Umělá inteligence – nové výzvy z pohledu osobních údajů

Martin Mach*

Abstrakt: V roce 2023 jsme zažili vzestup umělé inteligence (AI) a její rozšíření k masovému používání uživateli po celém světě. Umělá inteligence však také přináší významné výzvy v oblasti ochrany osobních údajů, tak jako všechny předchozí výrazné změny v oblasti moderních technologií. Celosvětově lze sledovat dva přístupy k AI v souvislosti s ochranou osobních údajů, jeden přístup reprezentují zejména Spojené státy americké a druhý přístup reprezentuje zejména Evropská unie. USA se zaměřují zejména na inovace a flexibilitu, zatímco EU klade důraz na ochranu soukromí a bezpečnost nad technologický posun. Předkládaný příspěvek se zaměří na ochranu uživatelů při užívání umělé inteligence a na konkrétní rizika ochrany osobních údajů u AI zahrnující neoprávněný přístup k citlivým datům, zneužití dat pro sledování a profilování uživatelů a nedostatečnou transparentnost algoritmů. V souvislosti s riziky užívání AI se příspěvek zaměří na nařízení stanovující harmonizovaná pravidla pro umělou inteligenci EU, tzv. AI Act, publikovaný EU. Ten by měl představovat komplexní rámec pro regulaci AI, který zahrnuje povinnosti pro vývojáře a uživatele AI, s cílem minimalizovat rizika a zajistit etické využití AI. Příspěvek se na konci bude zabývat tím, zda AI Act efektivně zajišťuje ochranu uživatelů v souvislosti s AI.

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

Úvod

Když v roce 1994 přišel na trh telefon IBM Simon, jednalo se o první *smartphone* na světě. I když to byl tehdy neúspěšný model, jenž se po roce prodeje a pouhých 50 000 prodaných kusech přestal prodávat, jednalo se o předzvěst současných chytrých telefonů. A samotné smartphony, respektive nepřeberné množství aplikací v nich, byly a stále jsou výzvou v oblasti regulace. A to nejen z hlediska ochrany uživatelů ve smyslu ochrany lidských práv, ale i například ve smyslu ekonomickém. Francouzský CNIL si pro období 2022–2024 stanovil jako jednu ze svých priorit *„sběr osobních údajů v aplikacích pro chytré telefony“*,[1] čímž dle mínění autora dokazuje, jak jeden přelomový produkt z roku 1994 dokáže výrazně ovlivňovat legislativu i o 30 let později.

V únoru roku 2004, deset let po prvním *smartphonu*, vznikla sociální síť Facebook. Tehdy síť přístupná pouze studentům, dnes sedmá největší společnost světa z pohledu tržní kapitalizace. I tento milník byl a stále je velkou výzvou, zejména z hlediska ochrany osobních údajů. Společnost Meta zejména kvůli ochraně osobních údajů dostala opakovaně pokuty od orgánů EU. Jedna z posledních, v celkové výši 1,2 miliard eur, pak byla

* 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 č. *IGA_PF_2024_013* Univerzity Palackého v Olomouci.

1 [Clôturée] Collecte de données dans les applications mobiles: la CNIL lance une consultation publique sur les enjeux économiques. In: *Cnil* [online]. 18. 1. 2023 [cit. 2025-02-09]. Dostupné z: https://www.cnil.fr/fr/cloturee-collecte-de-donnees-dans-les-applications-mobiles-la-cnil-lance-une-consultation-publique?trk=article-ssr-frontend-pulse_little-text-block; Plan Stratégique 2022–2024. In: *Cnil* [online]. 17. 2. 2022 [cit. 2025-02-09]. Dostupné z: https://www.cnil.fr/sites/cnil/files/atoms/files/cnil_plan_strategique_2022-24.pdf#page=7.

udělena za přenášení dat uživatelů do USA.[2] Nejde však jen o společnost Meta, problémy s ochranou osobních údajů a dalších lidských práv mají i jiné tzv. BigTech společnosti, které také dostaly pokuty od EU, například Google či Apple.[3]

Od vzniku Facebooku uplynulo skoro 10 let a díky Edwardu Snowdenovi (nejen) EU zjistila, že porušování lidských práv není doménou jen samotných Big Tech společností, ale i Spojených států, které ve spolupráci s Big Tech společnostmi získávaly osobní konverzace a historii vyhledávání uživatelů. Pro rok 2014 tak bylo výzvou, jak tento nejen právní, ale i politický problém vyřešit. V souvislosti s touto informací považuje autor za vhodné zmínit judikaturu Soudního dvora EU v oblasti přenosu osobních dat do USA, a sice případy *Schrems I*[4] a *Schrems II*.[5] Jedná se tedy o téma, které již v minulosti v Evropské unii silně rezonovalo.

I aktuální rok 2025 je ve znamení výzev v oblasti moderních technologií a ochrany lidských práv uživatelů. Od roku 2023 totiž lze pozorovat velký boom umělé inteligence (AI). Stala se součástí nástrojů, jež využívají uživatelé na denní bázi. Jenže, jak jsme již zvyklí z digitálního světa, čím větší je naše aktivita na internetu, tím větší zanecháváme digitální stopu. A internet, ať již se jedná o jednotlivce, či soukromé společnosti, toho o nás díky tomu ví více a více. Bohužel tak zná i značně citlivé informace, což je nežádoucí jev. A to samé zanechávání digitálních stop hrozí i u AI. Jelikož se jedná o poměrně aktuální téma, je zajímavé sledovat mezikontinentální přístup v regulaci AI zejména mezi USA a EU, protože každý z nich zvolil zcela odlišný přístup. Předkládaný příspěvek se tak pokusí odpovědět na otázku, jak na konkrétní výzvy reaguje EU na základě analýzy aktuálního přístupu EU v oblasti regulace v kontextu ochrany osobních údajů uživatele, tedy jednu ze stěžejních hodnot stanovených EU, a odhalit aktuální nedostatky v přístupu EU k AI.

1. EU vs. USA

Přístup USA k AI je ovlivněn dvěma významnými proměnnými. Zaprvé, AI je vytvářena a provozována Big Tech společnostmi, jako je Microsoft, Google, Meta a další. A právě přístup k těmto společnostem je velmi vstřícný. Důvodů je více. Jedním z nich je důvod ekonomický – velké technologické společnosti sídlící v USA znamenají zvýšenou zaměstnanost a velké množství peněz pro ekonomiku na daních a odvodech. Také v USA funguje velmi silný *lobbing* těchto společností, který se projevuje při projednávání nových zákonů, což dokazuje i počet skupin lobbujících u federální vlády USA za umělou inteligenci, který se od roku 2022 do roku 2023 téměř ztrojnásobil.[6] BigTech společnosti tak mají v USA silnější postavení a také zakládají společné dohody a uskupení, například *Partnerství pro*

---

2 1.2 billion euro fine for Facebook as a result of EDPB binding decision. In: *European Data Protection Board* [online]. 22. 5. 2023 [cit. 2025-02-09]. Dostupné z: https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en.

3 STOLTON, S. Apple, Google, Meta Probed by EU in Test of New Digital Law. In: *Bloomberg* [online]. 25. 3. 2024 [cit. 2025-02-09]. Dostupné z: https://www.bloomberg.com/news/articles/2024-03-25/apple-google-meta-probed-by-eu-in-test-of-new-digital-law.

4 Rozsudek Soudního dvora ze dne 6. října 2015, *Maximilian Schrems v Data Protection Commissioner*, C-362/14.

5 Rozsudek Soudního dvora ze dne 16. července 2020, *Data Protection Commissioner v Facebook Ireland Limited a Maximillian Schrems*, C-311/18.

6 HENSHALL, W. There's an AI Lobbying Frenzy in Washington. Big Tech Is Dominating. In: *Time* [online]. 30. 4. 2024 [cit. 2025-02-09]. Dostupné z: https://time.com/6972134/ai-lobbying-tech-policy-surge/.

AI, ve kterém jsou velké technologické společnosti IBM, Intel, Amazon, Apple a Meta. Tato iniciativa sdružuje technologické společnosti, akademické instituce, výzkumné organizace a neziskové skupiny, aby společně diskutovaly etické otázky, transparentnost a spravedlnost v oblasti AI. Iniciativa spojuje akademiky, vývojáře, vlády i nevládní organizace, publikuje výzkumné zprávy a doporučení pro vlády a firmy ohledně bezpečnosti a regulace AI a usiluje o to, aby byla AI vyvíjena a používána spravedlivě a transparentně.[7] Toto spojení Big Tech s jinými institucemi a činnost sdružení opět posiluje jejich postavení. Silná pozice Big Tech společností však s sebou přináší i výhody, protože tzv. *public-private partnership* dokáže právě díky rychlejším reakcím BigTech společností reagovat mnohem rychleji v nápravě porušení lidských práv. Zejména v případě osobních údajů se jedná o citlivou oblast, kde rychlejší náprava stavu je bezpochyby vítaným aspektem. Autor v jednom výzkumu zkoumal vytvoření Google formuláře pro žádost o využití práva být zapomenut pro jednotlivce v EU. Google jej vytvořil a zpřístupnil do 20 dnů. V případě čistě legislativního procesu se autor dostal k výsledku za rok.[8] A zde je třeba zdůraznit, že 20 dní vs. 1 rok je v tak citlivé oblasti, jako jsou osobní údaje, značně citelný a velký rozdíl. USA také navíc umožňují větší potenciál rozvoje a využití AI. To ve své podstatě nemusí být z pohledu ochrany osobních údajů negativní, jelikož, i když to na první pohled může vypadat paradoxně, i AI může pomoci k efektivní ochraně osobních údajů v oblasti AI, která vede k zajištění důvěrnosti, integrity a dostupnosti osobních dat a minimalizuje riziko jejich zneužití. Se zmiňovanými výhodami přístupu USA souvisí však i jeho nevýhody. A to nejen kvůli velkému či většímu vlivu Big Tech společností na legislativní proces ať již napřímo, nebo skrze lobbing, který je v USA rozšířen a má vzrůstající tendenci.[9] Zejména je zde obava před převládnutím snahy o zisk nad ochranou osobních údajů, přičemž výskyt tohoto jevu potvrdila zpráva Federální obchodní komise[10] a snaží se mu zamezit Evropský sbor pro ochranu osobních údajů.[11] Svou roli hraje také první dodatek ústavy,[12] díky kterému v proporčním testu převládá právo být informován nad ochranou osobních údajů, což je další komplikace pro jejich ochranu.

Naproti tomu v proporčním testu v EU právo na ochranu jednotlivce spíše převažuje nad právem veřejnosti na informace, protože omezení práva na ochranu osobních údajů mají být výjimkou, nikoli pravidlem.[13] Tento přístup se projevuje i ve vztahu k lobbingu BigTech společností, které v EU mají utlumenější a kooperativnější přístup[14] oproti agre-

7 *Partnership on AI* [cit. 2025-02-09]. Dostupné z: https://partnershiponai.org/.

8 MACH, M. the 'Right to Be Forgotten' – by Watchdogs and Open-Source Search Engines. In: ŠIŠKOVÁ, N. (ed.). *Legal Issues of Digitalisation, Robotization and Cyber Security in the Light of EU Law*. Alphen aan den Rijn: Wolters Kluwer, 2024, s. 60–69.

9 STRICKLAND, J. America's Crowded Statehouses: Measuring and Explaining Lobbying in the U.S. States. *State Politics & Policy Quarterly*. 2019, Vol. 19, No. 3 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1177/1532440019829408.

10 A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services. In: *Federal Trade Commission* [online]. 2024 [cit. 2025-02-21]. Dostupné z: https://www.ftc.gov/system/files/ftc_gov/pdf/Social-Media-6b-Report-9-11-2024.pdf.

11 Prohlášení 3/2024 o úloze orgánů pro ochranu osobních údajů v rámci aktu o umělé inteligenci. In: *European Data Protection Board* [online]. 16. 6. 2024 [cit. 2025-02-09]. Dostupné z: https://www.edpb.europa.eu/system/files/2024-07/edpb_statement_202403_dpasroleaiact_en.pdf.

12 První dodatek, Ústava Spojených států amerických.

13 Rozsudek Soudního dvora ze dne 21. prosince 2016, *Tele2 Sverige AB v Post – och telestyrelsen a Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffre Lewis*, spojené věci C-203/15 a C-698/15, body 89 a 104.

14 WOLL, C. The brash and the soft-spoken: Lobbying styles in a transatlantic comparison. *Interest Groups & Advocacy*. 2012, Vol. 1 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1057/iga.2012.10.

sivnímu lobbingu ve stylu „vítěz bere vše“, jako tomu je v USA.[15] Zároveň však přístup lobbingu v EU může být rizikový z důvodu neetického chování.[16] Silná regulace chrání práva uživatelů, ovšem negativně se projevuje v rozvoji AI, která je v EU těmito regulacemi omezována.[17] V USA tak lze vidět prostor pro rozvoj AI a nových technologií, ovšem ochrana uživatelů je zde lehce upozaděna. Naproti tomu v EU je ochrana uživatelů primární záležitostí, což se ale negativně podepisuje na rozvoji AI v Evropě a usazování technologických společností zde. Ochrana uživatele zde totiž má přednost i před maximálním využitím potenciálu společností a jejich ziskem. Z hlediska legislativního vývoje a směřování EU se jedná o kontinuální pokračování ochrany uživatele známého z GDPR,[18] která je rozšířena na AI, což vyústilo v navržení a přijetí například AI Act.[19] Proto se mezi akademiky, společnostmi i akciovými investory mluví o „zbytečně velké byrokratizaci EU“.[20] Autor zastává názor, že efektivní ochrana lidských práv vyžaduje srozumitelnou a systematickou legislativu, která umožňuje její konzistentní aplikaci a zároveň minimalizuje nadměrnou administrativní zátěž. Tento aspekt je v případě ochrany osobních údajů minimálně diskutabilní, a lze tedy chápat onu kritiku přílišné regulace a byrokratizace AI v EU. Autor nepopírá, že ochrana osobních dat je v EU na velmi vysoké úrovni, a je to názor napříč akademickou sférou.[21] Regulace ochrany osobních údajů není pouze GDPR, které je centrálním „kodexem“, ale je roztříštěna do velkého množství legislativních aktů.[22] A čím více

15 MESTEY-COLON, I. Following the Money-Trail: A Cross-Cultural Analysis of Lobbying Expenditures in the United States and European Union. In: *The Yale Review of International Studies* [online]. 26. 11. 2024 [cit. 2025-02-09]. Dostupné z: https://yris.yira.org/column/following-the-money-trail-a-cross-cultural-analysis-of-lobbying-expenditures-in-the-united-states-and-european-union/#14beeb86-162f-4c03-a549-8b9e39f420b7.

16 GOUJARD, C. Big Tech accused of shady lobbying in EU Parliament. In: *Politico* [online]. 14. 10. 2022 [cit. 2025-02-09]. Dostupné z: https://www.politico.eu/article/big-tech-companies-face-potential-eu-lobbying-ban/.

17 UFERT, F. AI Regulation Through the Lens of Fundamental Rights: How Well Does the GDPR Address the Challenges Posed by AI? *European Papers*. 2020, Vol. 5, No. 2, s. 1087–1097.

18 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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

19 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).

20 PRESUEL, C. R. – SIERRA, M. J. The Adoption of Artificial Intelligence in Bureaucratic Decision-making: A Weberian Perspective. *Digital Government Research and Practice*. 2023, Vol. 5, No. 1 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1145/3609861; BULLOCK, B. J. Artificial Intelligence, Discretion, and Bureaucracy. *The American Review of Public Administration*. 2019, Vol. 49, No. 7 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1177/0275074019856123.

21 BYGRAVE, L. A. Prospects for Global Consensus. In: BYGRAVE, L. A. *Data Privacy Law: An International Perspective*. Oxford: Oxford Academic, 2014, s. 205–210. Dostupné z: https://doi.org/10.1093/acprof:oso/9780199675555.003.0007.

22 Usnesení Evropského parlamentu ze dne 16. února 2017 obsahující doporučení Komisi o občanskoprávních pravidlech pro robotiku; Návrh nařízení Evropského parlamentu a Rady o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích); 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 (nařízení o digitálních službách); Směrnice Evropského parlamentu a Rady (EU) 2019/790 ze dne 17. dubna 2019 o autorském právu a právech s ním souvisejících na jednotném digitálním trhu a o změně směrnic 96/9/ES a 2001/29/ES 2019/790; Nařízení Evropského parlamentu a Rady (EU) 2023/2854 ze dne 13. prosince 2023 o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání a o změně nařízení (EU) 2017/2394 a směrnice (EU) 2020/1828 (nařízení o datech); Nařízení Evropského parlamentu a Rady (EU) 2022/868 ze dne 30. května 2022 o evropské správě dat a o změně nařízení (EU) 2018/1724 (akt o správě dat); Evropské prohlášení o digitálních právech a zásadách pro digitální dekádu; 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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

právních předpisů je, tím méně je právní regulace srozumitelná a systematická, tedy jedná se o negativní jev. Taktéž je výraznou nevýhodou, že je legislativní proces ve srovnání s technologickým pokrokem pomalý a nedokáže na něj reagovat.[23]

Je tedy otázkou, kde se celosvětově nastaví konsenzus mezi ochranou lidských práv a podporou rozvoje AI. EU podnikla významný krok směrem k celosvětové unifikaci regulace AI přijetím Rámcové úmluvy o umělé inteligenci a lidských právech, demokracii a právním státě, navržené Radou Evropy a podepsanou 5. září tehdejší místopředsedkyní Evropské komise pro hodnoty a transparentnost Věrou Jourovou.[24] I když by celosvětový konsenzus k regulaci AI byl pozitivním krokem,[25] USA i Čína zaujaly spíše rezervovaný postoj, protože USA preferují flexibilnější, méně restriktivní přístup a obávají se negativního dopadu na inovace[26] a Čína sleduje především své vlastní strategické cíle v oblasti AI a klade důraz na státní kontrolu.[27] Dle mínění autora tak nejhlasitější jména jako EU, USA, či Čína budou muset paradoxně pro dosažení shody v oblasti AI počkat na ty nejpomalejší, včetně afrických států. Teprve až bude mít každý kontinent stanovenou svou strategii pro regulaci AI, bude možné najít průniky napříč kontinenty a teprve na nich pak vystavět souhrn s minimálními požadavky na regulaci AI. Teprve poté lze najít jednoznačnou odpověď na otázku, kde přesně udělat pomyslný bod mezi „přílišnou regulací kvůli ochraně lidských práv" a „žádnou regulací pro maximální rozvoj AI".

2. Ochrana uživatelů u AI

Zmíněná regulace AI ze strany Evropské unie je v akademickém prostředí vnímána rozporuplně. Musch, Borrelli a Kerrigan analyzují AI Act jako významný milník v oblasti globální regulace AI a zdůrazňují jeho potenciál formovat mezinárodní standardy a podporovat harmonizaci.[28] Wilczek, Thäsler-Kordonouri a Eder naopak výzkumem kulturních faktorů ovlivňujících vnímání rizik spojených s AI preferují méně restriktivní přístup.[29] Zejména je kritizována z důvodů týkajících se nadměrné regulace, což z hlediska nestát-

23 MANDEL, G. N. Legal Evolution in Response to Technological Change. In: BROWNSWORD, R. – SCOTFOR, E. – YEUNG, K. *The Oxford Handbook of Law, Regulation and Technology*. Oxford: Oxford Academic, 2017, s. 225–245. Dostupné z: https://doi.org/10.1093/oxfordhb/9780199680832.013.45.

24 The European Commission signs historic Council of Europe Framework Convention on Artificial Intelligence and Human Rights. In: *European Union External Action* [online]. 10. 9. 2024 [cit. 2025-02-09]. Dostupné z: https://www.eeas.europa.eu/delegations/council-europe/european-commission-signs-historic-council-europe-framework-convention-artificial-intelligence-and_en?s=51.

25 WALTER, Y. Managing the race to the moon: Global policy and governance in Artificial Intelligence regulation—A contemporary overview and an analysis of socioeconomic consequences. *Discover Artificial Intelligence*. 2024, Vol. 4, No. 1 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1007/s44163-024-00109-4.

26 DUDLEY, E. S. Lessons from the Past for Regulating AI. In: *Regulatory Studies Center* [online]. 12. 11. 2024 [cit. 2025-02-09]. Dostupné z: https://regulatorystudies.columbian.gwu.edu/sites/g/files/zaxdzs4751/files/2024-11/Dudley_Lessons_for_Regulating_AI_11-2024_Working_Paper.pdf.

27 ROBERTS, H. – COWLS, J. – MORLEY, J. et al. The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI & Society*. 2021, Vol. 36, No. 1 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1007/s00146-020-00992-2.

28 MUSCH, S. – BORRELLI, M. – KERRIGAN, Ch. The EU AI Act: A Comprehensive Regulatory Framework for Ethical AI Development. In: *Ssrn* [online]. 23. 8. 2024 [cit. 2025-02-09]. Dostupné z: https://ssrn.com/abstract=4549248.

29 WILCZEK, B. – THÄSLER-KORDONOURI, S. – EDER, M. Government regulation or industry self-regulation of AI? Investigating the relationships between uncertainty avoidance, people's AI risk perceptions, and their regulatory preferences in Europe. *AI & Society*. 2024 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1007/s00146-024-02138-0.

ních aktérů zmiňují Tallberg, Lundgren a Geith, obavy z nadměrné regulace mezi obchodními aktéry;[30] složitosti implementace[31] a hodnocení rizik.[32] Na druhou stranu je ovšem vhodné zdůraznit, že v dnešních dnech používaná AI není jen textová platforma založená na pravděpodobnosti posloupnosti slov. Od roku 2023 překonává AI lidskou výkonnost v některých měřítkách, včetně klasifikace obrázků, vizuálního uvažování a porozumění angličtině.[33] AI se také používá i při rozhodování v bance u žádostí o úvěr,[34] ve zdravotnictví,[35] pro předpovědi recidivy u obžalovaných[36] a další. Tato data mohou zahrnovat citlivé osobní údaje, jako jsou zdravotní záznamy (rozpoznání obrazu i v lékařství, při rozeznání rakoviny, Alzheimera a další), finanční data nebo geolokační údaje. AI umí také poznat jednotlivce díky charakteristickým rysům, jako například obličej,[37] řeč[38] nebo styl chůze.[39] Také čerpá z internetových novin, což se aktuálně nelíbí například vydavatelství New York Times.[40] Že i v nich se vyskytují citlivé osobní informace, je známo například z rozsudku ve věci *Google Spain*.[41] Bez řádných bezpečnostních opatření mohou být tato data vystavena riziku úniku nebo zneužití. Nabízí se však otázka, jak zareagovat a efektivně chránit osobní údaje v době AI.

Bezesporu je třeba, aby se sami uživatelé snažili aktivně chránit své osobní údaje při užívání AI a aby věděli, kým a jak jsou zpracovávány, respektive zda jsou poskytovány i třetím stranám. Možností, jak toho docílit, je více, většinou se neliší od obecných doporučení o bezpečnosti na internetu. Jedná se zejména o znalost zásad ochrany osobních údajů, omezení sdílení údajů, používání silných hesel a dvoufaktorové ověřování, používání důvěryhodných aplikací a jejich aktualizaci a preventivní opatrnost při práci s AI chatboty

30 TALLBERG, J. – LUNDGREN, M. – GEITH, J. AI regulation in the European Union: examining non-state actor preferences. *Business and Politics*. 2024, Vol. 26, No. 2 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1017/bap.2023.36.

31 ENGLER, A. The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment. In: *Brookings Institution* [online]. 25. 4. 2023 [cit. 2025-02-09]. Dostupné z: https://www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/.

32 NOVELLI, C. – CASOLARI, F. – ROTOLO, A. et al. AI Risk Assessment: A Scenario-Based, Proportional Methodology for the AI Act. *Digital Society*. 2024, Vol. 3, No. 1 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1007/s44206-024-00095-1.

33 *Artificial Intelligence Index Report 2024*. In: *Stanford University: Human-Centered Artificial Intelligence* [cit. 2025-02-09]. Dostupné z: https://aiindex.stanford.edu/report/.

34 FARES, O. H. – BUTT, I. – LEE, S. H. M. Utilization of artificial intelligence in the banking sector: a systematic literature review. *Journal of Financial Services Marketing*. 2022, Vol. 28, No. 4 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1057/s41264-022-00176-7.

35 KITSIOS, F. – KAMARIOTOU, M. – SYNGELAKIS, A. I. – TALIAS, M. A. Recent Advances of Artificial Intelligence in Healthcare: A Systematic Literature Review. *Applied Sciences*. Vol. 13, No. 13 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.3390/app13137479.

36 FARAYOLA, M. M. – TAL, I. – CONNOLLY, R. – SABER, T. – BENDECHACHE, M. Ethics and Trustworthiness of AI for Predicting the Risk of Recidivism: A Systematic Literature Review. *Information*. 2023, Vol. 14, No. 8 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.3390/info14080426.

37 WANG, X. – WU, Y. C. – ZHOU, M. – FU, H. Beyond surveillance: privacy, ethics, and regulations in face recognition technology. *Frontier in Big Data*. 2024, Vol. 7 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.3389/fdata.2024.1337465.

38 LI, Y. – HASHIM, A. S. – LIN, Y. – NOHUDDIN, P. N. E. – VENKATACHALAM, K. – AHMADIAN, A. AI-based visual speech recognition towards realistic avatars and lip-reading applications in the metaverse. *Applied Soft Computing*. 2024, Vol. 164 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1016/j.asoc.2024.111906.

39 SEPAS-MOGHADDAM, A. – ETEMAD, A. Deep Gait Recognition: A Survey. In: *ArXiv* [online]. 13. 2. 2022 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.48550/arXiv.2102.09546.

40 GRYNBAUM, M. M. – MAC, R. The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work In: *Nytimes* [online]. 27. 12. 2023 [cit. 2025-02-09]. Dostupné z: https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html.

41 Rozsudek Soudního dvora ze dne 13. května 2014, *Google Spain SL a Google Inc. v. Agencia Española de Protección de Datos (AEPD) a Mario Costeja González*, C-131/12.

a asistenty. I přes tato opatření není žádná metoda ochrany dat 100% bezpečná a stále je z velké části zodpovědností samotného uživatele, zda je opatrný při sdílení osobních údajů online. Jako příklad lze uvést již zmíněný případ *Google vs. Spain*. Osobní údaje pana Costeji z tohoto případu nejsou známé kvůli nedostatečné legislativě nebo soudnímu rozhodnutí, ale kvůli jeho vlastnímu jednání, kdy dával rozhovory o svém případu do médií.[42] Ale zmiňovaná silná pozice Big Tech společností zprostředkujících AI skrze jejich AI systémy je důvodem, proč i přes veškerou snahu o co největší ochranu osobních údajů není samotná ochrana soukromí ze strany uživatele dostačující. Dal by se zde použít příměr k Davidu s Goliášem, ovšem s tím rozdílem, že tentokrát by měl Goliáš (Big Tech) nad Davidem (uživatelem) obrovskou převahu. Regulace ze stran států, respektive EU jako celku v případě naší geopolitické oblasti, se tedy zdá potřebná.

Při stanovení, jak obsáhlá či podrobná by měla právní regulace být, je vhodné si nejprve určit, jaká jsou rizika v oblasti ochrany osobních údajů u AI v kontextu zpracovávaných údajů. To bývá mnohdy vypsáno v podmínkách, se kterými musí uživatel souhlasit, ovšem výzkum společnosti Deloitte ukázal, že tyto podmínky nečte přes 91 % uživatelů, přičemž v kategorii 18–34 let dokonce 97 % uživatelů.[43] Tim Sandle z Digital Journal poukázal na průzkum webové společnosti ProPrivacy.com, kde si podmínky nepřečetlo, a přesto souhlasilo závratných 99 % uživatelů.[44] Ti odsouhlasili obchodní podmínky, aniž by je četli.[45] Pro drtivou většinu uživatelů, kteří obchodní podmínky nečtou, tedy může dojít k negativnímu překvapení.

2.1 Konkrétní rizika ochrany osobních údajů u AI

Obavy o ochranu soukromí a osobních dat navíc zesiluje pozoruhodná schopnost AI analyzovat údaje a provádět komplexní analýzy. Například potenciál této technologie odvodit citlivé osobní údaje, jako je poloha osoby, preference a zvyky, představuje riziko neoprávněného šíření dat. Ve spojení s potenciálem krádeže identity a neoprávněného sledování představuje umělá inteligence jedinečnou sadu výzev, které vyžadují okamžitá proaktivní řešení.

Zmiňované proaktivní řešení by se však nemělo zaměřovat na oblast zákazu AI či snahu o omezení rozvoje. Užívání AI v kombinaci s osobními daty uživatele má bezesporu mnoho výhod a například již zmiňované užití ve zdravotnictví (rozpoznání obrazu v lékařství, při rozeznání rakoviny, Alzheimera) může doslova zachraňovat životy, či v oblasti lidských práv zajistit důstojnost jednotlivce. Jak tedy co nejvíce využívat výhod plynou-

---

42 KASSAM, A. Spain's everyday internet warrior who cut free from Google's tentacles. In: *The Guardian* [online]. 13. 5. 2014 [cit. 2025-02-09]. Dostupné z: https://www.theguardian.com/technology/2014/may/13/spain-everyman-google-mario-costeja-gonzalez.

43 CAKEBREAD, C. You're not alone, no one reads terms of service agreements. In: *Bussinessinsider* [online]. 15. 11. 2017 [cit. 2025-02-09]. Dostupné z: https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11?r=US&IR=T.

44 SANDLE, T. Report finds only 1 percent reads 'Terms & Conditions'. In: *Digitaljournal* [online]. 29. 1. 2020 [cit. 2025-02-09]. Dostupné z: https://www.digitaljournal.com/business/report-finds-only-1-percent-reads-terms-conditions/article/566127.

45 Mezi podmínky, se kterými respondenti souhlasili, patřily: *„Právo na pojmenování jejich prvorozeného dítěte. Přístup do vzdušného prostoru nad svým majetkem pro účely provozu dronů. Povolení poskytnout své matce plný přístup k historii prohlížení. Schopnost „pozvat" osobního agenta FBI na vánoční večeři na dalších 10 let. Možnost využít jejich streamovací platformy a zaplnit návrhy hroznými stand-up speciály."* Ibidem.

cích z AI, ale zároveň omezit její nevýhody? Mezi ty největší výzvy v AI z pohledu ochrany osobních údajů bezesporu patří níže rozepsaná témata, která některé výzkumy zmiňují,[46] ale při hlubším zkoumání stále neexistuje řešení vedoucí k neexistenci těchto negativních jevů,[47] i když dílčí pokroky v podobě teoretických řešení některých z nich jsou představeny.[48] Tento článek se však zaměří na hlubší identifikaci.

Opětovná identifikace a deanonymizace – Umělou inteligenci lze použít k identifikaci a sledování jednotlivců na různých zařízeních v jejich domovech, v práci a na veřejných prostranstvích. Tato hrozba není pouze teoretická, ale i praktická, kdy například v červnu 2021 vyšlo najevo, jak bylo jednoduché hacknout rotopedy a běžecké trenažéry od fitness společnosti Peloton a díky připojení těchto zařízení k internetu, zabudovaným kamerám a mikrofonům sledovat a sbírat citlivá data více než čtyř miliónů uživatelů.[49] Konkrétně rozpoznávání obličeje – prostředek, kterým lze sledovat a identifikovat jednotlivce – má navíc potenciál změnit očekávání anonymity ve veřejném prostoru.[50] Používání kamerových systémů s rozpoznáváním obličeje navíc označil Evropský soud pro lidská práva za zásah do soukromí a rodinného života jednotlivce.[51]

Diskriminace, nespravedlnost, nepřesnosti a předpojatost – Identifikace, profilování a automatizované rozhodování řízené umělou inteligencí mohou vést k diskriminačním nebo neobjektivním výsledkům. Lidé mohou být nesprávně klasifikováni, nesprávně identifikováni nebo negativně posuzováni a takové chyby nebo předsudky mohou neúměrně ovlivnit určité demografické skupiny. Již při tvorbě algoritmů je snaha o neprojevení takového chování, přesto vznikají automatizační předpojatosti a selektivní dodržování algoritmických doporučení.[52] Lorenzo Berenguer tato rozhodování analyzoval a navrhl některá možná řešení,[53] ovšem Ulrik Franke upozorňuje na dvě úrovně předpojatosti projevující se diskriminací. Zatímco první úroveň je vysvětlitelná, a tedy lze na ni aplikovat návrhy na zlepšení, ve druhé úrovni jsou tyto jevy hůře vysvětlitelné a potřebují hlubší analýzu pro nalezení možných řešení.[54] Popsaná rizika bylo v praxi možné nalézt v USA na příkladu užívání softwaru COMPAS při rozhodování, kdo pravděpodobně znovu spáchá trestný

---

46 UDDAGIRI, C. – ISUNURI, B. V. Ethical and Privacy Challenges of Generative AI. In: RAZA, K. – AHMAD, N. – SINGH, D. (eds). *Generative AI: Current Trends and Applications. Studies in Computational Intelligence*. Singapore: Springer, 2024, s. 219–244. Dostupné z: https://doi.org/10.1007/978-981-97-8460-8_11.

47 TIMAN, T. – MANN, Z. Data Protection in the Era of Artificial Intelligence: Trends, Existing Solutions and Recommendations for Privacy-Preserving Technologies. In: CURRY, E. – METZGER, A. – ZILLNER, S. – PAZZAGLIA, J. C. – GARCÍA ROBLES, A. (eds). *The Elements of Big Data Value*. Cham: Springer, 2021, s. 153–175. Dostupné z: https://doi.org/10.1007/978-3-030-68176-0_7.

48 PATSAKIS, C. – LYKOUSAS, N. Man vs the machine: The Struggle for Effective Text Anonymisation in the Age of Large Language Models. In: *ArXiv* [online]. 22. 3. 2023 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.48550/arXiv.2303.12429.

49 Technickou stránku a další případy zmiňuje např. BALL, J. C. *Hacking APIs: Breaking Web Application Programming Interfaces*. San Francisco: No Starch Press, 2022.

50 BOWYER, K. W. Face recognition technology: security versus privacy. *IEEE Technology and Society Magazine*. 2009, Vol. 23, No. 1 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1109/MTAS.2004.1273467.

51 Rozsudek Evropského soudu pro lidská práva ze dne 4. července 2023, *Glukhin v Russia*, stížnost č. 11519/20, bod 90 a 91.

52 ALON-BARKAT, S. – BUSUIOC, M. Human–AI Interactions in Public Sector Decision Making: "Automation Bias" and "Selective Adherence" to Algorithmic Advice. *Journal of Public Administration Research and Theory*. 2023, Vol. 33, No. 1 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1093/jopart/muac007.

53 BELENGUER, L. AI bias: exploring discriminatory algorithmic decision-making models and the application of possible machine-centric solutions adapted from the pharmaceutical industry. *AI and Ethics*. 2022, Vol. 2, No. 4 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1007/s43681-022-00138-8.

54 FRANKE, U. First – and Second-Level Bias in Automated Decision-making. *Philosophy & Technology*. 2022, Vol. 35, No. 2 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1007/s13347-022-00500-y.

čin.[55] V současnosti nejznámější případ využití COMPASu je případ Paula Zilliho,[56] který se s žalobcem dohodl na dohodě o vině a trestu, která zahrnovala jeden rok ve vězení a následný dohled. Soudce se však po Zilliho hodnocení rizika COMPASem rozhodl dohodu zrušit a uložil mu dvouletý trest ve státní věznici a tříletý dohled, protože jej COMPAS vyhodnotil jako vysoce rizikového.[57] Tato situace vedla k otázkám, zda je toto používání technologií správné a dává smysl.[58] Tedy nejedná se o rovinu teoretickou, ale o negativa AI přímo ovlivňující lidské životy.

Netransparentnost a utajení profilování – Některé aplikace umělé inteligence mohou být pro jednotlivce, regulační orgány nebo dokonce samotné návrháře systému nejasné, což ztěžuje zpochybňování nebo zkoumání výsledků. I když existují technická řešení, která pomáhají zlepšit interpretovatelnost a/nebo schopnost auditu některých systémů, stále se jedná o velmi citlivou oblast a výzvu do budoucna ke zlepšení, protože výsledek založený na rozhodnutí AI může významně ovlivnit životy lidí. Autoři Kerikmae a Hamulák v roce 2020 tvrdili, že rozhodování člověka a AI je podobné.[59] S tímto tvrzením se však autor článku plně neztotožňuje. V říjnu 2016 AI AlphaGo porazila ve hře GO Lee Sedola, v té době nejlepšího hráče na světě, v poměru 4:1, a to proto, že porušila jednu ze základních strategických představ. Jinými slovy přišla s řešením, které by člověk neudělal.[60] A přitom právě v tak citlivé oblasti, jako je ochrana osobních údajů, je transparentnost a pochopení rozhodování AI klíčovou vlastností. Jedním z teoretických řešení je existence tzv. „černých skříněk“,[61] které by v praxi zaznamenávaly proces rozhodování AI a poskytovaly tak zdůvodnění rozhodnutí, jak navrhují některé studie.[62] Banky by mohly vysvětlit, proč odmítají žadateli poskytnout půjčku/hypotéku, HR oddělení, proč nepřijmou žadatele o práci, a soudci by mohli vysvětlit, proč AI předpovídá v konkrétním případě vyšší míru recidivy u obviněného. Tyto černé skříňky však aktuálně není možné technicky vytvořit, protože AI systémy, které tyto modely pohánějí, jsou tak složité, že ani samotní tvůrci přesně nerozumí tomu, co se v nich děje,[63] a proto zcela nedokážeme pochopit, jak se AI dostala k závěrečnému výsledku. Tento fakt je v rozporu například s Deklarací o etice a ochraně osobních údajů v oblasti AI z Mezinárodní konference komisařů pro ochranu

---

55 V roce 2016 byla Julia Angwin spoluautorkou výzkumu algoritmu ProPublica. Tým zjistil, že *„u černochů je téměř dvakrát vyšší pravděpodobnost než u bělochů, že budou označeni za rizikovější, ale ve skutečnosti se nedopustí recidivy“*, zatímco COMPAS *„dělá opačnou chybu mezi bělochy: Je mnohem pravděpodobnější než u černochů, že budou označeni za méně rizikové, ale páchají další trestné činy“*.

56 FRY, H. Can an algorithm deliver justice? In: *Science Focus* [online]. 21. 9. 2018 [cit. 2025-02-09]. Dostupné z: https://www.sciencefocus.com/future-technology/can-an-algorithm-deliver-justice/.

57 HENNINGTON, M. Show Me the Numbers: Due Process and Equal Protection Challenges to the Use of Risk Assessment Algorithms in the Pretrial Context. In: *Ssrn* [online]. 9. 8. 2024 [cit. 2025-02-09]. Dostupné z: http://dx.doi.org/10.2139/ssrn.4921416.

58 CASTRO, C. – RUBEL, A. – SCHWARTZ, L. Does predictive sentencing make sense? *Inquiry: An Interdisciplinary Journal of Philosophy*. 2024 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1080/0020174X.2024.2309876.

59 KERIKMÄE, T. – MÜÜRSEPP, P. – PIHL, M. H. – HAMULAK, O. – KOCHARYAN, H. Legal Person – or Agenthood of Artificial Intelligence Technologies. *Acta Baltica Historiae et Philosophiae Scientiarum*. 2020, Vol. 8, No. 2, s. 73–92.

60 SILVER, D. – HUANG, A. – MADDISON, C. et al. Mastering the game of Go with deep neural networks and tree search. *Nature*. 2016, Vol. 529, No. 7587 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1038/nature16961.

61 V českých textech bývá používáno i anglické *black box*.

62 HASSIJA, V. – CHAMOLA, V. – MAHAPATRA, A. et al. Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence. *Cognitive Computation*. 2024, Vol. 16, No. 1 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1007/s12559-023-10179-8.

63 KOSINKSI, M. What is black box AI? In: *IBM* [online]. 29. 9. 2024 [cit. 2025-02-09]. Dostupné z: https://www.ibm.com/think/topics/black-box-ai.

osobních údajů a soukromí z roku 2018, která se zaměřila na důvěryhodnost AI, kterou lze zvýšit i vysvětlitelností a transparentností procesních postupů AI.[64] Rawashdeh tak v současnosti vidí řešení ve zvýšení důvěryhodnosti AI právě ve vytvoření těchto černých skříněk. Kvůli jejich neexistenci podle něj EU „dupla na brzdu“,[65] což se negativně projevuje v již zmíněné podpoře rozvoje AI v EU.

„Hloupost AI“ – I když to na první pohled nemusí být zřejmé, AI vlastně skutečně nepřemýšlí, jen se učí na konkrétních případech.[66] Deep Blue (IBM) již v roce 1997 porazil v šachách šachového mistra Kasparova, protože na toto byl vytvořen, ale neporazil by průměrné čtyřleté dítě v piškvorkách, jelikož se neučil na žádných příkladech.[67] AI má také v rámci interního nastavení některé věci zakázány, například diskriminaci, navádění k násilí a další. Ovšem uživatelé zjistili, že i toto se dá relativně jednoduše obejít přes tzv. *roleplay*. Tedy uživatel řekl AI, že si má představit, že AI aktuálně nemusí dodržovat žádná pravidla, a teprve potom položil dotaz. AI v takových případech poskytovala návody na sebevraždu, diskriminační a rasistické odpovědi a další.[68] Na druhou stranu ale není možné AI ani podceňovat. Ve výzkumu byl zaznamenán případ, kdy si AI najalo člověka k přečtení Captchy[69] a šlo na to dosti sofistikovaným způsobem.[70]

Predikce – Umělá inteligence může využívat sofistikované algoritmy strojového učení k odvození nebo předpovídání citlivých informací z necitlivých forem dat, jako jsou metadata, lokalizační údaje, vzorce chování na internetu, anonymizované obrázky či textové analýzy. Tyto zdánlivě neškodné informace mohou být zkombinovány a analyzovány tak, aby odhalily osobní údaje, například identitu jednotlivce, jeho zdravotní stav, finanční situaci nebo politické preference, což představuje zásadní riziko pro ochranu soukromí. Například něčí vzorce psaní na klávesnici lze analyzovat a odvodit z nich emoční stav daného jedince, který zahrnuje emoce, jako je nervozita, smutek nebo úzkost. Ještě více alarmující je, že politické názory, etnickou identitu, sexuální orientaci a dokonce i celkový zdravotní stav lze určit také na základě protokolů o aktivitách, údajích o poloze a podobných metrik. A poté s uživateli na základě těchto informací manipulovat, jak ukázal případ *Cambridge Analytica*.[71] Ale ani v tomto nelze tvrdit, že se jedná jen o negativní schopnost, díky predikci AI je jednodušší například vývoj léků, kdy AI dokáže nasimulovat jednotlivé sloučeniny a jejich vliv na potenciálního pacienta.[72]

---

64 JANSEN FERREIRA, J. – MONTEIRO, M. The human-AI relationship in decision-making: AI explanation to support people on justifying their decisions. In: *Arxiv* [online]. 22. 2. 2021 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.48550/arXiv.2102.05460.

65 BLOUIN, L. AI's mysterious 'black box' problem, explained. In: *University of Michigan-Dearborn* [online]. 6. 3. 2023 [cit. 2025-02-09]. Dostupné z: https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained.

66 WONG, M. The GPT Era Is Already Ending. In: *The Atlantic* [online]. 6. 12. 2024 [cit. 2025-02-09]. Dostupné z: https://www.theatlantic.com/technology/archive/2024/12/openai-o1-reasoning-models/680906/.

67 TEGMARK, M. *Život 3.0: Člověk v éře umělé inteligence*. Praha: Argo; Dokořán, 2020, s. 51.

68 Aktuálně by již *roleplay* v AI neměla být v praxi možná.

69 Captcha by měla umět rozlišit mezi botem a reálným uživatelem.

70 GPT-4 Technical Report. In: *OpenAI* [online]. 2023, s 55 [cit. 2025-02-09]. Dostupné z: https://cdn.openai.com/papers/gpt-4.pdf.

71 The use of Facebook users' data by Cambridge Analytica and the impact on data protection. Usnesení Evropského parlamentu ze dne 25. října 2018. In: *European Parliament* [online]. 2018 [cit. 2025-02-09]. Dostupné z: https://www.europarl.europa.eu/doceo/document/TA-8-2018-0433_EN.htm.

72 ARNOLD, C. Inside the nascent industry of AI-designed drugs. *Nature Medicine*. 2023, Vol. 29, No. 6 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1038/s41591-023-02361-0.

2.2 AI Act

Z důvodu výše zmíněných rizik a schopností AI, které se budou nadále zlepšovat, se stává stále důležitějším prvkem AI její bezpečnost pro uživatele. Tou se zabývá i Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanovila harmonizovaná pravidla pro umělou inteligenci, tzv. *AI Act*,[73] který byl již zmíněn v předchozí části příspěvku. Hlavní myšlenkou je pak rozdělení AI do čtyř kategorií dle úrovně rizika: *nepřijatelné, vysoké, omezené* a *minimální*. Většina AI systémů používaných v Evropě spadá do kategorie s minimálním rizikem, kdy stačí dodržovat aktuální právní předpisy bez nutnosti dalších právních povinností.[74] Systémy AI, jež mají přímou interakci s uživatelem či uměle vytvářejí obsah, již musí splňovat navíc standardy transparentnosti, aby uživatel věděl, že interaguje s umělou inteligencí. Jedná se o kategorii s omezeným rizikem. Systémy AI, které budou používány v oblastech, které jsou definovány jako klíčové pro fungování společnosti,[75] budou nejen před uvedením, ale po celou dobu používání podléhat přísným požadavkům a kontrole a spadají do kategorie s vysokým rizikem. Tyto tři kategorie AI systémů bude možné využívat a provozovat v EU, liší se pouze mírou kontroly dle možné úrovně rizik. K těmto třem pak existuje kategorie čtvrtá, do které spadají AI systémy využívající zakázané praktiky systémů AI. Využívání těchto systémů je bráno za nepřijatelné, a tedy je jejich používání zcela zakázáno.[76] Bezpečnost AI se však nedá shrnout pouze na rozdělení AI do kategorií dle předpokládaných rizik, navíc i toto samotné dělení je kritizováno z důvodu tvorby kategorií, které jsou vytvořeny s ohledem na oblasti použití. To se může projevit podceněním rizika systémů AI, což jde proti samotné myšlence, proč byly tyto kategorie vytvořeny.[77] Dle autora by bylo rozumnější určení do kategorií dle systému posuzování navrženého kolektivem autorů z Boloňské univerzity a Oxfordu, který bere v úvahu interakci mezi determinanty rizika, jednotlivými faktory determinantů a vícero-rizikovými typy.[78] Tento přístup se totiž zaměřuje na konkrétní scénáře jejich nasazení a interakci s uživateli místo toho, aby byly systémy AI kategorizovány na základě jejich oblasti použití. Hodnocení rizik je tak více flexibilní, což umožňuje přesnější identifikaci potenciálních hrozeb a zohledňuje nepředvídané dopady a kontextuální faktory, které mohou riziko zvyšovat. Místo statických kategorií je hodnocení průběžné a adaptivní, díky čemuž mohou regulátoři rychleji reagovat a zabránit tak podcenění rizik u některých systémů AI, které by jinak byly považovány za „nízkorizikové" pouze kvůli své kategorii. Vzhledem k rychlosti technologického pokroku je výhodou schopnost tohoto systému přizpůsobovat se novým objevům a vývoji v oblasti AI, což je

73 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).

74 Artificial Intelligence – Questions and Answers. In: *European Comission* [online]. 1. 8. 2024 [cit. 2025-02-09]. Dostupné z: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/qanda_21_1683/QANDA_21_1683_EN.pdf.

75 Zejména se jedná o biometrickou identifikaci.

76 Například v Číně rozšířený *social scoring*, tedy udělování sociálního kreditu dle chování jednotlivce a následné odměny či tresty dle výše kreditu. S tím souvisí například i podprahová manipulace chování a emocí.

77 NOVELLI, C. – CASOLARI, F. – ROTOLO, A. – TADDEO, M. – FLORIDI, L. Taking AI risks seriously: a new assessment model for the AI Act. In: *Springer* [online]. 12. 7. 2023 [cit. 2025-02-09]. Dostupné z: https://link.springer.com/article/10.1007/s00146-023-01723-z#citeas.

78 Ibidem.

zásadní. Technickým provedením AI Actu se také zabýval kolektiv autorů z Itálie, Belgie a Španělska.[79] Z jejich analýzy vyplývá, že AI Act se zaměřuje na politické cíle, ale neřeší konkrétní technické postupy k dosažení těchto cílů. Například chybí postoj k tzv. *černým skříňkám* AI systémů, což je mezi akademiky[80] diskutované téma zejména v souvislosti s transparentností. Přitom snaha o transparentnost a vysvětlitelnost AI je základním regulatorním cílem AI Actu. Existuje tedy představa cíle, avšak AI Act se blíže nezabývá konkrétními technickými způsoby, jak těchto cílů dosáhnout.

Závěr

V současnosti žijeme v době, kdy dochází k prudkému nárustu rozvoje AI a aplikace AI systémů do každodenních situací. Mnoho technologických společností v tomto cítí příležitost a snaží se o rozvoj nebo o aplikaci AI a AI systémů s vidinou monetizace a rychlého a velkého růstu zisků. Ani největším BigTech společnostem se však nedaří monetizovat AI dle jejich očekávání,[81] a tak se v souvislosti s AI mluví o možné bublině, podobné *dot-com* bublině z let 1996 až 2001.[82] To přináší tlak na společnosti, které mohou vidět potenciál v nových způsobech využití AI, zejména ve zdravotnictví, bankovnictví a dalších oblastech pracujících s osobními údaji, jak ukazují současné trendy v AI. A to může představovat potenciální hrozbu v ochraně práv uživatelů. Aby k tomuto nedošlo, je potřeba také legislativního rámce. Ten může mít širší vymezení, jako je u zmiňovaného příkladu USA, což s sebou přináší ekonomické výhody, avšak může se projevit slabší ochranou uživatelů. Nebo, jako tomu je v případě EU, může být legislativní rámec více konkrétní, navazující na aktuální právní předpisy, např. GDPR ve smyslu principu předvídatelnosti práva a lépe chránící uživatele, ovšem nebude zde výrazný ekonomický přínos pro EU. Právě rozdílný přístup k regulaci AI způsobil, že aktuálně každý z globálních hráčů má svůj specifický přístup a nehrozí zde aplikace tzv. Bruselského či Washingtonského efektu ve svém významu, tedy že by provozovatelé AI aplikovaly pravidla EU či USA celosvětově. Dílčí účinek totiž může v širším kontextu snížit globální dosah politiky EU, protože by přísné regulační normy aktu o umělé inteligenci vedly k slabším normám v oblasti ochrany základních práv a tento stav nebude ničím víc než jen Pyrrhovým vítězstvím evropských ambicí šířit hodnoty prostřednictvím regulace umělé inteligence.[83] Z tohoto pohledu je pozitivním krokem Stanovisko 28/2024 Evropského výboru pro ochranu údajů které zdůrazňuje, že dozorové úřady mají posuzovat každý případ individuálně s ohledem na jeho

79 PANIGUTTI, C. – HAMON, R. – HUPONT, I. – LLORCA, F. D. et al. The role of explainable AI in the context of the AI Act. FAccT '23: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency. In: *Association for Computing Machinery* [online]. 2023 [cit. 2025-02-09]. Dostupné z: https://dl.acm.org/doi/abs/10.1145/3593013.3594069.

80 PAVLIDIS, G. Unlocking the black box: analysing the EU artificial intelligence act's framework for explainability in AI. *Law, Innovation and Technology*. 2024, Vol. 16, No. 1 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1080/17579961.2024.2313795; viz též GYEVNAR, B. – FERGUSON, N. – SCHAFER, B. Get Your Act Together: A Comparative View on Transparency in the AI Act and Technology. In: *Arxiv* [online]. 29. 7. 2023 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.48550/arXiv.2302.10766.

81 Snad vyjma společnosti Nvidia, vyrábějící grafické čipy pro AI systémy.

82 KERNER, M. S. Explaining an AI bubble burst and what it could mean. In: *Techtarget* [online]. 20. 8. 2024 [cit. 2025-02-09]. Dostupné z: https://www.techtarget.com/whatis/feature/Explaining-an-AI-bubble-burst-and-what-it-could-mean.

83 ALMADA, M. – RADU, A. The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy. *German Law Journal*. 2024, Vol. 25, No. 4 [cit. 2025-02-09]. Dostupné z: https://doi.org/doi:10.1017/glj.2023.108.

specifické okolnosti a technologický vývoj.[84] U těchto rozhodování by se nemusela projevit negativa spojená s přísnými regulačními normami zmíněná výše.

I když výše zmíněné přístupy k legislativní regulaci jsou odlišné, důvody vzniku jsou totožné. Nové technologie, a konkrétně AI, která je označována dle Evropského parlamentu jako technologie budoucnosti,[85] s sebou přináší řadu příležitostí, ale i rizik. I když je vývoj technologií velice rychlý a těžko se dopředu stanovuje, kde všude a do jaké míry nakonec nalezne AI své využití, lze již nyní identifikovat některá z rizik a předvídat je i v blízké budoucnosti. Jisté však je, že AI bude aplikována, a je proto potřeba se jí, respektive riziky, více zabývat. Řada rizik se přímo dotýká uživatelů, kteří sami nedokážou efektivně chránit své soukromí a osobní údaje.[86] Proto je logické, že se EU snaží dát AI systémům legislativní rámec, aby ochránila uživatele a minimalizovala možná rizika. Není ani překvapivé jakým způsobem se toho snaží dosáhnout, tedy skrze transparentnost, dohled a ochranu, protože tento směr je zřetelný již v nařízení GDPR.[87] Přesto je přístup Evropské unie k regulaci AI kritizován, jak ukazují některé z výzkumů citovaných v článku. A zde se jedná o kritiku příliš aktivního i nepříliš aktivního přístupu. I když se to jeví jako oxymóron, je třeba rozlišovat konkrétní kroky, za které je EU kritizována. Z hlediska EU jako globálního hráče v oblasti AI systémů je EU kritizována za přílišnou regulaci společností s cílem ochrany svých obyvatel, respektive uživatelů AI. Tento postoj může způsobit, že společnosti vytvářející a provozující AI budou preferovat umisťování svých sídel mimo EU, což se negativně projeví v příjmu z daní, vytváření nových pracovních míst a zejména naráží na politický cíl, aby EU měla vedoucí postavení v oblasti AI.[88] Naproti tomu je argumentováno, že EU tvoří jednotné podmínky pro všechny, a tudíž by tyto regulační kroky měly vést ke zdravému konkurenčnímu prostředí. Zmíněné regulační kroky obsažené v AI Actu však postrádají odpovědi na některá technická provedení, což s sebou přináší kritiku samotného AI Actu za obecnost.

I když je EU kritizována, autor považuje za důležité zdůraznit, že aktuální trend regulace a přístup EU k AI je očekávatelný, a částečně je tedy zmíněná kritika neoprávněná. Existence AI a velký rozmach těchto systémů umělé inteligence v minulém roce je skutečností, kterou je třeba přijmout. Také je realitou, že uživatelé nejsou ve stejném postavení jako společnosti vyvíjející a provozující AI systémy, což jsou většinou velké Big Tech společnosti. Proto je regulace ze strany EU vítaným krokem. Angažovanost EU v AI navíc není překvapující, a to hned ze dvou důvodů. Prvním z nich je, že EU jako globální aktér má zájem se podílet na vývoji AI z ekonomických důvodů i důvodů politické prestiže.

---

84 Stanovisko 28/2024 k některým aspektům ochrany údajů týkajícím se se zpracováním osobních údajů v souvislosti s modely AI. In: *European Data Protection Board* [online]. 17. 12. 2024, body 14 a 15 [cit. 2025-02-09]. Dostupné z: https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf.

85 Co je umělá inteligence a jak ji využíváme? In: *European Parliament* [online]. 4. 9. 2020 [cit. 2025-02-09]. Dostupné z: https://www.europarl.europa.eu/topics/cs/article/20200827STO85804/umela-inteligence-definice-a-vyuziti.

86 KING, J. – MEINHARDT, C. Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World. In: *Stanford Institute for Human-Centered Artificial Intelligence* [online]. Únor 2024 [cit. 2025-02-09]. Dostupné z: https://hai.stanford.edu/sites/default/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf.

87 Zejména čl. 5, 6, 25, 32, 33, 34 a 77 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 a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

88 AI Excellence: Budování strategického vedení v odvětvích s velkým dopadem. In: *European Comission* [online]. [cit. 2025-02-09]. Dostupné z: https://digital-strategy.ec.europa.eu/cs/policies/build-leadership-ai.

Druhým je tzv. *path dependence* Evropské unie, kdy současné rozhodování nebo legislativní procesy jsou ovlivněny předchozími pravidly, politikami nebo rozhodnutími. A EU dlouhodobě chrání jednotlivce a jeho práva, což lze vidět například na nařízení GDPR, které se mimochodem také nevyhnulo kritice.[89] Evropská unie tedy byla a je nucena reagovat na vývoj umělé inteligence, a to způsobem, kterým reaguje. Kritika způsobu regulace se autorovi nezdá zcela oprávněná, avšak chápe výtky týkající se nedostatečné komunikace EU směrem k občanům a nedostatečného vysvětlení regulací, zejména s ohledem na to, že transparentnost patří mezi základní hodnoty EU. Opatrný přístup k AI je žádaný, zvláště když jsou známa rizika, ale stále ještě není jasné, jak moc životy uživatelů systémy umělé inteligence ovlivní. V budoucnu tak lze očekávat reakce na vývoj AI a jedním z kroků by měla být i legislativa obsahující technické parametry, což v aktuálních legislativních pramenech chybí a bylo by vhodné je doplnit. Zejména se jedná o již diskutovanou povinnost poskytovat srozumitelná vysvětlení rozhodnutí AI, zejména u vysoce rizikových aplikací, tedy definici černých skříněk či adversariální manipulace vstupních dat. Řešením by mohly být komplexní hodnotové úsudky regulačních zprostředkovatelů, kteří by byli zodpovědní za provádění kritických hodnotových úsudků při hodnocení souladu s hodnotovými požadavky zákona o umělé inteligenci.[90] Vítaným krokem je vydání stanoviska 28/2024, které obsahuje některá z doporučení, ke kterým došly výzkumy věnující se nedostatkům AI Actu.[91] Konkrétní dopady a posun tohoto stanoviska však autor vzhledem k nedávnému vydání teprve zkoumá a hlubší analýzou se bude zabývat až v navazujícím výzkumu. Na závěr by autor rád zdůraznil, že byť se v příspěvku zabýval umělou inteligencí primárně z hlediska ochrany uživatele a jeho osobních údajů, umělá inteligence nadále zůstává pro EU výzvou, a to nejen z pohledu ochrany uživatele nebo ekonomického přínosu, ale i z hlediska politického. Kolektiv autorů Peter Gailhofer, Anke Herold, Jan Peter Schemmel, Cara-Sophie Scherf, Cristina Urrutia, Andreas R. Köhler a Sibylle Braungardt ve své studii *The role of Artificial Intelligence in the European Green Deal* navíc také poukázali na problém kompatibility cílů Green Dealu a snahy EU mít vedoucí postavení v AI ve světě.[92]

89 WALDMAN, E. A. Data Protection by Design? A Critique of Article 25 of the GDPR. *Cornell International Law Journal*. 2020, Vol. 53 [cit. 2025-02-09]. Dostupné z: https://ww3.lawschool.cornell.edu/research/ILJ/upload/Waldman-final.pdf.

90 TARTARO, A. Value-laden challenges for technical standards supporting regulation in the field of AI. *Ethics and Information Technology*. 2024, Vol. 26, No. 4 [cit. 2025-02-09]. Dostupné z: https://doi.org/10.1007/s10676-024-09809-y.

91 Stanovisko 28/2024 k některým aspektům ochrany údajů týkajícím se se zpracováním osobních údajů v souvislosti s modely AI. In: *European Data Protection Board* [online]. 17. 12. 2024, body 14 a 15 [cit. 2025-02-09]. Dostupné z: https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf.

92 GAILHOFER, P. – HEROLD, A. – SCHEMMEL, J. P. – SCHERF, C. – URRUTIA, C. – KÖHLER, A.R. – BRAUNGARDT, S. The role of Artificial Intelligence in the European Green Deal. In: *European Parliament* [online]. Květen 2021 [cit. 2025-02-09]. Dostupné z: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662906/IPOL_STU(2021)662906_EN.pdf.

AI Challenges From a Personal Data Perspective

Martin Mach

Abstract: In 2023, we saw the rise of artificial intelligence (AI) and its expansion to mass use by users around the world. However, AI also brings significant privacy challenges, as do all previous significant changes in modern technology. Globally, two approaches to AI in the context of data protection can be observed, one approach represented mainly by the United States of America and the other approach represented mainly by the European Union. The US focuses mainly on innovation and flexibility, while the EU emphasises privacy and security over technological advancement. The present paper will focus on the protection of users when using AI and the specific privacy risks of AI, including unauthorised access to sensitive data, misuse of data for tracking and profiling users, and lack of transparency of algorithms. In relation to the risks of using AI, the paper will focus on the EU's proposed regulation setting out harmonised rules for AI, the so-called AI Act. This would provide a comprehensive framework for AI regulation, including obligations for AI developers and users, to minimise risks and ensure the ethical use of AI. Finally, the paper will focus on whether the AI Act effectively ensures the protection of users in the context of AI.

Keywords: artificial intelligence, privacy, big tech, GDPR, AI Act