

ZODPOVEDNOSŤ VEREJNEJ SPRÁVY ZA NASADENIE UMELEJ INTELIGENCIE*

MARIANNA NOVOTNÁ,** ZUZANA ADAMOVÁ,***
MICHAL MASLEN****

Abstract: **Public Administration Responsibility for the Deployment of Artificial Intelligence**

The article analyzes legal aspects of public administration liability in the deployment of artificial intelligence systems, focusing on the European and Slovak legal frameworks, with reference to certain legal mechanisms of non-European origin that may serve as a source of inspiration. It identifies three main pillars of responsibility: regulatory obligations under the Artificial Intelligence Act, civil liability including specific regimes under Act No. 514/2003 Sb., and responsibility for the processing of personal data under the GDPR. The article (also in light of existing new foreign legislation regulating the use of artificial intelligence in public administration) points out the requirements placed on public institutions when using artificial intelligence and discusses the legal consequences of illegal or incorrect practices implemented through algorithms.

Keywords: public administration; artificial intelligence; legal liability; Artificial Intelligence Act; data protection; automated decision-making

Kľúčové slová: verejná správa; umelá inteligencia; právna zodpovednosť; Akt o umelej inteligencii; ochrana osobných údajov; automatizované rozhodovanie

DOI: 10.14712/23366478.2026.8

ÚVOD

Zavádzanie systémov umelej inteligencie do procesov verejnej správy predstavuje zásadnú výzvu z hľadiska právnej zodpovednosti štátu. Zodpovednosť za využívanie umelej inteligencie vo verejnej správe zahŕňa široké spektrum konceptov, ktoré sa týkajú automatizovaného rozhodovania, ochrany osobných údajov, etických

* Tento článok bol vypracovaný v rámci grantového projektu APVV č. APVV-20-0171 „Konkurencia nárokov z deliktov a kvázideliktov v mimozmluvných vzťahoch a na pomedzí zmluvného a vecného práva“.

** doc. JUDr. Marianna Novotná, PhD., univ. prof., Katedra občianskeho a obchodného práva, Právnická fakulta, Trnavská univerzita v Trnave; marianna.novotna@gmail.com.

*** JUDr. Zuzana Adamová, PhD., Ústav duševného vlastníctva, technológií a produktového práva, Právnická fakulta, Trnavská univerzita v Trnave; zuzana.adamova@gmail.com.

**** doc. JUDr. Michal Maslen, PhD., Katedra správneho práva, práva životného prostredia a finančného práva, Právnická fakulta, Trnavská univerzita v Trnave; michal.maslen@truni.sk.

otázok ako diskriminácia, otázky bezpečnosti systémov, monitorovania a hodnotenia umelej inteligencie a jej právnej regulácie. Verejné inštitúcie musia zabezpečiť, aby systémy umelej inteligencie fungovali transparentne, spravodlivo a bezpečne, pričom zodpovednosť za ich používanie a dôsledky by mali byť jasne definované a vykonávané.

Zodpovednosť verejných inštitúcií za rozhodnutia prijímané s využitím umelej inteligencie sa opiera o viaceré právne rámce – od vnútroštátnej úpravy zodpovednosti za škodu spôsobenú výkonom verejnej moci, až po európske právne predpisy, ako sú nariadenie GDPR¹ či Akt o umelej inteligencii.²

Nasadenie umelej inteligencie v oblasti verejnej správy môže viesť k plne alebo čiastočne automatizovaným rozhodnutiam, ktoré majú priamy dopad na životné situácie občanov, napríklad pri posudzovaní žiadostí o sociálne dávky, stanovovaní daňovej povinnosti či predikcii rizika kriminality. Dnes sa už dá nájsť veľké množstvo príkladov z celého sveta, kedy k využívaniu umelej inteligencie vo verejnej správe dochádza. Správa OECD³ napríklad uvádza, že Holandsko využíva umelú inteligenciu na počítanie ľudí na rôznych miestach v centre mesta na monitorovanie dopravy a hospodárskej aktivity. Vláda Queenslandu v Austrálii využíva strojové učenie a počítačové videnie na automatické mapovanie a klasifikáciu prvkov využívania pôdy na satelitných snímkach, čím znižuje náklady na mapovanie využívania pôdy a zlepšuje reakciu na biologickú bezpečnosť a prírodné katastrofy. Počas pandémie COVID-19 v Nórsku zase použil úrad práce a sociálnych vecí konverzačnú umelú inteligenciu s názvom Frida, ktorá pomáhala občanom pri prístupe k sociálnym dávkam 24 hodín denne, 7 dní v týždni a vyriešila 80 % otázok bez toho, aby potrebovala zásah úradníka. Kanada zase pilotne zaviedla používanie algoritmu hodnotenia rizík na posúdenie a identifikáciu potenciálne rizikového nákladu pred jeho naložením do prichádzajúceho lietadla. Veľká pozornosť sa v Kanade venuje aj automatizovanému rozhodovaniu v rámci imigračného a utečeneckého systému.⁴

Na Slovensku sú tiež známe prípady využitia umelej inteligencie vo verejnej správe, pričom menovať možno chatbot TAXANA na automatizované odpovede na daňové otázky, systém eKasa,⁵ do ktorého elektronické registračné pokladnice posielajú

¹ Nariadenie (EÚ) 2016/679 Európskeho parlamentu a Rady z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov – GDPR). *Úradný vestník Európskej únie*. L 119, 4. 5. 2016.

² 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). *Úradný vestník Európskej únie*. L 202, 12. 7. 2024.

³ OECD. *Governing with Artificial Intelligence: Are Governments Ready?* [online]. OECD Artificial Intelligence Papers No. 20. OECD Publishing, June 2024 [cit. 2025-06-10]. Dostupné na: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/governing-with-artificial-intelligence_f0e316f5/26324bc2-en.pdf.

⁴ MOLNAR, P. – GILL, L. *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System* [online]. University of Toronto, 2018 [cit. 2025-12-05]. Dostupné na: <https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf>.

⁵ K systému eKasa sa v nadväznosti na otázku vymedzenia osobných údajov a využívania osobných údajov na automatizované posudzovanie jednotlivcov vo svojom náleze vyjadril i Ústavný súd SR (Nález

údaje v reálnom čase, ktoré tento systém následne hodnotí pomocou rizikovoskórovacích algoritmov a označuje transakcie ako „neplatné“, „vklad“ alebo „výber“, či analytický informačný systém rizík AIS-R – nástroj pre predikciu rizík daňového neplatenia, ktorý hodnotí jednotlivých daňovníkov automaticky a pomáha tak pri výbere subjektov na kontrolu.⁶ Podľa správy AI Watch (Európska komisia) pre Slovensko⁷ je „*public sector dimension*“ štátneho akčného plánu digitálnej transformácie zameraná na experimentálne zavádzanie umelej inteligencie v rámci tzv. inovačných laboratórií, podporu digitálnych inovačných centier, testovanie pilotných projektov na úrovni miestnych aj štátnych správ, vrátane zdieľania dát a vývoja odborných kapacít.

Samozrejme, ak umelá inteligencia postupuje alebo rozhodne nesprávne, vyvstáva otázka, kto nesie právnu zodpovednosť za negatívne následky takéhoto konania – či verejná inštitúcia ako prevádzkovateľ systému, vývojár algoritmu umelej inteligencie, alebo iný subjekt zapojený do rozhodovacieho procesu.⁸

Známy je napríklad holandský prípad automatizovaného rozhodovania v oblasti sociálnych dávok z roku 2020 „Toeslagenaffaire“, v ktorom holandská daňová správa využívala systém umelej inteligencie na detekciu podvodov pri sociálnych dávkach, ktorý nesprávne označil tisíce rodičov ako podvodníkov. Právny základ automatizovaného systému SyRI (System Risk Indication) bol upravený v roku 2014 novelou holandského zákona *Wet SUWI* a súvisiaceho *SUWI Decree*, ktorý povoľoval spracovanie až 17 kategórií osobných údajov z rôznych štátnych databáz na analýzu rizika podvodu so sociálnymi dávkami. Súd síce uznal legitímny verejný záujem boja proti podvodom, avšak konštatoval, že zákon nebol dostatočne transparentný, keďže štát odmietol sprístupniť algoritmus, indikátory a kritériá hodnotenia. Súd v tomto prípade

Ústavného súdu SR sp. zn. PL. ÚS 25/2019, zverejnený v Zbierke zákonov SR pod č. 492/2021 Z. z.). Podľa ÚS SR „kvalifikácia toho, čo je osobný údaj, závisí od toho, akými údajmi už štátny orgán disponuje a aké má právne možnosti získania ďalších informácií. Pokiaľ orgán verejnej moci spracúvajúci údaje vzhľadom na svoje právomoci a iné informácie, ktoré má k dispozícii, dokáže po vynaložení primeraného úsilia identifikovať konkrétneho jednotlivca, stále ide o osobné údaje. Je preto nepodstatné, že ide o údaje, ktoré jednotlivca neidentifikujú priamo.“ Uvedené znamená, že aj údaje, ktoré samy osebe neidentifikujú jednotlivca priamo, sú chránené, ak v kontexte iných informácií môžu viesť k jeho určeniu. Ústavný súd ďalej konštatoval, že zákonodarcu musí posúdiť, ako čo najlepšie zužitkovať benefity automatizácie bez toho, aby tým zároveň ohrozil základné hodnoty právneho štátu a miesto jednotlivca v ňom. Aktuálne neexistuje zákon, ktorý by umožňoval finančnej správe osobné údaje zo systému eKasa používať na automatizované posudzovanie jednotlivcov. Ak chce zákonodarcu umožniť takúto automatizovanú posudzovanie na základe osobných údajov, musí zabezpečiť splnenie ústavnoprávných záruk. Pri preskúmaní systému eKasa Ústavný súd rozhodol, že zber daňového identifikačného čísla (DIČ) a údajov o tovare či službách je v súlade s ústavou, keďže sleduje legitímny cieľ (boj proti daňovým únikom) a zásah do súkromia je primeraný. Naopak, zber unikátneho identifikátora kupujúceho označil za protiústavný, pretože predstavuje neodôvodnený zásah do práva na ochranu súkromia a osobných údajov.

⁶ Slovakia. In: *TAXAdmin.AI* [online]. [cit. 2025-06-10]. Dostupné na: <https://taxadmin.ai/country/slovakia-ai-country-report/>.

⁷ Public sector dimension of AI national strategies: Slovakia. In: *European Commission: AI Watch* [online]. 2019 [cit. 2025-06-12]. Dostupné na: https://ai-watch.ec.europa.eu/topics/public-sector/public-sector-dimension-ai-national-strategies/slovakia-public-sector-dimension-ai-strategy_en.

⁸ VEALE, M. – BORGESIU, F. Z. Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International* [online]. 2021, Vol. 22, No. 4, s. 97–112 [cit. 2025-06-12]. Dostupné na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852.

rozhodol, že štát porušil základné práva občanov v zmysle čl. 8 Európskeho dohovoru o ľudských právach⁹ (právo na súkromný a rodinný život), pretože nebol dodržaný „spravodlivý pomer“ medzi štátnym záujmom a ochranou individuálneho súkromia. Na základe súdneho rozhodnutia holandská vláda ukončila používanie SyRI, pričom dotknutým subjektom vznikla právna zodpovednosť za spôsobenú škodu.¹⁰ V Spojenom kráľovstve zase rezonoval prípad z roku 2019 týkajúci sa biometrickej umelej inteligencie v polícii, kedy londýnska polícia testovala systém umelej inteligencie, ktorý využíval automatizované rozpoznávanie tváří (AFR) v reálnom čase na verejných miestach. Súd aj v tomto prípade rozhodol, že systém porušil právo na súkromie v zmysle čl. 8 Európskeho dohovoru o ľudských právach a zároveň normy ochrany osobných údajov a zásady rovnosti a že štát nesie právnu zodpovednosť za neprimerané zásahy do práv občanov.¹¹

Z hľadiska ochrany ľudských práv predstavuje použitie umelej inteligencie významné riziká. Algoritmy na rozpoznávanie tváre, profilovanie osôb či predikčné modely môžu viesť k porušeniu práva na súkromie, práva na rovnosť a zákazu diskriminácie, najmä ak sú trénované na nevyvážených alebo stereotypných dátach.¹² Napríklad štúdie preukázali, že prediktívne algoritmy používané v trestnom práve môžu systematicky znevýhodňovať určité rasové alebo socioekonomické skupiny.¹³

Zodpovednosť za zabezpečenie férovosti algoritmických rozhodnutí musí byť súčasťou riadiaceho a etického rámca systémov umelej inteligencie používaných verejnou správou. Vysokorizikové oblasti, ako sú zamestnanosť, vzdelávanie alebo poskytovanie verejných služieb, vyžadujú implementáciu mechanizmov na odhaľovanie a korekciu predpojatostí v rozhodovacích algoritmoch. Verejná správa musí preto zaviesť efektívne

⁹ Európsky dohovor o ochrane ľudských práv a základných slobôd, Rím, 4. 11. 1950 (vyhl. pod č. 209/1992 Zb.).

¹⁰ Systém automatizovaného systému SyRI (System Risk Indication) využíval automatizované profilovanie (napr. dvojité občianstvo, nízky príjem, netradičný etnický pôvod ako možné znaky rizika), čo spôsobilo desaťtisícim rodičov nespravodlivé označenie a následné škody. KUŽNIACKI, B. The Dutch childcare benefit scandal shows that we need explainable AI rules. In: *University of Amsterdam* [online]. 8. 2. 2023 [cit. 2025-06-09]. Dostupné na: <https://www.uva.nl/en/shared-content/faculteiten/en/faculteit-der-rechtsgeleerdheid/news/2023/02/childcare-benefit-scandal-transparency.html>; BOUWMEESTER, M. Keeping digital welfare systems in check: Learning from the Netherlands' institutional responses to the childcare benefits scandal. In: *University of Groningen* [online]. AI Summer School blog series. KU Leuven, 24. 6. 2025 [cit. 2025-05-10]. Dostupné na: <https://research.rug.nl/en/publications/keeping-digital-welfare-systems-in-check-learning-from-the-nether/>.

¹¹ LOIDEAIN, N. Lawfulness and Police Use of Facial Recognition in the United Kingdom. In: *The Cambridge Handbook of Facial Recognition in the Modern State* [online]. Cambridge: Cambridge University Press, 2024, s. 155–172 [cit. 2025-11-10]. Dostupné na: <https://www.cambridge.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/lawfulness-and-police-use-of-facial-recognition-in-the-united-kingdom/E360D81BBF9CFAC225D6047AEC3368A8>.

¹² WACHTER, S. – MITTELSTADT, B. – FLORIDI, L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law* [online]. 2017, Vol. 7, No. 2, s. 76–99 [cit. 2025-05-18]. Dostupné na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469.

¹³ ANGWIN, J. – LARSON, J. – MATTU, S. – KIRCHNER, L. Machine Bias. In: *ProPublica* [online]. 23. 5. 2016 [cit. 2025-06-27]. Dostupné na: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

auditovacie a monitorovacie postupy, ktoré zaručia dodržiavanie zásady rovnakého zaobchádzania.¹⁴

Z technického hľadiska predstavujú systémy umelej inteligencie aj potenciálne riziko kybernetických hrozieb, zlyhaní a zneužitia. Automatizované rozhodovanie môže byť cieľom útokov alebo neúmyselných chýb, ktoré môžu viesť k neoprávnenému zásahu do práv jednotlivcov. Právna úprava preto musí obsahovať jasné vymedzenie zodpovednosti za prevenciu a minimalizáciu týchto rizík, vrátane implementácie kybernetickej bezpečnosti, záložných mechanizmov a možnosti preskúmania rozhodnutia človekom.¹⁵

Cieľom príspevku je preskúmať povahu a rozsah zodpovednosti,¹⁶ ktorá môže vzniknúť ako dôsledok využitia systémov umelej inteligencie pri rozhodovaní alebo inom postupe verejnej správy s dosahom na veľmi široký okruh najmä osobnostných práv dotknutých osôb. Príspevok sa usiluje zodpovedať otázku, do akej miery sú súčasné právne rámce na úrovni únieového práva i vnútroštátneho práva Slovenskej republiky spôsobilé reagovať na špecifiká fungovania umelej inteligencie vo verejnej

¹⁴ European Parliament: Directorate-General for Internal Policies of the Union. *Artificial Intelligence in Law Enforcement and Criminal Justice: Impact on Fundamental Rights* [online]. Publications Office, 2020 [cit. 2025-06-30]. Dostupné na: <https://op.europa.eu/en/publication-detail/-/publication/4b1f19089-cfd4-11ea-adf7-01aa75ed71a1/language-en>.

¹⁵ FLORIDI, L. – COWLS, J. A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review* [online]. 2019, Vol. 1, No. 1 [cit. 2025-06-30]. Dostupné na: <https://hdr.mitpress.mit.edu/pub/10jsh9d1/release/8>.

¹⁶ Pojem zodpovednosť v tomto článku je používaný viacvrstovo, keďže najmä v kontexte úniovej legislatívy (nariadenie GDPR, AI akt) nadväzuje na tri odlišné koncepty pôvodne prevzaté z angloamerického právneho prostredia (responsibility, accountability a liability). Slovenský jazyk pre uvedené koncepty napriek určitým významovým odlišnostiam ich obsahu štandardne používa jednotný pojem zodpovednosť, pričom ich významové nuansy následne vyplývajú z kontextu, v ktorom boli použité. Nejde však len o problém slovenského jazyka, problematické a nejednoznačné je označovanie týchto konceptov i v iných jazykoch, dokonca samotné nariadenie GDPR používa tieto pojmy v mierne odlišnom kontexte ako AI akt a zároveň s odlišnými konotáciami ako ich pôvodný význam v common law, čo môže spôsobovať nežiaduce významové prekryvy príp. terminologické nezrovnalosti. Pojem responsibility v ponímaní GDPR nariadenia predstavuje zodpovednosť subjektu vyplývajúcu z jeho funkčného postavenia a autonómie pri vykonávaní úloh. Ide o koncepciu späť s voľbou, rozhodovaním a v určitom aspekte aj s morálnym rozmerom konania. „Zodpovedný aktér“ je ten, kto má právomoc konať v rámci svojich kompetencií a zároveň nesie zodpovednosť za spôsob, akým túto autonómiu uplatňuje. V kontexte GDPR nariadenia je koncept „responsibility“ upravený v prvej časti čl. 5 ods. 2 a v čl. 24 podľa ktorých je prevádzkovateľ zodpovedný („responsible for“) za dodržiavanie zásad spracúvania, teda má základnú povinnosť konať v súlade s právnymi požiadavkami a je povinný uskutočniť potrebné technické a organizačné opatrenia. Druhou rovinou je accountability, ktorá predstavuje kvalitatívne odlišný typ zodpovednosti. Nejde o autonómiu rozhodovania, ale o povinnosť preukázať, že subjekt konal správne. Accountability tak v sebe nesie požiadavku preukazovania – prevádzkovateľ má nielen dodržiavať GDPR, ale aj byť schopný toto dodržiavanie preukázať prostredníctvom interných procesov, dokumentácie a kontrolných mechanizmov. V čl. 5 ods. 2 GDPR je práve tento koncept označený termínom „accountability“, no vo viacerých jazykových verziách GDPR zaniká splynutím s všeobecným pojmom „responsibility“. Tretou vrstvou je koncept „liability“, ktorý predstavuje právnu zodpovednosť za následky porušenia povinností, najmä náhradu škody. V čl. 82 GDPR je použitý explicitne, čím sa zdôrazňuje, že vznik škody zakladá povinnosť subjektu niesť právne následky svojho konania alebo opomenutia. Uvedené tri roviny predstavujú samostatné, hoci vzájomne prepojené vrstvy jedného širšieho rámca, pričom každá z nich odkazuje na iný aspekt vzťahu subjektu k jeho konaniu a následkom konania.

správe, s dôrazom na identifikáciu limitov a medzier v existujúcej regulácii. V rámci stanoveného cieľa príspevok skúma najmä otázky, do akej miery sú súčasné právne predpisy (najmä Akt o umelej inteligencii, nariadenie GDPR a zákon č. 514/2003 Z. z.) použiteľné pri riešení ujmy spôsobenej rozhodnutiami alebo úkonmi realizovanými prostredníctvom umelej inteligencie, ako pristupujú vybrané zahraničné právne systémy k regulácii využívania automatizovaných rozhodovacích systémov vo verejnej správe a aké inšpiračné prvky možno v tomto kontexte identifikovať pre slovenské právne prostredie, aké sú limity zodpovednosti verejnej správy pri plne alebo čiastočne automatizovanom rozhodovaní a ako možno zabezpečiť ochranu najmä osobnostných práv jednotlivcov v takýchto situáciách.

Z metodologického hľadiska predchádzalo spracovaniu príspevku využitie metódy súpisu vlastností, pričom cieľom jej použitia bolo zosumarizovať dostupné poznatky a existujúci legislatívny rámec právnej úpravy na úrovni úniovej a slovenskej legislatívy príp. relevantných vnútroštátnych úprav vybraných európskych a mimoeurópskych štátov.

Nosnou metódou príspevku je využitie analýzy, prostredníctvom ktorej bol skúmaný rozsah a miera použiteľnosti existujúcich pravidiel na proces využívania umelej inteligencie v rozhodovacích a iných postupoch verejnej správy, s cieľom identifikovať aplikačné nedostatky v regulácii.

Popri analytickom prístupe je v príspevku rozsiahlym spôsobom uplatnená aj komparatívna metóda, ktorá umožnila porovnávať vnútroštátnu a európsku právnu úpravu s vybranými zahraničnými právnymi rámcami a praktickými prístupmi verejnej správy v oblasti využívania systémov umelej inteligencie. Komparatívna metóda slúžila najmä na odhalenie rozdielov a prienikov koncepčného uchopenia skúmanej problematiky a konkrétnych prístupov jednotlivých jurisdikcií, ako aj na identifikáciu inšpiračných prvkov, ktoré môžu byť relevantné pre úpravu slovenského právneho prostredia.

Pri identifikácii kľúčových zistení a informácií, ktoré majú význam pre ďalší postup skúmania, bola využitá metóda abstrakcie. Slúžila najmä na zhrnutie východiskových myšlienok a vymedzenie spoločných znakov právnych úprav, pričom takto spracované zistenia boli následne prostredníctvom syntézy spojené do jedného výstupu, ktorý nadväzuje na analytické závery a tvorí základ pre formuláciu záverov príspevku.

Štruktúra príspevku je koncipovaná tak, aby postupne a logicky nadväzovala na stanovený cieľ výskumu, ktorým je posúdenie existujúcej miery zodpovednosti za ujmy spôsobené nasadením systémov umelej inteligencie vo verejnej správe. Prvá časť príspevku sa zameriava na stručné vymedzenie základných právnych pilierov zodpovednosti verejnej správy v európskom kontexte. Pozornosť je venovaná najmä regulačným povinnostiam podľa Aktu o umelej inteligencii, otázkam zodpovednosti za spracúvanie osobných údajov v zmysle nariadenia GDPR ako aj krátkemu exkurzu dôvodov a dôsledkov zrušenia smernice o zodpovednosti za umelú inteligenciu a limitom novej smernice o zodpovednosti za chybné výrobky¹⁷ vo vzťahu k možnostiam jej aplikácie na škody spôsobené využívaním umelej inteligencie. Druhú časť príspevku tvorí

¹⁷ Smernica Európskeho parlamentu a Rady (EÚ) 2024/2853 z 23. októbra 2024 o zodpovednosti za chybné výrobky a o zrušení smernice Rady 85/374/EHS. *Úradný vestník Európskej únie*. L 312, 23. 10. 2024.

komparatívna analýza vybraných národných iniciatív, ktorých cieľom je regulovať využívanie automatizovaných rozhodovacích systémov vo verejnom sektore. Príspevok porovnáva legislatívne prístupy viacerých štátov, najmä Grécka, Kanady, Francúzska, Nemecka a Rakúska, a poukazuje na ich spoločné črty a rozdiely. Táto časť zároveň identifikuje tie prvky zahraničných úprav, ktoré môžu prispieť k formovaniu právneho rámca pre zodpovednosť verejnej správy pri využívaní umelej inteligencie. Tretia časť príspevku je zameraná na analýzu možností riešenia zodpovednosti za nasadenie umelej inteligencie vo verejnej správe v slovenskom prostredí. Pozornosť sa sústreďuje na aplikovateľnosť existujúcej právnej úpravy, najmä zákona č. 514/2003 Z. z. o zodpovednosti za škodu spôsobenú pri výkone verejnej moci, a na posúdenie, či tento rámec dokáže reagovať na špecifiká fungovania systémov umelej inteligencie. Súčasťou je aj určenie subjektu, ktorý nesie (mal by niesť) zodpovednosť za škodu spôsobenú rozhodnutím alebo konaním systému umelej inteligencie ako aj zhodnotenie otázky regresného postihu.

1. PRÁVNE PILIERE ZODPOVEDNOSTI VEREJNEJ SPRÁVY ZA SYSTÉMY UMELEJ INTELIGENCIE

Zodpovednosť verejnej správy za používanie systémov umelej inteligencie je v európskom kontexte postavená na troch základných právnych pilieroch: (1) regulačnom rámci vyplývajúcom z Aktu o umelej inteligencii, (2) civilnoprávnej zodpovednosti spravidla vnútroštátnej povahy s prípadným úniovým zarámčovaním (napr. smernica o zodpovednosti za chybný výrobok), a (3) osobitných pravidlách vyplývajúcich z nariadenia GDPR.

1.1 AKT O UMELEJ INTELIGENCII

Európsky Akt o umelej inteligencii prijatý v roku 2024 je prezentovaný ako prvý komplexný horizontálny regulačný rámec pre systémy umelej inteligencie v Európskej únii. Jeho štruktúra reflektuje prístup, ktorý je orientovaný na riziko a podľa ktorého sa právne povinnosti odvíjajú od miery rizika, ktoré systém AI predstavuje pre základné práva jednotlivcov, bezpečnosť alebo verejný záujem.

V kontexte verejnej správy je kľúčové, že prevažná časť AI systémov nasadzovaných štátom bude patriť do kategórie vysokorizikových systémov podľa čl. 6 ods. 2 a prílohy III AI Aktu, najmä ak pôjde o také systémy, ktoré sú určené na rozhodovanie o právach alebo povinnostiach jednotlivcov, ktoré sú využívané v oblasti sociálneho zabezpečenia, súdnictva, daní či rozdeľovania verejných zdrojov, alebo aj systémy, ktoré sú určené na biometrickú identifikáciu alebo profilovanie. Z toho pre verejné inštitúcie vyplývajú konkrétne regulačné povinnosti, z ktorých možno menovať najmä povinnosť vykonať posúdenie vplyvu na základné práva (ang. Fundamental Rights Impact Assessment) pred nasadením systému (čl. 29 AIA), či povinnosť zabezpečiť trasovateľnosť, auditovateľnosť a dokumentáciu systému vrátane uchovávaní logov, keďže vysokorizikové systémy AI musia technicky umožňovať automatické zaznamenávanie udalostí

(čl. 12 a čl. 23 AIA).¹⁸ Ďalej možno menovať požiadavku ľudského dohľadu a zásahu v rozhodovacom procese tam, kde môže AI vyvolať právne alebo faktické účinky na jednotlivca (čl. 14 AIA) a zákaz používania netransparentných alebo nevysvetliteľných systémov v oblastiach, kde AI ovplyvňuje základné práva (čl. 13 AIA), čo vyplýva z toho, že nasadzujúcim subjektom musí byť umožnené interpretovať výstupy systému a vhodne ich používať. Výpočet možno doplniť o povinnosť zabezpečiť technickú robustnosť, kybernetickú bezpečnosť a správu rizík počas celého životného cyklu systému (čl. 9 a čl. 15 AIA).

Tieto povinnosti sú pre verejný sektor intenzívnejšie ako pre súkromných používateľov, v tom zmysle, že orgány verejnej moci vykonávajú rozhodovaciu právomoc so zásahom do základných práv. Porušenie regulačných povinností môže zakladať správne sankcie v zmysle čl. 99 AIA, ale aj civilnoprávnu a ústavnoprávnu zodpovednosť za zásah do práv jednotlivca.

Z tohto dôvodu pôsobí Akt o umelej inteligencii nielen *ex ante* preventívne, ale zároveň slúži ako interpretačný štandard pri posudzovaní nezákonnosti rozhodnutí verejnej správy pri uplatňovaní vnútroštátnej zodpovednostnej úpravy.

1.2 ZODPOVEDNOSŤ PODĽA NARIADENIA GDPR

Osobitný pilier zodpovednosti verejnej správy tvorí ochrana osobných údajov podľa nariadenia GDPR. Aj v prípade, keď umelú inteligenciu využíva verejná správa, musí zabezpečiť, aby systémy umelej inteligencie spracúvali osobné údaje zákonne. Podľa článku 82 GDPR má dotknutá osoba nárok na náhradu škody, ktorá vznikla v dôsledku nezákonného spracúvania jej osobných údajov. Napr. ak systém umelej inteligencie v polícii alebo súdnictve neoprávnene profiluje občanov, môže dôjsť k aplikácii tohto článku GDPR, ktorý upravuje nárok na náhradu škody podľa únievého práva, ktorá vznikla v príčinnej súvislosti s nezákonným spracúvaním osobných údajov.

Okrem okolností, ktoré typicky súvisia s právom na ochranu osobných údajov (napr. nezákonné úradné spracúvanie formulárov žiadostí), je možné uplatniť nárok na náhradu škody podľa čl. 82 GDPR aj vtedy, ak konkrétne riziká (plne) automatizovaného rozhodovania v rozpore s čl. 22 GDPR vedie k vzniku škody dotknutej osobe, najmä, ak orgán verejnej moci uplatní výnimku podľa článku 22 ods. 2 písm. b) GDPR bez splnenia zákonných podmienok a primeraných záruk, čím fakticky nahradí ľudské rozhodovanie algoritmickým systémom.

Článok 22 GDPR totiž upravuje zákaz rozhodovania výlučne na základe automatizovaného spracúvania, ak takéto rozhodnutie vyvoláva právne účinky alebo obdobne

¹⁸ Mesarčík poukazuje na to, že požiadavka logovania slúži na tri kľúčové účely, a to zaznamenávanie udalostí súvisiacich s potenciálnymi rizikami alebo s potrebou podstatných úprav systému, uľahčenie monitorovania systémov umelej inteligencie po ich uvedení na trh a umožnenie monitorovania vysokorizikových systémov umelej inteligencie. MESARČÍK, M. – GYURÁSZ, Z. a kol. *Právo a umelá inteligencia* [online]. Bratislava: Právnická fakulta Univerzity Komenského v Bratislave, 2024, s. 89 [cit. 2025-11-08]. Dostupné na: https://www.flaw.uniba.sk/fileadmin/praf/Pracoviska/Ustavy/UPITPDV/E-KNIHY/Pravo_a_umela_inteligencia_ucebnica_01.pdf.

významne ovplyvňuje dotknutú osobu.¹⁹ Verejný orgán však môže takýto postup použiť vtedy, ak je to výslovne povolené právnym predpisom a súčasne sa stanovujú aj vhodné opatrenia zaručujúce ochranu práv a slobôd a oprávnených záujmov dotknutej osoby [čl. 22 ods. 2 písm. b) GDPR].²⁰ Dotknutá osoba má pritom právo na ľudský zásah, má právo vyjadriť svoj názor a má tiež právo napadnúť rozhodnutie.²¹ Európsky výbor pre ochranu osobných údajov vo svojom výklade zdôrazňuje, že „ľudský zásah“ musí byť reálny, kvalifikovaný a schopný zmeniť rozhodnutie, pričom formálny, symbolický alebo automatizovaný „dohľad“ nie je postačujúci.²²

Ak potom verejný orgán niektorú z týchto povinností poruší, a v príčinnej súvislosti s porušením GDPR vznikne škoda, môže si takto poškodená osoba uplatniť nárok na náhradu škody podľa čl. 82 GDPR, a to aj vo vzťahu k nemajetkovej ujme, napríklad v prípadoch nezákonnej diskriminácie alebo nespravodlivého profilovania.

Pre verejnú správu sú teda kľúčové dva právne režimy, a to článok 22 GDPR upravujúci pravidlá automatizovaného individuálneho rozhodovania a článok 82 GDPR, ktorý reguluje právo na náhradu škody pri porušení GDPR. Ide pritom o dva samostatné právne režimy, ktoré sa môžu, ale nemusia prekrývať.

Aplikácia systémov umelej inteligencie, najmä v oblasti profilovania, predikcie správania či automatizovaného rozhodovania (čl. 22 GDPR), si vyžaduje osobitnú pozornosť.²³ Medzi kľúčové podmienky zodpovednosti podľa GDPR patria preukázateľný

¹⁹ Judikatúra Súdneho dvora EÚ potvrdzuje, že aj rizikové skóre a profilovanie môžu byť považované za rozhodnutia podľa čl. 22 GDPR, pokiaľ orgán verejnej moci na tieto výstupy automaticky nadväzuje (napr. Rozsudok Súdneho dvora zo 7. decembra 2023 vo veci C-634/21 OQ proti Land Hessen, za účasti: SCHUFA Holding AG. ECLI:EU:C:2023:957).

²⁰ Naopak, ako vyplýva z početnej rozhodovacej praxe Európskeho výboru pre ochranu osobných údajov, súhlas nie je vhodným právnym základom pre automatizované rozhodovanie verejnými orgánmi vzhľadom na nerovnováhu moci medzi dotknutou osobou a orgánom verejnej moci: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251 rev.01). In: *European Commission: Newsroom* [online]. 22. 8. 2018, s. 21 [cit. 2025-11-08]. Dostupné na: <https://ec.europa.eu/newsroom/article29/items/612053/en>. V ďalšom dokumente potom Európsky výbor pre ochranu osobných údajov uviedol, že verejné orgány sa spravidla nachádzajú v situácii nerovnováhy moci vo vzťahu k dotknutým osobám, a preto je nepravdepodobné, že by súhlas od dotknutej osoby mohol byť považovaný za slobodne udelený v situácii, v ktorej verejný orgán žiada o súhlas na spracúvanie: Guidelines on Consent under Regulation 2016/679 (wp259 rev.01). In: *European Commission: Newsroom* [online]. 6. 7. 2018, s. 8–9 [cit. 2025-11-08]. Dostupné na: <https://ec.europa.eu/newsroom/article29/items/623051>.

²¹ Právna úprava musí obsahovať tieto záruky, inak by rozhodovanie bolo v rozpore s Chartou základných práv EÚ (najmä čl. 8 a čl. 47). Bližšie k problematike práva na vysvetlenie pozri VEALE, M. – EDWARDS, L. Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling. *Computer Law & Security Review* [online]. 2018, Vol. 34, No. 2, s. 398–404 [cit. 2025-11-08]. Dostupné na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3071679.

²² European Data Protection Board. Guidelines 05/2020 on Automated Decision-Making and Profiling. Version 1.1 [online]. 4. 5. 2020, body 24–37 [cit. 2025-11-08]. Dostupné na: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

²³ K analýze, ako členské štáty EÚ implementovali článok 22 GDPR o automatizovanom rozhodovaní, najmä pokiaľ ide o výnimky, záruky a právo na vysvetlenie, pozri MALGIERI, G. Automated Decision-Making in the EU Member States: The Right to Explanation and Other “Suitable Safeguards” in the National Legislations. *Computer Law & Security Review* [online]. 2019, Vol. 35, No. 5 [cit. 2025-06-19]. Dostupné na: <https://doi.org/10.1016/j.clsr.2019.05.002>.

vznik škody v príčinnej súvislosti s porušením právnych povinností, nezákonné spracovanie údajov (napr. profilovanie občanov bez právneho základu), nadmerná miera automatizácie bez adekvátneho ľudského zásahu a zlyhanie orgánu verejnej moci pri uplatnení povinnosti kontroly nad rozhodovacím procesom.

Kauzálny vzťah medzi rozhodnutím systému umelej inteligencie a škodou musí byť objektívne preukázaný. Nie je totiž postačujúce, že rozhodnutie prijal algoritmus, ale musí byť zrejmé, že v prípade zákonného postupu by orgán rozhodol inak (napr. ak by bol prítomný ľudský zásah), alebo že by došlo k reálnemu ovplyvneniu rozhodovacieho procesu, či odňatiu práva na procesnú ochranu, ktorá mohla viesť k inému výsledku.

Škoda je kompenzovateľná len vtedy, ak je spôsobená porušením pravidiel spracovania osobných údajov, avšak ak orgán automatizuje postup v rozpore s článkom 22 ods. 2 písm. b) GDPR alebo do rozhodovacieho procesu nezákonne nezapojí ľudský prvok, nevedie to nevyhnutne k vzniku kompenzovateľnej škody. Kauzálnym faktorom je právny následok, ktorý vyvolá výstup systému umelej inteligencie, nie skutočnosť, že rozhodnutie vydal automatizovaný (prípadne učiaci sa) systém.²⁴ Pre ustálenie kauzality by orgán musel v prípade zákonného konania (t. j. ak by dodržiaval predpisy o ochrane osobných údajov) prijať iné ako systémom prijaté rozhodnutie.

1.3 KONTEXT ZRUŠENEJ SMERNICE O ZODPOVEDNOSTI ZA UMELÚ INTELIGENCIU A NOVEJ SMERNICE O ZODPOVEDNOSTI ZA CHYBNÉ VÝROBKY

Európska komisia v roku 2022 predstavila návrh smernice o zodpovednosti za umelú inteligenciu,²⁵ ktorá mala doplniť Akt o umelej inteligencii o pravidlá mimozmluvnej občianskoprávnej zodpovednosti za škody spôsobené systémami umelej inteligencie v rámci Európskej únie. Návrh smernice sa však nestretol s konsenzom členských štátov a bol v roku 2024 stiahnutý.²⁶ Zámerom nebolo, aby smernica nahradila existujúce pravidlá o zodpovednosti za výrobky²⁷ (napr. keď umelá inteligencia

²⁴ Rozsudok Súdneho dvora (tretia komora) zo 4. 5. 2023 vo veci C300/21 UI proti Österreichische Post AG, ECLI:EU:C:2023:370; rozsudok Súdneho dvora (tretia komora) z 11. 4. 2024 vo veci C741/21 GP proti juris GmbH, ECLI:EU:C:2024:288. Súdny dvor EÚ sa aj vo viacerých ďalších rozhodnutiach explicitne zaoberal výkladom článku 82 GDPR. Z jeho rozhodnutí dnes jasne vyplýva, ako chápať rozsah, povahu a podmienky tohto práva.

²⁵ 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). 28. 9. 2022, COM(2022) 496 final [online]. [cit. 2025-11-10]. Dostupné na: <https://op.europa.eu/en/publication-detail/-/publication/16b4afba-3ff9-11ed-92ed-01aa75ed71a1/language-en>. K návrhu smernice pozri ZIOSI, M. – MÖKAN- DER, J. – NOVELLI, C. – CASOLARI, F. – TADDEO, M. – FLORIDI, L. The EU AI Liability Directive (AILD): Bridging Information Gaps. *European Journal of Law and Technology* [online]. 2023, Vol. 14, No. 3 [cit. 2025-11-10]. Dostupné na: <https://ejlt.org/index.php/ejlt/article/view/962>.

²⁶ Commission withdraws AI liability directive after Vance attack on regulation. In: *EURACTIV* [online]. 11. 2. 2025 [cit. 2025-06-19]. Dostupné na: <https://www.euractiv.com/section/tech/news/commission-withdraws-ai-liability-directive-after-vance-attack-on-regulation/>.

²⁷ K vzájomnému vzťahu smernice o zodpovednosti za umelú inteligenciu a smernice o zodpovednosti za chybné výrobky pozri HACKER, P. The European AI Liability Directives – Critique of a Half-Hearted

spôsobí fyzickú škodu na výrobkoch alebo zdraví), ale mala ich doplniť o digitálne aspekty²⁸ a najmä mala:

- zaviesť prezumpciu príčinnej súvislosti medzi porušením povinností súvisiacich s umelou inteligenciou a vznikom škody (ak by poškodený dokázal, že porušenie právnych povinností týkajúcich sa umelej inteligencie mohlo spôsobiť škodu, súd by mohol predpokladať, že škoda bola spôsobená systémom umelej inteligencie),
- zjednodušiť poškodeným prístup k dôkazom (aby mohli preukázať, že umelá inteligencia spôsobila škodu),
- zabezpečiť transparentnosť AI systémov (vývojári a prevádzkovatelia umelej inteligencie by mali povinnosť poskytnúť transparentné informácie o fungovaní ich systémov) a
- rozšíriť ochranu v oblastiach s vysokým rizikom, ako je zdravotníctvo, justícia, verejná doprava či finančné služby (s cieľom, aby si obeť mohla ľahšie uplatniť nárok na odškodnenie).

Niektoré členské štáty nesúhlasili s prezumpciou príčinnej súvislosti, keďže by to mohlo viesť k nadmernému právnemu riziku pre podniky. Európska komisia sa tak (aspoň dočasne) rozhodla ponechať reguláciu zodpovednosti za umelú inteligenciu na národné právne systémy namiesto jednotného európskeho rámca.

Po späťvzátí návrhu tak naďalej pretrváva regulačná medzera, ktorú nevyplní ani prijatá smernica o zodpovednosti za chybné výrobky. Smernica o zodpovednosti za chybné výrobky je vystavaná na koncepte jasného zlyhania – vady výrobku, ktoré pri umelej inteligencii, ktorá funguje autonómne a adaptívne, s ťažko uchopiteľnými a pochopiteľnými vnútornými procesmi, nemusí byť vždy jasne identifikovateľné.²⁹

Problematickým aspektom smernice o zodpovednosti za chybné výrobky vo vzťahu k jej aplikácii na škody spôsobené umelou inteligenciou je fakt, že smernica upravuje mechanizmy pre náhradu škody pri chybnom (vadnom) produkte (napr. technické zariadenia), avšak neuplatňuje sa na služby ako také. Napriek tomu, že pôsobnosť smernice je do istej miery rozšírená i na integrované alebo prepojené digitálne služby, tieto musia byť súčasťou (komponentom) výrobku, za ktorý sa zodpovedá v súlade so smernicou a zároveň musia byť pod kontrolou výrobcu (napr. navigačný systém, ktorý je ako softvér súčasťou produktu). Umelá inteligencia však môže byť službou samou o sebe, ktorá nie je integrovaná do výrobku alebo s ním prepojená (napr. samotný algoritmus alebo cloudové riešenie), teda nie je nevyhnutne výrobkom v ponímaní smernice, čo vytvára vo vzťahu k týmto systémom umelej inteligencie medzeru nepokrytú harmonizovanými európskymi pravidlami. Navyše samotný východiskový koncept smernice predpokladá, že škoda bola spôsobená vadou, ktorú možno spätne identifikovať v čase

Approach and Lessons for the Future. *Computer Law & Security Review* [online]. 2023, Vol. 51 [cit. 2025-11-11]. Dostupné na: <https://doi.org/10.1016/j.clsr.2023.105871>.

²⁸ Proposal for a directive on adapting non-contractual civil liability rules to artificial intelligence: Complementary impact assessment. In: *Think Thank: European Parliament* [online]. 19. 9. 2024 [cit. 2025-06-19]. Dostupné na: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU\(2024\)762861](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2024)762861).

²⁹ K vymedzeniu vady výrobku pozri bližšie BUITEN, M. Product Liability for Defective AI. In: *SSRN* [online]. 19. 7. 2023 [cit. 2025-11-10]. Dostupné na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4515202.

uvedenia produktu na trh.³⁰ Smernica je tak orientovaná na statický model (výrobok je buď chybný pri uvedení na trh alebo nie), avšak systémy umelej inteligencie spravidla fungujú v dynamickom modeli zmien správania systému v čase na základe strojového učenia, reakciou na nové vstupné dáta, adaptáciou na nové podmienky alebo používateľské správanie (napr. odklon rozhodovacej činnosti systému umelej inteligencie smerom k zohľadňovaniu diskriminačných aspektov v čase, pričom pri uvedení na trh takéto chybné algoritmy nepoužíval).

Smernica o zodpovednosti za chybné výrobky má vo vzťahu k zodpovednosti za umelú inteligenciu i ďalšie limity. Kompenzované podľa tejto smernice môžu byť len škody na majetku alebo na zdraví, avšak mnohé negatívne zásahy systémov umelej inteligencie, ako napríklad diskriminácia alebo narušenie súkromia, majú prevažne nemateriálny charakter a do rámca smernice o zodpovednosti za chybné výrobky nespádajú. Smernica o zodpovednosti za chybné výrobky navyše obmedzuje rozsah náhrady škody nielen na konkrétne typy škôd ale vo vzťahu k subjektom v postavení poškodeného len na fyzické osoby. Takto je napr. vylúčená náhrada za škodu na majetku používanom výlučne na profesijné účely (čo samozrejme reflektuje cieľ smernice zameraný na ochranu spotrebiteľov ako slabšej strany právnych vzťahov – podnikatelia a profesionálni používatelia si majú niesť vyššiu mieru rizika sami bez ochrany poskytovanej touto prosperiteľskou úpravou).

Napriek tomu, že v odôvodnení návrhu o zodpovednosti za umelú inteligenciu Európska komisia uvádzala, že súčasné vnútroštátne pravidlá zodpovednosti, najmä tie, založené na princípe zavinenia, nie sú vhodné na riešenie nárokov na náhradu škody spôsobenej výrobkami a službami s umelou inteligenciou a tiež, že niektoré prípady ujmy spôsobenej umelou inteligenciou môžu podľa vnútroštátneho práva spadať do „sedej zóny odškodnenia“, a teda nemusia poskytnúť obetiam úroveň ochrany zodpovednosti porovnateľnú s úrovňou, ktorú by dostali v podobných prípadoch, ktoré sa netýkajú umelej inteligencie, návrh podporu nezískal. Všeobecne teda platí, že koncept zodpovednosti dnes v EÚ vychádza z Aktu o umelej inteligencii a zo smernice o zodpovednosti za chybné výrobky s vyššie uvádzanými limitmi jej aplikovateľnosti.

2. VYBRANÉ NÁRODNÉ INICIATÍVY REGULUJÚCE VYUŽÍVANIE AUTOMATIZOVANÝCH SYSTÉMOV VO VEREJNOM SEKTORE

Hoci väčšina štátov nie je vo vzťahu k osobitnej právnej úprave explicitne adaptovaná na procesy využívania umelej inteligencie vo verejnej správe, niektoré krajiny už prijali národnú legislatívu (alebo jej návrh), ktorou upravujú alebo navrhujú upraviť zodpovednosť za používanie umelej inteligencie vo verejnej správe. Jedným

³⁰ Pozri čl. 11 ods. 1 písm. c) smernice o zodpovednosti za chybné výrobky vo vzťahu k možnosti liberácie zodpovedného subjektu: Dotknutý subjekt nezodpovedá za škodu spôsobenú vadným výrobkom, ak preukáže, „[...] že je pravdepodobné, že chybovosť, ktorá spôsobila škodu, neexistovala v čase, keď sa výrobok uviedol na trh alebo do prevádzky, alebo v prípade distribútora pri sprístupňovaní výrobku na trhu, prípadne že vznikla až po tomto okamihu [...]“.

z priekopníkov je Grécko, ktoré v roku 2022 prijalo zákon o nových technológiách, ktorý reguluje využívanie a používanie nových technológií s významným hospodárskym a sociálnym dopadom.³¹ Zákon zavádza konkrétne a záväzné povinnosti pre verejný sektor pri nasadzovaní systémov umelej inteligencie. Podľa čl. 4 zákona je používanie AI systémov vo verejnej správe povolené výlučne na základe osobitného zákonného ustanovenia, ktoré musí obsahovať primerané záruky ochrany práv fyzických aj právnických osôb. Pred nasadením takýchto systémov majú verejné orgány povinnosť vykonať posúdenie vplyvu algoritmov (Algorithmic Impact Assessment)³² ako doplnok k posúdeniu vplyvu na ochranu údajov podľa GDPR. Toto posúdenie má za cieľ identifikovať a zhodnotiť riziká, ktoré by mohli nastať vo vzťahu k právam, slobodám a oprávneným záujmom dotknutých osôb. Okrem toho musia orgány verejnej moci zverejňovať informácie o nasadení AI systémov, ich parametroch a rozhodnutiach, ktoré sú nimi ovplyvnené. Ďalšou významnou povinnosťou každej verejnej autority je vedenie verejného registra všetkých používaných AI systémov, vrátane základných údajov o použití, účele, technológii, hodnotení rizík a transparentnosti.³³ Napriek tomu, že zákon bol prijatý v r. 2022, podľa dostupných informácií zatiaľ neexistuje takáto verejne prístupná databáza, ktorá by uvedenú povinnosť naplňala v praxi.

Ďalším štátom, ktorý prijal záväzný rámec pre využívanie systémov automatizovaného rozhodovania (The Treasury Board Directive on Automated Decision-Making) vo verejnej správe je Kanada.³⁴ Smernica o automatizovanom rozhodovaní (s účinnosťou od roku 2019) sa vzťahuje na väčšinu federálnych inštitúcií, s výnimkou Kanadskej daňovej agentúry (Canada Revenue Agency), rovnako sa neaplikuje na úrovni provinčných či nižších administratívnych orgánov. Smernica sa vzťahuje na automatizované rozhodovacie systémy,³⁵ ktoré plne alebo čiastočne prijímajú administratívne rozhodnutia, ktoré majú vplyv na práva alebo právom chránené záujmy jednotlivcov alebo subjektov mimo verejnej správy (t.j. pôsobnosť smernice sa vzťahuje tak na systémy,

³¹ Zákon upravuje vertikálne povinnosti pre poskytovateľov produktov a služieb súvisiacich s umelou inteligenciou, internetom vecí a bezpilotnými prostriedkami v oblasti dopravy a horizontálne požiadavky na využívanie umelej inteligencie a 3D tlače, pričom kladie základy pre vykonávanie transakcií pomocou DLT a inteligentných zmlúv (BROUMAS, A. – CHARALAMPOUS, P. The regulation of Emerging Technologies in Greek Law. *JIPITEC* [online]. 2023, Vol. 14, s. 595 [cit. 2025-06-10]. Dostupné na: <https://www.jipitec.eu/jipitec/article/view/25/19>).

³² Inštitút hodnotenia vplyvu algoritmov zakotvený v gréckom zákone č. 4961/2022 čerpá inšpiráciu z obdobných inštitútov upravených v kanadskej smernici o automatizovanom rozhodovaní (Directive on Automated Decision Making) a v americkom zákone o algoritmickej zodpovednosti z roku 2022 (Algorithmic Accountability Act H.R. 6580).

³³ Čl. 8 gréckeho zákona o nových technológiách.

³⁴ Kanada sa snažila regulovať umelú inteligenciu na federálnej úrovni aj prostredníctvom zákona o umelej inteligencii a údajoch (Artificial Intelligence and Data Act – AIDA), ktorý bol súčasťou návrhu zákona C-27. Návrh zákona AIDA bol predložený v júni 2022, úspešne prešiel druhým čítaním a 24. apríla 2023 bol postúpený Stálemu výboru pre priemysel a technológie. K návrhu bolo vyjadrených množstvo znepokojivých pripomienok jednotlivcov a organizácií a hoci vláda navrhla v reakcii na kritiku zmeny a doplnenia AIDA, návrhu zákona sa na tomto výbere zasekol, pričom je už viac-menej jasné, že sa mu nepodarilo získať politickú vôľu potrebnú na pokračovanie v legislatívnom procese.

³⁵ Patria sem systémy, ktoré klasifikujú žiadosti podľa rizika či priority, ktoré identifikujú prípady na kontrolu alebo preskúmanie, systémy, ktoré odporúčajú schválenie alebo zamietnutie žiadosti alebo také, ktoré prijímajú konečné administratívne rozhodnutia bez ľudskej intervencie.

ktoré podporujú ako aj nahrádzajú ľudské rozhodovanie). Smernica definuje konkrétne požiadavky, ktoré musia federálne inštitúcie splniť pri zavádzaní systémov automatizovaného rozhodovania vrátane tých, ktoré využívajú (generatívnu) umelú inteligencia. Ide najmä o povinnosť informovať klientov a iné dotknuté osoby, že rozhodnutie bude vygenerované čiastočne alebo úplne automatizovaným systémom, povinnosť vybrať vhodnú licenciu s preferenciou *open-source* prístupu, uchovávať všetky verzie softvéru, priebežne monitorovať výstupy systému a zhodnocovať súlad s právnymi predpismi upravujúcimi základné práva a slobody, zabezpečiť ochranu pred manipuláciou, dokumentovať spätnú väzbu, zásahy ľudského prvku do systému, príp. jeho zlyhania ako aj zabezpečiť možnosť zásahu ľudského prvku do systému. Osobitná pozornosť je v smernici venovaná aj rizikám zaujatosti systému a nedostatočnej odôvodniteľnosti rozhodnutí, ktoré sú v rámci automatizovaného rozhodovania považované za dva najkritickejšie body. V reakcii na tieto riziká smernica obsahuje tzv. požiadavku vysvetlenia rozhodnutia, podľa ktorej musí byť systém schopný poskytnúť zrozumiteľné odôvodnenie prijatého rozhodnutia a požiadavku implementovania tzv. Quality Assurance mechanizmov, ktoré zahŕňajú testovanie dát a modelov kvôli zaujatosti systému (diskriminačných prvkov systému) už vo fáze návrhu systému. V záujme uľahčenia implementácie zverejnila kanadská vláda pre federálne inštitúcie Príručku o rozsahu pôsobnosti smernice o automatizovanom rozhodovaní (Guide on the Scope of the Directive on Automated Decision-Making)³⁶ a vo vzťahu k využívaniu generatívnej umelej inteligencie Príručku pre využívanie generatívnej umelej inteligencie (Guide on the use of generative artificial intelligence).³⁷

Napriek vyššie uvedeným výnimkám neexistuje vo väčšine štátov žiadny právny precedens (obdobný holandskému SyRI) alebo komplexný právny rámec upravujúci využívanie umelej inteligencie v štátnej správe. Napriek tomu vznikli v týchto štátoch viaceré neformálne iniciatívy a odporúčania, ktorých cieľom je nastaviť etické a technické štandardy pre automatizované rozhodovanie. Napríklad v Spojenom kráľovstve patrí medzi najaktívnejšie inštitúcie Úrad komisára pre informácie (Information Commissioner's Office – ICO), ktorý vypracoval usmernenia (Guidance on AI and data protection)³⁸ k opatreniam na zabezpečenie transparentnosti, znižovanie algoritmickej zaujatosti a k dôslednému vykonávaniu posudzovania vplyvov na ochranu údajov. Dôležitú úlohu tu zohrávajú aj výskumné inštitúcie ako inštitút Alana Turinga (Alan Turing Institute),³⁹ Úrad pre umelú inteligenciu (Office for Artificial Intelligence)⁴⁰ či v mi-

³⁶ Guide on the Scope of the Directive on Automated Decision-Making. In: *Government of Canada* [online]. [cit. 2025-07-10]. Dostupné na: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-scope-directive-automated-decision-making.html>.

³⁷ Guide on the use of generative artificial intelligence. In: *Government of Canada* [online]. [cit. 2025-07-10]. Dostupné na: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-use-generative-ai.html>.

³⁸ Guidance on AI and data protection. In: *ico* [online]. 15. 3. 2023 [cit. 2025-07-10]. Dostupné na: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/>.

³⁹ *The Alan Turing Institute* [online]. [cit. 2025-07-10]. Dostupné na: <https://www.turing.ac.uk>.

⁴⁰ Office for Artificial Intelligence. In: *GOV.UK* [online]. [cit. 2025-07-10]. Dostupné na: <https://www.gov.uk/government/organisations/office-for-artificial-intelligence>.

nulosti AI Council,⁴¹ výsledkom výskumu a práce ktorých sú nezáväzné dokumenty, poskytujúce usmernenia pri používaní umelej inteligencie. Takto bolo vo vzťahu k organizáciám verejného sektora v roku 2019 prostredníctvom UK Government's Digital Service a Office for Artificial Intelligence vydané Usmernenie o používaní umelej inteligencie vo verejnom sektore (Guide to Using AI in the Public Sector).⁴² Cieľom tohto usmernenia bolo poskytnúť praktické návody pre organizácie verejného sektora pri implementácii riešení umelej inteligencie vo verejnom sektore.⁴³

Vo Francúzsku rovnako neexistuje samostatný zákon, ktorý by systematicky upravoval zodpovednosť štátu za ujmy spôsobené umelou inteligenciou vo verejnej správe. Avšak národný dozorný orgán pre ochranu osobných údajov CNIL (Commission Nationale de l'Informatique et des Libertés) vydal v rokoch 2024–2025 sériu oficiálnych usmernení a metodík týkajúcich sa využitia umelej inteligencie, najmä v kontexte vývoja a implementácie AI systémov. V roku 2016 nadobudol účinnosť zákon o digitálnej republike (Loi pour une République numérique),⁴⁴ ktorý novelizoval správny poriadok (Code des relations entre le public et l'administration) v súvislosti s používaním algoritmických rozhodovacích systémov vo verejnej správe. Tento zákon výslovne zavádza povinnosť vysvetliť rozhodnutie verejného orgánu, ak bolo prijaté na základe algoritmického spracovania. Podľa zákona a následného vykonávacieho dekrétu⁴⁵ je správny orgán povinný na požiadanie poskytnúť dotknutej osobe informácie o dátach, parametroch rozhodovania a o hlavných charakteristikách algoritmu, ktoré sa na rozhodovanie vzťahovali. Toto ustanovenie ide nad rámec

⁴¹ AI Council. In: *GOV.UK* [online]. [cit. 2025-07-10]. Dostupné na: <https://www.gov.uk/government/groups/ai-council>.

⁴² Office for Artificial Intelligence, The Government Digital Service. *A guide to using artificial intelligence in the public sector* [online]. London: Government UK, 2020 [cit. 2025-07-10]. Dostupné na: https://assets.publishing.service.gov.uk/media/60828077d3bf7f013e451bc8/A_guide_to_using_AI_in_the_public_sector_Print_version.pdf.

⁴³ Bližšie k usmerneniu pozri PEETS, L. – HANSEN, M. – CHOI, S. J. – LEVIATIN, C. Algorithmic Decision-Making and Legal Frameworks. *Robotics, Artificial Intelligence & Law* [online]. November–December 2019, No. 6, s. 439–443 [cit. 2025-07-10]. Dostupné na: https://www.cov.com/-/media/files/corporate/publications/2019/11/uk_governments_guide_to_using_ai_in_the_public_sector.pdf?.

⁴⁴ Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (Code des relations entre le public et l'administration), čl. L311-3-1: „Lorsque l'administration prend une décision individuelle sur le fondement d'un traitement algorithmique, elle communique à l'intéressé qui en fait la demande [...]“. Text zákona je dostupný online (Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (1). In: *Légifrance* [online]. [cit. 2025-07-10]. Dostupné na: <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746>).

⁴⁵ Décret n° 2017-330 du 14 mars 2017, čl. R311-3-1-2: „Lorsque l'administration prend, sur le fondement d'un traitement algorithmique, une décision individuelle mentionnée à l'article L. 311-3-1, la communication à la personne intéressée comprend les informations suivantes:

1. Le degré et le mode de contribution du traitement algorithmique à la prise de décision

2. Les données traitées et leur source

3. Les paramètres de traitement et, le cas échéant, leur pondération, appliqués à la situation de l'intéressé

4. Les opérations effectuées par le traitement.“

Text dekrétu je dostupný online (Décret n° 2017-330 du 14 mars 2017 relatif aux droits des personnes faisant l'objet de décisions individuelles prises sur le fondement d'un traitement algorithmique. In: *Légifrance* [online]. [cit. 2025-07-10]. Dostupné na: <https://www.legifrance.gouv.fr/eli/decret/2017/3/14/2017-330/jo/texte>).

práva na vysvetlenie podľa GDPR, keďže sa vzťahuje nielen na rozhodnutia výlučne založené na automatizovanom spracovaní (čl. 22 GDPR), ale aj na rozhodovanie podporené algoritmickými nástrojmi. Zároveň možnosť zverejnenia váh použitých faktorov v algoritme naznačuje, že ide o povinnosť vysvetlenia konkrétneho rozhodnutia („*subject-based explanation*“), nie iba o všeobecnú dokumentáciu fungovania modelu („*model-based explanation*“). Francúzsky zákon tak vytvára právny rámec nielen pre vysvetlenie všeobecných zásad, ale aj pre interpretáciu konkrétnych rozhodnutí verejných orgánov voči jednotlivcom.⁴⁶

Nemecko prijalo viacero dokumentov na úrovni etických rámcov a výskumných iniciatív, pričom niektoré spolkové krajiny (napr. Bavorsko, Berlín) vyvíjajú vlastné AI stratégie s dôrazom na transparentnosť a participáciu.⁴⁷ Nemecký Bundestag zriadil v roku 2018 osobitnú komisiu (Enquete Kommission „Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale“), ktorej úlohou bolo komplexne preskúmať dopady umelej inteligencie na spoločnosť, štát a ekonomiku. Komisia analyzovala široké spektrum výziev a príležitostí spojených s umelou inteligenciou, pričom osobitná pozornosť bola venovaná regulačným, etickým a technologickým otázkam. Súčasťou jej mandátu bolo aj formulovanie odporúčaní pre legislatívne a politické opatrenia. Záverečná správa komisie, predložená Spolkovému snemu v októbri 2020 (BT-Drs. 19/23700),⁴⁸ predstavuje jeden z najkomplexnejších dokumentov o štátnej politike vo vzťahu k umelej inteligencii v európskom priestore. Správa vo vzťahu k zodpovednosti umelej inteligencie vyzýva, aby zodpovednosť za jej používanie vždy niesla konkrétna (právnická alebo fyzická) osoba a nie samotný technický systém, pretože umelá inteligencia sama osebe neposkytuje vhodné kritériá pre vytvorenie nových zákonných hraníc zodpovednosti. Správa uvádza, že všeobecné pravidlá zodpovednosti (klasická deliktná zodpovednosť ako aj zodpovednosť za riziko), rovnako ako špecifické režimy zodpovednosti (napr. zodpovednosť za vadný výrobok) sa v zásade vzťahujú aj na systémy umelej inteligencie (samozrejme s limitmi vyplývajúcimi z jednotlivých skutkových podstat zodpovednosti). Praktická aplikácia zodpovednostných režimov v Nemecku sa zatiaľ opiera o existujúce normy správneho,

⁴⁶ EDWARDS, L. – VEALE, M. Enslaving the Algorithm: From a “Right to an Explanation” to a “Right to Better Decisions”? *IEEE Security & Privacy* [online]. 2018, Vol. 16, No. 3, s. 49–50 [cit. 2025-07-10]. Dostupné na: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3052831; EDWARDS, L. – VEALE, M. Slave to the Algorithm? Why a “Right to an Explanation” Is Probably Not the Remedy You Are Looking For. *Duke Law & Technology Review* [online]. 2018, Vol. 16, No. 1, s. 18–84 [cit. 2025-07-10]. Dostupné na: <https://ssrn.com/abstract=2972855>.

⁴⁷ K nedávnym aktivitám na krajinskej úrovni pozri LIEBIG, L. – GÜTTEL, L. – JOBIN, A. – KATZENBACH, C. Subnational AI policy: shaping AI in a multi-level governance system. *AI & Society* [online]. 2024, Vol. 39, No. 5, s. 1477–1490 [cit. 2025-07-10]. Dostupné na: <https://doi.org/10.1007/s00146-022-01561-5>; JOBIN, A. – GÜTTEL, L. – LIEBIG, L. – KATZENBACH, C. AI Federalism: Shaping AI Policy within States in Germany. In: *arXiv:2111.04454* [online]. 2021 [cit. 2025-07-10]. Dostupné na: <https://arxiv.org/abs/2111.04454>.

⁴⁸ Deutscher Bundestag. Bericht der Enquete-Kommission Künstliche Intelligenz – Gesellschaftliche Verantwortung und wirtschaftliche, soziale und ökologische Potenziale. Drucksache 19/23700 [online]. 19. Wahlperiode, 28. 10. 2020 [cit. 2025-07-10]. Dostupné na: <https://dserver.bundestag.de/btd/19/237/1923700.pdf>.

ústavného a civilného práva, bez systematickej regulácie zodpovednosti v prípade škody spôsobenej AI systémami.

Rakúsko doposiaľ taktiež neprijalo osobitnú legislatívu, ktorá by upravovala zodpovednosť umelej inteligencie. V roku 2021 však bola prijatá národná stratégia Artificial Intelligence Mission Austria 2030 (AIM AT 2030),⁴⁹ ktorá predstavuje ucelený rámec pre vývoj a uplatňovanie umelej inteligencie a vznikla za účasti expertov z oblasti práva, technológií, verejnej správy a spoločenských vied. Jedným z kľúčových pilierov stratégie je i oblasť verejnej správy, v ktorej sa zdôrazňuje potreba modernizácie administratívnych procesov prostredníctvom umelej inteligencie, avšak pri zachovaní rozhodovacej právomoci človeka tam, kde má rozhodnutie právny alebo individuálny dopad. V rámci tohto rámca sa rozpracúvajú opatrenia ako sektorové dátové plány, hodnotenie rizikovosti algoritmických systémov pred ich nasadením a školenia pre zamestnancov verejnej správy v oblasti digitálnych kompetencií. Z hľadiska zodpovednosti sa na prípady nasadenia umelej inteligencie uplatňuje všeobecná právna úprava – najmä Amtshaftungsgesetz, ktorý upravuje nároky na náhradu škody spôsobenej pri výkone verejnej moci. Navyše, uplatňujú sa aj existujúce inštitúty z občianskeho a správneho práva.

Ak zhrnieme vyššie uvádzané národné iniciatívy, v základných črtách sú prístupy jednotlivých krajín viac-menej obdobné. Ak verejná správa používa umelú inteligencia, musí vykonať dôkladné testovanie a posúdenie rizík pred nasadením, poskytovať vysvetliteľné a transparentné rozhodnutia občanom, monitorovať fungovanie AI systémov a pravidelne ich auditovať a umožniť dotknutým subjektom odvolanie proti rozhodnutiu, generované čiastočne alebo úplne umelou inteligenciou.

Pokiaľ ide o zodpovednostné východiská, štáty sa v tomto štádiu opierajú vzhľadom k chýbajúcej špeciálnej úprave o existujúce vnútroštátne pravidlá zodpovednosti, najmä vnútroštátnu úpravu zodpovednosti štátu za výkon verejnej moci, ak takáto osobitná úprava bola v danom štáte prijatá, o smernicu o zodpovednosti za vadné výrobky⁵⁰ a jej transponovanú vnútroštátnu úpravu ako aj o vnútroštátnu úpravu všeobecnej zodpovednosti za škodu. Štát musí v prípadoch nasadenia umelej inteligencie vo verejnej správe zabezpečiť, aby v prípadoch, keď preventívne opatrenia nedokážu zabrániť ujmám, boli dotknuté subjekty odškodnené rovnakým spôsobom, ako keby konal orgán verejnej moci prostredníctvom svojho zamestnanca, keďže rovnako ako zamestnanec, tak i použitie umelej inteligencie spadajú do sféry rizika orgánu verejnej moci. Uvedené platí bez ohľadu na to, či je systém, ktorý spôsobil škodu, navrhnutý deterministicky, alebo či je schopný sa učiť, a teda (aspoň *ex ante*) nie je predvídateľný v každom jednotlivom kroku.

⁴⁹ Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology (BMK). Artificial Intelligence Strategy of the Austrian Federal Government: Artificial Intelligence Mission Austria 2030 (AIM AT 2030) [online]. Vienna: Federal Ministry for Climate Action, Environment, Energy, Mobility, Innovation and Technology, 2021 [cit. 2025-07-10]. Dostupné na: https://digital-skills-jobs.europa.eu/sites/default/files/2023-10/Artificial%20Intelligence%20Mission%20Austria%202030_AIM_AT_2030.pdf?

⁵⁰ Smernica Európskeho parlamentu a Rady (EÚ) 2024/2853 z 23. októbra 2024 o zodpovednosti za chybné výrobky a o zrušení smernice Rady 85/374/EHS.

3. MOŽNOSTI RIEŠENIA ZODPOVEDNOSTI ZA NASADENIE UMELEJ INTELIGENCIE VO VEREJNEJ SPRÁVE V SLOVENSKOM PROSTREDÍ

Oblasti verejnej správy, v ktorých podľa dostupných údajov nájde používanie systémov umelej inteligencie na Slovensku v najbližšom časovom horizonte potenciálne svoje širšie využitie sú najmä oblasti výpočtu daňovej povinnosti daňových subjektov či výpočtu predpokladanej výšky dôchodkov alebo sociálnych dávok, čím by mohlo dôjsť k zlepšeniu prístupnosti a personalizácie služieb verejnej správy.⁵¹ V týchto prípadoch nejde priamo o rozhodovanie o právach, právom chránených záujmoch alebo povinnostiach v oblasti verejnej správy, trendy využívania systémov umelej inteligencie však naznačujú, že práve užívateľsky priaznivé aplikácie zamerané napr. na výpočet daňovej povinnosti alebo rôzne aplikácie spojené s prevádzkovými poriadkami alebo aplikáciou metodík vo verejných inštitúciách budú spravované systémami umelej inteligencie. Obdobne môže ísť z administratívneho hľadiska o faktické úkony vo verejnej správe, ktoré sa nevykonávajú vo formalizovanom postupe (ako napr. riadenie dopravy na križovatke), spĺňajú však atribúty úradného postupu. Inou oblasťou úradných postupov môže byť zahrnutie systémov umelej inteligencie do postupov kontroly vo verejnej správe, a to najmä do vonkajšej kontroly (napr. kontrola realizovaná Najvyšším kontrolným úradom Slovenskej republiky vo vzťahu k obciam, alebo k nemocniciam, či iným subjektom čerpajúcim prostriedky verejných rozpočtov) a do postupov správneho dozoru. V spomenutej oblasti môžu nástroje AI zahŕňať automatickú sumarizáciu dokumentov, generovanie zápisov zo stretnutí a generovanie protokolu o kontrole.⁵²

V slovenskom právnom prostredí obdobne ako vo väčšine zahraničných jurisdikcií absenteje osobitná úprava, ktorá by komplexne riešila otázky zodpovednosti za využívanie umelej inteligencie vo verejnej správe. V praxi tak možno momentálne uvažovať iba o aplikácii existujúcej deliktnej úpravy, prednostne vo vzťahu k verejnej správe o zákone č. 514/2003 Z. z. o zodpovednosti za škodu spôsobenú pri výkone verejnej moci príp. o všeobecnej civilnoprávnej zodpovednostnej úprave. Žiadna z týchto noriem síce explicitne nepočíta so špecifikami nasadenia umelej inteligencie, napriek tomu však možno uvažovať, či vôbec príp. do akej miery sú tieto pravidlá využiteľné aj v prípadoch zapojenia umelej inteligencie do rozhodovacej činnosti alebo do úradných postupov verejnej správy.

Existencia uvedenej právnej úpravy predstavuje v zmysle judikatúry realizáciu základného práva podľa čl. 46 ods. 3 Ústavy Slovenskej republiky,⁵³ ktoré je ústavnoprávnym

⁵¹ Umelá inteligencia v službách štátu: Ako pomôže verejnej správe? In: *Microsoft: Source EMEA* [online]. 10. 4. 2024 [cit. 2025-08-07]. Dostupné na: <https://news.microsoft.com/source/emea/features/umela-inteligencia-v-sluzbach-statu-ako-pomoze-verejnej-sprave/?lang=sk>.

⁵² MACKO, O. Umelá inteligencia už prichádza do verejnej správy aj na Slovensku. In: *touchIT* [online]. 16. 7. 2025 [cit. 2025-08-07]. Dostupné na: <https://touchit.sk/umela-inteligencia-uz-prichadza-do-verejnej-spravy-aj-na-slovensku/746169>.

⁵³ Podľa uvedeného ustanovenia: „Každý má právo na náhradu škody spôsobenej nezákonným rozhodnutím súdu, iného štátneho orgánu či orgánu verejnej správy alebo nesprávnym úradným postupom.“

základom pre uplatňovanie reparačných nástrojov vo vzťahu k adresátom verejnej moci.⁵⁴ Zmyslu uvedenej právnej úpravy preto podľa judikatúry zodpovedá požiadavka, aby každá ujma spôsobená nesprávnym či nezákonným zásahom štátu proti občanovi bola odčinená, keďže štát musí niesť objektívnu zodpovednosť za konanie svojich orgánov, ak nimi zasiahol do základných práv adresáta verejnej moci⁵⁵ a to bez ohľadu na to, aké prostriedky a mechanizmy štát použil. Účelom zákona č. 514/2003 Z. z. je teda ustanoviť podmienky, za ktorých vzniká právo na náhradu škody spôsobenej nezákonným rozhodnutím orgánu alebo jeho nesprávnym úradným postupom.

Vo vzťahu k nezákonnému rozhodnutiu ako rozhodnutiu orgánu verejnej moci, ktoré je v rozpore s právnym poriadkom Slovenskej republiky⁵⁶ nie je čo do predpokladov vzniku zodpovednosti či právnych následkov rozdiel, či takéto rozhodnutie vydal orgán prostredníctvom ľudského prvku alebo prostredníctvom (polo)automatizovaného systému. Tak ako môže byť nezákonné rozhodnutie dôsledkom nesprávneho právneho posúdenia prípadu ľudským prvkom príp. nesprávneho alebo nedostatočne zisteného či vyhodnoteného skutkového stavu osobou konajúcou v mene daného orgánu, rovnako môže k takýmto či iným vadám konania, ktoré sú spojené s rozhodnutím vo veci samej dôjsť, ak ľudský prvok nahradí umelá inteligencia. Samozrejme aj pre rozhodnutia vygenerované umelou inteligenciou za súčasnej úpravy platí, že by museli byť z dôvodu nezákonnosti zrušené alebo zmenené príslušným orgánom.⁵⁷

Rozhodnutia sú len jedným druhom foriem činnosti verejnej správy, ktorý zatiaľ nie je v slovenských podmienkach realizovaný pomocou umelej inteligencie.

Súčasná úroveň využívania umelej inteligencie – napríklad prostredníctvom chatbotov poskytujúcich klientom informácie o postupoch správnych orgánov, automatizovaných sprievodcov pri vyplňovaní formulárov alebo analytických nástrojov predbežne vyhodnocujúcich údaje, však už dnes vytvára interakcie medzi občanom a orgánom verejnej správy sprostredkované algoritmom. Aj keď tieto systémy formálne nevydávajú rozhodnutia v správnom konaní, ich činnosť môže viesť k ujme na právom chránených statkoch občana. Typickým príkladom môže byť situácia, keď chatbot poskytne nesprávnu alebo neúplnú informáciu o lehotách na podanie opravného prostriedku, občan zmešká zákonnú lehotu, v dôsledku čoho dôjde uňho k ujme.

Samozrejme základným predpokladom pre uplatnenie nároku na kompenzáciu vzniknutej ujmy v takomto či obdobnom prípade použitia umelej inteligencie je posúdenie, či jej konanie napĺňa znaky úradného postupu, ktorý bol nesprávny. Zákon definuje nesprávny úradný postup ako výkon právomoci orgánom verejnej moci, pri ktorom dôjde k porušeniu právnou normou ustanoveného predpísaného postupu alebo k porušeniu účelu, ku ktorému postup orgánu verejnej moci pri výkone verejnej moci smeruje. Za nesprávny úradný postup sa považuje aj porušenie povinnosti orgánu verejnej moci urobiť úkon alebo vydať rozhodnutie v zákonom ustanovenej lehote, nečinnosť orgánu verejnej moci pri výkone verejnej moci, zbytočné prieťahy v konaní alebo iný

⁵⁴ Rozsudok Najvyššieho správneho súdu Slovenskej republiky sp. zn. I/Svk/9/2023, zo dňa 28. 3. 2024.

⁵⁵ Nález Ústavného súdu Slovenskej republiky sp. zn. I. ÚS 320/2016, zo dňa 7. 7. 2016.

⁵⁶ Nález Ústavného súdu Slovenskej republiky sp. zn. IV. ÚS 159/2012, zo dňa 3. 7. 2012.

⁵⁷ Uznesenie Ústavného súdu Slovenskej republiky sp. zn. I. ÚS 65/2019, zo dňa 6. 3. 2019.

nezákonný zásah do práv, právom chránených záujmov fyzických osôb a právnických osôb. Nesprávnym úradným postupom je teda porušenie povinnosti orgánu verejnej moci konať alebo nekonať v súlade s právnymi predpismi, pričom nie je nevyhnutné, aby výsledkom bol správny akt – postačí, že ide o akúkoľvek činnosť súvisiacu s výkonom verejnej moci, ktorá má nepriaznivý následok pre účastníka.

Definícia nesprávneho úradného postupu zavedená slovenským zákonodarcom v roku 2023 je podľa dôvodovej správy k zákonu č. 239/2023 Z. z. natoľko široká, že pokrýva všetky možnosti nesprávneho úradného postupu, a zahŕňa tak formalizované úkony orgánov verejnej moci v rámci konania, ako aj úkony mimo rámca formalizovaných procesov, tak postup, ktorý je v rozpore s právnymi predpismi, ako aj postup, ktorý nemusí byť vo výslovnom rozpore s právnymi predpismi, vrátane prípadov, ak podrobná úprava postupu absentuje, ale je v rozpore s účelom postupu orgánu verejnej moci.⁵⁸ Súdy teda v zásade nevolia vo vzťahu k výkladu a aplikácii pojmu nesprávny úradný postup reštriktívny výklad. Naopak pojem nesprávny úradný postup je podľa zákona č. 514/2003 Z. z. definovaný široko a otvorene s demonštratívnym výpočtom okolností, ktoré možno posúdiť ako nesprávny úradný postup, a taxatívnym výpočtom okolností, ktoré za nesprávny úradný postup považovať nemožno.

Uvedený prístup tak umožňuje zahrnúť do rámca nesprávneho úradného postupu rôzne formy zapojenia umelej inteligencie, a to aj také, ktoré nie sú výslovne upravené v procesných predpisoch, avšak svojou povahou, obsahom a dôsledkami predstavujú výkon verejnej moci.

Problematickým sa však podľa zákona javí pri využívaní umelej inteligencie uplatnenie regresného práva štátu voči subjektu, ktorý reálne ujmu na právom chránených záujmoch občana spôsobil. Ustanovenie § 22 ods. 1 písm. c) zákona č. 514/2003 Z. z. vychádza z predpokladu, že škoda spôsobená nezákonným rozhodnutím alebo nesprávnym úradným postupom má vždy identifikovateľného ľudského pôvodcu – fyzickú osobu oprávnenú konať pri výkone verejnej moci (ktorá vydala nezákonné rozhodnutie alebo sa podieľala na nesprávnom úradnom postupe ako osoba na to oprávnená), voči ktorej môže štát uplatňovať právo regresu. Tento koncept je však problematický pri aplikácii v kontexte umelej inteligencie, najmä ak je rozhodovací proces plne alebo prevažne automatizovaný.

Ak systém umelej inteligencie prijme rozhodnutie, ktoré sa následne ukáže byť nezákonným alebo realizuje nesprávny úradný postup, nevzniká jasná možnosť určiť „fyzickú osobu, ktorá rozhodnutie vydala alebo sa podieľala na nesprávnom úradnom postupe“ v zmysle § 22 ods. 1 písm. c). Funkcie, ktoré by v tradičnom prostredí vykonával úradník, sú totiž rozdelené medzi rôzne fázy návrhu, tréningu a implementácie algoritmu, pričom zodpovednosť sa v tomto prípade rozptyľuje medzi programátora, dodávateľa, správcu systému príp. iné subjekty, ktoré sa podieľali na vytvorení či fungovaní umelej inteligencie. To, že zákon č. 514/2003 Z. z. neobsahuje explicitnú úpravu regresu vo vzťahu k rozhodovacím procesom realizovaným prostredníctvom umelej inteligencie, neznamená, že regresný nárok podľa tohto zákona nemožno v prípade

⁵⁸ K tomu bližšie pozri: Dôvodová správa k zákonu č. 239/2023 Z. z. In: *najpravo.sk* [online]. 1. 8. 2024 [cit. 2025-07-28]. Dostupné na: <https://www.najpravo.sk/dovodove-spravy/rok-2023/dovodova-sprava-k-zakonu-c-239-2023-z-z.html>.

jej nasadenia uplatniť vôbec. V individuálne posúdených prípadoch je možné využiť regresné ustanovenia tohto zákona, ak sa pri stanovenej povinnosti dohľadu či kontroly nad umelou inteligenciou ľudským prvkom preukáže príčinná súvislosť medzi (ne) konaním konkrétnej fyzickej osoby pri výkone verejnej moci, hoci s asistenciou umelej inteligencie. Navyše, nemožno vylúčiť uplatnenie regresu alebo obdobných nárokov na základe svojbytných právnych titulov vyplývajúcich z iných ustanovení právneho poriadku, napríklad z občianskoprávnej alebo obchodnoprávnej zodpovednosti z rôznych typov zmluvných záväzkov, predpisov o kybernetickej bezpečnosti či osobitných sektorových úprav. Takýto prístup síce vyžaduje komplexnejšie právne posúdenie, avšak umožňuje za súčasného stavu absencie osobitnej úpravy reagovať aj na situácie vyvolané autonómnym alebo poloautonómnym fungovaním umelej inteligencie.

ZÁVER

Zodpovednostné aspekty pri využívaní umelej inteligencie vo verejnej správe sa opierajú o kombináciu rôznych právnych či odporúčacích rámcov, pričom však žiadny z nich nie je špecifickou záväznou zodpovednostnou úpravou pre využívanie umelej inteligencie. Kým niektoré z rámcov upravujú všeobecné otázky využívania umelej inteligencie so stanovením pravidiel a zásad tohto procesu (napr. Akt o umelej inteligencii), iné riešia špecifické otázky ťažiskovo sa dotýkajúce inej oblasti úpravy, do ktorej čiastočne môže zasiahnuť aj automatizácia (napr. nariadenie GDPR), pričom aplikovateľná zodpovednostná legislatíva v oblasti umelej inteligencie vychádza v súčasnosti prevažne z existujúcich všeobecných právnych rámcov, ktoré neboli pôvodne koncipované s ohľadom na špecifiká umelej inteligencie (napr. pravidlá upravujúce zodpovednosť štátu za škodu spôsobenú jeho orgánmi pri výkone verejnej moci alebo pravidlá upravujúce zodpovednosť za škodu spôsobenú vadným výrobkom, či pravidlá všeobecnej civilnoprávnej zodpovednosti). Tento stav prináša viacero interpretačných a aplikačných výziev, keďže tradičné kategórie zodpovednosti, ako je zavinenie, príčinná súvislosť či povinnosť náležitej starostlivosti, sa nie vždy jednoducho prenášajú na autonómne a adaptívne systémy.

Vo vzťahu k využívaniu umelej inteligencie vo verejnej správe možno z jednotlivých právnych rámcov uvádzaných v článku (vrátane prípadných inšpiračných zdrojov štátov, ktoré prijali špecifickú legislatívu k využívaniu umelej inteligencie vo verejnej správe) vyabstrahovať niektoré z ťažiskových povinností verejných inštitúcií, ktoré by mohli predstavovať základ pre kompenzáciu vzniknutej ujmy. Verejné inštitúcie by pri implementácii a prevádzkovaní systémov umelej inteligencie mali dodržiavať zásady zákonnosti, transparentnosti a vysvetliteľnosti algoritmov, používanie umelej inteligencie musí byť v súlade s právom na ochranu osobných údajov a nesmie porušovať právo na súkromie, rovnosť a zákaz diskriminácie. Musí zároveň umožniť ľudskú kontrolu nad rozhodovacími procesmi, najmä v oblastiach, ktoré môžu zásadne ovplyvniť práva a záujmy občanov. Ak systém umelej inteligencie nefunguje v súlade so stanovenými zásadami a právnymi normami, je zodpovednosť štátu za využívanie umelej inteligencie vo verejnej správe kľúčová pre ochranu občanov pred možnými právnymi a etickými

rizikami, ktoré automatizované rozhodovanie alebo iné nasadenie umelej inteligencie môže priniesť.

doc. JUDr. Marianna Novotná, PhD.
Právnická fakulta Trnavské univerzity v Trnave
marianna.novotna@gmail.com

JUDr. Zuzana Adamová, PhD.
Právnická fakulta Trnavské univerzity v Trnave
zuzana.adamova@gmail.com

doc. JUDr. Michal Maslen, PhD.
Právnická fakulta Trnavské univerzity v Trnave
michal.maslen@truni.sk