitých prípadoch by sa článok 22 GDPR mohol podľa nášho názoru vzťahovať aj na zobrazovanie obsahu na základe zozbieraných osobných údajov zo strany napríklad sociálnych médií.

Po výklade pojmu AIR prejdeme ku konkrétnym požiadavkám naň kladenými. Zahraničná doktrína akcentuje dva názory na výklad daného inštitútu – ide o všeobecný zákaz alebo právo namietať? Prvá skupina autorov (a Výbor na ochranu údajov)[16] tvrdí, že článok 22 GDPR reprezentuje všeobecný zákaz vykonávania individuálnych rozhodnutí automatizovaným spôsobom a takýto proces je možné vykonávať iba na základe výnimiek uvedených v článku 22 ods. 2 GDPR. Tieto výnimky predstavujú (i) plnenie zmluvy s dotknutou osobou; (ii) legislatívne povolenie v národnom právnom poriadku alebo poriadku EÚ so zakotvením vhodných opatrení zaručujúcich ochranu práv a slobôd a oprávnených záujmov dotknutej osoby alebo (iii) ak dotknutá osoba vyjadrila výslovný súhlas s takýmto spracúvaním. Literatúra v prospech danej argumentácie predovšetkým argumentuje koherentnosťou právneho rámca na ochranu osobných údajov v prospech dotknutej osoby a existenciou záruk a derogácií ustanovených v článku 22 GDPR.[17] K takémuto výkladu sa prihlásil aj generálny advokát Súdneho dvora EÚ vo svojom názore v prípade *OQ proti Land Hessen*.[18] Budúcnosť ukáže, či totožný postoj zaujme aj samotná súdna inštancia.

Druha skupina autorov argumentuje v prospech výkladu, že článok 22 GDPR je koncipovaný ako právo dotknutej osoby namietať voči daným rozhodnutiam. Svoje tvrdenia opierajú o juxtapozíciu predmetného inštitútu v kapitole právneho predpisu týkajúcich sa práv dotknutých osôb a absencie úmyslu zákonodarcu koncipovať článok 22 ako všeobecný zákaz vzhľadom na historický vývoj diskutovaného inštitútu. Ďalšími argumentmi v prospech výkladu článku 22 GDPR ako práva namietať sú ustanovenia týkajúce sa informačnej povinnosti, ktoré v sebe obsahujú aj povinnosť informovať o AIR či povinnosť vykonať posúdenie vplyvu na ochranu údajov podľa článku 35 GDPR v prípade systematického a extenzívneho

[15] Tamže.

[16] ARTICLE 29 DATA PROTECTION WORKING PARTY: *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* Adopted on 3 October 2017. As last Revised and Adopted on 6 February, s. 19.

[17] BYGRAVE, L. Automated individual decision-making, including profiling. In KUNER, CH. – BYGRAVE, L. – DOCKSEY, CH.: *The EU General Data Protection Regulation (GDPR). A commentary.* Oxford: Oxford University Press, 2020, s. 530 - 531.

[18] *Stanovisko Generálneho Advokáta Priit Pikamäe predneseného dňa 16.3.2023 vo veci C-634/21 OQ proti Land Hessen za účasti: SCHUFA Holding AG*, body 31 – 32.

monitorovania osobných aspektov dotknutých osôb vrátane AIR. V prípade všeobecného zákazu by predmetná povinnosť nemala zmysel, nakoľko jej poslaním je posúdiť spracúvanie osobných údajov pred jeho začatím vrátane rizík.[19] Výnimky uvedené v článku 22 ods. 2 GDPR by v takomto prípade predstavovali výnimky z práva namietať a reprezentovali by situácie, v ktorých dotknutá osoba nemôže takémuto spracúvaniu osobných údajov namietať.[20]
Prikláňame sa k názoru, že článok 22 GDPR je koncipovaný ako právo dotknutej osoby nebyť predmetom AIR. Zároveň je však potrebné poznamenať, že predmetný inštitút má komplikované vyjadrenie a zvádza k viacerým výkladom. V prospech výkladu ako práva jednoznačne hovorí jeho pozícia v právnom predpise a nedostatok úmyslu zákonodarcu koncipovať daný inštitút ako všeobecný zákaz. Navyše, samotné znenie GDPR na viacerých miestach pracuje s AIR ako „bežnou" spracovateľskou operáciou, ktorá podlieha viacerým špecifickým povinnostiam. V prípade všeobecného zákazu by tieto povinnosti stratili na účinku a boli by nadbytočné. Jediný všeobecný zákaz v súvislosti s AIR sa nachádza v ustanovení článku 22 ods. 4 GDPR, podľa ktorého je zakázané vykonávať AIR na základe citlivých osobných údajov. Prirodzene, aj z tohto zákazu existujú dve výnimky a to v prípade výslovného súhlasu dotknutej osoby a nevyhnutného verejného záujmu na základe právneho poriadku EÚ alebo národného právneho poriadku. Spoločnou podmienkou využitia vyššie uvedených výnimiek je zavedenie vhodných opatrení na zaručenie práv a slobôd a oprávnených záujmov dotknutej osoby zo strany prevádzkovateľa. Práve tu GDPR uvádza opatrenia ako právo na ľudský zásah zo strany prevádzkovateľa, právo vyjadriť svoje stanovisko a právo napadnúť rozhodnutie. Ide tak o špecifický koncept práv voči rozhodnutiam stroja, ktorý sa častokrát používa ako príklad pre budúcu reguláciu.

Posúdenie vplyvu na ochranu údajov (*Data protection impact assessment – DPIA*) je novým inštitútom pri spracúvaní osobných údajov, ktorý substituuje viaceré notifikačné povinnosti. DPIA je pevnou súčasťou zásady zodpovednosti (*accountability*), ktorá reflektuje preventívne povinnosti pre prevádzkovateľov predchádzať a zmierňovať neželané riziká pri spracúvaní osobných údajov. Podstatou daného inštitútu je analýza právnych rizík pri spracúvaní osobných údajov a vypracovanie dokumentu, ktorý danú povinnosť dokumentuje. Toto posúdenie sa musí vykonať pred[21] samotným začatím spracúvania osobných údajov. Tento inštitút

[19] Tamže, s. 531 – 532.
[20] Aj v prípade nemožnosti namietania však má prevádzkovateľ v zmysle článku 22 ods. 3 GDPR vykonať vhodné opatrenia na ochranu práv a slobôd a oprávnených záujmov dotknutej osoby, a to aspoň práva na ľudský zásah zo strany prevádzkovateľa, práva vyjadriť svoje stanovisko a práva napadnúť rozhodnutie.
[21] Pozri článok 35 ods. 1 GDPR.

je obzvlášť dôležitý v kontexte využívania nových technológií pri spracúvaní osobných údajov. Výbor vydal usmernenie k posúdeniu vplyvu na ochranu údajov, ktoré daný proces vysvetľuje a precizuje.[22]

Ak vezmeme do úvahy technické fungovanie odporúčacích systémov na sociálnych médiách, prostredníctvom ktorých sa dezinformácie efektívne šíria, musíme konštatovať že, že pre takúto činnosť ja naplnených viacero kritérií. Určite pôjde o vyhodnocovanie určitých aspektov týkajúcich sa dotknutej osoby na základe ich správania na sociálnych médiách. Zároveň nechávame otvorené vzhľadom na diskusiu vyššie, či pôjde o AIR s právnym alebo podobným účinkom. Každopádne, činnosť odporúčacích systémov je založená na spracúvaná veľkého množstva údajov, v ktorých môžu figurovať aj citlivé osobné údaje (ako údaje o zdravotnom stave či národnosti) a štandardne je tvorené kombináciou údajov z rôznych zdrojov na základe webovej aktivity konkrétneho užívateľa. Prevádzkovatelia takýchto systémov podliehajú povinnosti vykonať posúdenie vplyvu.

Z pohľadu šírenia dezinformácií na základe spracúvaných osobných údajov kľúčovú časť DPIA predstavuje posúdenie rizík pre práva a slobody dotknutých osôb. Posúdenie rizika pre práva a slobody dotknutých osôb by malo predstavovať právne cvičenie, ktoré spočíva v kreovaní modelových situácií, ktoré predstavujú riziko pre práva a slobody dotknutých osôb[23] (napr. únik údajov alebo kompromitovanie údajov) a následnú analýzu ohrozenia špecifických práv a slobôd dotknutých osôb.[24] Ak prevádzkovateľ zobrazuje obsah na základe zozbieraných osobných údajov užívateľov a v rámci neho sa šíria dezinformácie, malo by to byť riziko, ktoré by prevádzkovateľ mal identifikovať, zohľadniť a zmierniť v procese DPIA.

GDPR v článku 25 ustanovuje v európskej právnej kultúre pomerne nový inštitút špecificky navrhnutej a štandardnej ochrany osobných údajov. Predmetný článok však vychádza z filozofie špecificky navrhnutej ochrany súkromia, ktorý má svoje

---

[22] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation, 2016/679*.

[23] Napr. Úrad na ochranu osobných údajov SR vydal zoznam 156 práv a slobôd v zmysle právnej úpravy v Charte. Dostupné na: https://dataprotection.gov.sk/uoou/sites/default/files/otazka_uoou.pdf, s. 3.

[24] Vyhláška v danom prípade vyžaduje zohľadniť *„najmä riziko súvisiace s náhodným alebo nezákonným poškodením, zničením, stratou, zmenou, neoprávneným prístupom a poskytnutím alebo zverejnením osobných údajov, ako aj s akýmkoľvek iným neprípustným spôsobom spracúvania, pričom identifikuje*
a) hrozby a pravdepodobnosť ich výskytu,
b) zraniteľnosti zneužiteľné hrozbami,
c) riziká a pravdepodobnosť ich výskytu a závažnosť,
d) a zhodnotí mieru dopadu na práva fyzickej osoby v dôsledku straty integrity, dôvernosti a dostupnosti údajov,
e) vysoké riziko pre práva fyzickej osoby, ak neprijme opatrenia na zmiernenie rizika." (§ 5 ods. 2 Vyhlášky).

dlhoročné uplatnenie a miesto v anglo-americkej právnej tradícii. Možno teda konštatovať, že článok 25 GDPR vychádza a nadväzuje na koncepciu špecificky navrhnutej ochrany súkromia (*Privacy by Design*). Tento koncept rozvinula bývala kanadská dozorná úradníčka pre ochranu údajov Ann Cavoukian, ktorá určila sedem nosných zásad[25], na ktorých musí stáť každé poňatie vyššie diskutovaného inštitútu. Z filozofie *Privacy by Design* vychádza aj článok 25 GDPR. Diskutovaný článok je tvorený tromi veľmi komplikovanými vetnými štruktúrami, ktoré je potrebné analyzovať podrobnejšie.

Článok 25 ods. 1 GDPR reflektuje požiadavky špecificky navrhnutej ochrany osobných údajov: *„So zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou, ktoré spracúvanie predstavuje pre práva a slobody fyzických osôb, prevádzkovateľ v čase určenia prostriedkov spracúvania aj v čase samotného spracúvania prijme primerané technické a organizačné opatrenia, ako je napríklad pseudonymizácia, ktoré sú určené na účinné zavedenie zásad ochrany údajov, ako je minimalizácia údajov, a začlení do spracúvania nevyhnutné záruky s cieľom splniť požiadavky tohto nariadenia a chrániť práva dotknutých osôb.“*[26]

Diskutovaný inštitút vysvetľuje aj usmernenie Výboru.[27] Povinnosť zohľadniť tieto aspekty dopadá na všetkých prevádzkovateľov, vrátane prevádzkovateľov odporúčacích systémov. Podľa nášho názoru ide o jeden z kľúčových nástrojov pri zmierňovaní šírenia dezinformácií na základe spracúvaných osobných údajov, ktoré GDPR ponúka, nakoľko prevádzkovateľ by mal potenciálne riziká odhaliť už vo fáze dizajnu spracovateľských operácií. Tomuto konštatovaniu nasvedčuje aj výklad článku 25 optikou zásady spravodlivosti (fairness) v usmernení Výboru. Výbor akcentuje využívanie spravodlivých algoritmov. Prevádzkovateľ by mal pravidelne vyhodnocovať, či algoritmy fungujú v súlade s vytýčenými účelmi a modifikovať ich tak, aby sa zmiernili odhalené predsudky a zabezpečila sa spravodlivosť pri spracovaní.[28] Šírenie dezinformácií alebo nenávistného obsahu na základe nesprávne zvolených parametrov odporúčacích systémov nepredstavuje spravodlivé spracúvanie osobných údajov a nastavenie algoritmov. Práve článok 25 by už vo fáze dizajnu a nastavenia mal napomôcť prevádzkovateľov identifikovať toto riziko.

---

[25] CAVOUKIAN, A*: Privacy by Design – The Seven Foundational Principles*. Dostupné na https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

[26] GDPR, článok 25 ods. 1.

[27] EUROEPAN DATA PROTECTION BOARD: *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.* Version 2.0 Adopted on 20 October 2020. Dostupné na: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

[28] Tamže, s. 18.

Individuálne nástroje

Okrem systémovejších nástrojov obsahuje GDPR aj individuálne práva dotknutej osoby, ktoré si môže akákoľvek dotknutá osoba u prevádzkovateľa uplatniť. V kontexte šírenia dezinformácií o konkrétnej osobe považujeme za nevyhnutné diskutovať právo na opravu, právo na vymazanie (zabudnutie), právo namietať a ďalšie práva týkajúce sa podania sťažnosti na dozorný orgán a obrany na súde. Dotknuté osoby majú aj **právo na opravu**, v zmysle ktorého má dotknutá osoba *„právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účely spracúvania má dotknutá osoba právo na doplnenie neúplných osobných údajov, a to aj prostredníctvom poskytnutia doplnkového vyhlásenia.*"[29] Toto právo obsahuje v skutočnosti dva dielčie práva a to právo na opravu nesprávnych osobných údajov a právo na doplnenie neúplných osobných údajov. Ako jedno z mála práv v zmysle GDPR, neobsahuje konkrétnejšie podmienky na jeho uplatnenie a ani výnimky, kedy sa právo na opravu neuplatňuje. Pri šírení dezinformácií o svojej osobe by sa tak podľa nášho názoru vzťahovalo diskutované právo, nakoľko postačuje, že dotknutá osoba žiada o opravu údajov, ktoré sa *jej týkajú*. Potenciálnym problémom môže byť, že na opravu má dotknutá osoba nárok iba v prípade, ak sú osobné údaje nesprávne. GDPR neustanovuje žiadny test správnosti údajov a bude iba na dotknutej osobe, aby preukázala ich nesprávnosť. Tento aspekt môže pri šírení sofistikovanejších foriem dezinformácií predstavovať výzvu a problém, nakoľko v konečnom dôsledku to bude rozhodnutie prevádzkovateľa, či opravu vykoná alebo nie.

Článok 17 GDPR upravuje **právo na vymazanie**. V zmysle daného ustanovenia má dotknutá osoba právo dosiahnuť u prevádzkovateľa bez zbytočného odkladu vymazanie osobných údajov, ktoré sa jej týkajú, pričom prevádzkovateľ je povinný bez zbytočného odkladu vymazať osobné údaje, ak je splnený niektorý z dôvodov ustanovených v článku 17 ods. 1 GDPR. Prevádzkovateľ tak v prvom rade skúma, či existuje legitímny dôvod na vymazanie. Tieto dôvody sú nasledujúce: nepotrebnosť osobných údajov na účel, na ktorý sa získavali; odvolanie súhlasu a neexistencia iného právneho základu; ak prevádzkovateľ nevie preukázať prevahu oprávneného záujmu a namieta spracúvanie osobných údajov; nezákonnosť spracúvania osobných údajov; splnenie povinnosti kladenej právnym poriadkom SR alebo EÚ a ak sa osobné údaje získavali v súvislosti s ponukou služieb informačnej spoločnosti dieťaťu na základe jeho súhlasu podľa článku 8 ods. 1 GDPR.[30] Z vyššie uvedených dôvodov pri šírení dezinformácií a uplatnení daného práva je použiteľným dôvodom nezákonnosť spracúvania. Nezákonnosť spracúvanie je však potrebné pri uplatnení práva na vymazanie odôvodniť rozhodnutím správneho alebo súdneho orgánu. Pre dotknutú

[29] GDPR. článok 16.

[30] GDPR, článok 17 ods. 1.

osobu tak môže byť častokrát neskoro. Zároveň upozorňujeme, že právo na vymazanie obsahuje aj niekoľko výnimiek, kedy prevádzkovateľ nemusí právu na vymazanie vyhovieť. Jednou z nich je, ak prevádzkovateľ osobných údajov tieto údaje dotknutej osoby potrebuje na uplatnenie práva na slobodu prejavu a na informácie. Možno predpokladať, že právo na vymazanie a právo na slobodu prejavu sa pomerne často dostanú do konfliktu, pričom určitý návod na riešenie a vyváženie daných práv v konflikte predstavuje rozhodnutie SDEÚ vo veci *Google v. CNIL*.[31] Predmetná výnimka môže predstavovať výraznú prekážku pre úspešné uplatnenie práva na vymazanie o konkrétnej osobe v kontexte šírenia dezinformácií.

V prípade, ak prevádzkovateľ zverejnil osobné údaje a dotknutá osoba si úspešne uplatnila právo na vymazanie, so zreteľom na dostupnú technológiu a náklady na vykonanie opatrení je povinný podniknúť primerané opatrenia vrátane technických opatrení, aby informoval prevádzkovateľov, ktorí vykonávajú spracúvanie osobných údajov, že dotknutá osoba ich žiada, aby vymazali všetky odkazy na tieto osobné údaje, ich kópiu alebo repliky.[32]

Dotknutá osoba má taktiež **právo namietať** podľa článku 21 GDPR. Toto právo má v prípade, ak sú osobné údaje spracúvané na právnom základe verejného záujmu alebo oprávneného záujmu a v taktom prípade prevádzkovateľ musí vedieť preukázať prevahu takéhoto záujmu nad právami, slobodami a záujmami dotknutej osoby. Ak toto bremeno neunesie, spracúvanie osobných údajov musí prestať. Ak by spracúvanie osobných údajov napríklad v rámci odporúčacích systémov prebiehali na právnom základe verejného záujmu alebo oprávneného záujmu, dotknutá osoba môže na svoju obranu pri šírení dezinformácií o nej využiť aj právo namietať.

Okrem vyššie uvedených práv majú dotknuté osoby možnosť obrátiť sa na dozorný orgán alebo súd. Na dozorný orgán zriadený podľa GDPR (v slovenských podmienkach Úrad na ochranu osobných údajov SR) sa dotknuté osoby môžu obrátiť či už pre porušenie hmotnoprávnych ustanovení GDPR alebo pri neúspešnom uplatnení práv dotknutej osoby. Sťažnosť dozornému orgánu tak nie je limitovaná iba na využitie konkrétnych práv dotknutej osoby, ale dotknutá osoba prípadne osoby, ktoré tvrdia, že je priamo dotknutá na svojich právach[33] môžu podať podnet na preskúmanie súladu prevádzkovateľa s požiadavkami na automatizované individuálne rozhodovanie, špecificky navrhnutú ochranu osobných údajov či posúdenie vplyvu. Môže ísť teda o prínosný nástroj, ktorým disponuje dotknutá osoba pri šírení dezinformácií u konkrétneho prevádzkovateľa. Dozorné orgány môžu prevádzkovateľov kontrolovať a konať voči ním aj z úradnej povinnosti.

---

[31] Rozhodnutie SDEÚ z 24. septembra 2019 *GC a i. v. Commission nationale de l'informatique et des libertés (CNIL)*. Vec č. C-136/17.

[32] GDPR, článok 17 ods. 2.

[33] Zákon o ochrane osobných údajov, § 100 ods. 1.

Na inštitút podania sťažnosti nadväzuje možnosť podať súdny prostriedok nápravy voči týmto rozhodnutiam[34] či konkrétnemu prevádzkovateľovi alebo sprostredkovateľovi.[35]

Záver

Výsledky analýzy ukazujú, že GDPR nie je len nástrojom na ochranu súkromia jednotlivcov, ale aj kľúčovým prvkom v širšej stratégii boja proti online dezinformáciám. Ustanovenia GDPR prispievajú k zvýšeniu transparentnosti a zodpovednosti v online priestore, čím obmedzujú schopnosť škodlivých aktérov mikrocieliť jednotlivcov s klamlivým obsahom. Zavedením prísnych požiadaviek na spracovanie osobných údajov a poskytnutím práv dotknutým osobám sa GDPR stáva dôležitým nástrojom na ochranu demokratickej integrity a dôvery verejnosti.

Zoznam použitej literatúry

1. Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).
2. ROZHLAS A TELEVÍZIA SLOVENSKA. *Verdikt v spore lekára Sabaku s hnutím Republika by mohol padnúť o necelý mesiac*. Dostupné na: https://spravy.rtvs.sk/2023/06/sudny-spor-lekara-p-sabaku-s-hnutim-republika-vrcholi-verdikt-by-mohol-padnut-o-necely-mesiac/.
3. KUNER, CH. – BYGRAVE, L. – DOCKSEY, CH. *The EU General Data Protection Regulation (GDPR). A commentary*. Oxford: Oxford University Press, 2020, s. 121.
4. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.* Adopted on 3 October 2017. As last Revised and Adopted on 6 February, s. 19.
5. BYGRAVE, L. Automated individual decision-making, including profiling. In KUNER, CH. – BYGRAVE, L. – DOCKSEY, CH.: *The EU General Data Protection Regulation (GDPR). A commentary.* Oxford: Oxford University Press, 2020, s. 530 - 531.
6. *Stanovisko Generálneho Advokáta Priit Pikamäe predneseného dňa 16.3.2023 vo veci C-634/21 OQ proti Land Hessen za účasti: SCHUFA Holding AG*, body 31 – 32.
7. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation, 2016/679*.

[34] GDPR, článok 78.
[35] GDPR, článok 79.

8. *CAVOUKIAN, A. Privacy by Design – The Seven Foundational Principles*. Dostupné na https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.
9. Rozhodnutie SDEÚ z 24. septembra 2019 *GC a i. v. Commission nationale de l'informatique et des libertés (CNIL)*. Vec č. C-136/17.
10. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 4/2007 on the concept of personal data*. Adopted on 20th June, 01248/07/EN.WP 136, s. 6.
11. EUROEPAN DATA PROTECTION BOARD. *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.* Version 2.0 Adopted on 20 October 2020. Dostupné na: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

Kontaktné údaje

JUDr. Matúš Mesarčík, PhD., LL.M
matus.mesarcik@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta

AI ACT A VYUŽITELNOST SYSTÉMŮ UMĚLÉ INTELIGENCE V JUSTICI

AI ACT AND USABILITY OF ARTIFICIAL INTELLIGENCE SYSTEMS IN JUSTICE

Barbora Košinárová[1]

Abstrakt: Umělá inteligence si již našla místo téměř ve všech pracovních i osobních oblastech, kolikrát i tam, kde bychom to nečekali. Tam, kde dosud absentuje, lze předpokládat její nástup. Možnosti jejího využití jsou téměř bezbřehé. Na všechny tyto výzvy je zapotřebí legislativně reagovat, což Evropská unie učinila mimo jiné prostřednictvím AI Actu, který představuje pouhou část balíčku, kterým unie reaguje na vzestup umělé inteligence. Ta má potenciál významně ovlivnit rovněž justiční sféru. Nabízí řadu příležitostí pro zefektivnění a zlepšení právního systému, ale zároveň vyžaduje pečlivé zvažování etických a právních aspektů. Je nezbytné, aby vývoj a implementace těchto systémů probíhaly v souladu s právními předpisy, které zajistí jejich spolehlivou implementaci v oblasti provozní správy justice, tak jejich využitelnosti jako důkazních prostředků.

Kľúčové slová: Umělá inteligence, Evropská unie, justice, AI Act, rizika, etika.

Abstract: Artificial intelligence has already found a place in almost all work and personal areas, many times even where we would not expect it. Where it is still absent, its onset can be assumed. The possibilities of its use are almost endless. All these challenges require a legislative response, which the European Union has done, among other things, through the AI Act, which represents only part of the package with which the Union responds to the rise of artificial intelligence. This has the potential to significantly influence the judicial sphere as well. It offers many opportunities for streamlining and improving the legal system, but also requires careful consideration of ethical and legal aspects. It is essential that the development and implementation of these systems take place in accordance with legal regulations, which will ensure their reliable implementation in the field of operational administration of justice, as well as their usability as means of evidence

Key words: Artificial intelligence, European Union, justice, AI Act, risks, ethics.

[1] Vysoká škola CEVRO

Úvod

Umělá inteligence se postupně promítá do osobních i pracovních oblastí, do téměř všech průmyslových odvětví i služeb, kolikrát i tam, kde bychom to nečekali. Aplikace umělé inteligence, jako jsou ChatGPT, GitHub Copilot, Stable Diffusion a další, využívá veřejnost a zaujala snad každého svou schopností vést až nadpřirozenou konverzaci s uživatelem (McKinsey, 2023). Navíc se technologie generativní umělé inteligence vyvíjí rychleji, než se se systémem seznamuje veřejnost. Společnost McKinsey (McKinsey, 2023) ve své zprávě uvádí, že AI bude mít významný dopad do všech průmyslových odvětví, může změnit způsob práce a automatizovat pracovní činnosti.

Ale je to nejen laická veřejnost, která využívá výhod aplikací umělé inteligence. Co se týče českého právního prostředí nelze jinak než nezmínit Wair, aplikaci, která za pomocí sémantického vyhledávání v soudní judikatuře vytváří poměrně kvalitní a přesné právní rešerše.

S rychlým vývojem AI a jejím používáním napříč odvětvími se objevují a diskutují právní a etické otázky a s tím související první spory v souvislosti s AI. Podle předběžných odhadů to budou právě profese spojené s právem, které budou zasaženy těmito změnami nejvíce, jako, ale jiné odborné služby (např. Addy et al., 2024; Mazzini, Bagni, 2023; Ramos, Ellul, 2024). Jelikož je umělá inteligence využívána také k automatizaci opakujících se jednoduchých úkolů, může velmi snadno nahradit základní administrativní a právní práci. Nicméně tam, kde začínáme objevovat možnosti, které spojení umělé inteligence a práva přináší, narážíme zároveň i na limity a otázky, které jsou doposud nevyřešeny.

Evropská unie a AI Act

Neustálá expanze systémů umělé inteligence do téměř všech oblastí společenského života nutně vede k legislativní regulaci. Dne 13. 3. 2024 Evropský parlament schválil návrh Nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (AI Act) a mění určité legislativní akty unie (dále jen "AI Act") (Evropská komise, 2021). Podstata aktu o umělé inteligenci vychází z posouzení rizik, které tyto systémy přináší do lidské společnosti a podle tohoto posouzení určité postupy či prakticky rovnou proklamuje jako zakázané nebo jako vysoce rizikové. Zákaz určitých praktik vychází z jejich mimořádné škodlivosti a tedy nekompatibility se základními hodnotami unie, jako je ochrana základních lidksých práv. Co do vysoce rizikových systémů umělé inteligence akt zavádí poměrně přísnou metodiku řízení rizik, tak aby jejich použití bylo bezpečné, v souladu se základními principy ochrany lidských práv v Evropské unii a jejich použití vždy podléhalo lidskému dozoru (Evropská komise, 2021). Pehlivan (2024) uvádí, že se předpokládá, že, akt o umělé inteligenci se stane vzorem pro řízení umělé inteligence po celém

světě, a to podobným způsobem, jakým obecné nařízení o ochraně osobních údajů (GDPR) ovlivnilo regulaci ochrany údajů za hranicemi Evropy.
Především je třeba si říci, co vlastně tento akt rozumí pod pojmem systém umělé intelligence. Je jím jakýkoliv software, vyvinutý pomocí některé z technik uvedených v první příloze aktu, a který může za určitým cílem, který definuje člověk, generovat výstupy jako je obsah, predikce, doporučení nebo rozhodnutí, která ovlivňují prostředí, se kterým tento systém komunikuje.
Regulace navrhovaná aktem předně stanovuje seznam zakázaných postupů umělé inteligence. Tyto praktiky jsou považovány za nepřijatelné pro rozpor se základními hodnotami Evropské unie, zejména pro porušování základních lidských práv.
Zákazy se týkají postupů, které mohou manipulovat s fyzickými osobami prostřednictvím podprahových technik bez jejich vědomí. Případně zneužívají zranitelnosti konkrétních zranitelných skupin, jako jsou děti nebo osoby se zdravotním postižením, s cílem ovlivnit jejich chování způsobem, který by mohl jim nebo jiné osobě způsobit psychickou nebo fyzickou újmu. Návrh rovněž zakazuje přidělování sociálního kreditu na základě umělé inteligence pro účely orgánů veřejné moci, které by vedly k znevýhodňujícímu nebo nepříznivému zacházení s fyzickými osobami za aktem stanovených situací. A konečně je až na určité omezené výjimky zakázáno rovněž používání biometrické identifikace na dálku v reálném čase na veřejně přístupných místech pro účely prosazování práva.
Dále akt stanovuje speciální pravidla pro systémy umělé inteligence, které představují vysoké riziko pro zdraví a bezpečnost nebo pro základní práva fyzických osob. Tyto vysoce rizikové systémy umělé inteligence akt povoluje pod podmínkou, že budou splňovat určité závazné požadavky (Fraser & Villarino, 2023) a že bude provedeno posouzení shody ex ante neboli předem, tj. ještě před jejím použitím. Seznam vysoce rizikových systému umělé inteligence obsahuje třetí příloha aktu. S ohledem na téma tohto příspěvku, jde konkrétně o technologie užívané v oblasti:

- vymáhání práva, například technologie jako detektory lži a obdobné nástroje, nebo za účelem zjišťování emočního stavu fyzické osoby, dále použití tzv. deep fakes, hodnocení spolehlivosti důkazů, odhalování, vyšetřování nebo stíhání trestných činů;
- správy soudnictví a demokratických procesů, jako jsou technologie určené na pomoc soudním orgánům při zkoumání a výkladu a práva.

Zásadní ovšem je, že akt u použití všech vysoce rizikových systémů ukládá povinnost lidského dohledu. Lidský dohled je zaměřen na prevenci nebo minimalizaci rizik pro zdraví, bezpečnost nebo základní práva, která mohou vzniknout při používání vysoce rizikového systému umělé inteligence v souladu s jeho účelem nebo za podmínek důvodně předvídatelného nesprávného použití. Konkrétně to znamená, že všechny technologie využívající umělou inteligenci, které akt řadí mezi vysoce rizikové musí být navrženy a vyvinuty takových způsobem a za pomoci vhodných nástrojů při rozhraní člověk – stroj, aby na ni v situacích, kdy je umělá inteligence využívána,

mohli účinně dohlížet fyzické osoby. Ale jak vysvětluje Kalodanis et al. (2023) je třeba vzít v potaz rozdíl mezi navrhovanými požadavky a dostupnými bezpečnostními protiopatřeními umělé intelligence.

Využitelnost systémů AI v justici

Systémy AI mohou být v justiční sféře využívány dvojím způsobem. Jednak jako nástroj sloužící provozním záležitostem justice, tj. sloužící rozhodovacím a zejména administrativním procesům. V druhém případě můžeme hovořit o využitelnosti výstupů, produktů AI jako důkazních prostředků.

Systémy AI v provozní sféře justice

V justiční sféře má využití systémů umělé inteligence obrovský potenciál. Předně může být využita jako asistence soudcům při rozhodování. Jak bylo zmíněno výše, dříve náročné a zdlouhavé studování soudní judikatury, je v současnosti nahrazováno aplikacemi schopnými tvořit kvalitní rešerše soudní judikatury.
Umělá inteligence může výrazně zrychlit a zefektivnit soudní řízení. Systémy AI dokážou analyzovat velké objemy dat, identifikovat relevantní informace a dokonce generovat právní dokumenty. To může vést k úspoře času a nákladů na provoz soudů.
V oblasti predikcí a analýz mohou být systémy AI využity k predikci výsledků soudních sporů na základě analýzy historických dat a judikatury. To může pomoci právníkům a klientům lépe pochopit pravděpodobnost úspěchu v konkrétním případu.
AI může automatizovat různé administrativní úkony, jako je třídění dokumentů, správa případů a monitorování dodržování zákonných lhůt. To může výrazně snížit zátěž soudních úředníků a zvýšit efektivitu celého systému.
I přes nesporné výhody, využití AI v justici přináší i řadu etických a právních výzev. AI systémy mohou být náchylné k diskriminaci a zaujatosti, pokud jsou trénovány na datech, která obsahují předsudky. To může vést k nespravedlivým rozhodnutím v právních případech. V některých případech mohou klienti preferovat osobní interakci s lidským advokátem. AI může chybět lidský aspekt, jako je empatie a osobní porozumění, což může být zvláště důležité v citlivých právních záležitostech. Úspěch AI systémů v právním prostředí závisí na kvalitě a spolehlivosti dat, která mají k dispozici. Nedostatečnost nebo zkreslení dat může vést k nesprávným výsledkům a rozhodnutím.
Mimo to jednou z hlavních otázek je odpovědnost za rozhodnutí učiněná AI. Kdo ponese odpovědnost za chyby nebo nespravedlivá rozhodnutí AI? Dále je zde otázka transparentnosti a vysvětlitelnosti AI systémů. Je důležité, aby uživatelé a soudci rozuměli, jak AI dospěla k určitému rozhodnutí. Každopádně jak uvádí Skliarenko (2024) umělou inteligenci v justiční sféře nelze v současné chvíli chápat jako něco, co

má nahradit soudce. Ale naopak jako na něco, co má soudci pomáhat k výkonu spravedlnosti.

Je vůbec zákonné využívat systémy AI v justici?

Z předchozí části tohto příspěvku lze usuzovat, že využití systémů AI v provozní sféře justice může mít mnoho pozitivních dopadů. Ale je nutné se ptát, zda pro jejich využití existuje zákonný podklad? Na úrovni evropské legislativy je zřejmé, že AI Act s využitím v oblasti správy soudnictví jednoznačně počítá. Jak je to ale na úrovni národního zákonodárství? Jednoznačná zákonná úprava týkající se využití AI v oblasti správy justice prozatím absentuje. To ale neznamená, že by jejich využití bylo vyloučeno. Nepřímo se této problematiky dotkl Ústavní soud České republiky, a to v oblasti územního plánování (Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. III. ÚS 3817/17). Konstatoval, že Jjstě není a priori na překážku, když v 21. století existuje automatizovaný nástroj, který kontroluje předem jednoznačně stanovená pravidla regulace území, a to i na úseku územního plánování. Výtka obecných soudů, že není fakticky možné úplné přezkoumání správnosti aplikace tohoto algoritmu na konkrétní případy bez využití příslušné počítačové aplikace, je otázkou spíše technicistního charakteru a otázkou možnosti jednotlivých subjektů (žadatelů) ověřit soulad svého plánovaného záměru s územním plánem, což je však úkolem orgánů územního plánování v dalších řízeních, a bez dalšího to nemůže vést k nezpochybnitelnému závěru o nezákonnosti předmětné regulace. Jinými slovy řečeno, absence výslovné zákonné úpravy určitého systému neznamená a priory jeho nezákonnost.

Produkty systému AI jako důkazní prostředky

Využitelností výstupu AI jako důkazního prostředku se již zabýval Městský soud v Praze (Městský soud v Praze, sp. zn. 10 A 99/2023). V rámci řízení soud zamítl pro nadbytečnost dokazování některými žalobcem navrženými listinami, mj. i odpovědí ChatGPT na dotaz ohledně těžby jílu v předmětné oblasti.
Podle zdůvodnění soudu odpověď ChatGPT, které je určeno pro širokou veřejnost, nemůže ke zjištění skutkového stavu jakkoli přispět. Je totiž obecně známou skutečností, že veřejnosti aktuálně dostupná verze tohoto velkého jazykového modelu není spolehlivým zdrojem informací jakéhokoli druhu, jelikož v případě, že určitou informací nedisponuje, poskytuje informace vyfabulované, zhusta bez jakékoli opory v realitě či s odkazy na konkrétní, avšak neexistující, vymyšlené primární zdroje. Tyto případy přitom nelze, s výjimkou zjevných logických nebo věcných omylů, jednoduše rozlišit. Pravdivost odpovědí ChatGPT, ale i dalších komunikačních rozhraní jiných velkých jazykových modelů fungujících na stejných

principech, tak je třeba ověřit pomocí jiných zdrojů; v takovém případě by ovšem byly důkazními prostředky právě tyto jiné zdroje, a nikoli odpověď ChatGPT.
Lze konstatovat, že dosavadní český soudní přístup k produktům systémů AI je negativní. V kontextu výše uvedeného judikátu Městský soud označil konkrétní výstup za nevěrohodný. Je ovšem otázkou nakolik je takový přístup udržitelný, neboť je rovněž obecně známou skutečností, že systémy umělé inteligence procházejí neustálým vývojem a zlepšováním.
Na druhou stranu je nutné říci, že i co se týče přístupu soudů v České republice k systémům umělé inteligence, v současné době nelze hovořit o konstantní rozhodovací praxi. To znamená, že přístup k umělé inteligenci se může lišit případ od případu a závisí na konkrétních okolnostech a potřebách daného řízení. Kauzy spojené s využitím AI se prozatím objevují pozvolna.

Závěr

Evropská unie reaguje na nástup systémů umělé inteligence prostřednictvím komplexního právního rámce, který zahrnuje několik klíčových iniciativ a nařízení. Nejvýznamnějším z nich je AI Act, který byl navržen Evropskou komisí a aktuálně postupně nabývá účinnosti. Evropská unie se tak snaží vytvořit prostředí, které podporuje inovace a zároveň chrání občany před riziky spojenými s umělou inteligencí. Tento přístup má za cíl zajistit, aby EU zůstala konkurenceschopná na globálním trhu, zatímco zároveň poskytuje vysokou úroveň ochrany a etických standardů.
Současný evropský regulativní rámec těchto systémů však lze označit pouze za první nesmělé kroky k usměrňování tohoto technologického pokroku. Břemeno regulace leží zejména na národních legislativách, které v návaznosti na technologický proces provedo požadavky AI Actu v konkrétnějších rovinách. A to jak ve sféře správy justice, tak použitelnosti výstupů systémů umělé inteligence v oblasti dokazování.

Zoznam použitej literatúry

1. McKinsey (2023). The Economic potential of generative AI: The next productivity frontier. Online. Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier. [cit. 2024-09-21].
2. Addy, A. et al. (2024). Ghana's Public Health Act, AI algorithms and Vaccine Distribution in Ghana. International Journal For Multidisciplinary Research, vol. 6, DOI https://doi.org/10.36948/ijfmr.2024.v06i01.12144.
3. Mazzini, G. and Bagni, F. (2023). Considerations on the regulation of AI systems in the financial sector by the AI Act. Frontiers in Artificial Intelligence, vol. 6. DOI https://doi.org/10.3389/frai.2023.1277544.

4. Ramos, S. and Ellul, J. (2024). Blockchain for Artificial Intelligence (AI): Enhancing compliance with the EU AI Act through distributed ledger technology. A cybersecurity perspective. International Cybersecurity Law Review, vol. 5, pp. 1–20. DOI https://doi.org/10.1365/s43439-023-00107-9.
5. European Commission (2021). Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021) 206 final – 2021/01069(COD)). Online. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.
6. Pehlivan, C. (2024). The EU Artificial Intelligence (AI) Act: An Introduction. Global Privacy Law Review, vol. 5, pp. 31–42. DOI https://doi.org/10.54648/GPLR2024004.
7. Fraser, H. and Villarino, J.-M. (2023). Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough. European Journal of Risk Regulation, pp. 1–16. DOI https://doi.org/10.1017/err.2023.57.
8. Kalodanis, K., Rizomiliotis, P. and Anagnostopoulos, D. (2023). European Artificial Intelligence Act: An AI security approach. Information and Computer Security. Vol. ahead-of-print No. ahead-of-print. DOI https://doi.org/10.1108/ICS-10-2022-0165.
9. Skliarenko, V., I. (2024). Prospects for the use of artificial intelligence in civil justice. Uzhhorod National University Herald Series Law, 1(81):231-237, pp. 231–237. DOI: 10.24144/2307-3322.2024.81.1.36.
10. Rozsudek Městského soudu v Praze ze dne 9. 11. 2023, sp. zn. 10 A 99/2023.
11. Nález Ústavního soudu ze dne 14. 5. 2019, sp. zn. III. ÚS 3817/17.

Kontaktné údaje

JUDr. Barbora Košinárová, Ph.D.
barbora.kosinarova@vsci.cz
Vysoká škola CEVRO

ZMENY V OTÁZKACH ZODPOVEDNOSTI ZA ZDIEĽANIE DIGITÁLNEHO OBSAHU PO PRIJATÍ AKTU DSA[1]

CHANGES IN LIABILITY ISSUES FOR SHARING DIGITAL CONTENT AFTER ADOPTION OF THE DSA ACT

Lukáš Macko[2]

Abstrakt: Príspevok sa zaoberá zmenami v problematike uplatňovania zodpovednosti poskytovateľov digitálnych služieb v digitálnom prostredí po nadobudnutí účinnosti Aktu DSA. Príspevok približuje zmeny v uplatňovaní výnimiek zodpovednosti podľa znenia Smernice E-commerce oproti novej úprave podľa Aktu DSA.

Kľúčové slová: Akt DSA, zodpovednosť, digitálny obsah, Smernica E-commerce

Abstract: The paper deals with the changes in the issue of the application of the responsibility of digital service providers in the digital environment after the entry into force of the DSA Act. The contribution approximates the changes in the application of liability exceptions according to the wording of the E-commerce Directive compared to the new adjustment according to the DSA Act.

Key words: DSA Act, liability, digital content, E-commerce Directive

Úvod

V úvode príspevku možno načrtnúť, že úlohou Aktu DSA[3] je z pohľadu úpravy na úrovni Európskej únie potreba vytvoriť bezpečnejší digitálny priestor. Užívanie digitálnych služieb možno hodnotiť v dnešnej dobe ako súčasť bežného života každého spotrebiteľa. V súvislosti s využívaním digitálnych služieb možno

[1] Tento príspevok je publikovaný v rámci projektu VEGA č. 1/0431/23 s názvom Konkurencia záujmov spotrebiteľov a obchodníkov pri dodávaní digitálneho obsahu a digitálnych služieb na jednotnom digitálnom trhu s dôrazom na právne a ekonomické aspekty

[2] Odborný asistent, Univerzita Komenského v Bratislave, Právnická fakulta, Ústav práva informačných technológií a práva duševného vlastníctva

[3] Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách), ďalej v texte len „Akt DSA"

abstrahovať ale fundamentálne problémy, s ktorými je potrebné vysporiadať sa v rámci právnej teórie.
Prijatiu Aktu DSA predchádzali viaceré rozsiahle rozpravy. Podľa správy o hodnotení vplyvu boli občania členských štátov pred prijatím aktu DSA po prvé vystavení rastúcim rizikám a škodám v súvislosti s nezákonnými činnosťami až po riziká pre ich základné práva a iné spoločenské škody. Tieto problémy boli rozšírené v rámci online ekosystému, ale vzhľadom na ich dosah mali najväčší vplyv na veľmi veľké online platformy. Po druhé, dohľad nad online platformami v širšom zmysle do značnej miery bol nekoordinovaný a neefektívny, a to napriek systémovému významu takýchto služieb. Obmedzený rámec administratívnej spolupráce stanovený smernicou E-commerce[4] na riešenie cezhraničných otázok bol nedostatočne špecifikovaný a členské štáty ho využívali nejednotne. Po tretie, členské štáty začali regulovať duševné statky na vnútroštátnej úrovni, čo viedlo k novým prekážkam na vnútornom trhu. To viedlo ku konkurenčnej výhode pre zavedené veľmi veľké platformy a digitálne služby.[5] Na úrovni Európskej únie preto už dlhodobo panovala potreba úpravy zodpovednosti za šírenie digitálneho obsahu prostredníctvom digitálnych služieb výsledkom čoho bolo prijatie Aktu DSA. Akt DSA bol preto zverejnený v Úradnom vestníku dňa 27.10.2022 a nadobudol platnosť dňa 16.11.2022. Priamo uplatniteľný je v celej Európskej únií od 17.02.2024.[6]
Medzi základné ciele Aktu DSA patrí zabezpečenie riadneho fungovania jednotného digitálneho trhu, najmä poskytovanie cezhraničných online sprostredkovateľských služieb.
Je však nutné zdôrazniť, že Akt DSA bol prijatý vo forme nariadenia, pričom úprava zodpovednosti poskytovateľov služieb informačnej spoločnosti bola pred jeho prijatím komplexne upravená v Smernici E-commerce[7], čo v rámci aplikácie zodpovednosti za šírenie nelegálneho obsahu na internete možno považovať za značnú zmenu.

---

[4] Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode, ďalej v texte len „Smernica E-commerce"

[5] Zhrnutie správy o hodnotení vplyvu , návrh nariadenia Európskeho parlamentu a Rady o jednotnom trhu digitálnych služieb a o zmene doplnení smernice 2001/31 ES, {COM(2020) 825 final} – {SEC(2020) 432 final} – {SWD(2020) 348 final}, Dostupné na internete : https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-services-act

[6] Zhrnutie správy o hodnotení vplyvu , návrh nariadenia Európskeho parlamentu a Rady o jednotnom trhu digitálnych služieb a o zmene doplnení smernice 2001/31 ES, {COM(2020) 825 final} – {SEC(2020) 432 final} – {SWD(2020) 348 final}, Dostupné na internete : https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-services-act

[7] MACKO, Lukáš: Zodpovednosť za použitie a zdieľanie digitálneho obsahu na internete. Bratislava: C. H. Beck, 2024, 136 s., ISBN 978-80-8232-055-1

Uplatňovanie výnimiek zo zodpovednosti po prijatí Aktu DSA v porovnaní so Smernicou E-commerce

Pred prijatím Aktu DSA boli výnimky zo zodpovednosti všeobecne upravené v čl. 12 až 15 už spomínanej Smernice E-commerce. Momentálne sú upravené v čl. 4,5,6 a 8 Aktu DSA.

Právna úprava obsiahnutá v čl. 12 až 14 Smernice E-commerce je založená na tzv. inštitúte „safe harbours" (v preklade bezpečné prístavy). Uvedené prevzal do legislatívneho textu v podstate aj Akt DSA do už zmienených článkov 4,5,6. Článok 8 Aktu DSA hovorí o zákaze všeobecnej monitorovacej povinnosti, ktorá bola pôvodne upravená článkom 15 Smernice E-commerce. Je dôležité zdôrazniť, že čl. 4,5,6 a článok 8 Aktu DSA sa s pôvodnými článkami 12 až 15 Smernice E-commerce neprekrývajú a to s ohľadom na čl. 89 Aktu DSA, ktorý hovorí o tom, že články 12 až 15 Smernice E-commerce sa úplne vypúšťajú. Ďalej čl. 89, ods. 2 uvádza , že „ *odkazy na články 12 až 15 smernice 2000/31/ES sa považujú za odkazy na články* 4, 5, 6 a 8 *tohto nariadenia.*" Tu treba zdôrazniť, že nakoľko nariadenie, vo forme ktorého bol prijatý Akt DSA má priamy účinok čo značí, že členské štáty tieto výnimky nemusia osobitne inkorporovať do svojich vnútroštátnych poriadkov pomocou vnútroštátnych predpisov nakoľko Akt DSA je priamo aplikovateľný v každom vnútroštátnom práve, toho ktorého členského štátu.

Mere conduit

Táto výnimka bola zavedená prvý krát do účinnosti spomínaným článkom 12 Smernice E-commerce. Po nadobudnutí účinnosti Aktu DSA možno túto výnimku dohľadať v článku 4. Je potrebné zdôrazniť, že táto výnimka zo zodpovednosti spočíva v prenose informácií, ktoré sú poskytované príjemcom služby prostredníctvom komunikačnej siete alebo z poskytnutia prístupu do komunikačnej siete. Ak teda poskytovateľ služby informačnej spoločnosti spĺňa definičné znaky podľa čl. 4 Aktu DSA, nezodpovedá za nezákonný prenášaný obsah ak kumulatívne spĺňa podmienku, že:

- nezákonný prenos neiniciuje,
- nevyberá príjemcu prenosu,
- neupravuje prenášané informácie.

Uvedená výnimka sa teda napríklad vzťahuje aj podľa čl. 4 ods. 1 Aktu DSA na poskytovateľov Wifi pripojenia tak tomu bolo v prípade .[8]

Z vyššie uvedeného možno teda abstrahovať, že ak sú splnené vyššie uvedené podmienky podľa čl. 4 ods. 1 Aktu DSA, poskytovateľ služieb informačnej spoločnosti, ktorý poskytuje prístup do siete nebude zodpovedný za prípadné šírenie nelegálneho digitálneho obsahu a majiteľ autorských práv si nebude môcť voči nemu uplatňovať nároky titulom odškodnenia aj napriek tomu, že pripojenie bolo využité

[8] Rozsudok SDEÚ zo dňa 15. 9. 2016 vo veci Mc Fadden, C-484/14, ECLI:EU:C:2016:689, body 54

z neoprávneným šírením digitálneho obsahu. [9]
Samozrejme možno však podčiarknuť, že s ohľadom na početnú judikatúru Súdneho dvora Európskej únie, čl. 4 ods. 1 Aktu DSA nebráni tomu, aby osoba dotknutá na svojich právach žiadala správny alebo súdny orgán o vydanie zákazu proti tomuto poskytovateľovi, aby zabránil ďalšiemu nezákonnému prenosu. [10]
Caching
Túto výnimku zo zodpovednosti môžeme v Akte DSA nájsť obsiahnutú v čl. 5. Pred nadobudnutím účinnosti Aktu DSA bola výnimka upravená v čl. 13 Smernice E-commerce.
Znenie Aktu DSA koncepčne uvedenú výnimku zo zodpovednosti oproti legislatívnemu textu obsiahnutému v Smernici E-commerce príliš nepozmenilo. Výnimka pozostáva z premisy, že takáto služba informačnej spoločnosti je poskytovaná príjemcom tejto služby prostredníctvom komunikačnej siete a poskytovateľtejto služby nebude zodpovedať za dočasné, automatické a prechodné uloženie obsahu, ak je urobené výlučne s cieľom zefektívnenia ďalšieho prenosu. Samozrejme uplatnenie výnimky si vyžaduje kumulatívne uplatnenie požiadaviek uvedených v čl. 5 ods. 1 , tzv. ak poskytovateľ:
a) neupravuje informácie,
b) dodržiava podmienky prístupu k informáciám,
c) dodržiava pravidlá týkajúce sa aktualizácie informácií, ktoré sú špecifikované spôsobom všeobecne uznávaným a používaným v odvetví.[11]
Vo vzťahu ku cachingu a obyčajnému prenosu je dôležité ešte zdôrazniť uplatnenie čl. 21 odôvodnenia Aktu DSA, ktorý hovorí, že vyššie výnimky možno využiť len vtedy ak nie je poskytovateľ služby informačnej spoločnosti nijako zainteresovaný na informáciách, ktoré sú predmetom prenosu alebo prístupu.
Hosting
V prípade hostingu môžeme hovoriť o najvýznamnejšej výnimke zo zodpovednosti. Oproti pôvodnému zneniu obsiahnutému v Smernici E-commerce v jej čl. 14 možno povedať, že obsahovo preberá znenie tohto článku aj Akt DSA. Výnimka zo zodpovednosti podľa čl. 6 ods. 1 Aktu DSA hovorí o tom, že ak služba informačnej spoločnosti pozostáva z uchovávania informácií poskytovaných príjemcom služby poskytovateľ služby nie je zodpovedný za informácie uchovávané na žiadosť príjemcu služby pod podmienkou, že poskytovateľ:
a) nemá skutočnú vedomosť o nezákonnej činnosti alebo nezákonnom obsahu a vzhľadom na nároky na náhradu škody si nie je vedomý skutočností alebo okolností, z ktorých by bolo zrejmé, že ide o nezákonnú činnosť alebo nezákonný obsah alebo,
b) po získaní takejto vedomosti alebo povedomia urýchlene koná, aby nezákonný

[9] Rozsudok SDEÚ zo dňa 15. 9. 2016 vo veci Mc Fadden, C-484/14, ECLI:EU:C:2016:689, body 74.
[10] Pozri aj MACKO, Lukáš: Zodpovednosť za použitie a zdieľanie digitálneho obsahu na internete. Bratislava: C. H. Beck, 2024, 136 s., ISBN 978-80-8232-055-1
[11] Pozri aj HUČKOVÁ, Regina., TREŠČÁKOVÁ, Diana., ROZENFELDOVÁ, Laura. (eds.): Právo informačných technológií. Košice : Univerzita Pavla Jozefa Šafárika v Košiciach, 2020, 140 s., ISBN 978081529108

obsah odstránil alebo k nemu znemožnil prístup[12]
Výnimka zo zodpovednosti je však okliešťená na prípady podľa čl. 6 ods. 2, ktorý hovorí, že ods. 1 sa nebude uplatňovať ak príjemca služby podlieha kontrole poskytovateľa alebo je pod jeho kontrolou. Zároveň sa výnimka neuplatňuje ani v prípade platforiem, ktoré umožňujú spotrebiteľom uzatvárať s obchodníkmi zmluvy na diaľku, ak takáto online platforma predkladá konkrétnu informáciu alebo inak umožňuje konkrétnu transakciu takým spôsobom, ktorý by viedol priemerného spotrebiteľa k presvedčeniu, že informácie alebo výrobok či službu, ktoré sú predmetom transakcie, poskytuje buď samotná online platforma, alebo príjemca služby, ktorý jej podlieha alebo je pod jej kontrolou.
Okrem iného, tak ako v prípade cachingu, aj v prípade hostingu čl. 6 ods. 4 Aktu DSA priamo umožňuje, aby sa ten koho práva boli porušené domáhal súdneho zákazu v ďalšom šírení nezákonného obsahu, ak má poskytovateľ služby informačnej spoločnosti o šírení nezákonného obsahu vedomosť.
Okrem tohto v prípade, hostingu treba brať zreteľ aj na čl. 22 odôvodnenia Aktu DSA, ktorý hovorí o tom, že na získanie výnimky zo zodpovednosti, je potrebné aby poskytovateľ služby informačnej spoločnosti ihneď po tom čo získa vedomosť o nezákonných činnostiach alebo nezákonnom obsahu, urýchlene konal s cieľom odstrániť tento obsah alebo k nemu znemožnil prístup[13]
Okrem iného, oproti Smernici E-commerce sa Akt DSA líši zavedením nových pravidiel obsiahnutých v čl. 7. Tento článok obsahuje tzv. doložku o ,,dobrom Samaritánovi". Toto pravidlo predstavuje odchýlku od vyššie spomínanej Smernice E-commerce, ktorá túto klauzulu neobsahovala. V článku 7 DSA sa totiž uvádza, že ,,*poskytovatelia sprostredkovateľských služieb sa nepovažujú za nespôsobilých na výnimky zo zodpovednosti uvedené v článkoch 4, 5 a 6 len z toho dôvodu, že v dobrej viere a svedomite vykonávajú dobrovoľné vyšetrovania z vlastnej iniciatívy alebo prijímajú iné opatrenia zamerané na odhaľovanie, identifikáciu a odstraňovanie nezákonného obsahu alebo prijímajú opatrenia potrebné na dosiahnutie súladu s požiadavkami práva Únie a vnútroštátneho práva v súlade s právom Únie vrátane požiadaviek stanovených v tomto nariadení.*"
Uvedený článok možno chápať podľa nášho názoru ako stimul, aby poskytovatelia služieb informačnej spoločnosti neboli odrádzaní od vykonávania opatrení na identifikáciu a riešenie nezákonného obsahu alebo činností zo strachu, že stratia výnimku zo zodpovednosti. Samozrejme, je potrebné dodať, že opatrenia nesmú viesť k monitorovacej povinnosti, ktorá je zakázaná tak ako sme tou uviedli v úvode príspevku.

Uplatňovanie sekundárnej zodpovednosti podľa Aktu DSA

[12] Pozri bližšie článok 6 ods. 1 Aktu DSA

[13] Pozri bližšie článok 22 odôvodnenia Aktu DSA, ktorý približuje aj situácie kedy možno od poskytovateľa požadovať zvýšenú mieru vedomosti o nezákonnom obsahu

Problematickým pre uplatnenie tzv. sekundárnej zodpovednosti za neoprávnené šírenie digitálneho obsahu je podľa nášho názoru znenie odôvodnenia čl. 17 Aktu DSA, ktoré hovorí o tom, že *„v pravidlách týkajúcich sa zodpovednosti poskytovateľov sprostredkovateľských služieb stanovených v tomto nariadení by sa malo stanoviť len to, kedy dotknutý poskytovateľ sprostredkovateľských služieb nemôže niesť zodpovednosť za nezákonný obsah, ktorý poskytujú príjemcovia služby. Uvedené pravidlá by sa nemali chápať tak, že poskytujú pozitívny základ na stanovenie toho, kedy môže byť poskytovateľ braný na zodpovednosť, keďže to majú určiť uplatniteľné pravidlá práva Únie alebo vnútroštátneho práva. Výnimky zo zodpovednosti stanovené v tomto nariadení by sa okrem toho mali uplatňovať na akýkoľvek druh zodpovednosti, pokiaľ ide o akýkoľvek druh nezákonného obsahu, a to bez ohľadu na presný predmet alebo povahu uvedených právnych predpisov.*"
Znenie odôvodnenia totižto priamo v legislatívnom texte narába so skutočnosťou, že výnimky zo zodpovednosti sa budú uplatňovať na poskytovateľov služieb informačnej spoločnosti aj v prípade ak pôjde o tzv. priame porušenie ako aj o sekundárne porušenie („secondary contributory"). **V tejto súvislosti možno preto konštatovať, že ani Akt DSA nerozlišuje medzi priamym porušením a porušením, ktoré možno subjektu pričítať ako prispievajúce.**

Záver

V závere možno zdôrazniť, že základné rozdiely pri uplatňovaní výnimiek zo zodpovednosti podľa čl. 4,5,6 Aktu DSA sa koncepčne podobajú predošlej úprave obsiahnutej v čl. 12,13,14 Smernice E-commerce. Novým ustanovením oproti predošlej úprave je článok 7 Aktu DSA, ktorý má slúžiť ako určitý stimul pre poskytovateľov služieb informačnej spoločnosti vo vzťahu k odhaľovaniu nezákonného obsahu na internete. Zároveň treba podotknúť, že ani Akt DSA ako nariadenie, ktorého úlohou je zabezpečenie zdieľania zákonného obsahu na internete neprinieslo rozdiel medzi primárnou a sekundárnou zodpovednosťou, ale úpravu a mechanizmy posúdenia zodpovednosti ponechalo na právne poriadky členských štátov čo môže komplikovať situáciu pri posudzovaní nárokov subjektov poškodených zdieľaním nezákonného obsahu na internete.

Zoznam použitej literatúry

1. Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2065 z 19. októbra 2022 o jednotnom trhu s digitálnymi službami a o zmene smernice 2000/31/ES (akt o digitálnych službách)Bibliografický záznam
2. Návrh nariadenia Európskeho parlamentu a Rady o jednotnom trhu digitálnych služieb a o zmene doplnení smernice 2001/31 ES, {COM(2020) 825 final} – {SEC(2020) 432 final} – {SWD(2020) 348 final}, Dostupné na internete :

https://digital-strategy.ec.europa.eu/en/library/impact-assessment-digital-services-act
3. MACKO, Lukáš: Zodpovednosť za použitie a zdieľanie digitálneho obsahu na internete. Bratislava: C. H. Beck, 2024, 136 s., ISBN 978-80-8232-055-1
4. HUČKOVÁ, Regina., TREŚČÁKOVÁ, Diana., RÓZENFELDOVÁ, Laura. (eds.): Právo informačných technológií. Košice : Univerzita Pavla Jozefa Šafárika v Košiciach, 2020, 140 s., ISBN 978081529108
5. Rozsudok SDEÚ zo dňa 15. 9. 2016 vo veci Mc Fadden, C-484/14, ECLI:EU:C:2016:689
6. Smernica 2000/31/ES Európskeho parlamentu a Rady z 8. júna 2000 o určitých právnych aspektoch služieb informačnej spoločnosti na vnútornom trhu, najmä o elektronickom obchode

Kontaktné údaje

JUDr. Lukáš Macko, PhD.
lukas.macko@flaw.uniba.sk
Univerzita Komenského v Bratislave, Právnická fakulta, Ústav práva informačných technológií a práva duševného vlastníctva

PREDIKTÍVNA ANALÝZA ROZHODNUTIA SÚDU NA ZÁKLADE SKÚMANIA JUDIKATÚRY POMOCOU STROJOVÉHO UČENIA[1]

PREDICTIVE ANALYSIS OF A COURT DECISION BASED ON CASE LAW EXAMINATION USING MACHINE LEARNING

Andrej Oriňak, Regina Hučková[2]

Abstrakt: V predkladanom príspevku sme sa zaoberali skúmaním použitia strojového učenia na predikciu rozhodnutí súdu. Určili sme výskumnú otázku: "Môže byť integrácia prediktívnej analýzy prínosná pre súdnictvo?". V rámci predkladaného príspevku sme vychádzali zo šiestich predpokladov týkajúcich sa presnosti prediktívnej analýzy, schopnosti odhaľovať skryté vzorce, vplyvu na časové a ekonomické hľadisko, vplyvu na konzistenciu a objektivitu rozhodnutí súdov, identifikácie kľúčových právnych inštitútov a zvýšenia efektivity rozhodovania v súdnictve. Cieľom predkladaného príspevku bolo posúdiť, do akej miery môže spojenie uvedených technológií zefektívniť proces rozhodovania súdu. Z hľadiska praktického využitia považujeme strojové učenie v súdnictve za podporný prostriedok pre rozhodovanie sudcu, nie však za náhradu ľudského posúdenia. Výsledky indikujú vysokú presnosť predikcie, schopnosť odhaľovať vzorce, ktoré sú ľuďmi často prehliadané a priaznivý vplyv na konzistentnosť rozhodovania.

Kľúčové slová: spracovanie prirodzeného jazyka, strojové učenie, prediktívna analýza, analýza judikatúry

Abstract: In the presented paper, we examined the use of machine learning to predict court decisions. We identified the research question: "Can the integration of predictive analysis be beneficial to the judiciary?". We made six assumptions regarding the accuracy of predictions, the ability to detect hidden patterns, the impact on time and economics, the impact on the consistency and objectivity of court decisions, the identification of key legal institutes, and the increase in the efficiency of judicial decision making. The aim of the paper was

[1] Príspevok spracovaný v rámci plnenia grantových úloh projektu APVV-21-0336 *„Analýza súdnych rozhodnutí metódami umelej inteligencie*".

[2]Katedra obchodného práva a hospodárskeho práva, Právnická fakulta Univerzity Pavla Jozefa Šafárika v Košiciach

to assess the extent to which the combination of the above technologies can streamline the court's decision-making process. In terms of practical application, we consider machine learning in the judiciary as a support tool for judges, not as a substitute for human judgement. The results indicate high accuracy of prediction, the ability to detect patterns that are often overlooked by humans, and a positive impact on the consistency of decision making.

Key words: natural language processing, machine learning, predictive analysis, case law analysis

Úvod

Využitie umelej inteligencie a strojového učenia v súdnictve predstavuje značne inovatívny prístup ku koncepcii súdnych rozhodnutí. Tieto technológie dokážu analyzovať rozsiahle súbory dát a odhaliť vzory a korelácie, ktoré sú pre ľudské oči často skryté alebo prehliadané. S rastúcim počtom publikovaných súdnych rozhodnutí a dostupnosťou právnych textov na online platformách sa objavuje veľký potenciál na automatizáciu časti súdneho rozhodovania, najmä pokiaľ ide o predikciu výsledkov súdnych procesov.

Prediktívna analýza rozhodnutí súdov, založená na princípe skúmania judikatúry prostredníctvom strojového učenia prináša potenciál zefektívniť rozhodovací proces v súdnej praxi. Systémy využívajúce strojové učenie dokážu nielen predikovať výsledky na základe historických údajov z predošlých rozhodnutí, ale aj poskytovať advokátom a sudcom nové poznatky o skrytých vzorcoch a tendenciách v rozhodovaní. Tento prístup má obrovský význam najmä v zložitých právnych doménach, kde tradičné metódy právnej analýzy často čelia limitom týkajúcim sa rýchlosti, presnosti a konzistencie.

V kontexte právnych systémov existujú prípady, kedy advokáti a sudcovia hľadajú vzory a opierajú sa o minulé rozhodnutia, aby mohli aspoň zhruba predvídať budúce rozhodnutia v podobných skutkových veciach. Integrácia strojového učenia do tohto procesu prináša potenciál výrazne zvýšiť efektivitu rozhodovania v súdnictve. Predkladaný príspevok sa zameriava na skúmanie miery, do akej môže byť integrácia prediktívnej analýzy prínosná pre súdnictvo, a zameriava sa na zodpovedanie otázky, či moderné technológie ako napr. strojové učenie dokážu nahradiť tradičné analytické metódy.

Prediktívne modely sa opierajú o rozsiahle historické údaje, ktoré zahŕňajú nielen texty rozhodnutí, ale aj informácie o sudcoch, podrobnostiach prípadu, osobnostných pomeroch strán sporu, aplikovaných právnych normách, využitých právnych inštitútoch a ďalších faktoroch. Takéto modely môžu využívať techniky spracovania prirodzeného jazyka na extrakciu informácií z textu a strojového učenia

na identifikáciu vzorcov a predikciu budúcich rozhodnutí. Zároveň prinášajú do procesu rozhodovanie nové možnosti, ako je analýza tendencie rozhodovania istým spôsobom, identifikácia rizikových faktorov a podpora rozhodovania prostredníctvom generovania odôvodnenia rozhodnutia.

Výskumná otázka a hypotézy

V kontexte rastúceho využívania modelov umelej inteligencie a strojového učenia v právnej praxi je podľa nášho názoru potrebné skúmať, do akej miery môžu tieto technológie skutočne prispieť k zlepšeniu kvality a efektivity súdnych rozhodnutí. Výskumná otázka, ktorú sme si stanovili na účely predkladaného príspevku, je:
„Môže byť integrácia prediktívnej analýzy prínosná pre súdnictvo?"
Táto otázka je zameraná na hodnotenie prínosu prediktívnych modelov v právnej oblasti a ich potenciálu nahradiť alebo doplniť tradičné metódy rozhodovania v súdnictve. Aby sme túto otázku preskúmali podrobne, stanovili sme dva vedecké predpoklady, ktoré sa zaoberajú rôznymi aspektmi využitia prediktívnej analýzy v súdnictve, a to:
Hypotéza č. 1: *„Pomocou metód strojového učenia je možné vypracovať prediktívnu analýzu súdnych rozhodnutí s vysokou presnosťou na základe dát obsiahnutých v judikatúre, čo predstavuje prekonanie metódy klasickej právnej analýzy z hľadiska kvality, rýchlosti a presnosti."*
Hypotéza č. 2: *„Prediktívna analýza rozhodnutia súdu pomocou modelov strojového učenia má potenciál skrátiť čas a znížiť náklady potrebné na vypracovanie klasickej právnej analýzy tým, že poskytuje rýchlu a presnú predikciu na základe analýzy rozsiahleho množstva dát z judikatúry."*

Teoretické východiská a súčasný stav skúmanej problematiky

V posledných rokoch sa pozornosť čoraz viac výskumníkov a odborníkov z oblasti umelej inteligencie sústreďuje na využitie strojového učenia v predikcii súdnych rozhodnutí. Tieto snahy sa často označujú ako právna technológia (*legal tech*) a ich cieľom je zefektívniť a zlepšiť rozhodovacie procesy v súdnych konaniach.
Habernal a kolektív skúmali schopnosť modelov strojového učenia extrahovať a analyzovať právne argumenty z rozhodnutí súdov. Navrhnutá schéma zahŕňa dvojrozmerný prístup, kde sa argumenty delia na typy a aktérov. Typy argumentov zahŕňajú širokú škálu kategórií ako procedurálne argumenty, rôzne metódy interpretácie (textová, historická, systematická), test proporcionality a inštitucionálne argumenty. Medzi aktérov boli zaradené pojmy ako Európsky súd pre ľudské práva (ESĽP), žalobca, štát, tretie strany a komisia/komora. Habernal vytvoril tím šiestich študentov práva, dvoch post-doktorandov a dvoch profesorov, pričom spoločne manuálne anotovali korpus 373 súdnych rozhodnutí. Tento korpus

obsahoval približne 2,3 milióna tokenov. Následne si navzájom členovia tímu svoje anotácie skontrolovali, takže anotovanie bolo veľmi dôsledné. Výsledný korpus bol spracovaný a pripravený pre ďalšie *natural language processing* (NLP) experimenty. Modely boli trénované a testované na klasifikáciu argumentov a ich aktérov s použitím multitaskového prístupu, kde každý model predpovedal typ argumentu aj aktéra. Najlepšie výsledky dosiahol model RoBERTa-Large, ktorý bol ďalej pretrénovaný na právnych dátach. Model prekonal existujúce baseline modely, ako Legal-BERT a základnú verziu RoBERTa, v presnosti a schopnosti rozpoznať jemné rozdiely medzi rôznymi typmi argumentov.[3] **Hou a kol.** v rámci svojho výskumu čelili problému spojenému s tým, že pri analýze judikatúry a právnych článkov pomocou dovtedy dostupných modelov boli analyzované dáta obmedzené na jednotlivé prípady. To bolo hlavným podnetom pre autorov k návrhu nového modelu – **Feature Fusion Model for Law Article Prediction (FFMLAP)**, ktorý využíva charakteristiky spoločných prvkov medzi prípadmi. Tento model konštruuje globálnu grafovú štruktúru na extrakciu globálnych informácií z opisov prípadov, vytvára textové podgrafy, ktoré plne využívajú spoločné črty medzi prípadmi a využíva hierarchickú sieť pozornosti na extrakciu kľúčových opisov z dokumentov na úrovni viet, odsekov alebo aj celých dokumentov.[4] Jednou z hlavných oblastí, v ktorých sa umelá inteligencia využíva, je predikcia výsledkov súdnych rozhodnutí. **Medvedeva a kol.** vo svojom výskume analyzovali prípady ESĽP a vyvinuli model, ktorý využíval textové časti rozhodnutí ESĽP, ako napr. skutkový stav, procesný postup a relevantné právne predpisy, na predikciu prípadov. Textové prvky boli spracované ako n-gramy (sekvencie slov) a model sa učil identifikovať vzory spojené s porušením alebo neporušením článkov dohovoru. Skúmali taktiež presnosť predikcie vo vzťahu k prípadom, ktoré sa vyskytli po období tréningu modelu. Autori tiež testovali, či je možné predikovať rozhodnutia súdu len na základe mien sudcov zapojených do prípadu. Výsledky ukázali, že modely dokázali dosiahnuť presnosť predikcie na úrovni 65 %, čo naznačuje, že niekedy dokonca aj mená sudcov môžu byť spojené so špecifickými rozhodnutiami. Modely autorov v rámci tohto výskumu dosiahli priemernú presnosť 75 % pri predikcii rozhodnutí založených na textových častiach súdnych rozhodnutí. Pri predikcii rozhodnutí na základe tréningových dát z minulosti bola priemerná presnosť nižšia (58 % až 68 %), čo ukazuje, že rozhodnutia v budúcnosti môžu byť ovplyvnené zmenami v právnych normách a spoločenských

[3] HABERNAL, Ivan – FABER, Daniel – RECCHIA, Nicola – BRETTHAUER, Sebastian – GUREVYCH, Iryna – SPIECKER GENNANT DÖHMANN, Indra – BURCHARD, Christoph: Mining legal arguments in court decisions. In: Artificial Intelligence and Law, Roč. 32, č. 2 (2024), s. 557–594. DOI: https://doi.org/10.1007/s10506-023-09361-y.

[4] HOU, Yifan – CHENG, Ge – ZHANG, Yun – ZHANG, Dongliang: Methods of incorporating common element characteristics for law article prediction. In: Artificial Intelligence and Law, Roč. 32, č. 4 (2023), s. 487–503. DOI: https://doi.org/10.1007/s10506-023-09359-6.

hodnotách.[5] Za významný považujeme taktiež príspevok v tejto oblasti, ktorý publikoval **Vuong so svojimi kolegami**, ktorí navrhli metódu **SM-BERT-CR**, čo je hlboký učebný prístup na vyhľadávanie súdnych precedensov s podporujúcim modelom. Tento prístup rieši náročnú úlohu vyhľadávania relevantných právnych prípadov na základe zadaného dopytu. Tento postup zahŕňa dve fázy:

a) vyhľadávanie prípadov;
b) rozpoznávanie logického dôsledku medzi prípadmi.

Tieto úlohy sú obzvlášť náročné najmä z dôvodu rozsahu textu, náročnosti právnej terminológie a potreby rozsiahleho množstva dát, ktoré si vyžadujú odborné znalosti na ich vytvorenie.[6] Jedným z kľúčových aspektov pre používanie umelej inteligencie (UI) v právnych procesoch je vysvetliteľnosť (*explainability*) rozhodnutí, ktoré algoritmy navrhujú. Podľa **Benedetto a jej tímu** je dôležité nielen predikovať súdne rozhodnutia, ale aj poskytovať používateľom, najmä právnikom a sudcom, zrozumiteľné vysvetlenia, ktoré odôvodňujú, ako algoritmus dospel k danému výsledku. Benedetto a jej kolegovia navrhli model, ktorý využíva rozpoznávanie právnych entít (NER) na identifikáciu kľúčových pojmov v právnych textoch. Po identifikácii entít sú určité úseky textu zodpovedajúce právnym entitám maskované. Tento krok má dva hlavné ciele: zvýšiť schopnosť modelov extrahovať kľúčové pojmy tým, že zakryjú menej relevantné detaily, ako sú napríklad osobné údaje, a zároveň obmedziť šírenie týchto informácií, najmä s ohľadom na ochranu osobných údajov. Takže sa vyselektujú pojmy, resp. entity, ktoré sú pre rozhodnutie kľúčové, a tie, ktoré sú menej relevantné alebo nerelevantné, sú maskované. Autori zdôrazňujú problémy súvisiace s dĺžkou právnych dokumentov, ktoré často presahujú kapacitu súčasných modelov založených na technológii transformerov.[7]

Collenette a kolektív sa podobne ako Medvedeva zamerali na aplikáciu nástrojov umelej inteligencie v kontexte rozhodnutí ESĽP. Pri testovaní ich modelu pracovali s článkom 6 Európskeho dohovoru o ľudských právach. Autori vytvorili model založený na abstraktných dialektických rámcoch (ADF), ktorý dokáže zachytiť vrstvy právneho uvažovania od základných faktov až po konečné rozhodnutia. Model bol testovaný na 40-tich prípadoch z ESĽP, kde dosiahol 97 % presnosť z hľadiska zhody s reálnymi

[5] MEDVEDEVA, Masha – VOLS, Michel – WIELING, Martijn: Using machine learning to predict decisions of the European Court of Human Rights. In: Artificial Intelligence and Law, Roč. 28, č. 2 (2019), s. 237-266. DOI: https://doi.org/10.1007/s10506-019-09255-y.

[6] VUONG, Yen Thi-Hai – BUI, Quan Minh – NGUYEN, Ha-Thanh – NGUYEN, Thi-Thu-Trang – TRAN, Vu Minh – PHAN, Xuan-Hieu – SATOH, Ken – NGUYEN, Le-Minh: SM-BERT-CR: a deep learning approach for case law retrieval with supporting model. In: Artificial Intelligence and Law, Roč. 31, č. 2 (2023), s. 601–628. DOI: https://doi.org/10.1007/s10506-022-09319-6.

[7] BENEDETTO, Irene – KOUDOUNAS, Alkis – VAIANI, Lorenzo – PASTOR, Eliana – CAGLIERO, Luca – TARASCONI, Francesco – BARALIS, Elena: Boosting court judgment prediction and explanation using legal entities. In: Artificial Intelligence and Law, (2024), s. 1-20. DOI: https://doi.org/10.1007/s10506-024-09397-8

rozhodnutiami. To je výrazne vyššie v porovnaní s existujúcimi modelmi strojového učenia, ktoré dosahovali presnosť okolo **70 až 85 %**. Vo svojom výskume použili metódu argumentačných rámcov, ktoré poskytujú zrozumiteľné a právne podložené vysvetlenia pre užívateľov, čo považujeme za vysoko prínosné, možno aj v očiach verejnosti.[8]

S rastúcim využitím modelov strojového učenia v právnych systémoch vyvstávajú aj etické otázky týkajúce sa predsudkov v algoritmoch. Jedným z najznámejších prípadov je systém COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions*), ktorý sa používa najmä v Spojených štátoch amerických na predikciu rizika recidívy u obvinených. **Engel a jeho kolegovia** zistili, že tento systém vykazuje rasovú a vekovú zaujatosť, čo môže viesť k nespravodlivému zaobchádzaniu s niektorými obvinenými. Engel a jeho tím demonštrovali, že tieto predsudky môžu byť odstránené, no zároveň varovali, že to môže zvýšiť riziko, že niektorí obvinení budú nesprávne prepustení.[9] Z uvedeného dôvodu opäť vyjadrujeme naše presvedčenie, že dnes, ako aj v budúcnosti bude potrebné aby posledné slovo v rozhodovaní mal vždy človek a modely strojového učenia boli pre človeka iba pomôckou. V tomto kontexte sa s názorom Engela a jeho kolektívu stotožňuje aj **Campbell**, ktorý považuje za jednu z hlavných výziev pri využívaní umelej inteligencie v súdnictve otázku zaujatosti či predsudkov, tzv. *bias*, ktoré môže byť implicitne skryté v historických údajoch. Campbell upozorňuje, že algoritmy strojového učenia môžu nevedome preberať zaujatosť z historických súdnych rozhodnutí a na základe toho vytvárať nespravodlivé, zaujaté predpovede. Táto problematika je naviazaná najmä na predikciu recidívy v kriminalistike, kde sú historické údaje často poznačené rasovými alebo inými predsudkami. Problém podľa neho predstavujú taktiež nevyriešené technické výzvy, ako napríklad spracovanie veľkých objemov textových údajov alebo otázky spojené s dynamickými zmenami v právnych predpisoch.[10] Výskum **Barysė a Sarela** indikuje, že názory verejnosti a názory právnikov na používanie modelov strojového učenia v praxi, či v súdnictve sú odlišné. V rámci svojho výskumu zistili, že zatiaľ čo verejnosť je viac otvorená automatizácii pri zhromažďovaní a analýze informácií, menej priaznivo už vníma použitie umelej

[8] COLLENETTE, Joe – ATKINSON, Katie – BENCH-CAPON, Trevor: Explainable AI tools for legal reasoning about cases: A study on the European Court of Human Rights. In: Artificial Intelligence, Roč. 317, č. 103861 (2023), s. 1-22. DOI: https://doi.org/10.1016/j.artint.2023.103861

[9] ENGEL, Christoph – LINHARDT, Lorenz – SCHUBERT, Marcel: Code is law: how COMPAS affects the way the judiciary handles the risk of recidivism. In: Artificial Intelligence and Law, Roč. 32, č. 2 (2024), s. 117–146. DOI: https://doi.org/10.1007/s10506-024-09389-8.

[10] CAMPBELL, Ray Worthy: Artificial Intelligence in the Courtroom: The Delivery of Justice in the Age of Machine Learning. In: University of Illinois Law Review, (2020), s. 323-348. DOI: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4425791_code1272853.pdf?abstractid=4425791&mirid=1

inteligencie pri samotnom rozhodovaní a implementácii súdnych rozhodnutí. Autori uvádzajú, že verejnosť môže byť skeptická voči automatizovaným rozhodnutiam, najmä ak ide o rozhodovanie v citlivých oblastiach. Autori zastávajú názor, že právnici a sudcovia majú tendenciu byť opatrnejší, keď sa umelá inteligencia používa vo fázach rozhodovacieho procesu, ktoré majú priamy vplyv na výsledok súdneho sporu.[11] Využitie modelov strojového učenia v oblasti práva prináša mnoho výhod, avšak aj technických výziev. **Schepers a jej tím** analyzovali, ako sa techniky strojového učenia môžu použiť na predikciu citácií v rozhodnutiach holandských súdov. Ich výskum odhalil problémy s dĺžkou právnych textov, ktoré často presahujú kapacitu súčasných modelov, avšak dospeli k záveru, že pomocou NLP (*natural language processing*) je možné predpovedať, či bude rozhodnutie holandského súdu citované iným súdom. Spracované dáta pochádzali z holandského súdneho systému (www.rechtspraak.nl) a zahŕňajú rozhodnutia od najnižších súdov až po najvyšší súd. Použité boli techniky strojového učenia, ako je SVM (*Support Vector Machine*), na predikciu, či budú rozhodnutia citované. Modely boli trénované na historických dátach a testované na neskorších rozhodnutiach, pričom boli porovnávané rôzne kombinácie vlastností rozhodnutí, ako textové vlastnosti a metadáta. Model analyzoval rôzne charakteristiky rozhodnutí, ako napríklad dĺžku textu, počet odsekov, prítomnosť špecifických pojmov, odkazy na predchádzajúce rozhodnutia a legislatívu. Využívané boli aj n-gramy, teda sekvencie slov, ktoré umožnili modelu identifikovať dôležité časti textu, ktoré súvisia s mierou citovanosti. Metadátové modely, ktoré využívali len základné informácie o rozhodnutiach (bez textu), dosiahli takmer porovnateľné výsledky s textovými modelmi, čo naznačuje, že aj jednoduchšie modely môžu poskytovať užitočné informácie o tom, ako často je rozhodnutie citované.[12] Významnú výzvu taktiež predstavuje integrácia negatívnych precedensov do predikčných modelov. **Josef Valvoda** a jeho kolegovia poukázali na to, že existuje výrazná nerovnováha medzi schopnosťou modelov strojového učenia predikovať pozitívne a negatívne výsledky. Ich výskum ukázal, že väčšina súčasných modelov je optimalizovaná pre predikciu pozitívnych výsledkov, zatiaľ čo predikcia negatívnych rozhodnutí zostáva nedostatočne pokrytá. Podľa Valvodu každé rozhodnutie vytvára precedens buď rozšírením (*pozitívny precedens*), alebo zúžením právneho rámca (*negatívny precedens*). Pozitívne výsledky vedú k tomu, že právne fakty sú zahrnuté v právnom rámci, zatiaľ čo negatívne výsledky ho zužujú tým, že zamietajú nové fakty. Jeho štúdia identifikuje kľúčový problém v tom, že negatívne

[11] BARYSĖ, Dovilė – SAREL, Roee: Algorithms in the court: does it matter which part of the judicial decision-making is automated? In: Artificial Intelligence and Law, Roč. 32, č. 2 (2024), s. 117–146. DOI: https://doi.org/10.1007/s10506-022-09343-6.

[12] SCHEPERS, Iris – MEDVEDEVA, Masha – BRUIJN, Michelle – WIELING, Martijn – VOLS, Michel: Predicting citations in Dutch case law with natural language processing. In: Artificial Intelligence and Law, Roč. 32, č. 2 (2024), s. 807–837. DOI: https://doi.org/10.1007/s10506-023-09368-5.

precedensy sú často výsledkom sudcovského rozlišovania medzi prípadmi, čo je podstatne zložitejšia úloha, než aplikácia existujúceho precedensu. Preto je predikcia negatívnych výsledkov oveľa náročnejšia. Autori poukazujú na priestor pre vylepšovanie modelov a hlbšie pochopenie právnej dynamiky pri rozhodovaní súdov.[13] **Medvedeva a kolektív** si vo svojom ďalšom výskume stanovili tri hlavné úlohy: identifikáciu výsledkov súdnych rozhodnutí, kategorizáciu súdnych rozhodnutí a predikciu výsledkov súdnych rozhodnutí. Autori zdôraznili, že je dôležité pochopiť druh právnych údajov, s ktorými sa pracuje, aby sa správne určilo, ktorá úloha môže byť vykonaná, a ktorá nie. Identifikácia výsledkov znamená, že systém z celého textu súdneho rozhodnutia vyextrahuje verdikt, t. j. výroková časť rozhodnutia. Táto úloha sa často dá automatizovať jednoduchšími nástrojmi, napríklad vyhľadávaním kľúčových slov. Kategorizácia rozhodnutí na základe výsledkov zahŕňa klasifikáciu súdnych dokumentov na základe rozhodnutia, pričom sa z textu odstránia priame odkazy na verdikt. Tento proces môže byť užitočný na identifikáciu faktorov, ktoré majú vplyv na rozhodnutie. Proces predikcie výsledku rozhodnutia spočíva v nasledujúcich bodoch:

a) Zber údajov – základom pre predikciu súdnych rozhodnutí sú dáta, ktoré sú k dispozícii pred vynesením rozsudku. Tieto môžu zahŕňať napríklad písomné podania strán sporu, informácie zo súdov nižšej inštancie alebo fakty uvedené v komunikácii medzi stranami a súdom (napr. prípady komunikované Európskym súdom pre ľudské práva, ktoré zahŕňajú fakty predložené sťažovateľom);
b) Predspracovanie údajov – z textu je potrebné odstrániť informácie, ktoré by mohli priamo odkazovať na výsledok prípadu, aby systém nepredpovedal na základe týchto údajov, ale na základe informácií, ktoré boli dostupné pred rozhodnutím;
c) Kategorizácia údajov – údaje sa následne rozdelia na tréningové a testovacie množiny. Tréningová množina obsahuje historické prípady, z ktorých sa model učí vzory, zatiaľ čo testovacia množina obsahuje prípady, ktoré neboli použité na tréning a slúžia na overenie presnosti modelu;
d) Tréning modelu – pri použití strojového učenia sa model trénuje na základe vstupných dát a výsledkov (verdiktov) historických súdnych rozhodnutí. Model sa „učí" vzťahy a vzorce medzi vstupnými faktami a konečnými rozhodnutiami. Tréning modelu môže zahŕňať rôzne metódy, napríklad *Support Vector Machines (SVM)*, neurónové siete alebo iné algoritmy strojového učenia.

[13] VALVODA, Jozef – COTTERELL, Ryan – TEUFEL, Simone: On the Role of Negative Precedent in Legal Outcome Prediction. In: Transactions of the Association for Computational Linguistics, Roč. 11 (2023), s. 34-48. DOI: https://doi.org/10.1162/tacl_a_00532.

e) Testovanie a vyhodnotenie modelu – model sa testuje na nových prípadoch, ktoré neboli použité počas tréningu. Výkonnosť modelu sa meria pomocou veličín ako presnosť (*accuracy*) alebo F1 skóre, ktoré kombinujú presnosť a vyvolanie (*precision a recall*). Tieto veličiny hodnotia výšku kvality predpovedania nových prípadov takýmto modelom.

f) Predikcia – keď je model vyškolený, môže byť použitý na predikciu výsledkov nových súdnych prípadov. Predikcia je založená na vstupe dostupných informácií pred rozhodnutím a na vzoroch, ktoré sa model naučil počas tréningu.

g) Vysvetlenie výsledkov – niektoré modely umožňujú posúdenie miery dôležitosti rôznych faktorov, ktoré mali vplyv na rozhodnutie. Táto funkcia je obzvlášť dôležitá, pretože zabezpečuje vysvetliteľnosť rozhodnutia.

Medvedeva zdôrazňuje, že predikcia súdnych rozhodnutí je veľmi náročná úloha, a jej presnosť závisí od kvality a typu vstupných údajov, ako aj od použitého algoritmu strojového učenia. Autorský kolektív poukázal taktiež na potrebu jasnejšej terminológie a metodológie v tejto oblasti, pričom podľa ich názoru zohráva kľúčový význam interdisciplinárna spolupráca medzi technickými odbormi a právnikmi za účelom zlepšenia výsledkov výskumu.[14] S týmto názorom sa stotožňujeme.

Overenie výskumných predpokladov

Hypotézu č. 1 považujeme na základe záverov obsiahnutých vo výskumoch Medvedeva, Vols a Wieling (2019), ktorý preukázal, že NLP modely môžu dosiahnuť presnosť až 75 % pri predikcii výsledkov ESĽP a tiež na základe výsledkov Habernala a kolegov (2023), ktorí zistili, že modely môžu úspešne extrahovať právne argumenty s presnosťou až 97 %, **za potvrdenú**. **Hypotézu č. 2** potvrdzujú najmä výskumy Medvedevy a kolegov (2019) a Habernala a kolektívu (2023), ktoré indikujú, že automatizované modely dokážu spracovať veľké množstvo dát a to oveľa rýchlejšie ako ľudia, a zároveň poskytujú konzistentné a presné predpovede. Zastávame názor, že využitie modelov strojového učenia môže efektívne zmierniť pracovnú záťaž právnikov.

Záver

V rámci predkladaného príspevku sa integrácia prediktívnej analýza javí ako vysoko prínosná pre súdnictvo, čím považujeme výskumnú otázku za zodpovedanú. Samozrejme nie je možné nazerať na túto problematiku čierno-bielo, ale je potrebné

[14] MEDVEDEVA, Masha – WIELING, Martijn – VOLS, Michel: Rethinking the field of automatic prediction of court decisions. In: Artificial Intelligence and Law, Roč. 31, č. 2 (2023), s. 195–212. DOI: https://doi.org/10.1007/s10506-021-09306-3.

realizovať komplexné skúmanie týchto systémov, ktoré doslovne každým dňom napredujú a rozširujú svoje schopnosti a možnosti. Považujeme za potrebné upriamiť pozornosť v rámci výskumu na túto oblasť a sústrediť sa na hlavné problémy a technické výzvy spojené s využívaním umelej inteligencie, teda modelov strojového učenia, prirodzeného spracovania jazyka a extrakcie dát ako pomôcky pre advokátov či sudcov. Vyjadrujeme presvedčenie, že postupom času bude možné vykonávať pomocou modelov strojového učenia a spracovania prirodzeného jazyka prediktívnu analýzu na takej úrovni, ktorá bude bez predsudkov obsiahnutých v historických údajoch, bude možné vidieť celý proces, akým model dospel k rozhodnutiu, t. j. bude prítomný faktor *explainability* a taktiež bude možné analyzovať dáta, ktoré sú textovo rozsiahle a zároveň analýza nebude obmedzená na jednotlivý prípad, ale bude zohľadňovať vzájomné súvislosti medzi prípadmi. Ťažko skrývať nadšenie autorov nad tým, čo výskum v tejto oblasti v najbližších rokoch prinesie.

Zoznam použitej literatúry

1. BARYSĖ, Dovilė – SAREL, Roee: Algorithms in the court: does it matter which part of the judicial decision-making is automated? In: Artificial Intelligence and Law, Roč. 32, č. 2 (2024), s. 117–146. DOI: https://doi.org/10.1007/s10506-022-09343-6.
2. BENEDETTO, Irene – KOUDOUNAS, Alkis – VAIANI, Lorenzo – PASTOR, Eliana – CAGLIERO, Luca – TARASCONI, Francesco – BARALIS, Elena: Boosting court judgment prediction and explanation using legal entities. In: Artificial Intelligence and Law, (2024), s. 1-20. DOI: https://doi.org/10.1007/s10506-024-09397-8.
3. CAMPBELL, Ray Worthy: Artificial Intelligence in the Courtroom: The Delivery of Justice in the Age of Machine Learning. In: University of Illinois Law Review, (2020), s. 323-348. DOI: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID4425791_code1272853.pdf?abstractid=4425791&mirid=1.
4. COLLENETTE, Joe – ATKINSON, Katie – BENCH-CAPON, Trevor: Explainable AI tools for legal reasoning about cases: A study on the European Court of Human Rights. In: Artificial Intelligence, Roč. 317, č. 103861 (2023), s. 1-22. DOI: https://doi.org/10.1016/j.artint.2023.103861
5. ENGEL, Christoph – LINHARDT, Lorenz – SCHUBERT, Marcel: Code is law: how COMPAS affects the way the judiciary handles the risk of recidivism. In: Artificial Intelligence and Law, Roč. 32, č. 2 (2024), s. 117–146. DOI: https://doi.org/10.1007/s10506-024-09389-8.

6. HABERNAL, Ivan – FABER, Daniel – RECCHIA, Nicola – BRETTHAUER, Sebastian – GUREVYCH, Iryna – SPIECKER GENNANT DÖHMANN, Indra – BURCHARD, Christoph: Mining legal arguments in court decisions. In: Artificial Intelligence and Law, Roč. 32, č. 2 (2024), s. 557–594. DOI: https://doi.org/10.1007/s10506-023-09361-y.
7. HOU, Yifan – CHENG, Ge – ZHANG, Yun – ZHANG, Dongliang: Methods of incorporating common element characteristics for law article prediction. In: Artificial Intelligence and Law, Roč. 32, č. 4 (2023), s. 487–503. DOI: https://doi.org/10.1007/s10506-023-09359-6
8. MEDVEDEVA, Masha – WIELING, Martijn – VOLS, Michel: Rethinking the field of automatic prediction of court decisions. In: Artificial Intelligence and Law, Roč. 31, č. 2 (2023), s. 195–212. DOI: https://doi.org/10.1007/s10506-021-09306-3.
9. MEDVEDEVA, Masha – VOLS, Michel – WIELING, Martijn: Using machine learning to predict decisions of the European Court of Human Rights. In: Artificial Intelligence and Law, Roč. 28, č. 2 (2019), s. 237-266. DOI: https://doi.org/10.1007/s10506-019-09255-y.
10. SCHEPERS, Iris – MEDVEDEVA, Masha – BRUIJN, Michelle – WIELING, Martijn – VOLS, Michel: Predicting citations in Dutch case law with natural language processing. In: Artificial Intelligence and Law, Roč. 32, č. 2 (2024), s. 807–837. DOI: https://doi.org/10.1007/s10506-023-09368-5.
11. VALVODA, Jozef – COTTERELL, Ryan – TEUFEL, Simone: On the Role of Negative Precedent in Legal Outcome Prediction. In: Transactions of the Association for Computational Linguistics, Roč. 11 (2023), s. 34-48. DOI: https://doi.org/10.1162/tacl_a_00532.
12. VUONG, Yen Thi-Hai – BUI, Quan Minh – NGUYEN, Ha-Thanh – NGUYEN, Thi-Thu-Trang – TRAN, Vu Minh – PHAN, Xuan-Hieu – SATOH, Ken – NGUYEN, Le-Minh: SM-BERT-CR: a deep learning approach for case law retrieval with supporting model. In: Artificial Intelligence and Law, Roč. 31, č. 2 (2023), s. 601–628. DOI: https://doi.org/10.1007/s10506-022-09319-6.

Kontaktné údaje

Mgr. Andrej Oriňak
andrej.orinak@student.upjs.sk
Univerzita Pavla Jozefa Šafárika v Košiciach, Právnická fakulta
Katedra obchodného a hospodárskeho práva
doc. JUDr. Regina Hučková, PhD.
regina.huckova@upjs.sk
Univerzita Pavla Jozefa Šafárika v Košiciach, Právnická fakulta
Katedra obchodného a hospodárskeho práva

OSNOVA A TÉZY NOVEJ PRÁVNEJ ÚPRAVY ZAISŤOVANIA DIGITÁLNYCH ÚDAJOV V TRESTNOM KONANÍ[1]

OUTLINE AND THESIS OF A NEW LEGISLATION ON THE SEIZURE OF DIGITAL DATA IN CRIMINAL PROCEEDINGS

Petra Dražová, [2], Marek Kordík[3]

Abstrakt: Príspevok sa zaoberá tézami a princípmi právnej úpravy zaisťovania digitálnych údajov v trestnom konaní de lege ferenda, a to aj s prihliadnutím na rozhodovaciu prax Súdneho dvora EÚ k plošnému zaisťovaniu údajov a legislatívy v tejto oblasti.

Kľúčové slova: digitálne údaje, odpočúvanie, prevádzkové údaje, lokalizačné údaje, obsahové údaje

Abstract: The paper deals with the theses and principles of de lege ferenda legal regulation of digital data seizure in criminal proceedings, taking into account the decision-making practice of the Court of Justice of the European Union on blanket data seizure as well as the respective legislation.

Keywords: digital data, interception, traffic data, location data, content data

Úvod

Slovenská právna úprava zaisťovania počítačových údajov do trestného konania je atomizovaná a množstvo podstatných otázok necháva nezodpovedaných[4] a

[1] Príspevok je podporený projektom APVV-23-0519, Právne a technické výzvy inteligentnej mobility na zvýšenie bezpečnosti cestnej premávky.

[2] Univerzita Komenského v Bratislave, Právnická fakulta

[3] Univerzita Komenského v Bratislave, Právnická fakulta

[4] Uchovávanie a sprístupňovanie obsahu už uloženej komunikácie v zariadení, alebo na serveroch, nakoľko ide o porušenie telekomunikačného tajomstva, resp. tajomstva prepravovaných správ, použitie agenta vo virtuálnom prostredí, využitie prístupových údajov k elektronickej pošte, resp. profilu užívateľa, o ktorých sa dozvedeli orgány činné v trestnom konaní a súdy inak, než od dotknutej osoby (napr. pri odpočúvaní a zázname telekomunikačnej prevádzky podľa §115 zákona č. 301/2005 Z.z. Trestný poriadok v znení neskorších predpisov. Uchovávanie prevádzkových a lokalizačných údajov subjektmi, ktoré neboli resp. nie sú regulované zákonom č. 452/2021 Z. z. o elektronických komunikáciách v znení neskorších predpisov (ďalej len „*ZoEK*") ako telekomunikačný operátor - banky, iné subjekty finančného sektora, resp. subjekty, ktoré

nepokrýva komplexne potreby aplikačnej praxe pri zaisťovaní digitálnych dôkazov v trestnom konaní.[5] Aplikácia jednotlivých nástrojov na získavanie dôkazov je nejednotná a súčasne každý z týchto nástrojov je primárne určený na iný účel, s výnimkou ustanovenia § 91 Trestného poriadku, § 115 a § 116 Trestného poriadku. Čiastkové zmeny Trestného poriadku v otázke zaisťovania digitálnych dôkazov sa zameriavali najmä na odpočúvanie a zákonné podmienky jeho použitia, resp. novú úpravu uchovávania prevádzkových a lokalizačných údajov po rozhodnutí Ústavného súdu SR[6].

Súčasne je potrebné zdôrazniť, že autonómna zmena ustanovení Trestného poriadku bez potrebného premietnutia do zmien odvetvových predpisov[7]

---

zabezpečujú proces platieb (poskytovatelia služieb kryptoaktív, poskytovatelia platobných služieb - agregátory, platobné brány), subjekty poskytujúce autorizačné a verifikačné služby (najmä tokeny), štátne orgány , sprostredkovatelia ubytovacích kapacít alebo zdieľaných služieb prepravy osôb, subjekty kybernetickej bezpečnosti prijímajúce bezpečnostné opatrenia.

[5] Za súčasného stavu je možné digitálne dôkazy získavať do trestného konania použitím dožiadania podľa § 3 Trestného poriadku vrátane údajov, ktoré tvoria predmet bankového tajomstva podľa § 3 ods. 5 Trestného poriadku, vydaním veci podľa § 89 Trestného poriadku, uchovávaním a vydaním počítačových údajov podľa § 91 Trestného poriadku, odňatím veci podľa § 90 Trestného poriadku, prevzatím zaistenej veci podľa § 92 Trestného poriadku, prehliadkami podľa § 99 Trestného poriadku, odpočúvaním a záznamom telekomunikačnej prevádzky podľa § 115 a § 116 Trestného poriadku, použitím agenta podľa § 117 Trestného poriadku, porovnaním údajov v informačných systémov podľa § 118 Trestného poriadku niektorých zákonov, alebo obhliadkou podľa § 154 Trestného poriadku. V prípade, že do predmetu záujmu zahrnieme aj virtuálne meny, ako zvláštnu obdobiu digitálnych údajov, ktoré majú hospodársky vyčísliteľnú hodnotu, je potrebné sem zahrnúť aj ustanovenie § 96d Trestného poriadku.

[6] ÚS SR PL. ÚS 10/2014-78. Napr. ustanovenie § 91 Trestného poriadku, ktoré predstavuje najuniverzálnejšie ustanovenie o získavaní digitálnych údajov v trestnom konaní bol rozsiahlejšie zmenený až novelou Trestného poriadku zákonom č. 312/2020 Z .z. o výkone rozhodnutia o zaistení majetku a správe zaisteného majetku a o zmene doplnení, , pričom zmena ustanovenia bola vynútená zavedením nových zaisťovacích inštitútov pre účely odčerpávania výnosov z trestnej činnosti a nešlo o zmeny, ktorými by sa riešilo získavanie digitálnych dôkazov.
Ustanovenie § 115 Trestného poriadku bolo zmenené novelou č. 214/2019 Z. z., č. 312/2020 Z. z. a novelou č. 40/2024, pričom v zásade vždy došlo k čiastkovým zmenám rozsahu trestných činov, pri ktorých je možné odpočúvať resp. zapracovanie judikatúry NSSR o použiteľnosti dôkazu získaného odpočúvaním v inej trestnej veci a pod.

[7] Napr. zákon č. 483/2001 Z. z. o bankách a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákon č. 22/2004 o elektronickom obchode a o zmene a doplnení zákona č. 128/2002 Z. z. o štátnej kontrole vnútorného trhu vo veciach ochrany spotrebiteľa a o zmene a doplnení niektorých zákonov v znení zákona č. 284/2002 Z. z. zákon č.305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov; zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení neskorších predpisov.

upravujúcich uchovávanie digitálnych údajov, bude nedostatočná a samotný problém neriešiaca.[8]

Prístup k digitálnym údajom používateľa resp. k digitálnej identite entity

Či už ide o užívateľské údaje, ktoré osoba poskytla prevádzkovateľovi online platformy, poskytovateľovi služby elektronickej pošty, aplikácie pri zriadení resp. založení užívateľského profilu alebo údaje, ktoré užívateľský účet generuje bez aktívneho pričinenia človeka (napr. prevádzkové údaje) - v zásade sa jedná o rôznorodé údaje viažuce sa k určitému profilu, resp. užívateľskému kontu ako meno, priezvisko, mail určený pre obnovu konta, telefónne číslo pre účely dvojstupňového overovania, fotografie, identifikačný doklad a pod. podľa všeobecných podmienok poskytovania služby prevádzkovateľom.

V zásade možno uviesť, že účelom užívateľských údajov, ktoré sa zadávajú pri registrácií profilu resp. užívateľského konta, je identifikácia a overenie totožnosti užívateľa profilu. Pričom predmetom týchto údajov nie je telekomunikačné tajomstvo.[9]

Na základe uvedeného je možné vidieť analógiu s prístupnosťou a kvalitou informácie o vlastníkovi nehnuteľnosti, motorového vozidla, zbrane, cenných papierov, alebo majetkových práv, ktoré sa štandardne získavajú dožiadaním podľa § 3 ods.1, ods. 2 Trestného poriadku.

V prípade legislatívneho riešenia prístupu k digitálnym údajom používateľa je možné zaradiť do tejto skupiny údajov údaje o základňových staniciach verejnej telefónnej siete a databázou medzinárodných označení mobilných účastníkov (IMSI) ako i pevné internet protokol (IP) adresy, ktoré osoba využíva na pripojenie do internetu na základe používanej služby.[10]

---

[8] Pre úplnosť je potrebné dodať, že Súdny dvor EÚ uvedené rozhodnutia riešil len vo vzťahu k uchovávaniu a poskytovaniu údajov elektronickej komunikácie v súlade s čl. 2 smernice EÚ 2002/58, ktorý vymedzuje elektronickú komunikačnú službu a nie vo vzťahu k iným subjektom, ktoré však rovnako poskytujú služby v digitálnom priestore Súdny dvor nevylúčil, aplikáciu týchto ustanovení aj na iné subjekty, viac v: Rozsudok Súdneho Dvora EÚ vo veci C-511/18, C-512/18, 520/18, *La Quadrature*, para. 203-205, dostupné na: CURIA - Documents (europa.eu), a Rozsudok Súdneho dvora EÚ vo veci C 142/18, EU:Skype Communications, para. 37, dostupné na: CURIA – Dokumenty (europa.eu).

[9] §112 ods.1, písm. b) ZoEK *a contrario.*

[10] §117 ods. 5 ZoEK

Uvedené údaje sa poskytujú podľa platného právneho stavu však len štátnym orgánom[11] mimo rámec trestného konania[12], na základe žiadosti a prostredníctvom stáleho a nepretržitého prístupu k týmto údajom. Keďže uvedený režim je použiteľný pre spravodajské účely, za sa vhodný aj pre použitie postupu orgánov činných v trestnom konaní.
Vzhľadom na skutočnosť, že tieto údaje majú identifikačný charakter používateľa a jeho služby, aj vzhľadom na dikciu §117 ods. 5 ZoEK zaradiť tieto údaje pod režim dožiadania podľa § 3 ods.1, ods. 2 Trestného poriadku, pričom povinným dožiadaným subjektom by bol ten, kto má tieto údaje u seba. Podmienkou poskytnutia týchto údajov by malo byť ich oddelenie od akejkoľvek uskutočnenej konkrétnej komunikácie[13] resp. s iným subjektom, kedy by sa údaj napr. o IP adrese považoval už za predmet telekomunikačného tajomstva.[14]

Prístup k škodlivému digitálnemu obsahu, nezákonnému digitálnemu obsahu vrátane teroristického obsahu, alebo digitálnemu obsahu potrebnému pre účely dokazovania

Nová právna úprava získavania, dokumentovania a následného použitia digitálneho obsahu v trestnom konaní ako dôkazu by mala vychádzať z filozofie, že tento obsah je prístupný verejne alebo neverejne na diaľku, bez faktickej kontroly zariadenia, alebo dátového nosiča, na ktorom je uložený. V praxi sa jedná najmä o rôzne obrazové, zvukové, obrazovo-zvukové záznamy, textové záznamy alebo obsahy

[11] Podľa § 109 ods. 9 ZoEK sa týmto orgánom štátu rozumie:
- ozbrojený bezpečnostný zbor,
- ozbrojený zbor a
- štátny orgán, ktorý v rozsahu ustanovenom osobitnými predpismi (zákon č. 46/1993 Z. z. (o Slovenskej informačnej službe) v znení neskorších predpisov; zákon č. 171/1993 Z. z. (o Policajnom zbore) v znení neskorších predpisov; zákon č. 198/1994 Z. z. (o Vojenskom spravodajstve) v znení neskorších predpisov; zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) a o zmene a doplnení niektorých zákonov v znení neskorších prepisov; zákon č. 35/2019 Z. z. (o finančnej správe) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov) plní úlohy na úseku:
  - ochrany ústavného zriadenia,
  - obrany štátu,
  - vnútorného poriadku,
  - bezpečnosti štátu a
  - správy daní.

  Na účely plnenia úloh na úseku ochrany ústavného zriadenia, vnútorného poriadku, bezpečnosti štátu, obrany štátu a správy daní môže štátny orgán spracúvať a uchovávať údaje účastníkov získané od podniku podľa tohto zákona.

[12] §117 ods. 5 ZoEK, prvá veta.

[13] Kto, s kým, po akú dlhú dobu a kde sa zariadenie v čase komunikácie nachádzalo.

[14] §112 ods. 5 ZoEK.

webových stránok a úložísk. Súčasná právna úprava za týmto účelom používa ustanovenie § 91 Trestného poriadku o uchovávaní a vydaní počítačových údajov alebo obhliadku podľa § 154 Trestného poriadku. Nová právna úprava by mala zohľadňovať normatívnu povinnosť používať *hash* techniku pri dokumentovaní obsahu. Súčasne by nová právna úprava mala reagovať aj na požiadavku zabránenia prístupu k škodlivému obsahu alebo nezákonnému obsahu, tak ako i následného odstránenia obsahu, tak ako to predpokladá aj súčasné znenie § 91 Trestného poriadku. Z pohľadu novej právnej úpravy je na mieste rovnako vyriešiť otázku lehoty tohto príkazu resp. subjektu, ktorý by ho mal vydávať a súčasne by nová právna úprava mala zohľadniť previazanosť s ustanoveniami § 151 a nasl. zákona č. 264/2022 Z.z. o mediálnych službách a o zmene a doplnení niektorých zákonov (zákon o mediálnych službách) v znení neskorších predpisov.

Prístup k prevádzkovým a lokalizačným údajom na diaľku bez faktickej kontroly zariadenia

Druhým okruhom prípadov digitálnych údajov ,ktoré by mala nová právna úprava riešiť je uchovávanie a prístup k lokalizačným údajom, ktorých plošné uchovávanie bolo po rozhodnutí Ústavného súdu v SR vylúčené.[15] Ustanovenia ZoEK, ktoré stratili po rozhodnutí ÚS SR platnosť neboli nahradené novou úpravou a vzniklo tak právne vákuum, ktoré trvá dodnes.[16]

Princíp časovej obmedzenosti uchovávania digitálnych údajov

Vo vzťahu k prístupu k uchovávaným dátam požiadavka nevyhnutnosti súčasne znamená stanovenie lehoty uchovávania, zničenie údajov po skončení doby uchovávania a súdny prieskum.[17] Nie je možné preventívne uchovávanie ani v boji s organizovanou trestnou činnosťou.[18] Výnimku tvorí preventívne uchovávanie v prípade ohrozenia bezpečnosti, ktorá je akútna a predvídateľná, len po nevyhnutnú

---

[15] Ústavný súd SR vo veci PL. ÚS 10/2014-78. Pre kompletnú genézu rozhodnutí vo vzťahu k plošnému uchovávaniu prevádzkových a lokalizačných údajov a dopad týchto rozhodnutí na legislatívu pozri Beleš, A.; Uchovávanie a oznamovanie údajov o elektronickej komunikácií, Univerzita Komenského v Bratislave, Právnická fakulta, 2022, ISBN: 978-80-7160-637-6

[16] Uvedená situácia neplatí len vo vzťahu k SR, ale v zásade vo vzťahu k väčšine členských štátov EÚ, kde došlo obdobne k zneplatneniu právnej úpravy plošného uchovávania prevádzkových a lokalizačných údajov.

[17] Rozsudok Súdneho Dvora EÚ vo veci C-203/15, *Tele 2 Sverige*. Dostupné na: https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=SK&mode=lst&dir=&occ=first&part=1&cid=6375439

[18] Rozsudok Súdneho Dvora EÚ vo veci C-793/19, *SpaceNet.* Dostupné na: https://curia.europa.eu/juris/document/document.jsf?text=&docid=265881&pageIndex=0&doclang=sk&mode=lst&dir=&occ=first&part=1&cid=771573.

dobu a musí podliehať súdnemu prieskumu. Princípy novej legislatívy upravujúce dobu uchovávania a prístup k prevádzkovým údajom a lokalizačným údajom poskytovateľov elektronických komunikačných služieb, alebo iných subjektov informačnej spoločnosti sa môže v závislosti od údajov líšiť, v závislosti od toho, či ide o IP adresu, prevádzkové a lokalizačné údaje k hlasovej komunikácií, alebo k textovej komunikácií.

Princíp adresného uchovávania digitálnych údajov

Vo vzťahu k uchovávaniu a poskytovaniu údajov z dôvodu odhaľovania a objasňovania trestných činov, by poskytovanie týchto údajov malo byť naviazané na údaje máp kriminality vo forme presiahnutia určitého percentilu[19] na danú oblasť[20], resp. počtu závažných trestných činov na 1000 obyvateľov napr. v posledných 3 rokoch v jednotlivých okresoch.

Druhou možnosťou je, že ide o osoby identifikované ako hrozby pre verejnú alebo národnú bezpečnosť, alebo ktorých prevádzkové alebo lokalizačné údaje môžu súvisieť so závažnou trestnou činnosťou;[21] pričom hrozba musí byť skutočná, aktuálna a predvídateľná.[22]

Treťou možnosťou adresného uchovávania dát je podľa názoru Súdneho dvora EÚ aj odôvodnenie, že ide o miesto s vyšším rizikom výskytu bezpečnostného incidentu (napr. teroristický útok, rizikový zápas, významná politická udalosť preprava jadrového materiálu, zbraní)[23] alebo s významným prvkom kritickej infraštruktúry (napr. jadrová elektráreň, energetické, telekomunikačné uzly a ústredne) alebo

---

[19] Rozsudok Súdneho Dvora EÚ vo veci C-203/15, *Tele 2 Sverige*, para. 117-119. Dostupné na: https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=SK&mode=lst&dir=&occ=first&part=1&cid=6375439

[20] Napr. Mapy kriminality. Policie České republiky. Dostupné na: https://kriminalita.policie.cz/

[21] Rozsudok Súdneho Dvora EÚ vo veci C-511/18, C-512/18, 520/18 *La Quadrature*, para. 147-148. Dostupné na: CURIA - Documents (europa.eu). Je potrebné uviesť, že citovaný rozsudok para. 165-166 *expressis verbis* analyzuje aj možnosť urýchleného uchovávania podľa čl. 16 Dohovoru o počítačovej kriminalite (Oznámenie MZV SR č. 137/2008 Z.z.) s poukazom na čl. 15 ods. 1 smernice Európskeho parlamentu a Rady 2002/58/ES uviedol, že úprava okamžitého uchovávania je v rukách zákonodarcu, avšak vzhľadom na zásah do súkromia pri tzv. preventívnom uchovávaní údajov, by tento zásah mal byť vyvážený závažnosťou trestného činu, ktorého spáchanie hrozí, alebo sa pripravuje, nemalo by teda ísť o akýkoľvek trestný čin, resp. každý trestný čin. Avšak takéto konanie môže byť ohrozením verejnej, alebo národnej bezpečnosti. Súd súčasne naznačil, že dôvody pre okamžité uchovávanie sa nesmú zamieňať.

[22] Rozsudok Súdneho Dvora EÚ vo veci C-511/18, C-512/18, 520/18, *La Quadrature*, para.: 137. Dostupné na: CURIA - Documents (europa.eu)

[23] Rozsudok Súdneho Dvora EÚ vo veci C-203/15, *Tele 2 Sverige*, para. 117-119. Dostupné na: https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=SK&mode=lst&dir=&occ=first&part=1&cid=6375439

miesta s veľkým výskytom osôb (letiská, stanice, oblasti platenia mýta)[24], ale súčasne je splnený niektorý z predpokladov vyššie t. j., že sa tam môže/bude nachádzať osoba identifikovaná ako hrozba pre verejný poriadok alebo ide o oblasť so zvýšenou mierou kriminality.[25]

Boj proti závažnej trestnej činnosti, hlavne jej organizovaným formám, aj keď je legitímnym cieľom, nemôže sám osebe odôvodniť to, aby sa vnútroštátna právna úprava, ktorá stanovuje všeobecné a nediferencované uchovávanie všetkých údajov o prenose dát a polohe, považovala za nevyhnutnú na uvedený účel.[26]

Prípustnosť primeranej automatickej analýzy

Nová právna úprava zaisťovania a použitia digitálnych údajov v trestnom konaní by mala zohľadniť i možnosť automatickej analýzy prevádzkových údajov a lokalizačných údajov, ktorá je možná, ale je potrebné zaviesť určité ľudskoprávne záruky.[27] Ide najmä o kritéria a vzory automatickej analýzy týchto údajov, ktoré musia byť spoľahlivé a konkrétne a nesmú byť založené výlučne na analýze citlivých údajov.[28] Súčasne je potrebné, aby pozitívny výsledok automatizovanej analýzy bol pred prijatím rozhodnutia, ktoré má môže mať vplyv na práva a povinnosti dotknutej osoby, podrobený neautomatizovanému individuálnemu preskúmaniu.[29]

Princíp všeobecnej úpravy a princíp technologickej neutrality

Budúca právna úprava by mala upustiť od chápania prevádzkových a lokalizačných údajov ako údajov, ktoré majú poskytovať na základe súčinnosti výlučne telekomunikační operátori. Sme toho názoru, že prístup k uchovávaniu údajov je potrebný pre účinné vyšetrovanie, najmä v cezhraničných prípadoch. Súčasne je potrebné, aby každé riešenie uchovávania a prístupu k prevádzkovým a lokalizačným údajom bolo technologicky neutrálne, jednak z dôvodu, aby sa mohlo využívať aj pri

---

[24] Rozsudok Súdneho Dvora EÚ vo veci C-511/18, C-512/18, 520/18 *La Quadrature*, para. 150. Dostupné na: CURIA - Documents (europa.eu)

[25] Rozsudok Súdneho Dvora EÚ vo veci C-203/15, *Tele 2 Sverige*, *mutatis mutandis* para. 117-119. Dostupné na: https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=SK&mode=lst&dir=&occ=first&part=1&cid=6375439

[26] Rozsudok Súdneho Dvora EÚ vo veci C-203/15, *Tele 2 Sverige*. Dostupné na: https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=SK&mode=lst&dir=&occ=first&part=1&cid=6375439

[27] Výrok Rozsudku Súdneho Dvora EÚ vo veci C-511/18, C-512/18, 520/18, *La Quadrature*. Dostupné na: CURIA - Documents (europa.eu)

[28] Rozsudok Súdneho Dvora EÚ vo veci C-511/18, C-512/18, 520/18, *La Quadrature*, para. 181. Dostupné na: CURIA - Documents (europa.eu), ktorými by boli výlučne údaje o náboženstve, rase, príslušnosti k etnickej skupine, pohlaví atď.

[29] Tamtiež.

neustálom technickom vývoji a súčasne aby bolo použiteľné pre všetkých poskytovateľov vrátane malých resp. regionálnych subjektov.[30]

Pojmológia

Nová právna úprava by mala upustiť od pojmu počítačový údaj (*computer data*) a používať pojem digitálny údaj, ktorý vystihuje špecifickú podstatu a význam týchto údajov lepšie a súčasne nezvádza k jeho chápaniu ako výlučného produktu činnosti výpočtovej techniky, resp. určitého zariadenia. Na druhej strane však autori uznávajú, že tento zažitý pojem v aplikačnej praxi nespôsobuje problémy, i keď je vývojovo prekonaný.

Záver

Judikatúru Súdneho dvora EÚ ako i Ústavného súdu SR je potrebné prakticky uplatňovať, s čím sú spojené nemalé ťažkosti, ktoré znižujú účinnosť vyšetrovania trestných činov,[31] (t. j. cielené uchovávanie údajov na základe geografických kritérií a kategórií osôb). Vzhľadom na tieto úvahy by nový režim mal byť zameraný nielen na uchovávanie, ale aj na prístup k údajom. V zásade vychádzame z toho, že kritéria na uchovávanie údajov, z pohľadu praktickej aplikácie rozhodnutí Súdneho dvora by mali, respektíve mohli byť odlišné od kritérií prístupu k týmto údajom.[32] Na základe uvedeného je harmonizovaný prístup k uchovávaniu údajov až na úrovni EÚ nevyhnutný. Európska únia prijala, respektíve členské štáty využívajú viaceré právne nástroje, ktorými sa uľahčuje prístup k digitálnym dôkazom, avšak absencia povinností uchovávať údaje negatívne ovplyvňuje efektivitu postupu orgánov činných v trestnom konaní, keďže neexistuje povinnosť údaje uchovávať.[33] Tento právny rámec by mal taktiež upraviť rozsah metadát, ktorý by mali poskytovatelia služieb uchovávať, nakoľko súčasný právny rámec túto informáciu neposkytuje, resp.

---

[30] Pracovný dokument Skupiny na vysokej úrovni (HLG) k uchovávaniu dát. Dostupné na: https://data.consilium.europa.eu/doc/document/ST-7184-2023-REV-1/en/pdf

[31] Pracovný dokument Skupiny na vysokej úrovni (HLG) k uchovávaniu dát. Dostupné na: https://data.consilium.europa.eu/doc/document/ST-7184-2023-REV-1/en/pdf
K tomu pozri aj Juszczak, A.; Sason A. (2021) Recalibrating Data Retention in the EU: The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this only the Beginning? Eucrim – The European Criminal Law Associations´ Forum. 4/2021. P. 238 – 266. Dostupné na: https://eucrim.eu/articles/recalibrating-data-retention-in-the-eu/

[32] Juszczak, A.; Sason A. (2021) *Recalibrating Data Retention in the EU: The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this only the Beginning?* Eucrim – The European Criminal Law Associations´ Forum. 4/2021. P. 238 – 266. Dostupné na: https://eucrim.eu/articles/recalibrating-data-retention-in-the-eu/

[33] Juszczak, A.; Sason A. (2021) *Recalibrating Data Retention in the EU: The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this only the Beginning?* Eucrim – The European Criminal Law Associations´ Forum. 4/2021. P. 238 – 266. Dostupné na: https://eucrim.eu/articles/recalibrating-data-retention-in-the-eu/

vychádzajúc zo zmyslu rozhodnutí Súdneho dvora ako i účelu vyšetrovania trestnej činnosti, mali by sa uchovávať iba metadáta umožňujúce identifikáciu používateľa.[34]

Zoznam použitých zdrojov

1. Dohovor o počítačovej kriminalite, oznámenie MZV SR č. 137/2008 Z. z.
2. Policie České republiky. *Mapa kriminality.* Dostupné na: https://kriminalita.policie.cz/
3. Juszczak, A.; Sason A. (2021) *Recalibrating Data Retention in the EU: The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this only the Beginning?* Eucrim – The European Criminal Law Associations´ Forum. 4/2021. P. 238 – 266. Dostupné na: https://eucrim.eu/articles/recalibrating-data-retention-in-the-eu/
4. Pracovný dokument Skupiny na vysokej úrovni (HLG) k uchovávaniu dát. Dostupné na: https://data.consilium.europa.eu/doc/document/ST-7184-2023-REV-1/en/pdf
5. rozhodnutie pléna Ústavného súdu SR vo veci PL. ÚS 10/2014-78
6. rozsudok Súdneho Dvora EÚ vo veci C-793/19, *SpaceNet*
7. rozsudok Súdneho Dvora EÚ vo veci C-511/18, C-512/18, 520/18, *La Quadrature*
8. rozsudok Súdneho Dvora EÚ vo veci C-203/15, *Tele 2 Sverige*
9. rozsudok Súdneho dvora EÚ vo veci C 193/18, *Google*
10. rozsudok Súdneho dvora EÚ vo veci C 142/18, *EU: Skype Communications*
11. rozsudok Súdneho dvora EÚ vo veci C-140/20, *Garda Sionchána*

Kontaktné údaje autorov

Mgr. Petra Dražová, PhD.
petra.drazova@flaw.uniba.sk
Ústav práva informačných technológií a práva duševného vlastníctva
Univerzita Komenského v Bratislave
Právnická fakulta

doc. JUDr. Marek Kordík, PhD., LL.M.
marek.kordik@flaw.uniba.sk
Katedra trestného práva, kriminológie a kriminalistiky
Univerzita Komenského v Bratislave
Právnická fakulta

[34] Tzv. minimálna úroveň harmonizácie uchovávania metadát (t. j. údajov potrebných na identifikáciu používateľa).

Bratislavské právnické fórum 2024
Právo a technológie v 21. storočí optikou európskeho práva
Právnická fakulta, Univerzita Komenského v Bratislave
1. vydanie

ISBN 978-80-7160-728-1

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

ISBN: 978-80-7160-728-1