



PREHĽAD POLITÍK V OBLASTI UMELEJ INTELIGENCIE PRE NÁRODNÚ RADU SLOVENSKEJ REPUBLIKY č. 2/2026

Tento pravidelný prehľad prináša poslancom Národnej rady SR a zamestnancom Kancelárie NR SR stručnú syntézu dôležitých informácií v oblasti umelej inteligencie za posledné týždne. Primárne vychádza z európskeho regulačného a politického rámca a dopĺňa ho o vybrané globálne trendy. Cieľom je napomôcť odbornej, legislatívnej a kontrolnej činnosti Národnej rady SR.

Súhrn: Informácia o návrhu nariadenia o DNA, o výpočtovej suverenite EÚ, o probléme „deepfake ekonomiky“, o finalizácii pracovnej verzie zákona na ochranu detí v online priestore (MIRRI), o bezpečnosti a kybernetickej ochrane, rastúcom význame AI vo vedeckom výskume a globálnych trendoch s priamym dopadom na EÚ.

NÁVRH NARIADENIA O AKTE O DIGITÁLNYCH SIEŤACH (DNA)

1

Európska komisia [predložila](#) 21. januára 2026 návrh nariadenia o akte o digitálnych sieťach ([Digital Networks Act](#), DNA), ktorý prináša zásadný obrat v stratégii EÚ: pozornosť sa rozširuje od kontroly obsahu aj k budovaniu technickej infraštruktúry. Cieľom je harmonizovaný právny rámec s cieľom povzbudiť investície do moderných sietí, ktoré sú nevyhnutné pre fungovanie odolnej digitálnej infraštruktúry v EÚ, AI a cloudu. Implementačná úspešnosť tohto aktu v podmienkach Slovenskej republiky bude ovplyvnená schopnosťou štátnej správy zabezpečiť zosúladenie strategických rámcov s požiadavkami EÚ na dátovú pripravenosť a certifikované bezpečnostné protokoly pre kybernetickú odolnosť digitálnej infraštruktúry.

VÝPOČTOVÁ SUVERENITA EÚ: EUROHPC, AI TOVÁRNE A INŠTITUCIONÁLNE POSILNENIE

Dňa 20. januára 2026 EuroHPC JU [komunikoval](#) rozšírenie mandátu cez regulačnú úpravu, čo politicky potvrdzuje, že EÚ prestáva vnímať superpočítače len ako výskumný nástroj, ale robí z nich jadro priemyselnej politiky. V dôsledku toho spoločný podnik EuroHPC a jeho riadiaca štruktúra prijmú zmeny, ktoré zahŕňajú odborné znalosti v oblasti kvantových technológií. V nasledujúcich mesiacoch bude v rámci priemyselnej a vedeckej poradnej rady spoločného podniku EuroHPC zriadená nová poradná skupina pre kvantové technológie EuroHPC (QTAG). Tento inštitucionálny posun je nevyhnutný pre fungovanie siete tzv. „AI tovární“ (AI factories), ktoré majú poskytovať kritický výpočtový výkon európskym startupom a znižovať tak strategickú závislosť EÚ od mimoeurópskych cloudových poskytovateľov.

V tomto kontexte sa stabilizuje európsky naratív okolo exascale systémov vrátane Alice Recoque ([najnovší európsky exaskálny superpočítač](#)) ako súčasti siete, ktorá má

podporovať „AI továrne“ a poskytovať výpočtový výkon startupom a malým stredným podnikom (MSP). Táto iniciatíva je priamo relevantná pre posilnenie európskej konkurencieschopnosti a strategické znižovanie závislosti od mimoeurópskych cloudových poskytovateľov.

Pre Slovenskú republiku to vytvára dvojité výzvu: na jednej strane sa otvára možnosť prístupu k európskym kapacitám cez spoločné programy, na druhej strane rastie riziko, že bez národného plánovania dátovej pripravenosti a bezpečnostných štandardov nebude domáca ekonomika schopná tieto kapacity efektívne absorbovať a môže sa stať pasívnym konzumentom európskych kapacít bez reálneho dopadu na domáce MSP.

AI A OCHRANA OSOBNOSTI: POSUN K PRÁVU NA IDENTITU V „DEEPPFAKE EKONOMIKE“

[Nová analýza EPRS](#) upozorňuje, že s nástupom generátorov videí s umelou inteligenciou a platforiem zbierajúcich videá generované umelou inteligenciou sa objavili závažné bezpečnostné riziká ako je vydieranie, šikanovanie a sofistikované podvody. Tento vývoj podnietil diskusiu o prechode k novému právnemu konceptu „práva na identitu“, pričom inšpiráciou je dánsky model z leta 2025. Dánska vláda oznámila, že bude bojovať proti deepfake videám generovaným AI, cez ochranu osobných charakteristík ľudí, vrátane vzhľadu a hlasu, prostredníctvom autorského práva.

2 Na základe dánskej iniciatívy, podpísali ministri všetkých členských štátov (vrátane Slovenskej republiky) s výnimkou Maďarska a niektorých ďalších európskych krajín, [Deklaráciu](#) o nevyhnutnosti kultúry a médií ako záruky našich európskych demokracií – ktorá obsahuje hlavnú zásadu, že „naši občania musia byť chránení pred digitálnymi replikami ich osobných charakteristík bez ich súhlasu“.

Hoci je primárnym cieľom nových iniciatív posilniť právny základ pre nahlasovanie škodlivých deepfakes, aplikácia autorského práva na ľudskú identitu môže vytvoriť nepredvídateľné právne kolízie s nariadením GDPR. Pri riešení škôd spôsobených deepfake technológiami sa v súčasnosti kombinuje viacero právnych režimov súčasne, najmä ochrana osobnosti, autorské právo, nekalá súťaž, ochrana osobných údajov a trestné právo. Bez jasnej legislatívnej koordinácie týchto oblastí vzniká vysoké riziko nízkej vymožitelnosti práva a neúmerne vysoké transakčné náklady pre poškodených občanov.

Aktuálne trendy z oblasti dozoru nad ochranou údajov naznačujú, že regulačné orgány budú generatívne AI služby, vrátane nástrojov na „nudification“ (produkcia sexualizovaných obrázkov), klasifikovať ako vysokorizikové spracúvanie dát. V takom prípade bude problémom už samotná technická dostupnosť danej funkcionality, a nie až jej následné zneužitie koncovým používateľom.

Iniciatíva prichádza pred plánovaným preskúmaním smernice o autorských právach a súvisiacich právach na jednotnom digitálnom trhu. Na jar 2026 sa očakáva, že Európsky

parlament bude hlasovať o správe [z vlastnej iniciatívy](#) (spravodajca: Axel Voss, EPP, Nemecko) týkajúcej sa autorských práv a generatívnej AI.

MIRRI FINALIZUJE PRACOVNÚ VERZIU NÁVRHU ZÁKONA NA OCHRANU DETÍ V ONLINE PRIESTORE

Ministerstvo investícií, regionálneho rozvoja a informatizácie SR ako gestor ochrany detí v digitálnom priestore [finalizuje](#) prvú pracovnú verziu osobitného zákona, ktorý má priniesť reálne vymáhateľné pravidlá pre bezpečný online svet. Od 1. februára vzniká na ministerstve nové špecializované oddelenie, ktoré sa bude agende ochrany detí v digitálnom priestore dlhodobo venovať. Rezort v týchto dňoch finalizuje návrh paragrafového znenia osobitného zákona k ochrane detí v online prostredí, ktorého tvorba je zároveň podložená sériou odborných okrúhlych stolov za účasti Generálnej prokuratúry SR, Policajného zboru, Ministerstva spravodlivosti SR, Úradu na ochranu osobných údajov, Slovenskej advokátskej komory a ďalších relevantných subjektov.

Návrh zákona predpokladá zavedenie technicky vymáhateľnej vekovej hranice 16 rokov pre prístup na sociálne siete a vybrané AI služby, úpravu zodpovednosti za rodičovskú kontrolu, obmedzenie hazardných mechanizmov v detských hrách, reguláciu detskej práce online a právo na vymazanie digitálnej stopy detí.

3 BEZPEČNOSŤ A KYBERNETICKÁ OCHRANA

[Monitoring](#) OECD ohľadom kybernetických útokov ukazuje, že AI sa stáva multiplikátorom kybernetických útokov a zároveň nástrojom pre škodlivý obsah, čo zvyšuje nároky na prevenciu, detekciu a reakciu v štátnom aj súkromnom sektore. V roku 2025 čelili organizácie na celom svete rekordným 1 968 kybernetickým útokom týždenne – čo predstavuje 70 % nárast od roku 2023 – ktoré boli spôsobené útočníkmi využívajúcimi AI a automatizáciu. AI umožnila škálovateľnejšie, personalizovanejšie a koordinovanejšie útoky, čo viedlo k rozsiahlemu narušeniu prevádzky a poškodeniu organizácií vo viacerých sektoroch.

V nadväznosti na rastúce množstvo kybernetických útokov by mala Slovenská republika posilňovať kapacity CSIRT (Computer Security Incident Response Team Slovakia) a zároveň vzniká potreba legislatívneho ukotvenia vyšších štandardov pre odolnosť kritickej infraštruktúry a vyčlenenie dodatočných rozpočtových prostriedkov na personálnu stabilizáciu kybernetických expertov v štátnej správe.

RASTÚCI VÝZNAM AI VO VEDECKOM VÝSKUME

V priebehu roka 2025 AI zásadne transformovala softvérové inžinierstvo a prognózy na rok 2026 [predpokladajú](#) analogický, prelomový dopad na oblasť základného a aplikovaného vedeckého výskumu. Nové generácie systémov AI už vykazujú progres pri riešení komplexných otvorených problémov v matematike, fyzike, chémii, biomedicíne, nerovedách či astronómii, ktoré boli dlhodobo považované za technicky náročne nedosiahnuteľné. Podľa [aktuálnych dát](#) vzrástol priemerný týždenný počet interakcií v

pokročilých vedeckých disciplínach v priebehu minulého roka o 50 %, konkrétne z 5,7 milióna na 8,4 milióna správ týždenne. K januáru 2026 sa odhaduje, že približne 1,3 milióna používateľov týždenne využíva LLM modely na riešenie vysoko špecifických úloh, ako sú technické derivácie, inžinierske simulácie a pokročilé modelovanie. Tieto nástroje využíva vedecká komunita predovšetkým na rýchlu syntézu technickej literatúry, analýzu masívnych experimentálnych údajov, písanie kódu a plánovanie laboratórnych experimentov, čím výrazne skracujú inovačné cykly.

GLOBÁLNE TRENDY S PRIAMYM DOPADOM NA EÚ

V USA sa [prehlbuje dôraz](#) federálnej administratívy na urýchlené nasadzovanie AI a na odstránenie regulačných bariér, čo môže viesť k rýchlejšej komercializácii produktov, ktoré sa následne budú exportovať na európsky trh, čím sa zvýši tlak na európsky dohľad a zjednotenie digitálnych nástrojov, ktoré kontrolujú, či tieto technológie dodržiavajú zákony EÚ.

Súčasne sa mení spôsob uplatňovania pravidiel v oblasti ochrany spotrebiteľa, keď americká Federal Trade Commission [signalizuje](#) prísnejšie zameranie na klamlivé tvrdenia o výkonoch a schopnostiach AI, avšak zároveň opatrnejší prístup k zásahom, ktoré by sa dali interpretovať ako brzdenie inovácií, čo zvyšuje riziko vzdávania sa regulačných pravidiel medzi EÚ a USA.

4 Čína vydala [prvé predpisy](#) týkajúce sa AI už v roku 2021. Zameriavajú sa na najmä na kontrolu technologických firiem a obsahu, ktorý šíria prostredníctvom svojich platforiem. V Číne sa preto [kladie dôraz](#) na povinné označovanie obsahu vytvoreného AI a na štátom riadené pravidlá pre technológie, ktoré vytvárajú umelú realitu (tzv. deep synthesis). Tento prístup vytvára model, ktorý sa technicky podobá na európsku snahu o transparentnosť, ale s odlišnými hodnotovými prioritami (štátna kontrola pred slobodou informácií), čo bude pre EÚ relevantné pri medzinárodnom obchode a pri nastavovaní pravidiel pre šírenie digitálneho obsahu cez hranice.

--

Spracovali:

Natália Švecová (riaditeľka Parlamentného inštitútu) & Milan Hrabovský (výskumný analytik Parlamentného inštitútu)

12 február 2026

--

Materiál slúži najmä pre poslancov NR SR a zamestnancov Kancelárie NR SR a nemôže v plnej miere nahrádzať právne alebo iné odborné poradenstvo v danej oblasti. Údaje, použité v materiáli, sú aktuálne k dátumu jeho zverejnenia. Zverejňovanie je možné iba so súhlasom odboru Parlamentný inštitút a autorov. Materiál neprešiel jazykovou úpravou.