



Regulácia umelej inteligencie svet, Európa, Slovensko

Dr. h.c. mult. prof. Ing. Štefan Luby, DrSc. - slovenský fyzik, hlavný vedecký redaktor INTERCEDU

Úvod

Technológia hnaná ziskom investorov sa rozvíja omnoho rýchlejšie ako jej sociálne a zdravotné zábezpeky. Napr. nanotechnológie, ktorých moderná éra bola odštartovaná známou prednáškou R. Feynmana, tam na dne je veľa priestoru" na CALTECH v Kalifornii roku 1959 [1], dostali prvý štátny organizačný rámec vyhlásením Národnej nanotechnologickej iniciatívy USA prezidentom W. Clintonom roku 2000 [2]. Avšak prvé reprezentačné fórum nanoetiky bolo ustanovené vydavateľstvom Springer časopisom Nanoethics, ktorý sa stal tribúnou kritiky neriešenia následkov nanotechnológií v kozmetike, zdravotníctve, ekonómii, ochrane súkromia a inde, až roku 2007. Vznikla tiež nová vedná disciplína nanotoxikológia, ktorá má čo robiť aj v takom zdaniľavom benignom prostredí ako je grafén, o ktorom sa tendenčne hovorilo – veď je to len uhlík [3]. Prítom v oblasti umelej inteligencie (AI) je tento problém omnoho vypuklejší a zaostávanie regulácie a legislatívy je vzhľadom na expresný vývoj AI omnoho väčší ako to bolo vo sfére nanotechnológií či biotechnológií.



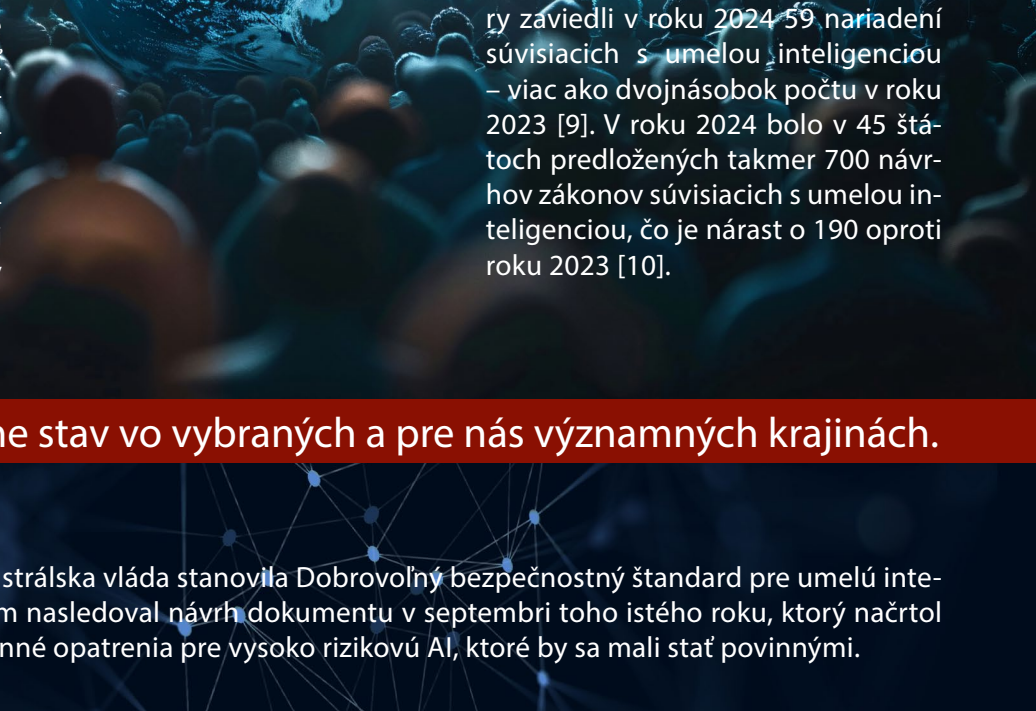
Zhrňme si najprv hlavné hrozby AI podrobne uvedené v práci [4]. Sú to:

- strata menej kvalifikovaných pracovných pozícií,
- enormná spotreba elektrickej energie a chladiacej vody hardvéru AI,
- ohrozenie súkromia, podvody, skandalizovanie,
- degradácia vzdelávania, keďže AI bude využívaná na písanie postupu-prac, využitie v zbraňových systémoch.

Poznamenávame však, že hrozby ohľadnutia planéty zo strany AI považujeme za konšpiračné teórie a hovädz. Táto štúdia čerpa z hlavných zdrojov [5, 6, 7] a ďalších citovaných na príslušných miestach.

Regulácie vo vybraných krajinách sveta

Od roku 2016 bolo publikovaných množstvo etických usmernení pre umelú inteligenciu s cieľom udržať sociálnu kontrolu nad touto technológiou [8]. Regulácia sa totiž považuje za nevyhnutnú na podporu inovácií v oblasti AI a riadenie súvisiacich rizík. Podľa indexu umelej inteligencie Stanfordskej univerzity



z roku 2025 sa legislatívne zmeny o AI od roku 2023 zvýšili v priemere o 21,3 % v 75 krajinách, čo predstavuje deväťnásobný nárast od roku 2016. Americká federálne agentúry zaviedli v roku 2024 59 nariadení súvisiacich s umelou inteligenciou – viac ako dvojnásobok počtu v roku 2023 [9]. V roku 2024 bolo v 45 štátoch predložených takmer 700 návrhov zákonov súvisiacich s umelou inteligenciou, čo je nárast o 190 oproti roku 2023 [10].

V ďalšom stručne zhrnieme stav vo vybraných a pre nás významných krajinách.

Austrália
V auguste 2024 austrálska vláda stanovila Dobrovoľný bezpečnostný štandard pre umelú inteligenciu, po ktorom nasledoval návrh dokumentu v septembri toho istého roku, ktorý načrtoval potenciálne ochranné opatrenia pre vysoko rizikovú AI, ktoré by sa mali stať povinnými.

Brazília
30. septembra 2021 brazílska poslanecká snemovňa schválila brazílsky právny rámec pre umelú inteligenciu. Cieľom tejto legislatívy bolo regulovať vývoj a používanie umelej inteligencie a zároveň podporovať výskum a inovácie v oblasti etických riešení, ktoré uprednostňujú kultúru, spravodlivosť, férovosť a zodpovednosť.

Čína
15. augusta 2023 oficiálne nadobudli účinnosť prvé čínske opatrenia v oblasti generatívnej umelej inteligencie, ktoré sa stali jedným z prvých komplexných národných regulačných rámcov. Tieto opatrenia sa vzťahujú na všetkých poskytovateľov, ktorí ponúkajú služby generatívnej umelej inteligencie čínskej verejnosti, vrátane zahraničných subjektov, a v konečnom dôsledku stanovujú pravidlá týkajúce sa ochrany údajov, transparentnosti a algoritmickej zodpovednosti.

Kanada
V novembri 2022 Kanada predložila zákon o implementácii digitálnej charty, ktorý navrhuje tri zákony, ktoré boli opísané ako holistický balík legislatívy pre dôveru a súkromie: zákon o ochrane súkromia spotrebiteľov, zákon o tribunáli pre ochranu osobných údajov a zákon o umelej inteligencii.

USA
Diskusie o regulácii umelej inteligencie v Spojených štátoch amerických zahŕňali témy ako aktuálnosť regulácie, povaha federálneho regulačného rámca na riadenie a podporu umelej inteligencie vrátane toho, ktorá agentúra by mala agendu viesť, regulačné a riadiace právomoci tejto agentúry a ako aktualizovať predpisy vzhľadom na rýchlo sa meniace technológie, ako aj úlohy štátnych vlád a súdov.

Švajčiarsko
Švajčiarsko v súčasnosti nemá žiadnu špecifickú legislatívu týkajúcu sa umelej inteligencie, ale 12. februára 2025 Federálna rada oznámila plány na ratifikáciu Dohovoru Rady Európy o umelej inteligencii a jeho začlenenie do švajčiarskeho práva.

UK
Vláda Spojeného kráľovstva naznačila svoju neochotu prijať momentálne legislatívne argumenty tým, že by to mohlo spomaliť rast sektora a že zákony by mohli rýchlo zastarať v dôsledku ďalšieho technologického pokroku.

Európska únia a Európa

EÚ je jednou z najväčších jurisdikcií na svete a zohráva aktívnu úlohu v globálnej regulácii digitálnych technológií prostredníctvom GDPR, zákona o digitálnych službách a zákona o digitálnych trhoch [11]. Najmä v oblasti umelej inteligencie sa zákon o AI z roku 2023 považuje za najrozsiahlejšiu reguláciu umelej inteligencie na svete [12].

Väčšina krajín Európskej únie (EÚ) má národné stratégie regulácie umelej inteligencie, ktoré sú do značnej miery konvergentné. Európska únia sa riadi Európskou stratégiou pre umelú inteligenciu [13], ktorú podporuje skupina expertov na vysokej úrovni. Skupina expertov EK vykonáva prácu na dôveryhodnej umelí inteligencii a komisia vydala správu o bezpečnostných a zodpovednostných aspektoch AI a o etike automatizovaných vozidiel. V roku 2020 si Európska komisia vyžiadala názory na návrh legislatívy špecifickej pre umelú inteligenciu a tento proces stále prebieha.

Európska komisia 2. februára 2020 zverejnila svoju Bielu knihu o umelej inteligencii – Európsky prístup k excelentnosti a dôvere [14]. Biela kniha pozostáva z dvoch hlavných stavebných kameňov, „ekosystém excelentnosti“ a „ekosystému dôvery“. „Ekosystém dôvery“ načrtáva prístup EÚ k regulačnému rámcu pre umelú inteligenciu. Vo svojom navrhovanom prístupe Komisia rozlišuje aplikácie umelej inteligencie na základe toho, či sú „vysokorizikové“ alebo nie. Do rozsahu pôsobnosti budúceho regulačného rámca EÚ by mali patriť iba vysokorizikové aplikácie umelej inteligencie. Aplikácia sa považuje za vysokorizikovú, ak funguje v rizikovom sektore (ako je zdravotníctvo, doprava alebo energetika) a „používa sa takým spôsobom, že pravdepodobne vzniknú značné riziká“. V prípade vysokorizikových aplikácií umelej inteligencie sa požiadavky týkajú najmä: „odbornej prípravy“, „údajov o školení“, „údajov a vedenia záznamov“, „informácií, ktoré sa majú poskytnúť“, „robustnosti a presnosti“ a „ľudského dohľadu“. Existujú aj požiadavky špecificke pre určité použitia, ako je napríklad dialgová biometrická identifikácia. Aplikácie umelej inteligencie, ktoré sa neklasifikujú ako „vysokorizikové“, by sa mohli riadiť dobrovoľným systémom označovania. Pokiaľ ide o dodržiavanie predpisov a presadzovanie predpisov, Komisia zvažuje predchádzajúce posúdenia zhody, ktoré by mohli zahŕňať „postupy testovania, kontroly alebo certifikácie“ a/alebo „kontroly databáz súborov údajov použitých vo fáze vývoja“. Európska štruktúra riadenia umelej inteligencie vo forme rámca pre spoluprácu príslušných vnútroštátnych orgánov by mohla uľahčiť implementáciu regulačného rámca [15].

V apríli 2021 Komisia predstavila svoj oficiálny „Návrh nariadenia, ktorým sa stanovujú harmonizované pravidlá pre umelú inteligenciu“. Krátko nato bol na tomto základe formálne navrhnutý zákon o umelej inteligencii (tiež známy ako zákon o AI) [16]. Tento návrh zahŕňa spresnenie prístupu z roku 2020 založeného na riziku, tentoraz so 4 kategóriami rizika: „minimálne“, „obmedzené“, „vysoké“ a „neprijateľné“. Návrh bol vo verejnej diskusii ostro kritizovaný. Akademici vyjadrili obavy z rôznych nejasných prvkov v návrhu – ako je napríklad široká definícia toho, čo predstavuje AI – a obávali sa nezamýšľaných právnych dôsledkov, najmä pre zraniteľné skupiny, ako sú pacienti a migranti. Kategória rizika „univerzálna AI“ bola pridaná do Zákona o umelej inteligencii (AI Act) a má zohľadňovať všestranne modely ako ChatGPT, ktoré nezodpovedali rámcu regulácie založenej na aplikáciách. Na rozdiel od iných kategórií rizika možno modely umelej inteligencie na všeobecné použitie regulovať na základe ich schopností, nielen ich použitia. Slabšie modely umelej inteligencie na všeobecné použitie podliehajú požiadavkám na transparentnosť, zatiaľ čo tie, ktoré sa považujú za „systémové riziká“ (najmä tie, ktoré sú tréňované s využitím výpočtových schopností presahujúcich 1025 FLOPS), musia tiež prejsť dôkladným procesom hodnotenia. Následná verzia zákona o umelej inteligencii bola nakoniec prijatá v máji 2024 [17]. Zákon o umelej inteligencii sa bude postupne presadzovať. Rozpoznávanie emócií a dialgová biometrická identifikácia v reálnom čase budú zakázané s určitými výnimkami, napríklad pre orgány činné v trestnom konaní.

Zákon Európskej únie o umelej inteligencii vytvoril regulačný rámec s významnými globálnymi dôsledkami. Táto legislatíva zavádza prístup založený na riziku pri kategorizácii systémov umelej inteligencie so zameraním na vysoké rizikové aplikácie, ako je zdravotníctvo, vzdelávanie a zemaním na vysoké rizikové organizácie, aby zabezpečili transparentnosť, správu údajov a ľudský dohľad vo svojich riešeniach umelej inteligencie. Hoci cieľom je podporiť etické používanie umelej inteligencie, prísne požiadavky by mohli zvýšiť náklady na dodržiavanie predpisov a oddialiť zavádzanie technológií, čo by malo vplyv na odvetvia zamerané na inovácie.

Pozorovatelia vyjadrili obavy z nárastu legislatívnych návrhov v rámci Komisie. EÚchla legislatívnych iniciatív je čiastočne ovplyvnená politickými ambíciami AI a mohla by ohroziť digitálne práva európskych občanov vrátane práva na súkromie, najmä vzhľadom na neisté záruky ochrany údajov prostredníctvom kybernetickej bezpečnosti. Medzi uvedené hlavné zásady v rámci legislatívnych návrhov v oblasti umelej inteligencie v rámci Komisie patria ciele strategickej autonómie a koncept digitálnej suverenity [18].

Zákon EÚ o umelej inteligencii (nariadenie (EÚ) 2024/1689) nadobudol účinnosť 1. augusta 2024 a vytvoril právny rámec pre systémy umelej inteligencie založené na riziku vrátane osobitných ustanovení pre všeobecné modely umelej inteligencie s účinnosťou od 2. augusta 2025 [19].

Česká republika

Česká republika prijala v roku 2019 Národnú stratégiu pre umelú inteligenciu a v roku 2024 ju aktualizovala Národnou stratégiou Českej republiky pre umelú inteligenciu do roku 2030. Aktualizovaná stratégia obsahuje ustanovenie na zabezpečenie účinnej legislatívy, vytvorenie etických kódexov pre vývojárov a používateľov, zriadenie dozorných orgánov a podporu etického používania umelej inteligencie.

Slovensko

Vláda SR vymenovala v júli historicky prvého splnomocnenca pre umelú inteligenciu. Stal sa ním štátny tajomník Ministerstva investícií, regionálneho rozvoja a informatizácie SR Radoslav Štefánek. Slovensko tak urobilo významný krok v oblasti regulácie AI. Splnomocnenc predstavil návrh zákona, ktorý vstupuje do medzirezortného pripomienkového konania.

Sumarizácia Zákona EÚ o umelej inteligencii

Zákon o umelej inteligencii klasifikuje umelú inteligenciu podľa jej rizika:

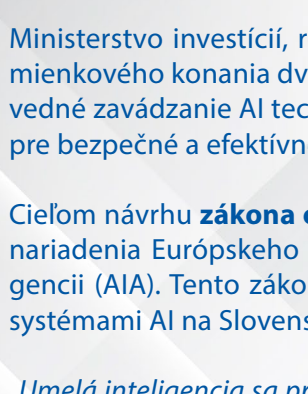
- Neprijateľné riziko je zakázané (napr. manipulatívna umelá inteligencia).
- Väčšina textu sa zaoberá vysokorizikovými systémami umelej inteligencie, ktoré sú regulované.
- Menšia časť sa zaoberá systémami umelej inteligencie s obmedzeným rizikom, čo spôsobuje povinnosti transparentnosti; vývojári a poskytovatelia musia zabezpečiť, aby si koncoví používatelia boli vedomí toho, že interagujú s umelou inteligenciou (chatboty a deepfake).

• Minimálne riziko nie je regulované (vrátane väčšiny aplikácií umelej inteligencie, ktoré sú v súčasnosti dostupné na jednotnom trhu EÚ; to sa zmení s generatívnou umelou inteligenciou).

Väčšina povinností pripadá na poskytovateľov (vývojárov) vysokorizikových systémov umelej inteligencie:

- menovite tých, ktorí majú v úmysle uviesť na trh alebo do prevádzky vysokorizikové systémy umelej inteligencie v EÚ, bez ohľadu na to, či majú sídlo v EÚ alebo v tretej krajine;
- a tiež na poskytovateľov z tretej krajiny, ak sa výstup vysokorizikového systému umelej inteligencie používa v EÚ. Používatelia sú fyzické alebo právnické osoby, ktoré nasadzujú systém umelej inteligencie v rámci profesionálnej činnosti, nie sú to dotknutí koncoví používatelia.
- Používatelia (nasadzovatelia) vysokorizikových systémov umelej inteligencie majú určité povinnosti, aj keď menšie ako poskytovatelia (vývojári).
- Toto sa vzťahuje na poskytovateľov so sídlom (EÚ) a používateľov z tretej krajiny, ak sa výstup systému umelej inteligencie používa v EÚ.

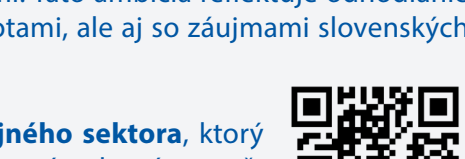
Zákazy umelej inteligencie (kapitola II, článok 5)



- používanie podprahových, manipulatívnych alebo klamlivých techník na skreslenie správania a zhoršenie informovaného rozhodovania, čo spôsobuje značnú škodu;
- zneužívanie zraniteľnosti súvisiacich s vekom, zdravotným postihnutím alebo sociálno-ekonomickými okolnosťami na skreslenie správania, čo spôsobuje značnú škodu;
- biometrické kategorizačné systémy odvodzujúce citlivé atribúty (rasa, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie, sexuálny život alebo sexuálna orientácia), s výnimkou označovania alebo filtrovania zákonne získaných biometrických súborov údajov, alebo keď orgány činné v trestnom konaní kategorizujú biometrické údaje;

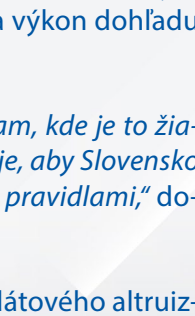
- sociálne bodovanie, t. j. hodnotenie alebo klasifikácia jednotlivcov alebo skupín na základe sociálneho správania alebo osobných vlastností, čo spôsobuje škodlivé alebo nepriaznivé zaobchádzanie s týmito ľuďmi;
- posudzovanie rizika spáchania trestných činov jednotlivcom výlučne na základe profilovania alebo osobnostných vlastností, s výnimkou prípadov, keď sa používa na doplnenie ľudských hodnotení založených na objektívnych, overiteľných skutočnostiach priamo súvisiacich s trestnou činnosťou;
- zostavovanie databáz rozpoznávania tvárí necieleným získavaním obrázkov tvárí z internetu alebo záznamov z priemyselnej televízie;
- odvodzovanie emócií na pracoviskách alebo vo vzdelávacích inštitúciách, s výnimkou prípadov z lekárskeho alebo bezpečnostných dôvodov;
- dialgová biometrická identifikácia (RBI) v reálnom čase vo verejne prístupných priestoroch pre orgány činné v trestnom konaní, s výnimkou prípadov;
- hľadania nezvestných osôb, obetí únosov a osôb, ktoré boli obeťmi obchodovania s ľuďmi alebo sexuálneho vykorisťovania;
- predchádzania značnému a bezprostrednému ohrozeniu života alebo predvídateľnému teroristickému útoku;
- identifikácie podozrivých zo závažných trestných činov (napr. vražda, znásilnenie, ozbrojený lup, obchodovanie s omamnými látkami a nelegálnymi zbraňami, organizovaný zločin a environmentálna kriminalita).

Zodpovedná digitalizácia: MIRRI predstavilo návrhy zákonov o umelej inteligencii a správe údajov [7]

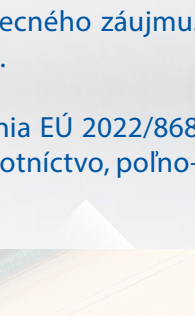


Ministerstvo investícií, regionálneho rozvoja a informatizácie SR (MIRRI) predkladá do medzirezortného pripomienkového konania dva kľúčové legislatívne návrhy. Zákon o umelej inteligencii má zabezpečiť férové a zodpovedné zavádzanie AI technológií v súlade s európskym právom, zatiaľ čo zákon o správe údajov nastavuje rámec pre bezpečné a efektívne zdieľanie chránených údajov verejného sektora.

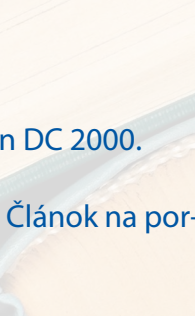
Cieľom návrhu **zákona o umelej inteligencii** je zabezpečiť uplatňovanie kľúčových ustanovení nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1689, známeho ako Akt o umelej inteligencii (AIA). Tento zákon určuje rámec pre inštitucionálne usporiadanie a výkon dohľadu nad systémami AI na Slovensku.



„Umelá inteligencia sa pre mnohých z nás už dnes stala neoddeliteľnou súčasťou každodenného života. Je preto našou povinnosťou na MIRRI zabezpečiť, aby jej využívanie bolo bezpečné, zodpovedné a zároveň predvídateľné. Pre občanov to znamená vyššiu mieru ochrany a právnej istoty, pre podnikateľov jasné pravidlá bez zbytočnej administratívnej záťaže. Naším cieľom aj pri tomto zákone je férová rovnováha medzi ochranou verejného záujmu a podporou inovácií,“ uviedol Radoslav Štefánek, štátny tajomník MIRRI a splnomocnenc vlády pre umelú inteligenciu.



Nariadenie AIA nadobúda postupne účinnosť od augusta 2025. Niektoré jeho časti si však vyžadujú národnú implementáciu – najmä v oblasti určovania orgánov dohľadu a ukládania sankcií. Hoci prvé ustanovenia európskeho aktu o umelej inteligencii sa začínajú uplatňovať už 2. augusta 2025, väčšina členských štátov Európskej únie je aktuálne ešte len vo fáze prípravy národnej legislatívy. Slovensko tak má reálnu príležitosť zaradiť sa medzi krajiny, ktoré budú mať vlastný vykonávací zákon v účinnosti medzi prvými. Táto ambícia reflektuje odhodlanie vlády aktívne formovať digitálnu budúcnosť v súlade s európskymi hodnotami, ale aj so záujmami slovenských občanov a podnikateľov.



Druhým návrhom je **zákon o správe vybraných kategórií údajov verejného sektora**, ktorý vytvára právny rámec pre opätovné použitie určitých údajov verejnej správy, ktorý nemožno na sprístupniť ako otvorené dáta – napríklad z dôvodu ochrany osobných údajov, obchodného tajomstva alebo dôverných štatistických údajov.

Zákon sprostredkovaná údaje, zavádza inštitút dátového altruizmu a zriaďuje jednotné informčné miesto, ktoré bude fungovať ako vstupná brána pre žiadosti o sprístupnenie chránených dát. Gestorom zákona a hlavným orgánom pre jeho implementáciu bude MIRRI SR, ktoré zároveň zodpovedá za správu registra a výkon dohľadu v spolupráci s ďalšími úradmi, najmä Štatistickým úradom SR.

„Zákon nenarúša zdieľanie citlivých údajov, ale nastavuje pravidlá, ako môžu byť sprístupnené tam, kde je to žiaduce a prospešné – napríklad pre medicínsky výskum či zlepšovanie verejných služieb. Naším cieľom je, aby Slovensko patrilo medzi krajiny, ktoré dokážu s dátami narábať moderne, zodpovedne a v súlade s európskymi pravidlami,“ doplnil Štefánek.

Zákon zároveň stanovuje pravidlá pre registráciu subjektov, ktoré chcú pôsobiť ako organizácie dátového altruizmu – napríklad neziskové subjekty, ktoré dobrovoľne sprístupňujú svoje údaje na účely všeobecného záujmu. Obsahuje tiež rámec pre dohľad, kontroly a sankcie v prípade porušenia stanovených povinností.

Prijatie zákona zabezpečí naplnenie povinností, ktoré Slovenskej republike vyplývajú z nariadenia EÚ 2022/868 a umožní naplno sa zapojiť do budovania európskych dátových priestorov v oblastiach ako zdravotníctvo, poľnohospodárstvo, priemysel či verejné služby.