

DeepSeek jako precedent – Test odolnosti evropské regulace umělé inteligence

Martin Mach*

Abstrakt: Článek se zabývá problematikou ochrany osobních údajů v souvislosti s AI modelem DeepSeek, který čelí podezřením z předávání osobních dat uživatelů do Číny. Výzkum analyzuje právní rámec ochrany osobních údajů v EU, zejména s ohledem na nařízení GDPR a AI Act, a hodnotí, zda DeepSeek splňuje požadavky těchto regulací. Studie rovněž reflektuje přístup Evropské unie k regulaci AI a aplikaci principu předběžné opatrnosti, který byl v minulosti využit například při omezení přístupu k některým digitálním službám v Evropě. Zároveň se věnuje i komparaci přístupu EU a USA vůči technologickým společnostem se sídlem v Číně, přičemž poukazuje na obdobný případ společnosti ByteDance, mateřské společnosti vlastníci sociální síť TikTok, která čelila obviněním ze sdílení dat s čínskými úřady. Autor hodnotí možné regulační scénáře pro DeepSeek, včetně zařazení na seznam bezpečnostních hrozeb, dočasného zákazu či trvalé blokace jeho služeb v EU. Zvláštní pozornost je věnována otázce proporcionality a účinnosti těchto opatření, a to jak z pohledu ochrany osobních údajů, tak z hlediska geopolitických důsledků. Studie dochází k závěru, že ačkoli EU klade důraz na dialog a možnost nápravy, v případě důvodných pochybností o bezpečnosti dat by bylo vhodné dočasně omezit provoz DeepSeeku, dokud neprokáže plný soulad s evropskými právními normami.

Klíčová slova: umělá inteligence, GDPR, AI Act, DeepSeek, ochrana osobních údajů

Úvod

Evropská unie bývá kritizována za nadměrnou legislativní regulaci umělé inteligence (AI) bránící rozvoji AI¹ a omezující konkurenceschopnost evropských podniků, což může vést k fragmentaci globálního digitálního trhu. Tato regulace bývá zdůvodňována větším důrazem na ochranu osobních údajů obyvatel EU. Toto zdůvodnění jde podložit prameny upravující AI, zejména Obecné nařízení o ochraně osobních údajů (GDPR),² Nařízením o harmonizaci pravidel pro umělou inteligenci (AI Act),³ Nařízením o jednotném trhu digitálních služeb (DSA)⁴ a Stanovisko Evropského výboru regionů 28/2024,⁵ které komplexně

* Mgr. Martin Mach, MA, doktorand, katedra mezinárodního a evropského práva Právnické fakulty Univerzity Palackého v Olomouci. E-mail: martin.mach@upol.cz. Tato práce byla podpořena studentským projektem IGA_PF_2024_013 Univerzity Palackého v Olomouci.

1 Fourteen major organizations sign joint letter warning the EU on the Second Draft of the General Purpose AI Code of Conduct. In: *AI chamber* [online]. 14. 2. 2025 [cit. 2025-03-04]. Dostupné z: <https://aichamber.eu/fourteen-major-organizations-sign-joint-letter-warning-the-eu-on-the-second-draft-of-the-general-purpose-ai-code-of-conduct/>.

2 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR). *Úřední věstník*. L 119, 4. května 2016, s. 1–88.

3 Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci). *Úřední věstník*. L, 12. července 2024.

4 Nařízení Evropského parlamentu a Rady (EU) 2022/2065 ze dne 19. října 2022 o jednotném trhu digitálních služeb a o změně směrnice 2000/31/ES (akt o digitálních službách). *Úřední věstník*. L, 27. října 2022.

5 Stanovisko Evropského výboru regionů – Posílení evropského správního prostoru (CompAct) 28/2024. *Úřední věstník*. C/2024/5369, 17. září 2024.

reagují na digitální výzvy a v praxi se vzájemně doplňují. GDPR představuje horizontální základ ochrany osobních údajů, ukládající povinnosti všem subjektům zpracovávajícím data fyzických osob, včetně AI modelů a jejich provozovatelů. Zajišťuje práva jednotlivců, jako je právo být zapomenut, a stanovuje přísné podmínky pro mezinárodní předávání dat, což je pro případy typu DeepSeek stěžejní. Paralelně s tím DSA cílí na odpovědnost a transparentnost online platform za obsah, který zprostředkovávají, ať už jde o obsah tvořený uživateli, nebo ten generovaný AI. Zavádí mechanismy pro řešení nezákonného obsahu a povinnosti pro velké online platformy týkající se řízení systémových rizik. AI Act přináší specifickou regulaci samotných AI modelů, klasifikuje je dle rizika a ukládá odpovídající požadavky na jejich bezpečnost, transparentnost a robustnost. Pro generativní AI modely, jako je DeepSeek, to znamená povinnost splnit transparentnostní požadavky a v případě vysokého rizika u AI modelu i náročnější certifikační procesy. Tato trojice nařízení tak vytváří komplexní síť, kde GDPR chrání data jako taková, DSA reguluje služby, které AI poskytuje, a AI Act dohlíží na samotnou AI technologii, což umožňuje řešit problematiku AI a ochrany dat z různých, avšak vzájemně propojených úhlů.

Zároveň však tento systém regulace může zapříčinit, že EU tímto není atraktivní pro investory a firmy vyvíjející AI. Pokud je to ale vyváжено ochranou soukromých údajů, je toto chování obhajitelné. Dne 20. ledna 2025 byl oficiálně představen čínský model AI s názvem DeepSeek-R1,⁶ který je podezříván právě z nedostatečné ochrany osobních údajů svých uživatelů. Jedním z důvodů pro tyto obavy bylo zjištění, že aplikace DeepSeek pro iOS, operační systém společnosti Apple, odesílá data na servery kontrolované společností ByteDance bez dostatečného šifrování, což může umožnit přístup čínské vládě k těmto informacím.⁷ Jedná se o první možnost EU prezentovat svůj přístup k AI jako opodstatněný. Příspěvek skrze případovou analýzu zkoumá, jaké jsou dopady a rizika spojené s používáním AI modelu DeepSeek v Evropské unii z hlediska ochrany osobních údajů a jeho souladu s evropskou legislativou a zda EU podniká kroky k zajištění adekvátní ochrany občanů EU, případně jaké kroky by měla podniknout. Odpověď na tuto otázku bude důležitá i do budoucna, protože nových AI modelů bude přibývat.

DeepSeek je AI model, který interaguje s uživatelem, což jej dle dělení do čtyř kategorií rizik dle AI Actu zařazuje do kategorie s omezeným rizikem, tzv. měkkou regulací.⁸ Musí tedy splňovat nároky na transparentnost, což však značí více než jen povinnost informovat uživatele, že komunikuje s AI modelem. Jedná se také o povinnost informovat o účelu a omezení AI modelu a informování, jak byla AI trénována.⁹ Mimo zmíněné existuje také povinnost zajistit mechanismy pro opravu nesprávných informací. V případě nesplnění těchto povinností, může být uložena pokuta do výše až 7 500 000 EUR nebo až do výše 1 % ročního obrátu podniku.¹⁰ Tedy v rámci 3 kategorií pokut definovaných v sankcích v AI Actu se jedná o nejnížší ze tří hranic.¹¹

⁶ DeepSeek-R1 Release. In: *Deepseek* [online]. [cit. 2025-03-04]. Dostupné z: <https://api-docs.deepseek.com/news/news-250120>.

⁷ HOOG, Andrew. NowSecure Uncovers Multiple Security and Privacy Flaws in DeepSeek iOS Mobile App. In: *Nowsecure* [online]. 6. 2. 2025 [cit. 2025-03-04]. Dostupné z: <https://www.nowsecure.com/blog/2025/02/06/nowsecure-uncovers-multiple-security-and-privacy-flaws-in-deepseek-ios-mobile-app/>.

⁸ Čl. 52, Akt o umělé inteligenci.

⁹ Čl. 53, ibidem.

¹⁰ Čl. 99, odst. 5, ibidem.

¹¹ Čl. 99, ibidem.

DeepSeek se však jeví jako problematický z několika důvodů, a to natolik, že v některých zemích bylo zakázáno jej nabízet ke stahování pro operační systémy Android a iOS, například v Jižní Koreji¹² či Itálii,¹³ a to zejména z důvodu neposkytnutí dostatečných informací o způsobu sběru a uchovávání osobních údajů uživatelů, na což upozorňují i Francie, Nizozemsko, Belgie, Lucembursko a další státy.¹⁴ Vyšetřování, jak DeepSeek zpracovává osobní údaje a zda je jeho fungování v souladu s evropskými předpisy na ochranu soukromí, probíhá také v Německu a Irsku.¹⁵ Své vyšetřování vede i Evropský výbor pro ochranu údajů (EDPB).¹⁶ Je však toto vyšetřování EPBD adekvátní odpovědí na DeepSeek?

EDPB zkoumá, zda DeepSeek poskytuje uživatelům dostatečné informace o tom, jak jsou jejich data shromažďována, zpracovávána a uchovávána. Právě nedostatečná transparentnost byla důvodem, proč italský úřad pro ochranu osobních údajů DeepSeek zablokoval. Vyšetřování se tedy soustředí na to, zda praktiky společnosti DeepSeek odpovídají požadavkům nařízení GDPR, které klade důraz na ochranu soukromí uživatelů v Evropské unii. V souvislosti s vyšetřováním v jednotlivých členských státech EDPB také koordinuje činnost národních úřadů pro ochranu osobních údajů v zemích, které již byly zmíněny, které zahájily vlastní šetření ohledně praktik společnosti DeepSeek při sběru dat. Cílem této koordinace je posílit spolupráci a výměnu informací mezi regulačními orgány v oblasti prosazování pravidel týkajících se umělé inteligence. Vyšetřování EPDB odráží širší snahu Evropské unie zajistit, aby nové technologie, včetně AI aplikací, byly v souladu s přísnými evropskými standardy ochrany osobních údajů a soukromí.

Případ DeepSeeku s jeho potenciálním předáváním dat do Číny navíc překračuje pouhou otázku souladu s GDPR či nařízením AI Act. Slouží jako ilustrativní příklad hlubších teoretických dilemat, jež prostupují regulaci generativní umělé inteligence. Jedná se především o koncepční střet globálního dosahu AI technologií s požadavkem na digitální suverenitu členských států EU a ochranu jejich ústavního pořádku. Digitální suverenita totiž není pouhou snahou o kontrolu dat v rámci fyzických hranic států. Je to širší koncept, který odráží schopnost státu (nebo společenství států, jako je EU) prosadit svůj právní a politický pořádek a ochránit své ústavně garantované hodnoty a principy v digitálním prostředí. Zahrnuje schopnost určovat vlastní pravidla pro digitální infrastrukturu, datové toky, správu digitálních služeb a ochranu občanů před škodlivými dopady digitálních technologií. V kontextu AI, která může ovlivnit prakticky všechny aspekty života, se digitální suverenita stává nezbytným předpokladem pro účinnou správu. Ústavní právo zde hraje dvojí, avšak komplementární roli: jednak poskytuje normativní základ a legitimitu

¹² SMITH, Chris. DeepSeek AI banned in South Korea – should the US be next? In: *BGR* [online]. 18. 2. 2025 [cit. 2025-03-04]. Dostupné z: <https://bgr.com/tech/deepseek-ai-banned-in-south-korea-should-the-us-be-next/>.

¹³ COMUNICATO STAMPA – Intelligenza artificiale: il Garante privacy blocca DeepSeek. In: *Garanteprivacy* [online]. 30. ledna 2025 [cit. 2025-03-04]. Dostupné z: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10097450>.

¹⁴ CHEE, Yun Foo. DeepSeek may face further regulatory actions, EU privacy watchdog says. In: *Reuters* [online]. 11. 2. 2025 [cit. 2025-03-04]. Dostupné z: <https://www.reuters.com/technology/deepseek-may-face-further-regulatory-actions-eu-privacy-watchdog-says-2025-02-11/>.

¹⁵ DeepSeek now in sights of EU data protection watchdogs. In: *Irish legal* [online]. 31. 1. 2025 [cit. 2025-03-04]. Dostupné z: <https://www.irishlegal.com/articles/deepseek-now-in-sights-of-eu-data-protection-watchdogs>; BOOTH, Robert – KRUPA, Jakub – GIUFFRIDA, Angela. DeepSeek blocked from some app stores in Italy amid questions on data use. In: *The Guardian* [online]. 29. 1. 2025 [cit. 2025-03-04]. Dostupné z: <https://www.theguardian.com/technology/2025/jan/29/deepseek-blocked-some-app-stores-italy-questions-data-use>.

¹⁶ CHEE, Yun Foo. *DeepSeek may face further regulatory actions, EU privacy watchdog says.*

pro snahy o digitální suverenitu, jako je ochrana ústavních hodnot a základních práv, konkrétně práva na ochranu soukromí a osobních údajů, svobodu projevu a principů právního státu; jednak působí jako nezbytný limit pro výkon digitální suverenity, aby přijatá opatření byla vždy proporcionální a nezbytná. Diskuse se přesouvá od prosté kontroly dat k otázce, jak stát může efektivně chránit základní práva svých občanů a zajistit demokratické procesy v prostředí, kde klíčové digitální infrastruktury a algoritmy mohou podléhat vlivu cizích jurisdikcí. Zároveň se objevuje naléhavá potřeba teoreticky uchopit problém důvěry a odpovědnosti v algoritmických rozhodnutích, neboť neprůhlednost a potenciální zkreslení generativních modelů mohou zásadně oslabit veřejnou důvěru v informace a legitimitu rozhodovacích procesů, které jsou stále více zprostředkovány technologiemi. Případ DeepSeeku tak neslouží jen jako případová studie pro analýzu souladu s regulací, ale především jako ilustrace a katalyzátor pro hlubší zamyšlení nad obecnými teoretickými důsledky regulace generativní AI.

Článek tedy analyzuje právní rámec ochrany osobních údajů v EU, zejména s ohledem na nařízení GDPR a AI Act, a hodnotí, zda DeepSeek splňuje požadavky těchto regulací, a klade si otázku, jakým způsobem aktuální a připravovaný právní rámec Evropské unie reaguje na výzvy spojené s ochranou osobních údajů a digitální suverenitou, které vystávají v souvislosti s provozem globálních generativních AI modelů, jako je DeepSeek, a jaké jsou teoretické a praktické důsledky uplatnění těchto regulačních nástrojů. Přičemž na základě prvotní analýzy lze formulovat hypotézu, že přesun dat uživatelů AI systémů sídlících mimo EU do třetích zemí bez odpovídajících záruk, jako je tomu v případě DeepSeeku, odhaluje inherentní napětí mezi globální povahou digitálních služeb a snahou EU prosadit svou digitální suverenitu a ochranu základních práv. Tato situace si vyžádá komplexní a potenciálně restriktivní regulační odpověď, jejíž efektivita a proporcionality budou klíčové pro udržení důvěry a zachování konkurenceschopnosti.

Zvolený metodologický rámec je založen na kvalitativní právní analýze, využívající případovou studii DeepSeeku k ilustraci aplikovatelnosti unijního práva a identifikaci relevantních regulačních dilemat. Studie rovněž zahrnuje komparativní analýzu přístupů EU a USA vůči technologickým společnostem se sídlem v Číně, poukazující na obdobný případ společnosti ByteDance, mateřské společnosti sociální sítě TikTok, která čelila obviněním ze sdílení dat s čínskými úřady. Reflektován je také přístup Evropské unie k regulaci AI a aplikace principu předběžné opatrnosti, jenž byl v minulosti využit například při omezení přístupu k některým digitálním službám v Evropě. Následně budou zhodnoceny možné regulační scénáře pro DeepSeek, včetně zařazení na seznam bezpečnostních hrozeb, dočasného zákazu či trvalé blokace jeho služeb v EU. Zvláštní pozornost je věnována otázce proporcionality a účinnosti těchto opatření, a to jak z pohledu ochrany osobních údajů, tak z hlediska geopolitických a širších teoretických důsledků.

1. Skutečný soulad s GDPR, nebo jen iluze?

Data uživatelů AI modelu DeepSeek jsou ukládána v Čínské lidové republice, přičemž chybí jakákoliv zmínka o zpracování osobních údajů v souladu s GDPR, a navíc je v DeepSeek uvedeno, že jurisdikcí pro zpracování osobních údajů je Čínská lidová republika.¹⁷ Tato

¹⁷ Zásady ochrany osobních údajů. In: *Deepseek* [online]. [cit. 2025-03-04]. Dostupné z: <https://deepseek.talkai.info/cs/privacy-policy/>.

deklarace DeepSeeku však nevylučuje aplikovatelnost práva Evropské unie. Evropská legislativa je totiž navržena tak, aby chránila evropské občany a trh bez ohledu na to, kde má sídlo poskytovatel digitální služby, pokud cílí na uživatele v EU. Klíčovým je zde princip extraterritoriální působnosti, která se vztahuje na zpracování osobních údajů subjekty usazenými mimo Unii, pokud je zpracování spojeno s nabízením zboží nebo služeb subjektům údajů v Unii nebo s monitorováním jejich chování, pokud k němu dochází v Unii.¹⁸ Vzhledem k tomu, že DeepSeek evidentně nabízí své služby uživatelům v členských státech EU a monitoruje jejich chování (např. pro zlepšování modelu), spadá pod působnost GDPR, a to bez ohledu na své prohlášení o jurisdikci.

Přenos osobních údajů do třetích zemí je povolen pouze za určitých podmínek stanovených v GDPR, které však DeepSeek nesplňuje.¹⁹ Ten je umožněn na základě rozhodnutí o odpovídající ochraně vydaném Evropskou komisí, které deklaruje, že určitá země zajišťuje odpovídající úroveň ochrany osobních údajů. Čína takové rozhodnutí nemá, což znamená, že přenosy osobních údajů do Číny nejsou automaticky povoleny.²⁰ V případě absence rozhodnutí o odpovídající ochraně, tedy v případě DeepSeeku a zpracovávání osobních údajů v Číně, musí správce nebo zpracovatel zajistit přiměřené záruky, například prostřednictvím standardních smluvních doložek schválených Evropskou komisí. V určitých případech může být přenos povolen na základě výjimek,²¹ například s výslovným souhlasem subjektu údajů po informování o možných rizicích.²² Pokud však DeepSeek přenáší osobní údaje uživatelů z EU do Číny bez splnění výše uvedených podmínek, představuje to významné porušení GDPR.

Zpracování osobních údajů občanů EU v Číně lze vykládat jako porušení přísných pravidel Evropské unie pro ochranu údajů. Vzhledem k tomu, že je tento AI model v Evropské unii snadno dostupný, jedná se o aktuální a prioritní téma. Počty stažení ze systému iOS nejsou veřejně dostupné, ovšem ze systému Android si DeepSeek měsíc po jeho zveřejnění stáhlo přes deset milionů uživatelů,²³ z toho přibližně 10–12 %, tedy více než milion uživatelů, jsou občany EU.²⁴ Za zmínku stojí, že nedodržování legislativních pravidel EU lze jako odpověď dostat od samotného AI modelu. Když byl model DeepSeek-R1 vyzván, aby posoudil své vlastní zásady ochrany osobních údajů z hlediska souladu s GDPR, kategoricky uvedl, že má několik mezer.²⁵

Důležitým aspektem u DeepSeeku je jeho open-source licence, protože dle AI Actu mají poskytovatelé odlišné a snížené regulační povinnosti stanovené v článku 53 odst. 1 písm. a) a b),²⁶ pokud budou jejich modely umělé inteligence „vydány pod svobodnou

¹⁸ Čl. 3 odst. 2 GDPR; čl. 13 odst. 1 DSA; čl. 2 odst. 1 a) c), AI Act.

¹⁹ Čl. 44–49, GDPR.

²⁰ Adequacy decisions. In: *Commission.Europa* [online]. [cit. 2025-03-04]. Dostupné z: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en?

²¹ Čl. 49, GDPR.

²² Čl. 49, odst. 1, písm. a), ibidem.

²³ DeepSeek – AI Assistant. In: *Obchod Play* [online]. [cit. 2025-03-04]. Dostupné z: <https://play.google.com/store/apps/details?hl=en-US&id=com.deepseek.chat>.

²⁴ CURRY, David. DeepSeek Revenue and Usage Statistics (2025). In: *Businessofapps* [online]. 13. 2. 2025 [cit. 2025-03-04]. Dostupné z: <https://www.businessofapps.com/data/deepseek-statistics/>.

²⁵ POEL, Van den Michaël. Talk of the (Brussels) town today: Deepseek and its relation to EU data protection law. In: *LinkedIn* [online]. Únor 2025 [cit. 2025-03-04]. Dostupné z: https://www.linkedin.com/posts/michael-van-den-poel_talk-of-the-brussels-town-today-deepseek-activity-7290006543016558593-A-bK/.

²⁶ Čl. 53, odst. 1, písm. a), b), Akt o umělé inteligenci.

a open-source licencí, která umožňuje přístup, používání, úpravy a distribuci modelu a její parametry, včetně vah, informací o architektuře modelu a informací o použití modelu, jsou veřejně dostupné.“²⁷ Nevztahují se tedy na něj povinnosti vypracovávat podrobnou technickou dokumentaci, zavést politiku autorských práv a zveřejnit dostatečně podrobný souhrn obsahu chráněného autorskými právy, který byl použit k trénování modelu, který od srpna 2025 bude vyžadovat AI Act.²⁸ V zásadách společnosti DeepSeek, v části *Jak používáme vaše informace*, v sekci „uchovávání údajů“ uvádí, že společnost DeepSeek použije osobní údaje „nezbytné pro splnění našich zákonných a regulačních povinností, včetně monitorování, odhalování a prevence podvodů; a pro naše daňové a účetní povinnosti a povinnosti v oblasti finančního výkaznictví“,²⁹ čímž formálně splňuje požadavky na zákonné zpracovávání osobních údajů uživatelů,³⁰ v praxi je však třeba brát v úvahu, že podezření týkající se nedodržování předpisů na ochranu osobních údajů a bezpečnosti, včetně možného sdílení dat s čínskou vládou, zpochybňují význam tohoto formálního souladu. V tomto případě tak nelze open-source povahu DeepSeeku považovat za polehčující okolnost, neboť zůstává otázka, zda model v rámci svého fungování neporušuje základní principy ochrany soukromí a transparentnosti.

Právě rizika však u DeepSeeku jsou. Primárně se jedná o již zmíněnou problematiku v oblasti ochrany osobních údajů uživatelů, kterou vyšetřují Evropský sbor pro ochranu osobních údajů i členské státy. Druhým rizikem, který se projeví zejména při vyšetřování, je nedůvěryhodnost společnosti DeepSeek z pohledu poskytovaných informací. To se projevilo například při tvrzení, že trénování DeepSeek stálo pouze 6 milionů dolarů a 2 048 grafických procesorů střední a vyšší třídy. Analytické studie však uvádí, že společnost DeepSeek vynaložila 1,6 miliardy dolarů na náklady na hardware a má flotilu 50 000 grafických procesorů Nvidia Hopper a A100.³¹ Jedná se pravděpodobně o snahu nepřiznat přístup k těmto procesorům, protože americká vláda neudělila exportní licenci pro export těchto nejvýkonnějších procesorů do Číny.³² Výzkumy v Číně sice přiznávaly přístup k těmto procesorům, avšak v řádu jednotek, nikoliv desítek tisíc, jako tomu je v případě DeepSeeku.³³ Tato skutečnost dle autora příspěvku snižuje důvěryhodnost informací poskytovaných společností během vyšetřování a vyžaduje důkladné vyšetřování bez opomenutí jakýchkoliv aspektů. Vzhledem k těmto pochybnostem je pozitivním krokem iniciativa vzniku týmu rychlé reakce, který bude sloužit ke koordinaci opatření orgánů pro ochranu údajů.³⁴

²⁷ Čl. 53, odst. 2, ibidem.

²⁸ Bod 179, ibidem.

²⁹ Zásady ochrany osobních údajů. In: *Deepseek* [online]. [cit. 2025-03-04]. Dostupné z: <https://deepseek.talkai.info/cs/privacy-policy/>.

³⁰ Čl. 6, GDPR.

³¹ PATEL, Dylan – KOURABI, AJ – O'LAUGHLIN, Doug – KNUHTSEN, Reyk. *DeepSeek Debates: Chinese Leadership On Cost, True*. In: *SemiAnalysis* [online]. 31. 1. 2025 [cit. 2025-03-04]. Dostupné z: <https://semianalysis.com/2025/01/31/deepseek-debates/>.

³² Form 8-K, Current report. In: *United States Securities and Exchange Commission* [online]. 26. 8. 2022 [cit. 2025-03-04]. Dostupné z: <https://www.sec.gov/ix?doc=/Archives/edgar/data/0001045810/000104581022000146/nvda-20220826.htm>.

³³ TITCOMB, James. Chinese researchers sidestep US sanctions on Nvidia chips. In: *The Telegraph* [online]. 16. 3. 2024 [cit. 2025-03-04]. Dostupné z: <https://www.telegraph.co.uk/business/2024/03/16/china-ai-researchers-sidestep-biden-nvidia-chip-sanctions/>.

³⁴ EDPB adopts statement on age assurance, creates a task force on AI enforcement and gives recommendations to WADA. In: *European Data Protection Board* [online]. 12. 2. 2025 [cit. 2025-03-04]. Dostupné z: https://www.edpb.europa.eu/news/news/2025/edpb-adopts-statement-age-assurance-creates-task-force-ai-enforcement-and-gives_en.

2. Princip předběžné opatrnosti a regulační dilema DeepSeeku

I když se jedná dle názvu o „tým rychlé reakce“, nelze považovat tuto rychlost za dostačnou, a tedy za adekvátní přístup od EPDB, respektive EU. Otázka předávání dat do Číny není novým problémem, jak ukazuje případ společnosti ByteDance, mateřské společnosti sociální sítě TikTok. Tento problém byl intenzivně řešen i ve Spojených státech, kde bylo zahájeno řízení proti ByteDance kvůli možnému sdílení uživatelských dat s čínskými úřady.³⁵ ByteDance je čínská společnost a podle čínských zákonů, zejména podle zákona o národní bezpečnosti,³⁶ by mohla být nucena sdílet data s čínskými úřady. Americké zpravodajské služby se obávaly, že TikTok může být využíván ke špionáži, sledování uživatelů a šíření propagandy,³⁷ protože TikTok sbírá velké množství dat (např. polohu, kontakty, biometrické údaje), což vzbuzuje obavy, že by mohla být data zneužita k profilování uživatelů. Studie také ukazují, že TikTok cenzuruje obsah, který je v rozporu s čínskými zájmy (např. zmínky o Tchaj-wanu, Hongkongu, Ujgurech).³⁸ Tato cenzura odlišných názorů od oficiálního stanoviska Čínské lidové republiky může vést k manipulaci veřejného mínění a podporuje dezinformační kampaně. ByteDance, stejně jako DeepSeek, není důvěryhodným partnerem při vyšetřování, protože i on podával nepravdivé informace. ByteDance měl přístup k datům amerických uživatelů, přestože firma tvrdila, že se data ukládají na serverech v USA.³⁹ Předpokládaným řešením by mohlo být oddělení sociální sítě TikTok od ByteDance, aby měla kontrolu nad svými uživatelskými daty prodejem TikToku.⁴⁰ Tuto pozici potvrdil i Nejvyšší soud USA, který zároveň potvrdil ústavnost zákona Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA).⁴¹ Tento zákon zakazuje společnosti v USA poskytovat služby pro distribuci, údržbu nebo aktualizaci sociální sítě TikTok, pokud její provoz v USA není oddělen od čínské kontroly. Soud dospěl k závěru, že i kdyby tato regulace vlastnictví podniků zasahovala do práv na svobodu projevu uživatelů TikToku, obstála by při přezkumu podle střední úrovně přísnosti (*intermediate scrutiny*). Soud uvedl, že Kongres považuje divestici za nezbytnou k řešení dobře podložených obav o národní bezpečnost týkajících se

³⁵ Rozsudek Nejvyššího soudu USA ze dne 17. ledna 2025. *TikTok Inc. v. Garland*. Dostupné z: <https://www.supremecourt.gov/opinions/24pdf/24-656-ca7d.pdf>.

³⁶ National Security Law of the People's Republic of China, No. 29/2015. Dostupné z: <https://govt.chinadaily.com.cn/s/201812/11/WS5c0f1b56498eefb3fe46e8c9/national-security-law-of-the-peoples-republic-of-china-2015-effective.html>.

³⁷ TikTok Concerns and Vulnerabilities. In: *National Counterintelligence and Security Center* [online]. Březen 2023 [cit. 2025-03-04]. Dostupné z: https://www.dni.gov/files/NCSC/documents/nittf/OPSEC_Advisory_TikTok_Concerns_and_Vulnerabilities.pdf.

³⁸ FINKELSTEIN, Danit – YANOVSKY, Sonia – ZUCKER, Jacob – JAGDEEP, Anisha – VASKO, Collin – JAGDEEP, Ankita – JUSSIM, Lee – FINKELSTEIN, Joel. Information manipulation on TikTok and its relation to American users' beliefs about China. *Frontiers in Social Psychology*. 2024, Vol. 2 [cit. 2025-03-04]. Dostupné z: <https://doi.org/10.3389/frsps.2024.1497434>; FINKELSTEIN, Joel – JUSSIM, Lee – FARMER, John – GOLDENBER, Alex – ZUCKER, Jacob – FINKELSTEIN, Danit – YANOVSKY, Sonia. The CCP's Digital Charm Offensive: How TikTok's Search Algorithm and Pro-China Influence Networks Indoctrinate GenZ Users in the United States. In: *Network Contagion Research Institute* [online]. [cit. 2025-03-04]. Dostupné z: https://networkcontagion.us/wp-content/uploads/NCRI-Report_The-CCPs-Digital-Charm-Offensive.pdf.

³⁹ BAKER, Emily. TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens. In: *Forbes* [online]. 22. 11. 2022 [cit. 2025-03-04]. Dostupné z: <https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/>.

⁴⁰ JOANNAVITHULA, Ani – SAYED, Pantho. The TikTok Bill Isn't Only About TikTok. In: *Jolt* [online]. 26. 4. 2023 [cit. 2025-03-04]. Dostupné z: <https://jolt.law.harvard.edu/digest/the-tiktok-bill-isnt-only-about-tiktok>.

⁴¹ Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA).

praktik sběru dat TikTok a jeho vztahu s cizím protivníkem a že zákon neporušuje práva stěžovatelů podle Prvního dodatku Ústavy.⁴²

Společnost ByteDance figuruje také u AI modelu DeepSeek, který obsahuje její komponenty pro sběr dat. Společnost Privado, která se zabývá ochranou soukromí, identifikovala konkrétní čtyři sady pro vývoj softwaru ByteDance v aplikaci DeepSeek pro Android, včetně systémů pro analýzu, monitorování provozu a sběr dat o výkonu.⁴³ Podobně analýza síťového provozu odhalila, že verze aplikace DeepSeek pro iOS odesílá nešifrovaná citlivá uživatelská data na servery vlastněné ByteDance,⁴⁴ objevují se tedy obdobné pochybnosti o ochraně dat jako v případě sociální sítě TikTok v USA. Jihokorejská Komise pro ochranu osobních údajů (PIPC) vznesla obvinění z předávání uživatelských dat společnosti ByteDance, když zjistila, že DeepSeek sdílí data uživatelů s ByteDance bez jejich vědomí.⁴⁵

Podezření na nedodržování GDPR⁴⁶ a AI Actu⁴⁷ AI modelem DeepSeek se jeví jako oprávněné, samotné vyšetřování by tedy mělo zejména odpovědět na otázku, zda tato skutečnost představuje nepřijatelné riziko pro uživatele. V případě kladné odpovědi by mohl být DeepSeek v EU významně omezen, nebo dokonce zakázán.⁴⁸

Zákaz DeepSeeku na základě zmíněných skutečností by byl v souladu s přístupem EU k digitálním technologiím i AI. EU často uplatňuje princip předběžné opatrnosti (*precautionary principle*) při regulaci nových technologií, včetně AI. Tento princip umožňuje přijímat preventivní opatření v situacích, kdy vědecké důkazy o potenciálních rizicích jsou nejisté, ale možné následky by mohly být závažné. Podle analýzy Evropského parlamentu z roku 2015 princip předběžné opatrnosti „umožňuje tvůrcům rozhodnutí přijímat preventivní opatření, když jsou vědecké důkazy o environmentálním nebo zdravotním riziku nejisté a sázky jsou vysoké.“⁴⁹ Tento princip bývá kritizován názory, že aplikace principu předběžné opatrnosti by mohla omezit inovace a adopci AI technologií, což by mohlo negativně ovlivnit ekonomický růst a společenský pokrok.⁵⁰ Autor však považuje princip předběžné opatrnosti za racionální a žádoucí, zejména v citlivé oblasti ochrany osobních údajů. Zejména pokud se jedná o aplikaci principu na základě podezření vycházejících z aktuálně známých informací, jako tomu je v případě DeepSeek, nikoliv z jednání bez

⁴² Rozsudek Nejvyššího soudu USA ze dne 17. ledna 2025. *TikTok Inc. v. Garland*. Dostupné z: https://www.supremecourt.gov/opinions/24pdf/24-656_ca7d.pdf.

⁴³ ANTIL, Vaibhav. DeepSeek App: A Closer Look at Its Privacy Posture. In: *Privado* [online]. 29. 1. 2025 [cit. 2025-03-04]. Dostupné z: <https://www.privado.ai/post/deepseek-app-a-closer-look-at-its-privacy-posture>.

⁴⁴ LEKANDER, Alex. DeepSeek iOS App Sends Cleartext Data to ByteDance Servers. In: *Cyberinsider* [online]. 7. 2. 2025 [cit. 2025-03-04]. Dostupné z: <https://cyberinsider.com/deepseek-ios-app-sends-clear-text-data-to-bytedance-servers/>.

⁴⁵ Tisková zpráva PIPC o dočasném pozastavení poskytování aplikací společnosti DeepSeek v Jižní Koreji. In: *Government of the Republic of Korea* [online]. [cit. 2025-03-04]. Dostupné z: https://www.pipc.go.kr/eng/user/ltm/new/noticeDetail.do?bbsId=BBSMSTR_000000000001&nttId=2784#none.

⁴⁶ Čl. 44–49, GDPR.

⁴⁷ Čl. 5, Akt o umělé inteligenci.

⁴⁸ Čl. 58, odst. 2, ibidem.

⁴⁹ The precautionary principle: Definitions, applications and governance. In: *European Parliament* [online]. 9. 12. 2015 [cit. 2025-03-04]. Dostupné z: https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA%282015%29573876.

⁵⁰ CASTRO, Daniel – McLAUGHLIN, Michael. Ten Ways the Precautionary Principle Undermines Progress in Artificial Intelligence. In: *Information Technology & Innovation Foundation* [online]. 4. 2. 2019 [cit. 2025-03-04]. Dostupné z: <https://itif.org/publications/2019/02/04/ten-ways-precautionary-principle-undermines-progress-artificial-intelligence/>.

znalostí či informací. To odpovídá povaze AI Actu o vyvážení mezi podporou inovací a zajištěním bezpečnosti a důvěryhodnosti AI modelů.⁵¹

EPBD však v rámci svého šetření přistupuje k DeepSeeku na základě důkazů a hodnocení rizik již vzniklé situace spíše než preventivních opatření předem, tedy přístupem charakteristickým zejména pro USA.⁵² V USA je preferováno hodnocení na základě empirických dat a konkrétních případů. Tento přístup kontrastuje s principem předběžné opatrnosti, který je častěji uplatňován v evropských zemích a zahrnuje preventivní regulaci technologií na základě potenciálních, i když dosud neprokázaných rizik. Princip předběžné opatrnosti v souvislosti s AI modelem DeepSeek aplikovaly zmíněné státy jako Itálie, či Jižní Korea, avšak ne EPBD.

Evropská unie je známá svou pokročilou legislativou na ochranu osobních údajů, která je považována za komplexní a efektivní.⁵³ Efektivita ochrany osobních údajů však do značné míry závisí na procesním výkonu, nejen legislativním pramenu, a současný stav zpracování takto citlivých dat nelze považovat za adekvátní. DeepSeek je stahován velkým množstvím obyvatel EU, v řádu jednotek milionů. Přitom u DeepSeeku existuje reálné podezření, že není v souladu s právními předpisy EU, zejména v oblasti ochrany osobních údajů. Tato oblast je natolik citlivá, že v případě byt jen důvodného podezření na nedostatečnou ochranu či na přesun a manipulaci s daty, včetně sbírání dat a tvorby digitální podoby uživatele v Číně, je nutné se zabývat i možností zakázání, respektive pozastavení možnosti jeho fungování v EU, dokud nebude celá situace řádně prošetřena.

Princip předběžné opatrnosti v tomto případě aplikovaly státy, které DeepSeek zakázaly, ať již v měkčí, nebo tvrdší formě zákazu. Měkčí zákaz zvolil jihokorejský úřad pro ochranu osobních údajů, který nařídil společnostem Apple a Google odstranit aplikaci DeepSeek z jejich obchodů s aplikacemi. Je však důležité poznamenat, že přístup k němu prostřednictvím webového prohlížeče zůstává v zemi nadále možný, nejde tedy o jeho úplný zákaz. Tvrdší zákaz naopak zvolily italské úřady, které se rozhodly dočasně zakázat DeepSeek kvůli obavám o ochranu osobních údajů ve všech podobách, tedy nejen ve formě aplikace, ale i přístupu prostřednictvím webového prohlížeče.

Tato forma preventivní opatrnosti přístupu k AI modelům, u kterých existuje důvodné podezření na porušování legislativních aktů, má vyjma menšího zásahu do osobních údajů občanů EU ještě jeden významný pozitivní aspekt. AI modely jsou stále ve svých počátcích a dle studie zabývající se patenty v oblasti AI současný trend naznačuje rostoucí počet AI modelů a jejich implementaci v různých odvětvích.⁵⁴ Ponechání AI modelu k dispozici občanům EU i přes důvodné podezření na nedodržování legislativních předpisů EU může vést k inflaci takovýchto modelů. Protože bude jednodušší je vytvořit a EPDB tak může být přetížen jednotlivými vyšetřováními, která budou nad jeho personální kapacity.

⁵¹ FRASER, Henry – VILLARINO, José-Miguel Bello y. Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough. *European Journal of Risk Regulation*. 2024, Vol. 15, No. 2 [cit. 2025-03-04]. Dostupné z: <https://doi.org/10.1017/err.2023.57>.

⁵² Blueprint for an AI Bill of Rights. In: *Biden White House* [online]. [cit. 2025-03-04]. Dostupné z: <https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/>.

⁵³ LYNKEY, Orla. Complete and Effective Data Protection. *Current Legal Problems*. 2023, Vol. 76, No. 1 [cit. 2025-03-04]. Dostupné z: <https://doi.org/10.1093/clp/cuad009>.

⁵⁴ GONZALES, Julius Tan. Implications of AI innovation on economic growth: a panel data study. *Journal of Economic Structures*, 2023, Vol. 12 [cit. 2025-03-04]. Dostupné z: <https://doi.org/10.1186/s40008-023-00307-w>.

3. Regulační scénáře pro DeepSeek

Při posuzování reakce na potenciální rizika spojená s provozem AI modelů EU disponuje řadou nástrojů s různou mírou intenzity. Primární kroky při snaze o sjednání nápravy směřují k méně invazivním, avšak závazným opatřením, jejichž cílem je vynutit soulad s unijním právem. Mezi taková opatření patří formální varování ze strany příslušného dozorového orgánu, uložení administrativních pokut za porušení GDPR či AI Actu, nařízení specifických technických a organizačních opatření k zajištění ochrany dat a bezpečnosti systému nebo požadavek na určení právního zástupce DeepSeeku v EU, který by byl přímo odpovědný za dodržování právních předpisů. Dále by bylo možné nařídit zvýšený dohled a pravidelné audity datových toků a procesů či případně dočasné omezení určitých funkcionalit systému, které představují nejvyšší rizika. Cílem těchto kroků je dát provozovateli možnost k nápravě a minimalizovat dopady na uživatele a digitální trh.

Jedním z možných opatření EU by v případě DeepSeeku bylo jeho zařazení na seznam bezpečnostních hrozeb, což by umožnilo přijmout cílené restriktce vůči jeho provozu. Tato úvaha pramení ze závažných a přetrvávajících obav ohledně nedostatečné ochrany osobních údajů uživatelů a rizika jejich neoprávněného přístupu či předávání do třetích zemí bez odpovídajících právních záruk, což by mohlo zpochybňovat soulad s esenciálními požadavky unijního práva a představovat hrozbu pro digitální suverenitu občanů EU. Evropské vlády by následně mohly rozhodnout o jeho částečné či úplné blokaci, například prostřednictvím poskytovatelů internetových služeb. Tento postup byl v minulosti aplikován v případě některých ruských webových stránek po začátku války na Ukrajině, kdy došlo k jejich plošnému zablokování v rámci unijní reakce na hybridní hrozby a dezinformační kampaně.⁵⁵ Primárním nástrojem u scénáře DeepSeeku se jeví uložení povinnosti poskytovatelům internetových služeb (ISP) v členských státech provést blokaci na úrovni DNS (*Domain Name System*). Tento mechanismus, který byl efektivně využit například zmíněným zákazem italským úřadem Garante pro ochranu osobních údajů, zamezuje překladu doménového jména služby na její IP adresu, čímž znemožňuje připojení. Doplnkově by mohlo být zváženo případné IP blokování, avšak to je technicky náročnější a méně flexibilní. Ačkoliv je nutné uznat, že se nejedná o blokaci absolutní, a technicky zdatní uživatelé mohou takové blokace obejít (např. použitím VPN či alternativních DNS serverů), tato opatření se v současnosti jeví jako nejefektivnější a nejrychlejší cesta k plošnému omezení přístupu pro většinu běžných uživatelů, a sloužila by jako silný signál pro zajištění souladu s evropskými předpisy.

V případě DeepSeeku by podobná opatření mohla zahrnovat zákaz přístupu ke službě v rámci veřejných institucí, vyloučení z kritické infrastruktury či úplné odpojení od evropského internetového prostoru prostřednictvím rozhodnutí regulačních orgánů. Takový krok by však měl zásadní dopady nejen na dostupnost DeepSeeku v EU, ale mohl by mít i dopad na širší geopolitické vztahy mezi Unií a Čínou, zejména v kontextu digitální

⁵⁵ EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU. In: *Council of the EU* [online]. 2. 3. 2022 [cit. 2025-03-04]. Dostupné z: <https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-russia-today-and-sputnik-s-broadcasting-in-the-eu/>; Russia's war of aggression against Ukraine: Council bans broadcasting activities in the European Union of four more Russia-associated media outlets. In: *Council of the EU* [online]. 17. 5. 2024 [cit. 2025-03-04]. Dostupné z: <https://www.consilium.europa.eu/en/press/press-releases/2024/05/17/russia-s-war-of-aggression-against-ukraine-council-bans-broadcasting-activities-in-the-european-union-of-four-more-russia-associated-media-outlets/>.

suverenity a ochrany strategických datových toků. Osobní údaje občanů EU by však byly chráněny před možným zneužitím. Trvalý zákaz je však radikálním řešením, u kterého by autor očekával napadení takového rozhodnutí DeepSeekem u Soudního dvora, tedy obdobnou reakci jako v případě zákazu TikToku v USA.⁵⁶ Evropská unie navíc obvykle dává přednost dialogu a spolupráci s dotčenými subjekty před uvalením přímých zákazů. Cílem je dosáhnout souladu s právními předpisy prostřednictvím konstruktivního procesu, který umožňuje společností napravit své postupy bez nutnosti okamžitých restriktivních opatření. Je zároveň třeba zmínit, že případné trvalé omezení přístupu je komplexní a vyvolává řadu dilemat, zejména ve vztahu k právům a svobodám uživatelů. Potenciální regulační opatření, jako je plošná blokáce, by také mohla vyvolat otázky ohledně svobody projevu a přístupu k informacím, garantovaných například Listinou základních práv EU⁵⁷ nebo Evropskou úmluvou o lidských právech.⁵⁸ Omezení přístupu k digitálním službám by tak mohlo být vnímáno jako zásah do práv uživatelů na komunikaci a získávání informací z různých zdrojů. Dále je nezbytné zvážit dopad na právo na přístup k technologiím, které, ačkoliv není v současné době explicitně zakotveno jako samostatné, formální, mezinárodně uznávané lidské právo, ale spíše chápáno jako právo instrumentální nebo facilitující, je v digitální éře klíčové pro participaci na společenském a ekonomickém životě. Každé takové opatření proto musí striktně podléhat testu proporcionality a nezbytnosti v demokratické společnosti, aby bylo zajištěno, že legitimní cíl (jako je ochrana osobních údajů a národní bezpečnost) je dosažen co nejméně invazivním způsobem a nepřiměřeně neomezuje práva jednotlivců. Kromě dopadů na práva uživatelů by plošná blokáce jednoho z AI modelů mohla mít důsledky i pro hospodářskou soutěž v EU. Zákaz jednoho z modelů na rychle se rozvíjícím trhu generativní AI by mohl sice krátkodobě zvýhodnit stávající konkurenty, avšak dlouhodobě by mohl vést k omezení konkurence a inovací, potenciálně i k vyšším cenám či nižší kvalitě pro evropské uživatele. Dále by takový krok přispěl k fragmentaci globálního digitálního trhu a mohl by vyvolat riziko odvetných opatření ze strany třetích zemí vůči evropským technologickým firmám. Je tedy zásadní posuzovat každé restriktivní opatření nejen z pohledu ochrany dat a národní bezpečnosti, ale i s ohledem na jeho širší dopady na dynamiku trhu a celkový digitální ekosystém EU.

V případě zmiňovaného dočasného zákazu na základě principu předběžné opatrnosti však je nutné určit, kdy bude zákaz ukončen, případně potvrzen. Ten by měl trvat, dokud provozovatel nesjedná nápravu,⁵⁹ případně do stanovení data, do kterého má k nápravě dojít. Pokud by se DeepSeek, případně obecně jakýkoliv AI model, který nesplňuje legislativní požadavky EU, rozhodl vyhovět evropské regulaci, aby si udržel přístup na trh EU, musel by změnit současný stav. To by mohlo zahrnovat například zřízení evropského datového centra, podobně jako OpenAI a další velcí hráči. DeepSeek by mohl začít ukládat a zpracovávat data pouze v EU a zajistit, že žádná data nebudou odesílána do Číny. Součástí těchto opatření by byl také soulad s GDPR, včetně jmenování zástupce v EU, jak požaduje legislativa. Tento krok je povinný pro zahraniční společnosti, které zpracovávají

⁵⁶ KERN, Rebecca. TikTok sues to challenge law forcing sale or ban. In: *Politico* [online]. 5. 7. 2024 [cit. 2025-03-04]. Dostupné z: <https://www.politico.com/news/2024/05/07/tiktok-sues-to-challenge-law-forcing-sale-or-ban-00156517>.

⁵⁷ Čl. 11, Listina základních práv EU.

⁵⁸ Čl. 10, Evropská úmluva o lidských právech.

⁵⁹ Čl. 68, čl. 71, Akt o umělé inteligenci; čl. 58, odst. 2, čl. 83, GDPR.

data občanů EU, a zajišťuje, že mají v Unii právního zástupce.⁶⁰ Kromě toho by DeepSeek musel zavést transparentnější pravidla a upravit zásady zpracování osobních údajů. Tím by si DeepSeek zachoval přístup na trh EU a také by to posílilo důvěru uživatelů v jeho služby.

Druhou variantou v případě dočasného zákazu by bylo nesplnění legislativních požadavků EU. Důvodů pro toto nesplnění existuje vícero, například by stále panovala obava ze zpřístupnění osobních údajů občanů EU čínské vládě, tím by DeepSeek mohl mít problém se získáním evropského certifikátu důvěryhodnosti podle AI Actu, případně by si náklady na provoz v EU vyhodnotil jako vysoké. Pokud tedy i po stanoveném datu EU dojde k závěru, že DeepSeek porušuje GDPR a AI Act, a proto zahájí vyšetřování a případné následné sankční řízení.⁶¹ Pokud DeepSeek pokuty nezaplatí nebo se přizpůsobí jen formálně, může dojít k trvalé blokaci jeho služeb v EU. Ta by se dala také chápat jako signál, že ochrana soukromí není jen teorie v legislativních pramenech EU. Zároveň by mohlo dojít k eliminaci podobného chování u ostatních společností provozujících AI modely.

Závěr

Evropská unie se dlouhodobě profiluje jako globální lídr v regulaci umělé inteligence a ochrany osobních údajů. Tento přístup je často kritizován pro údajné zpomalování technologického pokroku a konkurenceschopnosti evropského trhu. Případ DeepSeeku představuje test, zda jsou tyto kritiky oprávněné a zda EU dokáže efektivně čelit výzvám spojeným s potenciálně nebezpečnými AI modely.

DeepSeek vykazuje závažné nedostatky jeho souladu s GDPR a AI Actem, přičemž klíčová rizika spočívají v přenosu dat do Číny, netransparentním nakládání s osobními údaji a potenciálním přístupem čínských státních orgánů k těmto datům. Některé státy, jako například Itálie či Jižní Korea, uplatnily formu zákazu DeepSeeku na svém území. Evropská unie oproti tomu dosud k tomuto opatření nepřistoupila, přestože princip předběžné opatrnosti, který často uplatňuje v jiných případech, by nasvědčoval dočasnému nebo trvalému omezení přístupu této technologie na unijní trh.

Z pohledu právního rámce je EU na podobné případy připravena, ale její reakce by měla být aktivnější. Příspěvek proto dospívá k závěru, že Unie by měla zvážit dočasný zákaz DeepSeeku do doby, než bude zajištěn plný soulad s evropskou legislativou, což může být zejména vytvoření datových center v EU, zavedení specifických šifrovacích protokolů, změna procesů zpracování dat, aby splňoval požadavky EU práva, určení zástupce v EU a další. Tento postup by nejen ochránil osobní údaje občanů EU, ale také by vytvořil důležitý precedens pro další problematické AI modely. Současně je nezbytné posílit spolupráci mezi členskými státy a dozorovými orgány, aby bylo možné pružně a efektivně reagovat na podobné hrozby v budoucnu.

Případ DeepSeeku představuje významný milník v oblasti regulace AI a ochrany osobních údajů. Pokud EU neprokáže schopnost prosadit vlastní pravidla vůči zahraničním technologickým subjektům, mohla by oslabit svou pozici v oblasti digitální suverenity. Naopak důsledné vymáhání právních předpisů by nejen zvýšilo ochranu uživatelů, ale

⁶⁰ Čl. 27, GDPR.

⁶¹ Čl. 83, GDPR.

zároveň by vyslalo jasný signál dalším poskytovatelům AI modelů o nutnosti dodržování evropských standardů. Evropská unie má několik možností, jak reagovat na bezpečnostní rizika spojená s DeepSeekem. Mezi nejprísnější opatření by patřilo jeho zařazení na seznam bezpečnostních hrozeb, což by mohlo vést až k úplné blokaci jeho služeb v EU, podobně jako v minulosti u některých ruských webových stránek. Přestože by takový krok posílil ochranu osobních údajů občanů EU, zároveň by měl zásadní geopolitické důsledky a pravděpodobně by vyvolal právní spor před Soudním dvorem EU, podobně jako zákaz TikToku v USA. Toto potenciální regulační opatření, jako je plošná blokáce ať již dočasná, nebo trvalá, by také mohla vyvolat otázky ohledně svobody projevu a přístupu k informacím, což bylo otázkou i ve zmíněném právním sporu v USA týkající se regulace TikToku, který se rovněž zabýval otázkou zásahů do práv uživatelů, zejména práva na svobodu projevu, přičemž Nejvyšší soud USA dospěl k závěru, že i kdyby taková regulace skutečně zasahovala do lidských práv, při přezkumu by mohla být shledána jako oprávněná, což může argumentačně podpořit zmíněnou blokaci v EU.

V souladu s dosavadním přístupem EU je však pravděpodobnější snaha o dialog a nalezení řešení, které by umožnilo DeepSeeku pokračovat v činnosti při dodržení unijních pravidel. To by mohlo zahrnovat zřízení evropského datového centra, dodržování požadavků GDPR včetně jmenování zástupce v EU a zavedení transparentnějších zásad ochrany osobních údajů. Pokud by DeepSeek tyto podmínky nesplnil, mohla by EU prodloužit dočasný zákaz jeho činnosti nebo zahájit sankční řízení. Neochota DeepSeeku přizpůsobit se evropské legislativě by mohla vést k trvalé blokaci jeho služeb, což by posloužilo jako precedens pro přísnější vymáhání pravidel i vůči dalším AI modelům. Tento případ tak představuje důležitý test toho, nakolik EU dokáže efektivně chránit digitální suverenitu a práva svých občanů v kontextu globalizovaného trhu s umělou inteligencí.

DeepSeek as a Precedent – A Test of the Resilience of European AI Regulation

Martin Mach (<https://orcid.org/0009-0005-8437-6869>)

Abstract: This article discusses the privacy issues surrounding the DeepSeek AI system, which is facing allegations of transferring user data to China. The author analyses the legal framework for data protection in the EU, in particular with regard to the GDPR and the AI Act, and assesses whether DeepSeek complies with the requirements of these regulations. The study also reflects on the European Union's approach to AI regulation and the application of the precautionary principle, which has been used in the past, for example, to restrict access to certain digital services in Europe. The paper also compares the EU and US approach to technology companies based in China, highlighting the similar case of ByteDance, TikTok's parent company, which faced allegations of data sharing with Chinese authorities. The author assesses possible regulatory scenarios for DeepSeek, including security threat listing, temporary banning or permanent blocking of its services in the EU. Particular attention is paid to the question of proportionality and effectiveness of these measures, both in terms of data protection and geopolitical implications. The study concludes that, although the EU emphasises dialogue and redress, if there are reasonable doubts about data security, it would be appropriate to temporarily restrict DeepSeek's operations until it demonstrates full compliance with European legal standards.

Keywords: artificial intelligence, GDPR, AI Act, DeepSeek, data protection