ACTA FACULTATIS IURIDICAE UNIVERSITATIS COMENIANAE
Tomus XLIII
2/2024

VPLYV REGULÁCIE UMELEJ INTELIGENCIE NA LEGISLATÍVU KYBERNETICKEJ BEZPEČNOSTI VO VEREJNEJ SPRÁVE (1. DIEL)

PhDr. JUDr. Mgr. Ervín Šimko, MBA, LL.M.

Akadémia policajného zboru v Bratislave
Katedra informatiky a manažmentu
ervin.simko@akademiapz.sk

JUDr. Matúš Mesarčík, PhD., LL.M.

Univerzita Komenského v Bratislave, Právnická fakulta
Ústav práva informačných technológií a práva duševného vlastníctva
matus.mesarcik@flaw.uniba.sk

Vplyv regulácie umelej inteligencie na legislatívu kybernetickej bezpečnosti vo verejnej správe (1. diel)

Rýchly rozvoj umelej inteligencie (AI) výrazne mení spôsob fungovania rôznych oblastí spoločenského a hospodárskeho života, vrátane verejnej správy. Táto technológia prináša so sebou nové možnosti, ako sú automatizácia procesov, efektívnejšie spracovanie dát a poskytovanie kvalitnejších služieb občanom. Na druhej strane však AI predstavuje aj nové hrozby, najmä v oblasti kybernetickej bezpečnosti, keďže zvyšuje riziká útokov na digitálne systémy a infraštruktúru. Preto je nevyhnutné, aby sa existujúca legislatíva kybernetickej bezpečnosti vo verejnej správe prispôsobila týmto technologickým zmenám. Cieľom tohto článku je detailne analyzovať, akým spôsobom regulácia AI ovplyvňuje legislatívu kybernetickej bezpečnosti vo verejnej správe Slovenskej republiky. Hlavnou súčasťou skúmania bude dôkladná analýza dopadov nariadenia Európskej únie č. 2024/1689, známeho ako Akt o umelej inteligencii, na právne predpisy týkajúce sa kybernetickej bezpečnosti a ich aplikáciu v praxi. Výsledkom bude identifikácia kľúčových oblastí, v ktorých sa vyžadujú úpravy a doplnenia legislatívnych rámcov.

The impact of AI regulation on cybersecurity legislation in public administration (Part 1)

The rapid development of artificial intelligence (AI) is significantly changing the functioning of various areas of social and economic life, including public administration. This technology brings new opportunities, such as process automation, more efficient data processing, and the provision of higher-quality services to citizens. On the other hand, AI also introduces new threats, particularly in the field of cybersecurity, as it increases the risks of attacks on digital systems and infrastructure. Therefore, it is essential that the existing cybersecurity legislation in public administration adapts to these technological changes. The aim of this article is to analyze in detail how AI regulation impacts cybersecurity legislation in the public administration of the Slovak Republic. A key part of the research will focus on the thorough analysis of the effects of the European Union regulation no. 2024/1689, known as the Artificial Intelligence Act, on legal provisions related to cybersecurity and their practical application. The outcome will be the identification of key areas where amendments and updates to the legislative framework are required.

Kľúčové slová: umelá inteligencia, kybernetická bezpečnosť, informačné technológie vo verejnej správe

Key words: Artifical intelligence, cybersecurity, information technologies in public governance

https://doi.org/10.62874/afi.2024.2.08

Úvod

Umelá inteligencia (*articial intelligence*, AI) preniká do všetkých sfér nášho života, vrátane verejnej správy, a prináša so sebou revolučné zmeny. Potenciál AI na zefektívnenie procesov, zlepšenie rozhodovania a poskytovanie personalizovaných služieb je obrovský. Od inteligentných chatbotov, ktoré odpovedajú na otázky občanov, až po sofistikované algoritmy, ktoré analyzujú veľké dáta a predpovedajú budúce trendy na úrovni štátu, AI mení spôsob, akým verejná správa funguje.

Zároveň však rýchly vývoj AI prináša aj nové výzvy, najmä v oblasti kybernetickej bezpečnosti. Zraniteľnosti v systémoch poháňaných AI môžu byť zneužité na rôzne účely, od krádeže citlivých údajov až po manipuláciu s výsledkami volieb. Tretie strany môžu využiť pokročilé

techniky strojového učenia na obchádzanie bezpečnostných opatrení a vytvoriť sofistikované phishingové útoky, ktoré sú takmer nerozoznateľné od legitímnej komunikácie. Z toho plynie nebezpečenstvo pri existujúcich špecifických technologických výzvach týkajúcich sa AI, na ktoré zatiaľ neboli zavedené žiadne overené bezpečnostné praktiky ani konkrétne štandardy na ich riešenie.[1]

Výzvy v kybernetickej bezpečnosti a AI môžeme rozdeliť do dvoch hlavných oblastí: (i) organizačné výzvy, ktoré sa týkajú harmonizácie samotnej terminológie, riadenia bezpečnosti životného cyklu AI a prispôsobenia existujúcich bezpečnostných opatrení pre AI; a (ii) výskumné a vývojové výzvy, ktoré sa zameriavajú na hodnotenie útokov na modely strojového učenia, vývoj špecifických bezpečnostných opatrení pre AI, definovanie metrík pre kybernetickú bezpečnosť AI a vyhodnocovanie rovnováhy a kompromisov medzi presnosťou a bezpečnosťou. Tieto výzvy zdôrazňujú potrebu komplexného prístupu na zabezpečenie bezpečnosti AI systémov.[2]

Ako sa teda má legislatíva kybernetickej bezpečnosti vo verejnej správe prispôsobiť tejto novej realite? Súčasné právne predpisy boli síce navrhnuté pre digitálne prostredie, ale AI predstavuje pre ich aplikáciu zásadnú výzvu. Aj z tohto dôvodu Európska únia (EÚ) na jar roku 2024 prijala prvý právny rámec pre AI v Európe v podobe 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 len ako Akt o AI alebo AIA).[3] Predmetný právny rámec nie je možné vnímať izolovane od ostatných právnych predpisov, nakoľko napríklad otázky kybernetickej bezpečnosti či verejnej správy reguluje iba minimálnym spôsobom a z tohto dôvodu je nevyhnutné aplikovať aj osobitné právne rámce, ktoré sa týchto otázok týkajú.

Cieľom predkladaného článku je analyzovať, aký vplyv má regulácia AI v podobe Aktu o AI na legislatívu kybernetickej bezpečnosti vo verejnej správe. Zameriame sa na otázky, ako je AI využívaná vo verejnej správe. Hlbšie analyzujeme nedávno prijatý Akt o AI, pričom sa

[1] PAPERNOT, N. et al. *Towards the Science of Security and Privacy in Machine Learning*. ArXiv [online]. [cit. 10-9-2024]. Dostupné na:: https://doi.org/10.48550/arXiv.1611.03814.

[2] JUNKLEWITZ, H. et al. *Cybersecurity of Artificial Intelligence in the AI Act*. Publications Office of the European Union, Luxembourg, 2023. [online]. [cit. 10-9-2024]. Dostupné na: doi:10.2760/271009, JRC134461.

[3] Ú. v. EÚ L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj.

osobitne budeme sústrediť na otázky kybernetickej bezpečnosti. Tieto poznatky následne budeme syntetizovať a posúdime pripravenosť právneho rámca kybernetickej bezpečnosti vo verejnej správe v rámci právneho poriadku Slovenskej republiky. Na zodpovedanie otázok bude použitá kombinácia deskriptívnej a analytickej metódy. Autori vykonali výskum relevantnej literatúry, právnych predpisov, a verejne dostupných medializovaných prípadov. Výsledky analyzovali a interpretovali v kontexte súčasného stavu kybernetickej bezpečnosti a vývoja AI. Na základe vykonanej analýzy sú formulované konkrétne odporúčania pre týkajúce sa legislatívy kybernetickej bezpečnosti vo verejnej správe v kontexte rozvoja AI. Tento článok poskytne prehľad o vzájomnom pôsobení regulácie AI a legislatívy kybernetickej bezpečnosti vo verejnej správe.

1. Umelá inteligencia vo verejnej správe

Ako sme už spomenuli, umelá inteligencia nachádza čoraz širšie uplatnenie aj vo verejnej správe, nie iba v súkromnom sektore. Mnohí odborníci veria, že AI môže výrazne zefektívniť spravodlivé verejné služby. OECD dokonca zdôrazňuje[4] jej kľúčovú úlohu pri budovaní moderných verejných administratív. Príklady využitia AI sú rôznorodé: od inteligentných chatbotov pre komunikáciu s občanmi[5] až po prediktívnu analýzu pre optimalizáciu služieb[6] a prevenciu podvodov.[7]

Podľa prehľadovej štúdie využitia AI vo verejnej správe[8] možno umelú inteligenciu využiť vo verejnej správe na výrazné zvýšenie efektívnosti, účinnosti a schopnosti reagovať na potreby administratívy. Schopnosť AI rýchlo a presne spracovať a analyzovať obrovské množstvo údajov umožňuje reprezentantom štátu prijímať informovanejšie rozhodnutia. Konkrétne, AI dokáže identifikovať vzory a trendy

[4] UBALDI, B. et al. *State of the art in the use of emerging technologies in the public sector*. OECD Working Papers on Public Governance No. 34, GOV/PGC/EGOV(2019)13. [online]. [cit. 10-9-2024]. Dostupné na: https://doi.org/10.1787/932780bc-en.

[5] KARLIN, M. et al. *Responsible Artificial Intelligence in the Government of Canada: Digital Disruption.* White Paper Series, Version 2.0, s. 3.

[6] KUBLER, K. State of Urgency: Surveillance, Power and Algorithms in France's State of Emergency. In 4:2 *Big Data & Soc* 1, 2019.

[7] ROOSEN, M. *What SyRi can teach us about technical solutions for societal challenges*. Global Data Justice (20 February 2020). [online]. [cit. 10-9-2024]. Dostupné na: https://globaldatajustice.org/2020-02-20-roosen-syri.

[8] HAMIRUL, D. The Role of Artificial Intelligence in Government Services: A Systematic Literature Review. In *Open Access Indonesia Journal of Social Sciences* 6 (3), 998-1003. Dostupné na: https://doi.org/10.37275/oaijss.v6i3.163.

v demografických, ekonomických a sociálnych údajoch, ktoré sú neoceniteľné pre tvorbu politík a strategické plánovanie.[9] Chatboty a virtuálni asistenti poháňaní umelou inteligenciou sa využívajú na poskytovanie nepretržitej pomoci verejnosti, čím sa účinne skracuje čas čakania a ľudské zdroje sa môžu sústrediť na zložitejšie úlohy.[10] Tieto systémy AI dokážu efektívne vybavovať otázky, nahlasovať problémy a ponúkať pomoc, čím zlepšujú poskytovanie verejných služieb. Okrem toho aplikácie AI zefektívňujú administratívne procesy, ako je spracovanie žiadostí o licencie, platenie daní a iných dokumentov, čím znižujú byrokraciu a zvyšujú spokojnosť verejnosti.[11] Prediktívna analytika, ďalšia dôležitá aplikácia AI, pomáha vládam predvídať a zmierňovať budúce riziká, ako sú hospodárske zmeny alebo environmentálne riziká, čo umožňuje proaktívne rozhodovanie.[12]

Osobitne je potrebné zvýrazniť vplyv AI v sektore kritickej infraštruktúry. Umelá inteligencia sa čoraz viac využíva v kritickej infraštruktúre štátov na zvýšenie bezpečnosti, efektívnosti a odolnosti. Kritická infraštruktúra zahŕňa základné služby a zariadenia, ako sú energetické, vodné, dopravné, zdravotnícke a komunikačné systémy. Aplikácie AI v týchto sektoroch sa zameriavajú na prediktívnu údržbu, odhaľovanie hrozieb, optimalizáciu a automatizáciu, čím sa zvyšuje prevádzková spoľahlivosť a schopnosť reakcie.

V energetickom sektore sa AI využíva na optimalizáciu riadenia energetickej siete a integráciu obnoviteľných zdrojov energie. AI analyzuje údaje z inteligentných sietí s cieľom predpovedať dopyt po energii, riadiť distribúciu zaťaženia a predchádzať výpadkom.[13] Prediktívna údržba využívajúca AI identifikuje potenciálne poruchy zariadení skôr, ako nastanú, čím sa znižujú prestoje a náklady na údržbu. AI môže napríklad monitorovať stav transformátorov a iných kritických komponentov a upozorňovať operátorov na problémy, ktorým treba venovať pozornosť.

[9] MIKHAYLOV, S. et al. Artificial intelligence for the public sector: opportunities and challenges of cross-sector collaboration. In *Philos Trans R Soc*. 376(2128):20170357.

[10] LAMBERTI, L. et al. Benefits sought by citizens and channel attitudes for multichannel payment services: evidence from Italy. In *Gov Inf Q*. 31(4), s. 596–609.

[11] AGARWAL, P. Public Administration Challenges in the World of AI and Bots. In *Public Administration Review*. Volume 78, Issue 6, s. 917-921

[12] GOBBLE, M. Digital strategy and digital transformation. In *Res Technol. Manag*. 61(5), s. 66–71.

[13] MICRO.AI. Enabling Predictive Maintenance in Energy Production. [online]. [cit. 10-9-2024]. Dostupné na: https://micro.ai/resources/enabling-predictive-maintenance-in-energy-production.

Sektor dopravy využíva výhody AI prostredníctvom inteligentných systémov riadenia dopravy, ktoré analyzujú údaje v reálnom čase s cieľom znížiť preťaženie a zvýšiť bezpečnosť. AI dokáže predpovedať dopravné modely, optimalizovať časovanie svetelných signálov a poskytovať vodičom alternatívne trasy.[14] Vo verejnej doprave AI zlepšuje plánovanie cestovných poriadkov a trás, čo vedie k efektívnejšej prevádzke a lepším službám pre cestujúcich.

Umelá inteligencia zohráva kľúčovú úlohu aj v hospodárení s vodou, pretože predpovedá vzorce spotreby, zisťuje úniky a optimalizuje procesy úpravy vody. Inteligentné senzory monitorujú kvalitu vody a distribučné siete v reálnom čase, čím zabezpečujú bezpečné a spoľahlivé dodávky vody.[15]

V oblasti kybernetickej bezpečnosti AI zvyšuje ochranu kritickej infraštruktúry tým, že účinnejšie odhaľuje hrozby a reaguje na ne. Algoritmy strojového učenia analyzujú sieťovú prevádzku, identifikujú anomálie a reagujú na kybernetické útoky v reálnom čase. Bezpečnostné systémy riadené umelou inteligenciou poskytujú nepretržité monitorovanie a dokážu sa prispôsobiť novým hrozbám, čím zabezpečujú odolnosť kritickej infraštruktúry voči kybernetickým hrozbám.[16]

2. Regulácia umelej inteligencie v EÚ

Európska únia sa od roku 2021 intenzívne venuje regulácii umelej inteligencie. Po originálnom návrhu Európskej komisie a stanoviskách Rady EÚ a Európskeho parlamentu sa v decembri 2023 podarilo dosiahnuť politickú dohodu na konečnom znení nariadenia o umelej inteligencii (AIA alebo AI Akt). Samotné nariadenie vstúpi do platnosti v niekoľkých fázach v priebehu rokov 2025 až 2027. Európska únia sa rozhodla regulovať umelú inteligenciu z niekoľkých dôvodov: obavy o bezpečnosť, ochranu súkromia a ľudských práv, nedostatok jasných pravidiel pre firmy a orgány činné v trestnom konaní, a tiež kvôli

[14] JARRAHI, M.H. et al. Artificial intelligence and knowledge management: A partnership between human and AI. In *Business Horizon*s. Volume 66, Issue , January–February 2023, s. 87-99.

[15] KRISHNAN, S.R. et al. Smart Water Resource Management Using Artificial Intelligence – A Review. In *Sustainability* 2022, 14, 13384. Dostupné na: https://doi.org/10.3390/su142013384.

[16] SAKHNINI., J. et al. In: CHOO, KK., DEHGHANTANHA, A. (eds) Handbook of *Big Data Privacy*. Springer, Cham. Dostupné na: https://doi.org/10.1007/978-3-030-38557-6_2.

potrebe jednotného európskeho trhu.[17] AIA má za cieľ harmonizovať pravidlá pre vývoj a používanie AI v celej Európe. Zakáže najrizikovejšie systémy AI, stanoví požiadavky pre systémy s vysokým rizikom (napríklad tie, ktoré sa používajú v zdravotníctve alebo pri nábore zamestnancov) a zabezpečí transparentnosť pre ostatné systémy. AIA je formulovaná ako produktová regulácia a porovnať to možno s požiadavkami na produkty ako napríklad zdravotnícke pomôcky alebo elektronické výrobky pri uvedení na trh. To znamená, že určuje špecifické vlastnosti a požiadavky na systémy AI, ktoré musia byť splnené pri uvedení na trh a veľkú zodpovednosť ponecháva na samotných prevádzkovateľoch týchto systémov prostredníctvom inštitútu posúdenia zhody (*conformity assessment*). Takmer vôbec sa regulácia netýka systémov AI nízkeho resp. minimálneho rizika, kde ustanovuje iba požiadavky na transparentnosť a odporúčanie prijatia kódexov správania, ktoré výrobcovia a prevádzkovatelia takýchto AI systémov budú dodržiavať. Osobitne AIA upravuje povinnosti pre systémy umelej inteligencie na všeobecné účely (pôvodne základné modely, z originálu *foundation models*).

Zaujímavosťou sú aj sankcie za porušenie AIA. Tie sú upravené ešte striktnejšie ako pri nariadení o ochrane údajov. Za porušenie ustanovení AIA bude možné uložiť pokutu až do výšky 35 000 000 EUR, alebo ak je porušiteľom spoločnosť, až do výšky 6,5 % jej celkového svetového ročného obratu za predchádzajúci účtovný rok, podľa toho, ktorá suma je vyššia za porušenie zakázaných praktík a nesúlad s požiadavkami na správu údajov. Ďalej AIA umožňuje správne pokuty do výšky 15 000 000 EUR a 7 500 000 EUR.[18]

AIA ustanovuje povinnosť pre členské štáty kreovať alebo určiť dozorný orgán, ktorý bude vykonávať štátny dozor. Na úrovní EÚ zároveň vznikne Európska rada pre umelú inteligenciu a Úrad pre umelú inteligenciu (*AI Office*). Zároveň bude musieť každý členský štát dezignovať národný dozorný orgán.

Kľúčovou definíciou regulácie je pojem systémy AI. Ten je definovaný ako *„strojový systém, ktorý je navrhnutý tak, aby fungoval s rôznou úrovňou autonómie a ktorý môže pre explicitné alebo implicitné ciele vytvárať výstupy, ako sú predpovede, odporúčania alebo*

[17] EURÓPSKA KOMISIA. *Commission staff working document impact assessment accompanying the 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} - {SEC(2021) 167 final} - {SWD(2021) 85 final}.

[18] AIA, článok 71.

rozhodnutia, ktoré ovplyvňujú fyzické alebo virtuálne prostredie."[19] Predmetná definícia vychádza z dokumentov na úrovni Organizácie pre hospodársku spoluprácu a rozvoj (OECD).

AIA diferencuje medzi niekoľkými subjektami, ktoré hrajú významnú alebo menej významnú rolu pri vývoji, nasadzovaní a používaná systémov AI. Regulácie pracuje s pojmami poskytovateľ (*provider*), subjekt, ktorý systém nasadzuje (*deployer*), dovozca (*importer*), distribútor (*distributor*) a prevádzkovateľ (*operator*).[20] AIA by sa mala vzťahovať na poskytovateľov systémov AI bez ohľadu na to, či sú v EÚ usadení alebo nie, postačí, ak je splnené kritérium, že budú systémy AI uvádzať na trhu alebo prevádzkovať v rámci EÚ.[21] Extrateritoriálna pôsobnosť AIA je zvýraznená aj tým, že sa bude vzťahovať na poskytovateľov používateľov systémov AI z tretích krajín, ak výstupy tvorené ich systémami sa využívajú v EÚ.[22] Špecifické požiadavky sú smerované aj na subjekty, ktoré AI nasadzujú. Z hľadiska negatívnej pôsobnosti sa AIA nevzťahuje na systémy umelej inteligencie vyvinuté alebo používané výlučne na vojenské účely a na produkty v rámci právnych aktov výslovne vymenovaných v článku 2 ods. 2 AIA. Z pôsobnosti sú vyňate systémy AI vyvíjané na výskumné účely a pre výlučné osobnú (*non-professional*) potrebu. Do pôsobnosti AIA taktiež nepatria open-source systémy AI, ktoré nepredstavujú vysoké riziko z pôsobnosti AIA.

3. Regulácia AI v kontexte verejnej správy s osobitným zreteľom na požiadavky kybernetickej bezpečnosti

AIA sa automaticky nevzťahuje na všetky systémy AI, ale prevažne sa bude aplikovať na systémy AI, ktoré sú súčasťou produktu v rámci špecifickej produktovej právnej úpravy[23] ako sú hračky alebo medicínske pomôcky. Ak je AI súčasťou alebo samostatným produktom pri niektorej z uvedených produktových regulácií, vzťahuje sa na nich kľúčová časť AIA, ktorá obsahuje drvivú väčšinu povinností pre systémy AI.

[19] AIA, článok 3 bod 1.

[20] K vysvetleniu pojmov pozri bližšie KPMG. Decoding the EU AI Act. [online]. [cit. 10-9-2024]. Dostupné na: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2024/02/decoding-the-eu-artificial-intelligence-act.pdf.

[21] AIA, článok 2.

[22] AIA, článok 2 ods. 1 písm. c).

[23] Tieto výslovne AIA menuje v Prílohe I.

Ak systém AI nespadá pod osobitnú reguláciu, prevádzkovatelia skúmajú prílohu III AIA, ktorá ustanovuje oblasti AI vysokého rizika, na ktoré sa následne právny akt vrátane kľúčovej tretej časti aplikuje. Konkrétne ide o oblasti:

- Diaľková biometrická identifikácia, biometrická kategorizácia osôb na základe citlivých alebo chránených atribútov a rozpoznávanie emócií;
- Riadenie a prevádzka kritickej infraštruktúry, vrátane digitálnej infraštruktúry;
- Vzdelávanie a odborná príprava;
- Zamestnanosť, riadenie pracovníkov a prístup k samostatnej zárobkovej činnosti;
- Prístup k základným súkromným a verejným službám a dávkam a ich využívanie;
- Presadzovanie práva;
- Migrácia, azyl a riadenie kontroly hraníc; a
- Výkon spravodlivosti a demokratické procesy.

Každá z vyššie uvedených oblastí je následne v Prílohe III charakterizovaná prostredníctvom viacerých konkrétnych aplikácií. Napríklad, oblasť spravodlivosti a demokratických procesov zahŕňa *„systémy AI, ktoré má používať justičný orgán alebo ktoré sa majú používať v jeho mene na pomoc justičnému orgánu pri skúmaní a interpretácii skutkových okolností a práva a pri uplatňovaní práva na konkrétny súbor skutkových okolností alebo ktoré sa majú používať obdobným spôsobom pri alternatívnom riešení sporov.“*[24] V kontexte verejnej správy sú osobitne zaujímavé oblasti riadenia a prevádzky kritickej infraštruktúry, presadzovania práva a prístup k základným verejným alebo súkromným službám. Z pohľadu prevádzkovania kritickej infraštruktúry do tejto oblasti spadajú systémy AI, ktoré *„sa majú používať ako bezpečnostné komponenty pri riadení a prevádzke kritickej digitálnej infraštruktúry, cestnej premávky alebo pri dodávkach vody, plynu, tepla alebo elektriny.“*[25] Kritickú digitálnu infraštruktúru bude osobitne definovať implementácia európskej smernice o odolnosti kritickej infraštruktúre,[26] ktorú budeme diskutovať v nasledujúcich častiach. V súvislosti s prístupom k základným verejným službám

[24] AIA, Príloha III, bod 8 písm. a).

[25] AIA, Príloha III, bod 2.

[26] Smernica Európskeho parlamentu a Rady (EÚ) 2022/2557 zo 14. decembra 2022 o odolnosti kritických subjektov a o zrušení smernice Rady 2008/114/ES, Ú. v. EÚ L 333, 27.12.2022, s. 164 – 198.

je možné akcentovať AI systémy využívané orgánmi verejnej moci alebo ktoré sa majú používať v ich mene na hodnotenie oprávnenosti fyzických osôb na základné dávky a služby verejnej pomoci vrátane služieb zdravotnej starostlivosti[27] či systémy AI určené na hodnotenie a klasifikáciu tiesňových volaní fyzických osôb alebo na vysielanie záchranných služieb prvej reakcie vrátane zo strany polície, hasičov a zdravotníckej pomoci.[28] Osobitne ako oblasť vysokého rizika AIA reguluje orgány presadzovania práva a využívanie AI systémov na rôzne účely ako napríklad polygrafy alebo profilovanie.[29] Je teda evidentné, že minimálne vo vyššie uvedených oblastiach prijatý AI Akt ovplyvní reguláciu a implementáciu AI vo verejnej správe.

Drvivá väčšina požiadaviek v AIA sa zameriava na regulácie systémov AI vysokého rizika. Ak bude chcieť poskytovateľ uviesť vysokorizikový systém AI na trh a následne do praxe, bude musieť v zmysle požiadaviek AIA splniť niekoľko krokov a požiadaviek. Je nutné poznamenať, že AIA dáva obrovský dôraz na splnenie požiadaviek pred uvedením na trh (*ex ante*), aby sa minimalizovali riziká AI z hľadiska bezpečnosti a rešpektovania základných ľudských práv pri jej používaní. Kľúčovým krokom je vykonanie tzv. posudzovania zhody (*conformity assessment*), čo je proces známy aj z iných regulácií. Jeho zmyslom je, aby výrobca systémov AI sám dbal na dodržiavanie požiadaviek AIA, ktoré mu nariadenie ustanovuje. Ako príklady možno uviesť požiadavky na správnosť a reprezentatívnosť údajov, ktoré umelá inteligencia spracúva či nutnosť procesov na zisťovanie potenciálnych skreslení (predsudkov).[30] Ďalšie požiadavky sa týkajú vyhotovenia technickej dokumentácie[31] či transparentnosti v podobe informovania užívateľov.[32]

3.1 AI Akt a kybernetická bezpečnosť

AI Akt v rámci požiadaviek na vysokorizikové systémy AI explicitne ustanovuje aj súlad v oblasti kybernetickej bezpečnosti. Všeobecnú požiadavky na kybernetickú bezpečnosť upravuje článok 15 ods. 1: *„Vysokorizikové systémy AI musia byť dizajnované a vyvinuté tak, aby dosahovali primeranú úroveň presnosti, spoľahlivosti*

[27] AIA, Príloha III, bod 5 písm. a).
[28] AIA, Príloha III, bod 5 písm. d).
[29] AIA, Príloha III, bod 6.
[30] AIA, článok 10.
[31] AIA, článok 11.
[32] AIA, článok 12.

a kybernetickej bezpečnosti a aby v týchto ohľadoch fungovali konzistentne počas celého svojho životného cyklu.“[33] Predmetné ustanovenia osobitne zdôrazňujú odolnosť systémov AI vysokého rizika voči pokusom neoprávnených tretích strán o zmenu ich používania, výstupov alebo výkonu využívaním zraniteľností systému.[34] Špecificky *„…technické riešenia zamerané na zabezpečenie kybernetickej bezpečnosti vysokorizikových systémov AI musia byť primerané príslušným okolnostiam a rizikám. Technické riešenia zamerané na zraniteľnosti špecifické pre AI v prípade potreby zahŕňajú opatrenia na prevenciu, detekciu, reakciu, riešenie a kontrolu v prípade útokov, ktoré sa pokúšajú manipulovať súbor trénovacích údajov (ďalej len „otrávenie údajov“) alebo vopred natrénované komponenty používané pri tréningu (ďalej len „otrávenie modelov“), vstupov koncipovaných tak, aby model AI urobil chybu (ďalej len „odporujúce si príklady“ alebo „oklamanie modelov“), útokov na dôvernosť alebo nedostatkov modelu.“*[35] Tieto požiadavky možno zhrnúť nasledovne: (i) vysoko rizikové systémy AI by mali byť zabezpečené a navrhnuté tak, aby boli odolné voči pokusom o ich zmenu, využitie, správanie a na ohrozenie ich bezpečnosti zo strany škodlivých tretích strán prostredníctvom využitia zraniteľností; (ii) na dosiahnutie týchto cieľov sa musia zaviesť organizačné a technické opatrenia; (iii) pre vysokorizikové systémy umelej inteligencie sa vykoná posúdenie rizika z pohľadu kybernetickej bezpečnosti; a (iv) technické riešenia musia byť primerané príslušným okolnostiam a rizikám.[36]

Recitál 77 AIA dopĺňa, že vysokorizikové systémy umelej inteligencie (AI), ktoré spĺňajú základné požiadavky kybernetickej bezpečnosti stanovené v nariadení o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami, sa automaticky považujú za spĺňajúce aj požiadavky kybernetickej bezpečnosti tohto nariadenia. Toto platí za predpokladu, že súlad je preukázaný v EÚ vyhlásení o zhode. Pri posudzovaní rizík vysokorizikových systémov AI sa musia zohľadniť aj riziká pre kybernetickú odolnosť systému, vrátane rizík spojených so zraniteľnosťami špecifickými pre AI, ako je otrávenie údajov.[37]

---

[33] AIA, článok 15 ods. 1.

[34] AIA, článok 15 ods. 5.

[35] Tamže.

[36] SOLER GARRIDO, J. et al. *Analysis of the preliminary AI standardisation work plan in support of the AI Act*, EUR 31518 EN, Publications Office of the European Union, Luxembourg, 2023, ISBN 978-92-68-03924-3, doi:10.2760/5847, JRC132833.

[37] AIA, Recitál 77.

Osobitné požiadavky na kybernetickú bezpečnosť ustanovuje nariadenie pre tzv. modely na všeobecné účely so systémovým rizikom. Poskytovatelia týchto modelov musia sledovať relevantné informácie o závažných incidentoch a možných nápravných opatrenia na ich riešenie a zabezpečiť *„primeranú úroveň kybernetickobezpečnostnej ochrany pre model AI na všeobecné účely so systémovým rizikom a fyzickú infraštruktúru modelu.“*[38]

Po nadobudnutí účinnosti AI Aktu budú musieť všetky vysokorizikové systémy AI prejsť procesom posúdenia zhody a splniť požiadavky na kybernetickú bezpečnosti predtým, ako sa budú môcť používať alebo uviesť do prevádzky na trhu EÚ. Existujú dve hlavné možnosti zabezpečenia zhody. Jednou možnosťou je súlad s harmonizovanými normami, ako sa ustanovuje v kapitole 5 AIA. V recitály 121[39] a článku 40 sa uvádzajú požiadavky na to, ako môžu harmonizované normy poskytnúť predpoklad zhody s požiadavkami právnych predpisov. Harmonizované normy sú vždy dobrovoľné a poskytovateľ systému AI môže vždy preukázať zhodu s požiadavkami nariadenia bez toho, aby sa spoliehal na harmonizované normy, čo poskytuje druhú možnosť zabezpečenia zhody.

V máji 2023 Európska komisia formálne požiadala o vyhotovenie štandardov pre podporu AI Aktu zo strany CEN-CENELEC.[40] Okrem referencie na AI Akt sa v prípade kybernetickej bezpečnosti v žiadosti o tvorbu štandardov pre AI odkazuje aj na navrhovaný Akt o kybernetickej odolnosti (CRA).[41] Európske normalizačné výstupy by mali zohľadniť aj základné požiadavky na výrobky s digitálnymi prvkami, ktoré sú uvedené v oddieloch 1 a 2 prílohy I v CRA. Ak systém AI spadá do rozsahu pôsobnosti CRA aj AI Aktu a spĺňa základné požiadavky CRA, mal by sa považovať za vyhovujúci požiadavkám kybernetickej bezpečnosti uvedených v článku 15 AIA.[42]

[38] AIA, článok 55 ods. 1 písm. d).

[39] AIA, Recitál 121: *„Normalizácia by mala zohrávať kľúčovú úlohu pri poskytovaní technických riešení poskytovateľom na zabezpečenie súladu s týmto nariadením v súlade s aktuálnym stavom vývoja s cieľom podporovať inováciu, ako aj konkurencieschopnosť a rast na vnútornom trhu.“*

[40] European Committee for Standardization a European Committee for Electrotechnical Standardization.

[41] EU Cyber Resilience Act. Dostupné na: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

[42] Pozri Recitál 29 CRA.

Čiastkové závery

AI zásadne transformuje verejnú správu, pričom prináša nielen nové možnosti, ale aj významné výzvy. AI má potenciál optimalizovať administratívne procesy, zlepšiť rozhodovanie a personalizovať poskytovanie služieb. Príklady zahŕňajú využitie inteligentných chatbotov a prediktívnej analýzy, ktoré zefektívňujú interakciu s občanmi a optimalizujú služby. Avšak, súčasne s týmto pokrokom vznikajú nové riziká v oblasti kybernetickej bezpečnosti, čo vyžaduje prispôsobenie existujúcich legislatívnych rámcov. Z pohľadu kybernetickej bezpečnosti AI predstavuje špecifické technologické výzvy, ktoré sa delia na organizačné a výskumné aspekty. Organizačné výzvy sa týkajú harmonizácie terminológie, riadenia bezpečnosti životného cyklu AI a prispôsobenia existujúcich bezpečnostných kontrol. Na druhej strane, výskumné výzvy sa zameriavajú na hodnotenie zraniteľností modelov strojového učenia a vývoj adekvátnych bezpečnostných opatrení. Tieto faktory podčiarkujú potrebu komplexného prístupu k zabezpečeniu AI systémov, ktorý zohľadňuje dynamiku a komplexnosť kybernetických hrozieb.

Akt o umelej inteligencii predstavuje zásadný krok k harmonizácii právnych rámcov pre reguláciu AI. Toto nariadenie sa zameriava na systémy s vysokým rizikom a stanovuje prísne požiadavky na ich vývoj a implementáciu. Dôležitým aspektom je kybernetická bezpečnosť AI systémov, ako aj zavedenie sankcií za porušenie stanovených pravidiel.

Z tohto pohľadu je preto nevyhnutné tento právny rámec reflektovať aj v oblasti regulácie kybernetickej bezpečnosti platnej pre verejnú správu v Slovenskej republike. V rámci ďalšieho dielu tejto štúdie načrtneme právny rámec kybernetickej bezpečnosti v Slovenskej republike a akým spôsobom ho regulácia AI v podobe AI Aktu ovplyvní, prípadne aké iné zmeny je potrebné vykonať.

Zoznam použitej literatúry

1. AGARWAL, P. Public Administration Challenges in the World of AI and Bots. In Public Administration Review. Volume 78, Issue 6, s. 917-921
2. EU Cyber Resilience Act. Dostupné na: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.
3. EURÓPSKA KOMISIA. Commission staff working document impact assessment accompanying the 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} - {SEC(2021) 167 final} - {SWD(2021) 85 final}.
4. GOBBLE, M. Digital strategy and digital transformation. In Res Technol. Manag. 61(5), s. 66–71.
5. HAMIRUL, D. The Role of Artificial Intelligence in Government Services: A Systematic Literature Review. In Open Access Indonesia Journal of Social Sciences 6 (3), 998-1003. Dostupné na: https://doi.org/10.37275/oaijss.v6i3.163.
6. JARRAHI, M.H. et al. Artificial intelligence and knowledge management: A partnership between human and AI. In Business Horizons. Volume 66, Issue , January–February 2023, s. 87-99.
7. JUNKLEWITZ, H. et al. Cybersecurity of Artificial Intelligence in the AI Act. Publications Office of the European Union, Luxembourg, 2023. [online]. [cit. 10-9-2024]. Dostupné na: doi:10.2760/271009, JRC134461.
8. KARLIN, M. et al. Responsible Artificial Intelligence in the Government of Canada: Digital Disruption. White Paper Series, Version 2.0, s. 3.
9. KPMG. Decoding the EU AI Act. [online]. [cit. 10-9-2024]. Dostupné na: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2024/02/decoding-the-eu-artificial-intelligence-act.pdf.
10. KRISHNAN, S.R. et al. Smart Water Resource Management Using Artificial Intelligence —A Review. In Sustainability 2022, 14, 13384. Dostupné na: https://doi.org/10.3390/su142013384.
11. KUBLER, K. State of Urgency: Surveillance, Power and Algorithms in France's State of Emergency. In 4:2 Big Data & Soc 1, 2019.
12. LAMBERTI, L. et al. Benefits sought by citizens and channel attitudes for multichannel payment services: evidence from Italy. In Gov Inf Q. 31(4), s. 596–609.
13. MICRO.AI. Enabling Predictive Maintenance in Energy Production. [online]. [cit. 10-9-2024]. Dostupné na: https://micro.ai/resources/enabling-predictive-maintenance-in-energy-production.
14. MIKHAYLOV, S. et al. Artificial intelligence for the public sector: opportunities and challenges of cross-sector collaboration. In Philos Trans R Soc. 376(2128):20170357.
15. PAPERNOT, N. et al. Towards the Science of Security and Privacy in Machine Learning. ArXiv [online]. [cit. 10-9-2024]. Dostupné na:: https://doi.org/10.48550/arXiv.1611.03814.
16. ROOSEN, M. What SyRi can teach us about technical solutions for societal challenges. Global Data Justice (20 February 2020). [online].

[cit. 10-9-2024]. Dostupné na: https://globaldatajustice.org/2020-02-20-roosen-syri.

17. SAKHNINI., J. et al. In: CHOO, KK., DEHGHANTANHA, A. (eds) Handbook of Big Data Privacy. Springer, Cham. Dostupné na: https://doi.org/10.1007/978-3-030-38557-6_2.
18. SOLER GARRIDO, J. et al. Analysis of the preliminary AI standardisation work plan in support of the AI Act, EUR 31518 EN, Publications Office of the European Union, Luxembourg, 2023, ISBN 978-92-68-03924-3, doi:10.2760/5847, JRC132833.
19. UBALDI, B. et al. State of the art in the use of emerging technologies in the public sector. OECD Working Papers on Public Governance No. 34, GOV/PGC/EGOV(2019)13. [online]. [cit. 10-9-2024]. Dostupné na: https://doi.org/10.1787/932780bc-en.