UNIVERZITA KARLOVA

Právnická fakulta

Lucie Hendrychová

Technologie založené na umělé inteligenci: právní aspekty ochrany dat a soukromí

Rigorózní práce

Pověřený akademický pracovník: doc. JUDr. Magdaléna Svobodová, Ph.D.

Tematický okruh: Evropské právo

Datum vypracování práce (uzavření rukopisu): 25. 2. 2024

Prohlašuji, že jsem předkládanou rigorózní práci vypracovala samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 216 975 znaků včetně mezer.

V Praze, dne 25. 2. 2024

.....

Lucie Hendrychová

Děkuji doc. JUDr. Magdaléna Svobodová, Ph.D. za vstřícnost, odborné vedení a cenné připomínky, které mi poskytla při psaní rigorózní práce.

Obsah

1. Úvod

Umělá inteligence stále více proniká do našeho každodenního života. Otevírá nové možnosti funkčnosti zařízení v domácnosti, pomáhá nám při překladu cizojazyčných frází, podporuje mobilní aplikace. Tím, že je už dnes takřka „všudepřítomná“, zvyšuje se potřeba ustanovit pro ni zákonný rámec.

Tento rámec může pojímat již existující legislativu obecnějšího charakteru. Čelíme pak ale nebezpečí, zda tato právní úprava dokáže reflektovat specifické rysy předmětné materie. V našem případě půjde např. o Obecné nařízení o ochraně osobních údajů známé pod zkratkou GDPR. Vedle toho je třeba upravit i ona zmíněná specifika, kterými se umělá inteligence vyznačuje, což vede k vytvoření zcela nových právních předpisů. Přestože se o umělé inteligenci mluví již několik desetiletí, právně se ukotvuje až nyní. Předpisem, jenž se soustředí výlučně na umělou inteligenci, je na poli Evropské unie Akt o umělé inteligenci, který je v listopadu 2023 v prvním čtení v Evropském parlamentu.

Legislativa v oblasti umělé inteligence čelí hned několika výzvám. Jedna skupina výzev je spjata s etickými otázkami. K nim můžeme zařadit nebezpečí diskriminace, s nímž se u systémů umělé inteligence setkáváme již dnes. Druhá skupina výzev vyvěrá ze samotného charakteru umělé inteligence. Tím, že je systém umělé inteligence schopen pracovat do určité míry samostatně, tedy bez zásahu člověka, je jeho chování mnohdy nepředvídatelné, a z toho důvodu stěží regulovatelné. Další úskalí představuje otázka, jak k umělé inteligenci přistoupit na zákonodárné úrovni, abychom regulací nesnížili konkurenceschopnost Evropské unie. Při tvorbě jednotlivých ustanovení je proto třeba myslet na výzkum a možnosti inovace a zvážit, zda je nelze určitými nástroji podpořit.

Cílem této práce je zmapovat stěžejní platnou a připravovanou legislativu na úrovni Evropské unie související s umělou inteligencí a na základě toho identifikovat její případné nedostatky. Na bázi této analýzy lze dojít k závěru, zda z pohledu ochrany dat a soukromí existují rizika, která vznikají u technologií založených na principech umělé inteligence.

Vzhledem k širokému záběru umělé inteligence naznačenému již výše se tato práce soustředí především na konverzační aplikace opírající se o umělou inteligenci, hlasové asistenty v domácnosti, pomocí níž můžeme ovládat domácí zařízení, a hlasové asistenty sloužící ke konverzaci. Vedle dopadů současné a plánované legislativy se zaměřením na Akt o umělé inteligenci a Obecné nařízení o ochraně osobních údajů (GDPR) se budeme snažit odpovědět na otázku jak zpracovávat data, která uživatel aplikaci sdělí, aniž by jej k tomu aplikace vyzvala.

2. Termín umělé inteligence

Umělá inteligence se v současnosti těší nevídané pozornosti. Přestože počátky jejího výzkumu sahají až do padesátých let minulého století, do centra dění a společenského diskurzu se dostala především v posledních letech. Jednou z příčin tohoto průlomu je bezpochyby fakt, že stále více proniká do našeho každodenního života ať už prostřednictvím chytrých mobilních telefonů či domácích zařízení. Přesto je pro mnoho lidí umělá inteligence, známá také pod zkratkou AI pocházející z anglického sousloví *artificial intelligence*, stále opředena až bájnými legendami a málokoho nechá chladným. Někteří v ní vidí jednoznačně pozitivní potenciál, jiní si v souvislosti s ní vybaví nadčasová literární díla spisovatele Karla Čapka a spojují si s ní především hrozbu. I tyto názory dokládají, jak málo dosud o umělé inteligenci a jejích schopnostech víme, a zejména jak malé je skutečné povědomí o jejích možnostech mezi laickou veřejností. Co vše může dokázat? V čem všem nám může pomoci? Je na místě se obávat, že by se někdy mohla pro člověka stát nebezpečím? Nebo jím už snad je? A co vlastně umělá inteligence znamená?

Hned na úvod je třeba konstatovat, že neexistuje jedna jediná definice umělé inteligence, jež by byla všeobecně přijímána. Naopak můžeme nalézt desítky pokusů fenomén umělé inteligence co nejpřesněji uchopit. Lze předpokládat, že se nemalé množství definic odvíjí od skutečnosti, že umělá inteligence prostupuje do stále více vědeckých odvětví a s tím i oblastí života, jak již bylo zmíněno výše. Proto pak každá definice zrcadlí specifika daného oboru, anebo se snaží zůstat na co nejobecnější úrovni, aby byla široce použitelná. Úskalí definice umělé inteligence může souviset také s faktem, že umělou inteligenci a komplexnost jejích schopností stále objevujeme a přehodnocujeme, přestože ji lidstvo zkoumá již několik dekád. Ani na legislativní úrovni nepanuje úplná shoda, jaké prvky by měla definice umělé inteligence zahrnovat.

Pod umělou inteligencí si dnes hodně lidí představí tzv. neuronové sítě, které fungují obdobně jako sítě v lidském mozku. Neuronové sítě se skládají z procesních jednotek, jež jsou stejně jako neurony v lidském mozku vzájemně rozličně propojené. Chápání umělé inteligence jako neuronové sítě je ovšem příliš úzké, protože s neuronovými sítěmi je spjata jen tzv. konekcionistická umělá inteligence. Oproti ní stojí druhý základní typ umělé inteligence, a to symbolická, k níž se řadí mimo jiné

sémantické sítě[1], jež se zakládají na sémantických vztazích mezi jednotlivými prvky. Symbolická neboli klasická umělá inteligence klade důraz na vytváření systémových pravidel. Pokud tak dojde k jevu, s nímž tato systémová pravidla počítají, zachová se systém odpovídajícím způsobem.[2]

2. 1 Definice umělé inteligence

2. 1. 1 Obecné definice umělé inteligence

Pokud se oprostíme od dělení umělé inteligence na dva primární směry, jež jsou vymezeny v předešlém odstavci, a současně se budeme držet obecné nelegislativní roviny, lze umělou inteligenci chápat jako „*schopnost stroje se učit, poněvadž učení je jedna ze základních charakteristik inteligentního chování*“.[3] Tato definice Jaimeho G. Carbonella, Ryszarda S. Michalského a Toma M. Mitchella je jednoduchá, srozumitelná a stručná, proto ji můžeme aplikovat snad ve všech vědeckých oborech.

Stejným směrem jde také pojetí umělé inteligence jako „*simulace procesů lidské inteligence počítačovými a jinými systémy*“.[4] O prvek počítače se opírají také Pavel Hamet a Johanne Tremblay, kteří spatřují umělou inteligenci v „*užívání počítače k modelování inteligentního chování s minimálním zásahem člověka*“.[5] Jedna z nejčastěji zmiňovaných definic umělé inteligence pochází od amerického profesora Johna McCarthyho a jeho kolegů Marvina L. Minského, Nathaniela Rochestera a Clauda E. Shannona. Tento kolektiv vymezil umělou inteligenci na příkladu stroje, který se podle nich chová takovým způsobem, jejž bychom označili za inteligentní, kdyby se tímto způsobem choval člověk. Přestože toto pojetí pochází z padesátých let minulého století, je dosud platné a hojně citované. [6]

---

[1] KOLAŘÍKOVÁ, Linda, HORÁK, Filip. *Umělá inteligence & právo*. Praha: Wolters Kluwer ČR. 2020, 9, 13. ISBN 9788075987839.
[2] ABBOTT, Ryan. *The reasonable robot: artificial Intelligence and the law*. Cambridge: Cambridge University Press, 2020, viii, 28. ISBN 9781108459020.
[3] MCKEOWN, Tara, Jamila MUSTAFINA, Rustem MAGIZOV a Camila GATAULLINA. AI in Law Practices. Online. *2020 13th International Conference on Developments in eSystems Engineering (DeSE).* IEEE, 2020, 27. Dostupné z: doi:10.1109/DeSE51703.2020.9450780. [cit. 2023-01-21].
[4] WALKER-OSBORN, Charlotte, CHAN, Christopher. Artificial intelligence and the law. Online. *ITNow*. 2017, 59(1), 36. ISSN 1746-5702. doi:10.1093/itnow/bwx017. [cit. 2023-01-21].
[5] LUI, Alison, RYDER, Nicholas. *FinTech, Artificial Intelligence and the Law*. New York, NY: Routledge, 2021, 34. ISBN 9781032012469.
[6] ŠTĚDROŇ, Bohumír. *Právo a umělá inteligence*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020, 25. ISBN 9788073808037.

John McCarthy, jenž je považován za otce pojmu umělé inteligence, ji také vymezil jako samostatnou vědeckou disciplínu. Umělou inteligenci totiž označil za „*vědu a techniku vytváření inteligentních strojů, zejména inteligentních počítačových programů*“[7], čímž ji nadobro ukotvil na poli vědy.

Společným jmenovatelem výše uvedených definic je vedle vysoké míry obecnosti a souvztažnosti ke člověku také určitá chytrost neboli inteligence. Užití slova inteligence v definici termínu umělé inteligence sice může být vnímáno jako náznak tautologie, ale na druhou stranu na ni můžeme nahlížet jako na samostatný druh inteligence. Nehledě na to, že ani pojem inteligence není dosud jednoznačně definován, na což narážíme jak v následujícím odstavci, tak v rámci vyjádření Odborné skupiny na vysoké úrovni pro umělou inteligenci uvedeného v kapitole 2. 1. 2 Legální definice.

Ne všichni zastávají názor, že umělá inteligence má se samotnou inteligencí co do činění. Pod obecný termín inteligence totiž někteří automaticky řadí také emoční inteligenci včetně schopnosti mít emoce, sociální rozhodování a schopnost prakticky uvažovat, čímž doposud žádné stroje nedisponují. Někteří skeptikové proto na umělou inteligenci v dnešní podobě nahlížejí spíše jako na pouhé počítačové zpracování či strojové učení.[8] Termínu inteligence se mimo jiné ve svém vysvětlení vyhnul také profesor Michal Pěchouček z Českého vysokého učení technického v Praze. Podle něj je umělá inteligence vedle vědecké disciplíny také „*soubor softwarových a hardwarových technologií pomáhající automatizovat, zrychlovat, zpřesňovat nebo škálovat lidské kognitivní schopnosti – vnímat, poslouchat, uvažovat a reagovat*“.[9] Pod umělou inteligenci zařazuje explicitně jak softwarové, tak hardwarové technologie, čímž se odlišuje od definic dosud zmíněných. Jak je vidno v následující kapitole, tak ani u legálních definic není explicitní rozlišování mezi hardwarem a softwarem vždy přítomné, což je mimo jiné i případ připravovaného evropského Aktu o umělé inteligenci. Na druhou stranu absence zmínky o hardwaru nemusí být nutně chápána jako nedostatek. Pokud je hardwarové řízení „uměle inteligentní“, je umělá inteligence

[7] ŠTĚDROŇ, Bohumír. *Právo a umělá inteligence*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020, 25. ISBN 9788073808037.
[8] BAKER, Dennis J., ROBINSON, Paul. H. *Artificial Intelligence and the Law: Cybercrime and Criminal Liability*. Routledge. 2020, 1-2. ISBN 9781000210644.
[9] KOLAŘÍKOVÁ, Linda, HORÁK, Filip. *Umělá inteligence & právo*. Praha: Wolters Kluwer ČR. 2020, 2. ISBN 9788075987839.

součástí jeho softwaru, nikoliv hardwaru. Umělá inteligence se tak výlučně vztahuje k softwaru a je jen na člověku, zda ho zabuduje do hardwaru, či nikoliv. Lze tak konstatovat, že zmínka hardwarových zařízení v definici umělé inteligence hraničí s redundancí.

2. 1. 2 Legální definice umělé inteligence

Jak již bylo naznačeno výše, ani na legislativní úrovni nepanuje shoda, jaké parametry by měla definice umělé inteligence zohlednit. Legální definice, jež můžeme chápat jako „*závazné vymezení významu určitého právního pojmu v zákoně*“[10], by měla být maximálně výstižná a jednoznačná. V případě České republiky nenalezneme žádnou legální definici umělé inteligence, jež by pocházela z pera českého zákonodárného sboru. Česká republika v této oblasti přejímá definice obsažené v legislativních pramenech Evropské unie (dále také „EU“ či „Unie“) včetně nezávazného soft law.

Ke dnešnímu dni neexistuje žádný závazný legislativní akt Unie, který by umělou inteligenci definoval. Je třeba ovšem upozornit na plánovanou legislativu EU, která již započala svůj řádný legislativní proces a která by měla definovat pojem *systém umělé inteligence*. Jedná se o návrh *Nařízení Evropského Parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie* (dále také „Návrh aktu o umělé inteligenci“ či „Akt o umělé inteligenci“), který je nyní v prvním čtení v Evropském parlamentu[11]. Tím, že se jedná o nařízení, bude akt bezprostředně závazný pro všechny členské státy EU a jejich občany. Jedním z důvodu, proč se evropští legislativci uchýlili k formě nařízení, a nikoliv směrnice, je právě jednotná definice systému umělé inteligence, jejíž nezbytnost je osvětlena v rámci důvodové zprávy k předmětnému nařízení. Vedle definice termínu zahrnuje Návrh aktu o umělé inteligenci přílohu I se seznamem přístupů a technik, jež se uplatňují při vývoji systému umělé inteligence.[12] Článek 3 odst. 1 Návrhu aktu o

[10] GERLOCH, Aleš. Legální definice. HENDRYCH, Dušan a kol. Právnický slovník. 3. vydání. Praha: C. H. Beck, 2009. Dostupné z: https://app-beck-online-cz.ezproxy.is.cuni.cz/bo/document-view.seam?documentId=nnptembqhfpw64zrguxgyzlhmfwg42k7mrswm2lonfrwk. [cit. 2023-01-22].
[11] Návrh Nařízení Evropského Parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:52021PC0206. [cit. 2023-02-10].
[12] Návrh Nařízení Evropského Parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie – důvodová zpráva. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:52021PC0206. [cit. 2023-02-10].

umělé inteligenci definuje systém umělé inteligence jako „*software, který je vyvinut pomocí jedné nebo více technik a přístupů uvedených v příloze I a který může pro danou sadu cílů definovaných člověkem generovat výstupy, jako je například obsah, predikce, doporučení nebo rozhodnutí ovlivňující prostředí, s nimiž komunikují*“, přičemž ona zmíněná příloha I zahrnuje v nynější podobě tři základní kategorie přístupů, mezi něž se řadí přístupy strojového učení, přístupy založené na logice a znalostech a statistické přístupy.[13]

Vedle stále ještě neúčinného Aktu o umělé inteligenci vymezují pojem umělé inteligence také nezávazné právní akty Evropské unie. Jedním z prvních je například sdělení Evropské komise *Umělá inteligence pro Evropu* z 25. dubna roku 2018. Umělou inteligenci chápe jako „*systémy vykazující inteligentní chování v podobě vyhodnocování svého okolí a následného rozhodování či vykonávání kroků – s určitou mírou autonomie – k dosažení konkrétních cílů*“.[14] Na rozdíl od Aktu o umělé inteligenci Evropská komise (dále také „Komise“) pojímá umělou inteligenci šíře, jelikož ji explicitně neomezuje jen na úroveň softwaru. Pro ilustraci demonstrativně uvádí konkrétní příklady. U softwarových technologií jsou to například hlasoví asistenti či systém rozpoznávající hlas a obličej, u hardwarových pak autonomní vozidla nebo drony.[15]

Na výše uvedenou definici Evropské komise reagovala 18. prosince téhož roku Odborná skupina na vysoké úrovni pro umělou inteligenci. V úvodu vyjadřuje přesvědčení, že definovat termín umělé inteligence pomocí pojmu inteligence není nejšťastnější volba vzhledem k tomu, že ani pojem inteligence nebyl doposud uspokojivě definován. Jako alternativu nabízí pojem racionality jako schopnosti zvolit nejlepší možnou akci/jednání k dosažení vytyčeného cíle za určitých podmínek. Po podrobném vysvětlení jednotlivých složek definice nabízí tato skupina poněkud obšírnou definici, pod níž také zahrnuje nahlížení na umělou inteligenci jako na vědu. „*Umělá inteligence (AI) zahrnuje systémy navržené lidmi, které při zadání komplexního*

[13] Návrh Nařízení Evropského Parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:52021PC0206. [cit. 2023-01-22].
[14] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Umělá inteligence pro Evropu. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:52018DC0237. [cit. 2023-01-22].
[15] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Umělá inteligence pro Evropu. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:52018DC0237. [cit. 2023-01-22].

cíle jednají ve fyzickém nebo digitálním světě tím, že vnímají své prostředí, interpretují shromážděná strukturovaná nebo nestrukturovaná data, uvažují na základě znalostí získaných z těchto dat a rozhodují o nejlepší akci (nejlepších akcích), aby dosáhly daného cíle (podle předem definovaných parametrů). Systémy umělé inteligence mohou být také navrženy tak, aby se naučily přizpůsobovat své chování analýzou toho, jak je prostředí ovlivněno jejich předchozím chováním. Umělá inteligence jako vědní disciplína zahrnuje několik přístupů a technik, jako je strojové učení (jehož specifickými příklady jsou hluboké učení a posilovací učení), strojové uvažování (které zahrnuje plánování, rozvrhování, reprezentaci znalostí a uvažování, vyhledávání a optimalizaci) a robotika (která zahrnuje řízení, vnímání, senzory a aktuátory, jakož i integraci všech ostatních technik do kyberneticko-fyzických systémů).“[16] Ve srovnání s předchozí definicí Komise zachovává odborná skupina stěžejní prvek posouzení situace, na jehož základě se systém rozhodne pro určité jednání, aby dosáhl požadovaného cíle. Celý proces ovšem rozebírá odborná skupina v porovnání s Komisí do větších detailů. Definici Komise obohacuje o zcela nový element adaptace systému na okolní prostředí. Navíc vymezení systému, jenž se zakládá na umělé inteligenci, doplňuje o vymezení umělé inteligence jako vědní disciplíny. V tomto případě lze ocenit demonstrativní výčet přístupů a technik, který napomáhá k utvoření celistvé představy.

Pro srovnání doplňme státy, jež nejsou členskými státy EU a zároveň pojem umělé inteligence vymezují na legislativní úrovni. Jedním z nich je Velká Británie. Velká Británie definuje umělou inteligenci v dokumentu, který má z pohledu práva Evropské unie povahu prováděcího aktu, a to k britskému zákonu o bezpečnosti a investicích z roku 2021. Umělá inteligence je tady vymezena jako technologie, která „*umožňuje naprogramovat či natrénovat zařízení nebo software tak, aby prostřednictvím dat dokázala vnímat prostředí, aby dokázala data interpretovat na základě automatizovaného zpracování, jež se podobá kognitivním schopnostem, a aby dokázala činit doporučení, predikce a rozhodnutí s ohledem na dosažení konkrétního*

[16] The European Commission’s High-level Expert Group on Artificial Intelligence. *A Definition of AI: Main Capabilities and Scientific Disciplines*. Online. Futurium. 2018. Dostupné z: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf. [cit. 2023-01-22].

cíle“.[17] Všechny vyjmenované složky musejí být splněny kumulativně. Z hlediska pojmových znaků koresponduje definice s pojetím Odborné skupiny na vysoké úrovni pro umělou inteligenci. Výjimku tvoří pouze schopnost adaptace, kterou britský prováděcí dokument nezmiňuje.

Spojené státy americké se také řadí mezi země, jež vymezují umělou inteligenci na zákonodárné úrovni. Dne 1. ledna 2021 nabyl účinnosti Národní akt iniciativy umělé inteligence z roku 2020.[18] V oddílu E sekci 5002 (3) je umělá inteligence definována jako „*strojový systém, který může pro daný soubor cílů definovaných člověkem učinit predikce, doporučení nebo rozhodnutí ovlivňující reálné nebo virtuální prostředí*“.[19] Ve srovnání s definicemi uvedenými výše je toto pojetí poněkud stručné. Je obsažena schopnost činit predikce či rozhodnutí, ale prvky vnímání okolního prostředí a interpretace dat jsou zcela opomenuty.

2. 2 Milníky ve vývoji umělé inteligence

Jak již bylo zmíněno výše, první zmínka o umělé inteligenci pochází z druhé poloviny padesátých let dvacátého století. Společně s termínem umělé inteligence a její definicí zazněly tehdy v roce 1956 i první odhady, jak rychle se bude umělá inteligence vyvíjet. Některé z nich byly poměrně odvážné jako např. predikce, že v roce 1970 bude umělá inteligence schopna porozumět přirozenému jazyku člověka a že bude schopna jazyk překládat. Žádná z prognóz nakonec nebyla naplněna.[20] V sedmdesátých letech naopak nastala tzv. první zima umělé inteligence neboli *first AI war*, někdy také nazývána „*dobou ledovou*“[21], která se projevila neúspěchem řady vědeckých pokusů a

[17] The National Security and Investment Act 2021 (Notifiable Acquisition) (Specification of Qualifying Entities) Regulations 2021. Online. 2021. Dostupné z: https://www.legislation.gov.uk/uksi/2021/1264/schedule/3/made. [cit.2023-01-22].
[18] *National Artificial Intelligence Initiative*. Online. AI.GOV. 2023. Dostupné z: https://ai.gov/. [cit. 2023-01-22].
[19] M. THORNBERRY, WILLIAM. *National Defense Authorization Act for Fiscal Year 2021: Conference Report to Accompany H.R. 6395*. Online. 2020, 1210. Dostupné z: https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210. [cit. 2023-01-22].
[20] ŠTĚDROŇ, Bohumír. *Právo a umělá inteligence*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020, 109-110. ISBN 9788073808037.
[21] ŠTĚDROŇ, Bohumír. *Právo a umělá inteligence*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020, 109. ISBN 9788073808037.

s tím souvisejícím vystřízlivěním z počátečního optimismu ohledně rychlého vývoje umělé inteligence.[22]

V osmdesátých letech pak umělá inteligence slavila znovu úspěch, a to v podobě inteligence založené na expertních systémech. Tato inteligence pracovala na základě logických pravidel, jež byla odvozena od znalostí odborníků. Pomocí těchto pravidel byla schopna řešit určitý druh problémů.[23] V roce 1987 také proběhl první ročník mezinárodní konference o umělé inteligenci a právu *ICAIL (International Conference on Artificial Intelligence and Law),* kde se zrodilo společenství, jež definitivně propojilo svět práva a umělé inteligence.[24] Poté ovšem umělá inteligence zažila opět propad. Situace byla natolik vážná, že někteří vědci se od pojmu umělá inteligence distancovali a své práce, které se fakticky stále vztahovaly k umělé inteligenci, prezentovali z perspektivy jiných oborů.[25]

Znovu na výsluní se obor umělé inteligence dostal v druhé polovině devadesátých let, když např. v roce 1997 šachový program Deep Blue porazil v regulérním zápase tehdejšího mistra světa v šachu Garriho Kasparova.[26] Od té doby zažívá umělá inteligence svou zlatou éru, a jelikož je její výzkum a zařazování do každodenní společnosti kontinuální, začalo se umělou inteligencí intenzivněji zabývat také právo.

2. 3 Spolupráce v oblasti umělé inteligence

Velký potenciál umělé inteligence pro lidstvo má za následek vznik nepřeberného množství strategií a výzkumných společenství, jež akcentují význam spolupráce. Státy, nadnárodní celky nebo dobrovolná sdružení cítí potřebu explicitně deklarovat, že mají zájem na tom držet se ve výzkumu umělé inteligence na předních

[22] ABBOTT, Ryan. *The reasonable robot: artificial Intelligence and the law*. Cambridge: Cambridge University Press, 2020, viii, 21. ISBN 9781108459020.
[23] ABBOTT, Ryan. *The reasonable robot: artificial Intelligence and the law*. Cambridge: Cambridge University Press, 2020, viii, 21. ISBN 9781108459020.
[24] BENCH-CAPON, T, M ARASZKIEWICZ, K ASHLEY, et al. A history of AI and Law in 50 papers: 25 years of the international conference on AI and Law. *Artificial intelligence and law* Online. Dordrecht: Springer Netherlands, 2012, 20(3), 216-217. ISSN 15728382. doi:10.1007/s10506-012-9131-x. [cit. 2023-02-10].
[25] ABBOTT, Ryan. *The reasonable robot: artificial Intelligence and the law*. Cambridge: Cambridge University Press, 2020, viii, 21. ISBN 9781108459020.
[26] ŠTĚDROŇ, Bohumír. *Právo a umělá inteligence*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020, 112. ISBN 9788073808037.

pozicích, a vytyčují si více či méně konkrétní cíle, jejichž naplněním se zařadí mezi vědeckou špičku.

V této kapitole je uveden výběr iniciativ, v nichž působí Česká republika. Jako příklad zmiňme Deklaraci spolupráce na AI, jež byla v roce 2018 přijata 42 členskými státy EU a Norskem. Přestože je dokument velice obecný, dokazuje vůli evropských států spolupracovat, a společně tak pracovat na konkurenceschopnosti Evropy v oblasti umělé inteligence.

2. 3. 1 Globální partnerství pro umělou inteligenci

V lednu 2022 se Česká republika stala součástí Globálního partnerství pro umělou inteligenci.[27] Tato iniciativa se původně zrodila na poli sdružení ekonomicky nejvyspělejších zemí světa G7 a postupně se rozšířila mezi současných 29[28] členů ze čtyř kontinentů, mezi nimiž nechybí Brazílie, Korejská republika či Evropská unie. Platforma, jejíž sekretariát je součástí Organizace pro hospodářskou spolupráci a rozvoj (*OECD*), prosazuje zodpovědný vývoj a přístup k umělé inteligenci, které jsou v souladu s lidskými právy, základními svobodami a demokratickými hodnotami.[29] Vedle podpory výzkumu umělé inteligence a promítnutí jeho poznatků do praxe usiluje o to, aby se mezinárodní spolupráce neomezovala pouze na vědecké prostředí, ale aby se rozvíjela také na úrovni průmyslu, mezinárodních organizací či mezivládních konferencí.[30]

Globální partnerství pro umělou inteligenci se v současnosti rozpadá do čtyř základních pracovních skupin, které sídlí buď v Paříži, nebo v kanadském Montrealu a navzájem spolupracují, přestože každá z nich pokrývá jinou doménu, do níž umělá inteligence zasahuje. Skupina pro zodpovědnou umělou inteligenci na ni nazírá z pohledu, jak by mohla být lidstvu prospěšná. Další dvě skupiny se zabývají vlivem

[27] *Česká republika vstoupila do Globálního partnerství pro umělou inteligenci*. Online. Ministerstvo zahraničních věcí České republiky. 2022. Dostupné z: https://mzv.gov.cz/jnp/cz/udalosti_a_media/archiv_zprav/rok_2022/ceska_republika_vstoupila_do_globalniho.html. [cit. 2023-02-18].

[28] *The Global Partnership on Artiificial Intelligence*. Online. The Global Partnership on Artiificial Intelligence. Dostupné z: https://www.gpai.ai/community/. [cit. 2023-02-18].

[29] *The Global Partnership on AI (GPAI)*. Online. The Global Partnership on AI (GPAI). Dostupné z: https://oecd.ai/en/gpai. [cit. 2023-02-18].

[30] *The Global Partnership on Artiificial Intelligence*. Online. The Global Partnership on Artificial Intelligence. Dostupné z: https://www.gpai.ai/community/. [cit. 2023-02-18].

umělé inteligence na pracovní trh či inovacemi a komercionalizací umělé inteligence. Čtvrtá skupina se věnuje správě dat. Tato pracovní skupina se zaměřuje na způsob, jak umělá inteligence nakládá s daty, a navazuje přitom na dosavadní výzkum. Podporuje mechanismy, které zabezpečí, aby umělá inteligence nakládala s daty v souladu s obecně přijímanými principy lidských práv, a současně dokazuje, že tyto mechanismy nutně nebrání jejímu využití a rozvoji. Skupina publikuje každý rok výroční zprávy, v nichž reflektuje, nakolik byly naplněny vytyčené cíle, a uvádí, na co se zaměří v nadcházejícím období.[31]

V současnosti se soustředí na tři oblasti. První z nich spočívá v podpoře vzniku datových trustů, které by měly zajistit, že ze sdílení dat bude prosperovat celá společnost. Sdílení dat by pak v konečném důsledku mělo být bezpečné, spravedlivé a legální. Druhá souvisí s podporou „datové spravedlnosti". V souvislosti s ní usiluje pracovní skupina o širší perspektivu, než je ochrana soukromí pouhého jednotlivce, a tak například u posuzování negativních vlivů umělé inteligence na rovnost příležitostí není výchozím hlediskem jedinec, ale komunita. Třetí cílová sféra je reprezentována technologiemi, tzv. *PETs* (*privacy-enhancing technologies*), jež umožňují užívat a sdílet data takovým způsobem, že soukromí ani integrita jednotlivce nejsou dotčeny.[32]

2. 3. 2 Národní strategie umělé inteligence v České republice

Koncepční dokumenty, jež mají podpořit výzkum a rozvoj umělé inteligence vznikají také na vládní úrovni. Nejinak je tomu v případě České republiky, jež v květnu 2019 na výzvu Evropské komise přijala Národní strategii umělé inteligence v ČR (dále také „NAIS"), jež navazuje na vládní Inovační strategii 2019-2030 a program Digitální Česko. Za jejím vznikem a realizací stojí Ministerstvo průmyslu a obchodu, které NAIS vypracovalo za pomocí zástupců z akademické půdy a ostatních ministerstev.[33]

---

[31] *Working Group on Data Governance*. Online. The Global Partnership on Artificial Intelligence. Dostupné z: https://www.gpai.ai/projects/data-governance/. [cit. 2023-02-18].

[32] *Data Governance Working Group Report: November 2022 - GPAI Tokyo Summit*. Online. The Global Partnership on Artiificial Intelligence. 2022, 10-13. Dostupné z: https://www.gpai.ai/projects/data-governance/gpai-data-governance-wg-report-2022.pdf. [cit. 2023-02-18].

[33] *Umělá inteligence*. Online. Vláda České republiky. 2021. Dostupné z: https://vlada.gov.cz/cz/evropske-zalezitosti/umela-inteligence/umela_inteligence/umela-inteligence-192765/#N%C3%A1rodn%C3%AD%20strategie%20%C4%8CR%20pro%20um%C4%9Blou%20inteligenci. [cit. 2023-02-19].

Vláda v čele s tehdejším premiérem Andrejem Babišem v NAIS deklaruje cíl stát se v rámci dvanácti let jedním z evropských lídrů na poli inovací a technologií. Této mety chce vláda dosáhnout primárně pomocí podpory sedmi klíčových oblastí. Výsadnímu postavení se těší podpora výzkumu, jež mimo jiné zahrnuje také podporu spolupráce napříč evropskými vědeckými obcemi či vybudování Evropského centra excelence v umělé inteligenci, jemuž se věnuje samostatná kapitola 2. 3. 3 Evropské centrum excelence v umělé inteligenci. S tím souvisí druhá klíčová sféra v podobě financování výzkumu a podpora start-upové scény. Třetí stěžejní odvětví, na nějž je třeba se v souvislosti s rozvojem umělém inteligence zaměřit, je ekonomika a digitální infrastruktura. Čtvrtá a pátá oblast souvisí se skutečností, že systémy vybavené umělou inteligencí v určitých odvětvích brzy nahradí lidskou pracovní sílu. V návaznosti na to je nezbytné rozvíjet u lidí ty dovednosti, jež umělá inteligence (alespoň v dohledné době) nedokáže nahradit a již v procesu vzdělávání je nutné vzít v úvahu, jak bude vypadat budoucí pracovní trh a v čem všem se bude lišit od toho současného. Šestou oblast představuje uzpůsobení legislativy, které tematizuje následující odstavec. Poslední spočívá v apelu na důraznější zapojení České republiky do mezinárodní spolupráce.[34]

Kapitola, jež se soustředí na právní aspekty umělé inteligence, upomíná na nezbytnost vytvoření uceleného právního rámce pro užívání a rozvoj umělé inteligence. Legislativa musí být nastavena tak, aby výzkum a vývoj umělé inteligence podporovala, nikoliv ztěžovala. Mezi krátkodobými cíli, jež mají být naplněny do roku 2021, nalezneme například analýzu rizik, jež umělá inteligence představuje pro ochranu soukromí, analýzu překážek, které brání využívání dat nezbytných k rozvoji umělé inteligenci, či revizi modelu, který pojímá ochranu práv duševního vlastnictví k předmětům, které vytvořila umělá inteligence. Střednědobé cíle s předpokládaným splněním do roku 2027 jsou formulovány již obecněji a vesměs akcentují aktivitu na mezinárodním poli a s tím spjatou spolupráci. Mezi dlouhodobé cíle do roku 2035, jež

[34] *Národní strategie v umělé inteligenci v České republice*. Online. Vláda České republiky. 2019, 4-6, 30. Dostupné z: https://www.vlada.cz/assets/evropske-zalezitosti/umela-inteligence/NAIS_kveten_2019.pdf. [cit. 2023-02-19].

jsou ještě méně konkrétní, je třeba zařazena vize České republiky jako země s prvotřídním a inovativním přístupem k umělé inteligenci.[35]

2. 3. 3 Evropské centrum excelence v umělé inteligenci

Dne 4. března 2020 podepsaly Univerzita Karlova, České vysoké učení technické v Praze a brněnská Masarykova univerzita memorandum o vzniku Evropského centra excelence v umělé inteligenci. Vznik centra předvídá už Národní strategie umělé inteligence, jež byla vládou přijata o rok dříve, tzn. v roce 2019, a memorandum tak představuje významný krok k naplnění tohoto cíle.[36]

Cílem této české iniciativy je kromě navázání spolupráce se zahraničními univerzitami a dalšími evropskými centry excelence v umělé inteligenci také zlepšit podmínky pro výzkum a dostat do evropského povědomí dosavadní české vědecké úspěchy. Centrum se má opírat o tři pilíře, z nichž první má podobu organizované komunikace, jež má zajistit sdílení poznatků napříč Evropskou unií. Druhý pilíř přestavuje platforma pro zkoumání společensko-právních dopadů umělé inteligence. Poslední pilíř je vymezen nejméně určitě, a to jako podpora pokročilého výzkumu, jež zahrnuje například pomoc prostřednictvím dotací.[37]

Jak již bylo naznačeno v odstavci výše, evropských center excelence v umělé inteligenci je více. Jejich rozvoj je realizován v rámci výzkumného a inovativního programu Unie Horizon Europe (2021-2027) pod záštitou Evropské sítě evropských center excelence v umělé inteligenci (*ELISE*), kterou koordinuje finská Aaltova univerzita. Cílem ELISE je zajistit a zdokonalit evropskou konkurenceschopnost na poli umělé inteligence, a to především skrze podporu výzkumu a spolupráce napříč centry.[38]

---

[35] *Národní strategie v umělé inteligenci v České republice*. Online. Vláda České republiky. 2019, 35-38. Dostupné z: https://www.vlada.cz/assets/evropske-zalezitosti/umela-inteligence/NAIS_kveten_2019.pdf. [cit. 2023-02-19].

[36] *Evropské centrum excelence v umělé inteligenci*. Online. Národní portál pro evropský výzkum. 2020. Dostupné z: https://www.evropskyvyzkum.cz/cs/novinky/evropske-centrum-excelence-v-umele-inteligenci. [cit. 2023-02-18].

[37] *Přední české univerzity spouští projekt Evropského centra excelence v umělé inteligenci*. Online. Ministerstvo průmyslu a obchodu. 2020. Dostupné z: https://www.mpo.cz/cz/rozcestnik/pro-media/tiskove-zpravy/predni-ceske-univerzity-spousti-projekt-evropskeho-centra-excelence-v-umele-inteligenci--253258/. [cit. 2023-02-18].

[38] *European Network of AI Excellence Centres*. Online. European Network of AI Excellence Centres. Dostupné z: https://www.elise-ai.eu/. [cit. 2023-02-18].

2. 4 Podoba umělé inteligence v každodenním životě

Umělá inteligence již dlouho není pouhým předmětem vědeckého bádání. Její schopnosti a možnosti můžeme pozorovat v rámci každodenní rutiny, aniž bychom si to uvědomovali. Bereme ji totiž za neodmyslitelnou součást našeho života a často jí nevědomky plně důvěřujeme, třeba když nám navrhne novou skladbu, která zapadá do našeho preferovaného hudebního stylu, nebo nám doporučí nejrychlejší cestu do kýženého cíle.[39]

Jako první ilustrační příklad uveďme chytrou domácnost, neboli *smart home*. Tento pojem zahrnuje širokou škálu produktů a asistentů. Jedním z nich je třeba chytrý hlasový asistent, kterého bychom v roce 2020 našli v každé čtvrté americké domácnosti. Jedná se o virtuálního asistenta, jenž se vizuálně podobá reproduktoru a s nímž člověk může komunikovat díky programu založenému právě na umělé inteligenci. Ať už Siri od společnosti Apple, Alexa od Amazonu, nebo jakýkoliv jiný asistent tak zpravidla odpovídá na faktické otázky uživatele nebo mu na požádání přehraje jeho oblíbenou hudbu. Lze ho však také propojit s dalšími chytrými zařízeními v domácnosti. Tímto způsobem můžeme hlasově ovládat jednotlivé prvky domácnosti, jako jsou například světla či topení.[40] Pokud nedisponujeme hlasovým asistentem, můžeme spotřebiče řídit chytrým mobilním telefonem bez ohledu na to, zda se zrovna nacházíme doma. Na dálku můžeme zapnout pračku či sušičku a sledovat její chod.[41]

Se zařízeními chytré domácnosti, a především pak s hlasovými asistenty úzce souvisí tzv. internet věcí (*internet of things, IoT*). Používá ho významná část populace, přestože se s tímto konkrétním termínem dosud nesetkala. Internet věcí je síť, která navzájem propojuje jednotlivá chytrá zařízení, a umožňuje jim tak předávat si relevantní data a reagovat na sebe. Tato síť se však neomezuje pouze na objekty v domácnosti, její

[39] *Data Governance Working Group Report: November 2022 - GPAI Tokyo Summit*. Online. The Global Partnership on Artiificial Intelligence. 2022, 4. Dostupné z: https://www.gpai.ai/projects/data-governance/gpai-data-governance-wg-report-2022.pdf. [cit. 2023-02-18].
[40] DE BRUYNE, Jan a VANLEENHOVE, Cedric (ed.). *Artificial Intelligence and the Law.Intersentia*, 2021, 174. ISBN 9781839701047.
[41] ŠTĚDROŇ, Bohumír. *Právo a umělá inteligence*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020, 134-135. ISBN 9788073808037.

využití je daleko širší. S internetem věcí se můžeme také setkat například na poli průmyslu.[42]

Internet věcí je také zapojen do infrastruktury inteligentních měst, neboli *smart cities*. Vedle komunikačních technologií je jednou z platforem, kterou inteligentní města využívají při monitoringu infrastruktury, její koordinaci a zabezpečení. Jejich cílem je co možná největší efektivita, úspora energie a s ní spojená udržitelnost, což se v praxi projevuje například tím, že se pouliční osvětlení zeslabí, když se v okolí nenachází žádný člověk či automobil. Tuto informaci získají od jiných zařízení prostřednictvím inteligentních senzorů.[43]

S umělou inteligencí se dnes můžeme setkat i v bankovnictví, kde slouží v mnoha ohledech. Napomáhá při identifikaci osoby a doporučuje klientům produkty, přičemž využívá data, jež přispívají k personalizaci nabízených služeb. Pro samotné banky je přínosem v oblasti řízení rizik, při němž vyhodnocuje solventnost klienta a jeho ochotu plnit své závazky.[44]

Významným sektorem z pohledu užití umělé inteligence je vedle bankovnictví zdravotnictví. Kromě široké škály aplikací, jež se soustředí na oblasti od zdravého životního stylu po včasnou detekci vážných onemocnění, asistuje umělá inteligence při řadě diagnóz, vyšetření a operací. Samostatnou kapitolu pak tvoří zdravotní asistenti v podobě robotů, kteří mohou u určitých úkonů nahradit jinak nezbytnou zdravotní sestru. Právě v kontextu zdravotních asistentů se často naráží na palčivou otázku odpovědnosti v případě, kdyby došlo k újmě na zdraví.[45] Tématu odpovědnosti se věnuje samostatná kapitola.

[42] ŠTĚDROŇ, Bohumír. *Právo a umělá inteligence*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020, 126-127. ISBN 9788073808037.
[43] ŠTĚDROŇ, Bohumír. *Právo a umělá inteligence*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020, 133. ISBN 9788073808037.
[44] KOLAŘÍKOVÁ, Linda, HORÁK, Filip. *Umělá inteligence & právo*. Praha: Wolters Kluwer ČR. 2020, 35. ISBN 9788075987839.
[45] DE BRUYNE, Jan a VANLEENHOVE, Cedric (ed.). *Artificial Intelligence and the Law.Intersentia*, 2021, 488-492. ISBN 9781839701047.

3. Legislativa Evropské unie v oblasti umělé inteligence

Jak již bylo naznačeno, primárním zdrojem legislativy v oblasti umělé inteligence je pro Českou republiku právo Evropské unie. Nejedná se pouze o závazné směrnice či nařízení, ale také třeba o doporučení Evropské komise, které společně s dalšími doporučeními a stanovisky tvoří tzv. soft law, které významným způsobem doplňuje platné právo. Právo Evropské unie je stejně jako právní řády členských zemí dynamické a neustále se rozvíjí a obměňuje. Z tohoto důvodu je do přehledu zařazena i plánovaná legislativa, jež by se měla v dohledné době dočkat schválení, a tím povýšení na legislativu platnou a účinnou. Tato kapitola mapuje stav evropské legislativy platný v říjnu 2023.

Zároveň je třeba upozornit, že ambicí této práce není podat vyčerpávající výčet všech pramenů, jež mohou být pro technologie založené na umělé inteligenci významné. Jak už bylo vysvětleno v kapitole 2. Termín umělé inteligence, lze umělou inteligenci využít u širokého spektra technologií. Tato rigorózní práce se však omezuje pouze na konverzační aplikace založené na umělé inteligenci, a především na aspekt ochrany údajů. Právě z této perspektivy byl vytvořen přehled pramenů. Nenajdeme v něm tak např. právní úpravu autonomních automobilů[46], protože ta je pro zmíněné aplikace irelevantní.

Současně je nutno podotknout, že i přes vymezenou perspektivu je pramenů, které stojí za zmínku, nemálo. Tím, že přehled legislativy nemá být těžištěm práce, jsou některé předpisy uvedeny pouze okrajově, a stěžejním právním úpravám je naopak věnována větší pozornost.

3. 1 Rozdělení pramenů Evropské unie

Právo Evropské unie (dále také „unijní právo“) se rozpadá na dvě základní větve, a to na primární právo a sekundární. Primární právo zahrnuje zakládací smlouvy v původním i revidovaném znění, Listinu základních práv Evropské unie, rozpočtové

[46] např. A common EU approach to liability rules and insurance for connected and autonomous vehicles z roku 2018 zmíněný v KOLAŘÍKOVÁ, Linda, HORÁK, Filip. *Umělá inteligence & právo*. Praha: Wolters Kluwer ČR. 2020, 41. ISBN 9788075987839.

smlouvy a přístupové smlouvy, na jejichž základě se evropské společenství rozrostlo o nové členské státy.[47]

Sekundární právo tvoří právní akty, jejichž existenci primární právo předpokládá. Jedná se o nařízení, směrnice, rozhodnutí, doporučení a stanoviska. Nařízení plní úlohu normativního právního aktu, který je stejně jako zákon bezprostředně obecně závazný pro všechny členské státy a jejich občany. K nařízení se Evropská unie přiklání tehdy, kdy je třeba danou oblast jednotně regulovat napříč všemi členskými státy.[48]

Směrnice naopak umožňuje členským státům upravit si danou materii samostatně za předpokladu, že budou respektovat minimální standardy vytyčené onou směrnicí. Závazek plynoucí ze směrnice tak směřuje pouze vůči členským státům EU, nikoliv občanům, protože je právě na těchto státech směrnici tzv. transponovat. Tento akt na rozdíl od unifikujícího nařízení slouží „pouhé" harmonizaci vnitrostátních právních řádů členských států.[49]

Rozhodnutí dělíme na normativní a individuální podle toho, pro koho je závazné. Normativní rozhodnutí, kterým může být například schválena mezinárodní smlouva mezi EU a třetí stranou, je stejně jako nařízení závazné pro všechny, zatímco individuální rozhodnutí se vztahuje pouze na okruh subjektů, jichž se rozhodnutí týká. Doporučení a stanoviska orgánů EU sice nejsou oficiálně právně závazná a vynutitelná, ale i přesto by měla být orgány EU a členskými státy respektována.[50] Do skupiny nezávazných aktů spadají vedle doporučení a stanovisek také usnesení Evropského parlamentu a sdělení Evropské komise nebo třeba níže zmíněné Etické pokyny pro zajištění důvěryhodnosti umělé inteligence, jež vypracovala Odborná skupina Evropské komise.

[47] TOMÁŠEK, Michal, TÝČ, Vladimír. *Právo Evropské unie*. 1. vydání Praha: Leges. 2013. 100-103. ISBN 9788087576533
[48] TOMÁŠEK, Michal, TÝČ, Vladimír. *Právo Evropské unie*. 1. vydání Praha: Leges. 2013. 107-109. ISBN 9788087576533
[49] TOMÁŠEK, Michal, TÝČ, Vladimír. *Právo Evropské unie*. 1. vydání Praha: Leges. 2013. 109-110. ISBN 9788087576533
[50] TOMÁŠEK, Michal, TÝČ, Vladimír. *Právo Evropské unie*. 1. vydání Praha: Leges. 2013. 111. ISBN 9788087576533

Kromě legislativních aktů a nezávazných pramenů rozlišujeme ještě tzv. nelegislativní akty. Rozdělení aktů na legislativní a nelegislativní přinesla Lisabonská smlouva z roku 2009. Nelegislativní akty neprošly řádným či zvláštním legislativním procesem jako nařízení a směrnice. Mezi nelegislativní akty se řadí akty v přenesené působnosti a prováděcí akty. Typickým příkladem prvního uvedeného nelegislativního aktu je nařízení Komise v přenesené působnosti. Tím Komise reaguje na legislativní akt (nařízení, nebo směrnice) tak, že ho doplňuje, případně ho mění v částech, které nejsou pro daný legislativní akt stěžejní. Naopak prováděcí akty specifikuji podmínky, za jakých má být legislativní akt aplikován.[51]

3. 2 Nařízení, směrnice a jejich návrhy

Tato kapitola představuje nařízení a směrnice, které se dotýkají přímo umělé inteligence, nebo upravují oblasti, jež s využíváním umělé inteligence úzce souvisí, jako je třeba ochrana osobních údajů. Vedle „nařízení" a „směrnice" se v názvech předpisů objevuje také „akt" (například Akt o umělé inteligenci), ale fakticky se nejedná o nic jiného než nařízení.

V této kapitole jsou uvedeny také návrhy těchto závazných předpisů. Přestože jsme si vědomi skutečnosti, že se tyto návrhy mohou v čase měnit, neboť jsou stále v legislativním procesu, věnujeme jim nemalou pozornost, poněvadž jsou v oblasti umělé inteligence stěžejní a do budoucna se má jednat o hlavní pilíře unijní úpravy v této oblasti.

3. 2. 1 Obecné nařízení o ochraně osobních údajů (GDPR)

Vzhledem k tomu, že se práce věnuje ochraně dat v kontextu technologií založených na umělé inteligenci, nelze opomenout stěžejní evropský předpis v oblasti ochrany osobních údajů, a to *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)* (dále také „GDPR"), jež nabylo účinnosti dne 25. května 2018. Vzhledem k jeho rozsahu se omezíme pouze na dvě záležitosti, a to na ustanovení

[51] TOMÁŠEK, Michal, TÝČ, Vladimír. *Právo Evropské unie*. 1. vydání Praha: Leges. 2013. 111-112. ISBN 9788087576533

relevantní zaprvé pro tvůrce konverzačních hlasových asistentů a konverzačních aplikací založených na principech umělé inteligence a zadruhé pro uživatele těchto asistentů a aplikací.

Osobními údaji se dle čl. 4 bodu 1 GDPR rozumí „*veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby*“. Uživatel námi výše vymezených hlasových asistentů a aplikaci je tak z hlediska tohoto ustanovení *subjektem údajů*. Detailněji se definici osobních údajů věnujeme v kapitole 4. 1. 2. 1 Čtyři elementy osobních údajů.

Tvůrce asistenta/aplikace naopak naplňuje znaky *správce*, případně i *zpracovatele*, přičemž *zpracováním* je podle čl. 4 bodu 2 GDPR myšlena „*jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení*“. Termín *správce* je v čl. 4 bodě 7 GDPR definován jako „*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení*“.

3. 2. 1. 1 Shrnutí GDPR z perspektivy tvůrce a uživatele konverzačního asistenta a konverzační aplikace

Není pochyb, že se na poskytovatele služeb hlasového asistenta či konverzační aplikace vztahují zásady zpracování osobních údajů uvedené v čl. 5 GDPR. Dodržování těchto zásad má vést k tomu, že budou zpracovány pouze nezbytné osobní údaje, a to jen k jasně vytyčenému účelu, a údaje budou uloženy pouze po nezbytnou dobu. Zpracování musí být samozřejmě zákonné, což upravuje hned následující čl. 6 GDPR.

Z naší perspektivy je relevantní skutečností, která zajišťuje zákonnost zpracování, souhlas uživatele, resp. souhlas subjektu údajů, jenž musí naplňovat v tomto a následujícím článku vymezené parametry. Souhlasu se zpracováním údajů a dalším zásadám zpracování se podrobněji věnujeme v kapitole 4. 2 Vybrané zásady zpracování osobních údajů.

Dále je tvůrce aplikace/asistenta povinen uživateli poskytnout informace, které o uživateli sbírá, což podrobněji rozvádí čl. 12 GDPR a následující. S tím úzce souvisí práva subjektu údajů stanovená čl. 15-18 GDPR (viz kapitola 4. 3 Vybraná práva subjektu údajů), konkrétně právo na přístup k osobním údajům, jejich opravu, výmaz (známé také pod populárnějším názvem „právo být zapomenut“) či omezení zpracování. Subjekt údajů má také podle čl. 77 a 79 GDPR právo podat stížnost u dozorového úřadu nebo se domáhat soudní ochrany v případě, že se domnívá, že zpracování jeho osobních údajů nebylo v souladu s GDPR. S tím souvisí také právo na náhradu vzniklé újmy (ať už hmotné či nehmotné) vůči správci/zpracovateli upravené v čl. 82 GDPR.

Ruku v ruce se zásadami zpracování osobních údajů zmíněnými výše jsou povinnosti správce či zpracovatele stanovené v čl. 24 a následujících. Jedná se zejména o přijetí technických a organizačních opatření, která podpoří zabezpečenost osobních údajů a jejich zákonné zpracování. K takovým nástrojům se vedle povinnosti vést záznamy o činnosti zpracování řadí také např. pseudonymizace, která zajišťuje prostřednictvím systematického oddělení údajů nemožnost přiřadit zpracovávané údaje ke konkrétní osobě a které je společně s anonymizací věnován prostor v kapitole 4. 1. 2. 3 Způsob zpracování osobních údajů.

Za zamyšlení stojí čl. 9 GDPR, který a priori zakazuje zpracování osobních údajů vypovídajících např. o rasovém původu, politickém přesvědčení či zdravotním stavu (tzv. *osobní údaje zvláštní kategorie*). Tento zákaz může být podle čl. 9 odst. 2 za určitých podmínek prolomen, např. udělením speciálního souhlasu se zpracováním právě těchto údajů. Poskytovatelé konverzační aplikace / hlasového asistenta si však mohou klást otázku, jak postupovat v případě, kdy jim uživatel (subjekt údajů) tyto informace sdělí sám bez vyzvání. Představme si, že máme konverzační aplikaci, která funguje na základě hlasového vstupu uživatele. Poskytovatel takové aplikace nemá jak ovlivnit, co mu uživatel při užívání aplikace sdělí. Uživatel může poskytovateli

dobrovolně sdělit i osobní údaje zvláštní kategorie, aniž by k tomu byl poskytovatelem vyzván. Je třeba pak tyto údaje považovat také za osobní údaje zvláštní kategorie a příslušně s nimi nakládat? Ustanovení čl. 9 odst. 2 písm. e) GDPR sice praví, že je zákaz zpracování takových údajů prolomen, jestliže se zpracování „*týká osobních údajů zjevně zveřejněných subjektem údajů*“. Lze ale náš ilustrativní případ podřadit pod zveřejnění? To je velice nejisté.

Na závěr zmiňme Směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) (dále v tomto odstavci také jen „směrnice“), která je pro téma této práce také relevantní. Vztah mezi směrnicí a GDPR je upraven v čl. 95 GDPR, přičemž tento článek konstatuje, že GDPR osobám ve vztahu ke službám definovaným v této směrnici neukládá další povinnosti v oblasti zpracování v tom rozsahu, v němž tyto povinnosti ukládá směrnice. Nadto uvádíme, že dle bodu 173 recitálu GDPR by bylo záhodno onu směrnici v souvislosti s přijetím GDPR revidovat a v souladu s tím novelizovat. K takové novelizaci však zatím nedošlo.

3. 2. 2 Nařízení o rámci pro volný tok neosobních údajů v EU

Předmětná rigorózní práce se sice zaměřuje primárně na osobní údaje, ovšem neopomíjí ani údaje neosobní. Neosobní údaje upravuje na evropské úrovni *Nařízení Evropského parlamentu a Rady (EU) 2018/1807 ze dne 14. listopadu 2018 o rámci pro volný tok neosobních údajů v Evropské unii* (dále také „nařízení o rámci pro volný tok neosobních údajů v EU“), které je účinné od roku 2019.

Hlavní myšlenkou nařízení o rámci pro volný tok neosobních údajů v EU je, jak už název napovídá, garantovat volný pohyb neosobních údajů v rámci Unie s výjimkou omezení, které je ospravedlněno veřejnou bezpečností.

Význam nařízení z hlediska tématu rigorózní práce spočívá především ve vymezení neosobních údajů a postupu v případě, kdy lze osobní údaje od neosobních oddělit jen stěží. Údaje jsou v tomto nařízení definované čl. 3 bodem 1 tohoto nařízení jako „*údaje jiné než osobní údaje ve smyslu čl. 4 bodu 1*“ GDPR. Recitál nařízení o rámci pro volný tok neosobních údajů v EU doplňuje tuto stručnou definici o ilustrativní

příklady uvedené v bodě 9 jako např. soubory dat, jež jsou anonymizované a využívané pro analýzu. V našem případě konverzačních aplikací se tak jedná o data, která uživatel sdělí v rámci konverzace, ale nelze je definovat jako osobní údaje (např. pokyn uživatele směrem k asistentovi, jeho koníčky či co měl dnes k obědu).

Jestliže jsou neosobní údaje s osobními údaji neoddělitelně propojeny, užije se v souladu s čl. 2 odst. 2 předmětného nařízení GDPR, nikoliv předmětné nařízení. Pokud tedy v našem ilustrativním případě konverzačních aplikací nelze určitá konverzační data striktně rozdělit na osobní a neosobní údaje, má správce dat povinnost s celým souborem dat nakládat jako s údaji osobními.

3. 2. 3 Návrh Aktu o umělé inteligenci

Akt o umělé inteligenci, celým názvem *Nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie* (dále v této kapitole také „Akt“ či „návrh nařízení“), by měl představovat stěžejní prvek evropské právní úpravy umělé inteligence. Z tohoto důvodu je mu v této práci věnován větší prostor v porovnání s dalšími evropskými předpisy. V době, kdy vzniká tato rigorózní práce, je toto nařízení stále v řádném legislativním procesu a probíhá první čtení, ovšem Rada a Evropský parlament se již shodly na základních bodech.[52]

Tento návrh nařízení, jenž pochází z pera Evropské komise, volně navazuje na Bílou knihu o umělé inteligenci publikovanou dne 19. 2. 2020. Tímto dokumentem si Komise vytyčila dva cíle v oblasti umělé inteligence, a to podporu výzkumu a inovací na jedné straně a důsledná právní pravidla na straně druhé (více viz kapitola 3. 3. 5 Bílá kniha o umělé inteligenci – evropský přístup k excelenci a důvěře).

Akt se soustředí právě na vymezení právních mantinelů, které zajistí důvěryhodnou umělou inteligenci.[53] Tyto mantinely mají zaručit především právní jistotu, bezpečnost systémů umělé inteligence, které jsou k dispozici na trhu Evropské

[52] *AI Act: Parliament and Council Reach Provisional Agreement on World's First AI Rules*. Online. Eucrim. 2024. Dostupné z: https://eucrim.eu/news/ai-act-parliament-and-council-reach-provisional-agreement-on-worlds-first-ai-rules/. [cit. 2024-02-01].
[53] Návrh Nařízení Evropského Parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie – důvodová zpráva. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:52021PC0206. [cit. 2023-08-18].

unie a jejich soulad se základními právy a svobodami. Dále mají napomoci účinnějšímu vymáhání právních předpisů v této oblasti a celkově podpořit jednotný trh pro aplikace založené na umělé inteligenci a zabránit jeho rozštěpení. Dle důvodové zprávy není Aktem dotčeno GDPR, poněvadž ho Akt pouze doplňuje o pravidla určitých systémů umělé inteligence.[54]

Právním základem tohoto aktu je článek 114 Smlouvy o fungování Evropské unie, podle něhož má Akt za úkol harmonizovat právní předpisy členských států, a tím podpořit vnitřní trh.[55] Návrh se rozpadá do celkem dvanácti hlav a zahrnuje devět příloh.

3. 2. 3. 1 Stěžejní definice Návrhu Aktu o umělé inteligenci

Hlava I vymezuje vedle toho, co návrh nařízení upravuje, také základní definice a pravidla, jimiž se má řídit uvádění systémů umělé inteligence na evropský trh a jejich užívání.

Mimo jiné je v této hlavě, konkrétně v čl. 3 bodě 1 Aktu, definován stěžejní termín systém umělé inteligence, kterým se rozumí „*software, který je vyvinut pomocí jedné nebo více technik a přístupů uvedených v příloze I a který může pro danou sadu cílů definovaných člověkem generovat výstupy, jako je například obsah, predikce, doporučení nebo rozhodnutí ovlivňující prostředí, s nimiž komunikují*“. Příloha I zmíněná v definici tak doplňuje Hlavu I o seznam technik a přístupů umělé inteligence. V případě konverzační aplikace založené na umělé inteligenci se tak bude jednat především o přístup uvedený pod písmenem a), tzn. „*přístupy strojového učení, včetně učení s učitelem, bez učitele a posilovaného učení, používající celou řadu metod, včetně hlubokého učení*“. Článek 4 Aktu umožňuje přílohu I aktualizovat, aby ideálně vždy odrážela vývoj technologií a trhu. Pravomoc měnit přílohu I přísluší Evropské komisi.

V následujícím bodě, tzn. v čl. 3 bodě 2 Aktu je vymezena osoba poskytovatele systému umělé inteligence jako „*fyzická nebo právnická osoba, orgán veřejné moci,*

[54] Návrh Nařízení Evropského Parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie – důvodová zpráva. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:52021PC0206. [cit. 2023-08-18].
[55] Návrh Nařízení Evropského Parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie – důvodová zpráva. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:52021PC0206. [cit. 2023-08-18].

agentura nebo jiný subjekt, které vyvíjí nebo nechávají vyvíjet systém UI za účelem jeho uvedení na trh nebo do provozu pod svým vlastním jménem nebo ochrannou známkou, ať už za úplatu, nebo zdarma“, která je zároveň dle čl. 1 bodu 8 provozovatelem.

3. 2. 3. 2 Kategorizace systémů umělé inteligence

Hlava II definuje postupy, které jsou v oblasti umělé inteligence zakázány. Právě z této části návrhu nařízení implicitně vyplývá, že systémy umělé inteligence jsou rozděleny do více kategorií, které se od sebe liší mírou rizika a pravidly pro fungování systémů. Dohromady se jedná o tři kategorie – nepřijatelně rizikové systémy, vysoce rizikové systémy a systémy s nízkým či minimálním rizikem. Tato hlava se věnuje pouze první zmíněné skupině a tvoří ji jeden jediný článek, a to článek 5 Aktu.

Do kategorie nepřijatelně rizikových systémů se řadí celkově čtyři druhy systémů. Obecně lze říci, že se jedná o systémy, jejichž použití by mohlo způsobit fyzickým osobám psychickou či fyzickou újmu nebo by mohlo vést k diskriminaci osob. Také je dle čl. 5 odst. 1 písm. d) Aktu v zásadě zakázáno užití systémů, které využívají „*biometrickou identifikaci v reálném čase na veřejně přístupných místech k prosazování práva*“. Výjimku z této zásady tvoří čtyři případy, jež jsou taxativně vymezeny v tomtéž odstavci.

3. 2. 3. 3 Vysoce rizikové systémy umělé inteligence

Hlava III se zabývá druhou kategorií systémů umělé inteligence, a sice vysoce rizikovými systémy, pro něž stanovuje speciální pravidla, která musí tyto systémy (resp. jejich poskytovatele) splnit, aby mohly být uvedeny na evropský trh. Tím, že se jedná o skupinu systémů, která je nejvíce regulována, jedná se suverénně o nejobsáhlejší hlavu Aktu. Konkrétně zahrnuje více než polovinu článků celého návrhu nařízení, a proto této hlavě věnujeme pozornost, přestože do kategorie vysoce rizikových systémů konverzační aplikace či hlasový asistent jistě nespadají.

Hned první článek Hlavy III Aktu, čl. 6 Aktu, vymezuje, co vše spadá do této kategorie. Systém umělé inteligence je klasifikován jako vysoce rizikový, jestliže splňuje obě podmínky stanovené čl. 6 odst. 1 Aktu, nebo je uveden v příloze III Aktu, k jejíž aktualizaci je stejně jako v případě Přílohy I zmocněna Evropská komise.

Kapitola 2 této hlavy uvádí požadavky, jež míří na vysoce rizikové systémy. Vedle tzv. systému řízení rizik, který spočívá v konstantní analýze rizik systémů, je třeba zmínit článek 10 Aktu, jenž se dle svého názvu věnuje datům a jejich správě. Je ovšem nezbytné upozornit na to, že se článek nevěnuje vstupním datům, jimiž jsou dle čl. 3 bodu 32 Aktu „*data poskytovaná systému UI nebo přímo získaná tímto systémem, na jejichž základě tento systém vytváří výstup*“. Obecně lze konstatovat, že Akt vstupním datům věnuje minimální pozornost. Onen čl. 10 Aktu se tak omezuje pouze na tréninková data, která slouží k trénování systému umělé inteligence, testovací data, jež slouží k vyhodnocení funkčnosti systému, a tzv. data pro ověření platnosti[56]. Článek 10 odst. 5 Aktu umožňuje za daných podmínek využít v rámci výše zmíněných druhů dat také data spadající do zvláštní kategorie osobních údajů dle čl. 9 odst. 1 GDPR. Zbývající články této kapitoly upravují mimo jiné povinnost informovanosti uživatele a lidský dohled.

Další kapitoly Hlavy III zavádějí právní imperativy směřující vůči poskytovatelům systémů umělé inteligence, jejich distributorům, uživatelům a oznamujícím orgánům. Pro ilustraci můžeme uvést čl. 17 Aktu, který zavádí minimální požadavky na systém řízení kvality.

3. 2. 3. 4 Další části Návrhu Aktu o umělé inteligenci

Hlava IV představuje systémy, na něž se vztahuje zvláštní povinnost transparence. Jsou to systémy, které komunikují s lidmi, zpracovávají biometrické údaje, nebo generují obsah či s ním určitým způsobem manipulují (tzv. *deep fakes*). Všechny zmíněné systémy mají společný atribut, jímž je právě určité riziko manipulace. Z tohoto důvodu podléhají povinnosti transparence, jež spočívá v informovanosti uživatele. Je tak povinností poskytovatele systému umělé inteligence, aby uživateli srozumitelně zprostředkoval informaci, že např. interaguje se systémem umělé inteligence nebo že k rozpoznání uživatelových emocí je využita umělá inteligence.

Výše uvedená povinnost transparence je relevantní pro náš ilustrační příklad konverzačních aplikací, protože ty jsou zpravidla založeny na generování obsahu a

[56] Čl. 3 bod 30 Aktu uvádí, že „*data používaná pro vyhodnocení trénovaného systému UI a pro vyladění jeho parametrů, které se nelze naučit, a jeho procesu učení, mimo jiné s cílem zabránit přeučení; přičemž soubor dat pro ověřování platnosti může být samostatný soubor dat nebo součást souboru tréninkových dat, ať už jako pevné, nebo variabilní rozdělení*“

často také na mechanismu rozpoznání emocí. Podle toho, jaká emoce je rozpoznána, je uživateli prezentován konkrétní obsah.

Hlava V se zaměřuje na inovace. Vedle sníženého stupně regulace pro začínající, malé a střední podniky je zde stanovena podpora testování inovací v kontrolovaném prostředí (tzv. „*regulační pískoviště umělé inteligence*“), přičemž v případě inovativního systému, jenž zpracovává osobní údaje, je na členských státech, aby do takového prostředí integrovaly také příslušný vnitrostátní orgán pro ochranu údajů. Článek 54 Aktu uvádí podmínky pro zpracování osobních údajů v rámci regulačního pískoviště.

Na základě Hlavy VI vznikne nový institut EU. Evropská rada pro umělou inteligenci bude mít na starost vedle poradního hlasu především koordinaci dozorových úřadů jednotlivých členských států a Evropské komise v oblasti umělé inteligence. Ruku v ruce s tím vzniká povinnost členských států Unie zřídit takové dozorové orgány na vnitrostátní úrovni. Členem Evropské rady pro umělou inteligenci je vedle zástupců vnitrostátních dozorových orgánů také evropský inspektor ochrany údajů.

Hlava VII upravuje svým jediným článkem 60 Aktu unijní databázi vysoce rizikových systémů, kterou bude spravovat Evropská komise.

Hlava VIII se soustředí na monitorování systémů umělé inteligence na trhu, dozor nad trhem a informovanost. V souvislosti s tím ukládá poskytovatelům systémů oznamovací a monitorovací povinnosti a dozorovým orgánům povinnosti spočívající v kontrole vysoce rizikových systémů.

Hlava IX se věnuje kodexu chování. Ten má za cíl podpořit poskytovatele systémů umělé inteligence, jež nespadají do kategorií nepřijatelně či vysoce rizikových systémů, aby se i přesto snažili o dodržování pravidel platných pro vysoce rizikové systémy. Tvorba a obsah kodexu jsou zcela v gesci jednotlivých poskytovatelů a poskytovatelé si do něj mohou zahrnout i další dobrovolné závazky, jakými může například být udržitelnost životního prostředí. Tím, že se kodexy zakládají čistě na bázi dobrovolnosti, je otázkou, nakolik by kodexy do praxe pronikly.

Hlava X uvádí maximální výše sankcí za jednotlivá porušení Aktu. Také akcentuje povinnost vnitrostátních orgánů, aby zachovaly důvěrnost informací a údajů,

k nimž získají přístup během výkonu své činnosti. Hlava XI obsahuje přenesení pravomoci a Hlava XII uzavírá Akt závěrečnými ustanoveními.

3. 2. 3. 5 Shrnutí Návrhu Aktu o umělé inteligenci z perspektivy ochrany dat

Je třeba konstatovat, že z hlediska ochrany údajů Akt o umělé inteligenci příliš nového nepřináší, přestože se jedná o stěžejní evropský pramen práva v oblasti umělé inteligence, jejíž úprava se dosud omezovala převážně na soft law. Například vstupním datům se Akt věnuje velice okrajově. Jak uvádí samotný Akt v bodě 41 recitálu, nemá být toto nařízení chápáno jako „*právní základ pro zpracování osobních údajů, případně včetně zvláštních kategorií osobních údajů*“, přičemž z obsahu Aktu není zcela zřejmé, jaké všechny předpisy jsou pro ochranu dat v souvislosti se systémy umělé inteligence relevantní. Zvláštní pravidla v oblasti ochrany dat poskytuje pouze ve dvou případech. Prvním jsou systémy využívající biometrickou identifikaci a druhým testování systémů ve veřejném zájmu na tzv. regulačních pískovištích.

Jestliže si vezmeme jako demonstrativní příklad systému umělé inteligence konverzační aplikaci či virtuálního asistenta, lze konstatovat, že takové systémy spadají do kategorie nízkorizikových systémů, poněvadž nenaplňují podmínky stanovené v čl. 6 Aktu ani nejsou uvedené v příloze č. III Aktu. Vztahují se na ně tak vedle obecné Hlavy I také Hlava IV s výše zmíněnou povinností transparence, Hlava V o inovacích, kapitola III Hlavy osmé, jež se věnuje prosazování práva, a Hlava IX s kodexem chování.

3. 2. 4 Návrh Aktu o správě dat

Dalším pramenem práva, který je v době psaní této rigorózní práce stále v legislativním procesu, je *Návrh Nařízení Evropského parlamentu a Rady o evropské správě dat (akt o správě dat)* (dále také „návrh Aktu o správě dat“). Tento připravovaný akt je dle důvodové zprávy navrhovaného Aktu o umělé inteligenci jedním z pilířů podpory inovací, jež se opírají o umělou inteligenci.[57]

[57] Návrh Nařízení Evropského Parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie – důvodová zpráva. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:52021PC0206. [cit. 2023-08-20].

Návrh tohoto aktu vychází z Evropské strategie pro data z února roku 2020[58], mezi jehož hlavní pilíře se řadí podpora dostupnosti a sdílení dat v rámci Evropské unie, což v konečném důsledku podporuje vznik evropského jednotného trhu s daty. Jak už samotný název aktu napovídá, neomezuje se dokument pouze na určitou kategorii dat, ale naopak se uplatní jak na údaje osobní, tak neosobní povahy. V případě sféry osobních údajů doplňuje akt o správě dat GDPR a směrnici o soukromí a elektronických službách. Oba prameny jsou detailněji rozpracovány v samostatných kapitolách této práce. Tento návrh nařízení souvisí také se zásadou pro „FAIR" data. Dle této zásady by měla být data dohledatelná (*findable*), přístupná (*accesible*), interoperabilní (*interoperable*) a opakovaně použitelná (*reusable*). Právním základem je stejně jako v případě Aktu o umělé inteligenci čl. 114 Smlouvy o fungování Evropské unie.[59]

Jak je nastíněno výše, cílem tohoto připravovaného právního předpisu je evropský jednotný trh s daty pocházejícími ze soukromého i veřejného sektoru. Přestože budou data sdílena a dále využívána, osoby soukromého práva by dle důvodové zprávy Aktu o správě dat nad nimi neměly ztratit kontrolu. Jednotný trh s daty by také mohl pozitivně přispět ve světě vývoje technologií a inovací, na což mimo jiné odkazuje recitál návrhu aktu. Sdílení dat by tak mohlo významně posílit konkurenceschopnost Unie v globálním měřítku.[60] Co se týče vztahu mezi tímto návrhem a nařízením GDPR, není dle bodu 3 recitálu tohoto návrhu nijak nařízení GDPR dotčeno.

3. 2. 4. 1 Relevantní definice Návrhu Aktu o správě dat

Návrh Aktu o správě dat se rozpadá do osmi kapitol. Kapitola I obligatorně stanovuje, co nařízení upravuje, a definuje termíny v něm uvedené. Zmiňme jen ty stěžejní s významem pro téma této práce.

Daty se dle čl. 2 bodu 1 návrhu Aktu o správě dat rozumí „*veškeré digitální záznamy jednání, skutečností nebo informací a všechny soubory takových jednání,*

[58] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Evropská strategie pro data COM/2020/66 final
[59] Návrh Nařízení Evropského Parlamentu a Rady o evropské správě dat (akt o správě dat) – důvodová zpráva. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020PC0767. [cit. 2023-08-20].
[60] Návrh Nařízení Evropského Parlamentu a Rady o evropské správě dat (akt o správě dat) – důvodová zpráva. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020PC0767. [cit. 2023-08-20].

skutečností nebo informací, včetně v podobě zvukové, vizuální nebo audiovizuální nahrávky“.

V čl. 2 bodě 2 návrhu je definováno opakované použití jako „*použití dat v držení subjektů veřejného sektoru fyzickými nebo právnickými osobami pro komerční nebo nekomerční účely jiné, než je původní účel, v rámci veřejného úkolu, pro který byla data vytvořena, kromě výměny dat mezi subjekty veřejného sektoru výhradně při plnění jejich veřejných úkolů*“. Z definice vyplývá, že se institut opakovaného použití aplikuje pouze na data, jež pochází z veřejného sektoru, nikoliv soukromého.

V případě vymezení neosobních údajů se návrh Aktu o správě dat omezuje pouze na „*údaje jiné než osobní údaje ve smyslu čl. 4 odst. 1*“ nařízení GDPR, což je definice, kterou zakotvuje již dříve zmíněné nařízení o rámci pro volný tok neosobních údajů v EU (více viz kapitola 3. 2. 2 Nařízení o rámci pro volný tok neosobních údajů v EU).

Jako poslední termín, jenž návrh Aktu o správě dat přináší, uveďme metadata, která jsou v čl. 2 bodě 4 návrhu vysvětlena jako „*shromážděná data o jakékoli činnosti fyzické nebo právnické osoby za účelem poskytování služby sdílení dat, včetně údajů o datu a čase a geolokačních údajů, doby trvání činnosti, kontaktů s jinými fyzickými či právnickými osobami, které navázala osoba využívající službu*“. V případě konverzační aplikace půjde typicky právě o časový údaj, kdy konverzace proběhla, či o informace o geografické poloze uživatele, kterou mobilní aplikace čerpá z dostupných dat mobilního zařízení.

3. 2. 4. 2 Opakované použití dat

Problematiku opakovaného použití určité kategorie dat, která je představena čl. 3 odst. 1 návrhu Aktu o správě dat, upravuje kapitola II Návrhu Aktu. Jedná se o data, která jsou ve veřejném sektoru chráněna a na něž se nevztahuje již zmíněná směrnice o otevřených datech.[61] Akt o správě dat je tak vůči této směrnici v tomto ohledu *lex specialis*.

[61] Návrh Nařízení Evropského Parlamentu a Rady o evropské správě dat (akt o správě dat) – důvodová zpráva. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020PC0767. [cit. 2023-08-20].

Přestože se rigorózní práce zaměřuje na aplikace založené na umělé inteligenci, které jsou spjaty primárně se soukromým sektorem, je část návrhu aktu věnovaná veřejné sféře pro nás relevantní. V závazné části návrhu sice k tomu příliš nenalezneme, ale recitál uvádí podnět podstatný i pro aplikace a výzkum vedený provozovateli takových aplikací. V bodě 5 recitálu je prezentována myšlenka, že by z dat, k jejichž vytvoření přispěly prostředky z veřejných rozpočtů, měla těžit ideálně celá společnost. Proto by měla být sdílena. V tomto místě se však naráží na problém. I data ve veřejných databázích obsahují údaje, jež podléhají ochraně, a nejsou tím pádem zpřístupněna ani k výzkumným účelům. Vedle osobních údajů to může být například obchodní tajemství či práva duševního vlastnictví. Jaké je tedy řešení? Bod 5 recitálu návrhu Aktu o správě dat uvádí, že je třeba u zpřístupnění potenciálně citlivých dat dbát na „*určité technické a právní procesní požadavky*“, které zaručí ochranu práv dotčených osob k takovým datům. I když je tak nastíněna možnost, že by za určitých podmínek mohla být data z veřejného sektoru obecně sdílena, není tady bohužel detailněji rozvedeno, v čem „*technické a právní procesní požadavky*“ spočívají a jakými prostředky lze splnění požadavků dosáhnout. Lze předpokládat, že obdobné požadavky budou platit i pro soukromý sektor, i když k jejich splnění povedou například jiné nástroje.

Je zde také prostor pro výklad, že prostředky, kterými lze splnit „*určité technické a právní procesní prostředky*“, jsou metody zmíněné v bodě 6 recitálu návrhu aktu o správě dat, ovšem není to zcela jednoznačné. V bodě 6 recitálu návrhu aktu o správě dat jsou uvedeny metody „*anonymizace, pseudonymizace, diferenciální soukromí, generalizace nebo suprese a randomizace*“ bez bližšího vysvětlení. Každá z těchto metod by měla dle zmíněného bodu recitálu zajistit „*bezpečné opakované použití osobních údajů a důvěrných údajů obchodní povahy pro účely výzkumu a inovací a pro statistické účely*“. Recitál se tak znovu omezuje pouze na výzkumné účely a nenavazuje na celoplošné užití dat napříč společnosti vyjádřené v bodě 5 recitálu.

3. 2. 4. 3 Další obsah Návrhu Aktu o správě dat

Ústředním tématem kapitoly III je sdílení údajů a jeho pravidla. Klíčovým principem je v tomto případě oznamovací postup, na jehož dodržování mají dohlížet vnitrostátní orgány. Předmětná kapitola zahrnuje také podmínky pro poskytování služeb

sdílení dat, které mají mimo jiné za cíl posílit důvěryhodnost sdílení a spolupráci mezi jednotlivými stranami.[62]

Kapitola IV otvírá dveře tzv. datovému altruismu, který spočívá v dobrovolném sdílení dat. Skutečnost, že je právnická osoba registrovaná jako „*organizace pro datový altruismus uznaná v Unii*“, znamená, že pracuje s daty, které jí poskytly přímo právnické či fyzické osoby na základě souhlasu dle nařízení GDPR. Taková organizace je pak fyzickými a právnickými osobami vnímána jako důvěryhodná, jelikož pro registraci musí splnit určité Aktem stanovené podmínky a vztahují se na ni povinnosti jako třeba povinnost transparence.

Kapitola V zavádí povinnosti příslušných orgánů zapojených do procesu sdílení dat. V rámci kapitoly VI je položen základ pro Evropský sbor pro datové inovace, jenž má vedle poradního hlasu Komise plnit úlohu koordinátora spolupráce příslušných orgánů členských států. Kapitoly VII a VIII se věnují přenesení pravomoci a přechodným a závěrečným ustanovením.

3. 2. 4. 4 Shrnutí Návrhu Aktu o správě dat z perspektivy ochrany dat

Akt by měl poskytnout ochranu určité kategorii údajů především s ohledem na sdílení dat. Přestože se soustředí na veřejný sektor, jehož subjekty mohou data poskytnout k opakovanému použití vymezených dat, jsou zde pasáže relevantní i pro soukromoprávní subjekty, jako je např. datový altruismus.

Bohužel Návrh Aktu o správě dat obsahuje i nejasností či nekonkrétností, a to převážně v recitálu, který má přitom sloužit jako interpretační berlička k závazné části předpisu. Např. v souvislosti s neosobními údaji je v bodě 18 recitálu tohoto návrhu uvedeno, že k odvrácení neoprávněného přístupu k neosobním údajům je třeba, aby osoby přijaly „*veškerá přiměřená opatření, která brání v přístupu k systémům, v nichž jsou uloženy neosobní údaje, včetně šifrování dat nebo firemních politik*“. Ovšem zmíněná opatření nejsou nikde detailněji rozvedena. To samé platí pro hned následující bod 19 recitálu, který pracuje s pojmem „*vysoce citlivé neosobní údaje*“, aniž by bylo vysvětleno, co termín znamená, případně odkázáno na jeho vysvětlení v rámci jiného

[62] Návrh Nařízení Evropského Parlamentu a Rady o evropské správě dat (akt o správě dat) – důvodová zpráva. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020PC0767. [cit. 2023-08-21].

právního předpisu. Recitál tak zakládá další nejasnosti v podobě komentování normativního obsahu nejednoznačnými pojmy.

Další nejasnost se týká například faktu, zda a případně za jakých okolností se aplikuje nařízení GDPR. Působnosti aktu se věnuje pouze čl. 1 aktu, který se v druhém odstavci omezuje pouze na obecné konstatování, že aktem „*nejsou dotčena zvláštní ustanovení v jiných právních aktech Unie týkající se přístupu k určitým kategoriím dat či jejich opakovaného použití nebo požadavky související se zpracováváním osobních či neosobních údajů*“. Zmínku o vztahu GDPR a Aktu v jeho závazné části nenalezneme.

Stejně tak není jasné, na jaké osobní údaje se vztahuje směrnice o otevřených datech. Bod 7 recitálu Návrhu Aktu o správě dat uvádí následující: „*Osobní údaje nespadají do oblasti působnosti směrnice (EU) 2019/1024*[63]*, pokud režim přístupu vylučuje či omezuje přístup k takovýmto datům z důvodů ochrany údajů, soukromí a osobnosti jednotlivce, zejména v souladu s pravidly ochrany údajů*“. Otázkou je, co znamená onen *režim přístupu*. Zmíněná směrnice o otevřených datech sice pracuje s termínem „*režim přístupu*“ často v kontextu členských států, ovšem tento termín nedefinuje. Termín není vymezen ani v Návrhu Aktu o správě dat. Na první pohled tak není jisté, zda na náš ilustrativní příklad s konverzačními aplikacemi a asistenty založené na umělé inteligenci směrnice o otevřených datech dopadá, a je tak třeba sledovat její transpozici, či nikoliv. Nedokážeme totiž říci, zda je v tomto případě naplněna podmínka bodu 7 recitálu Aktu, tedy že „*režim přístupu vylučuje či omezuje přístup k takovýmto datům z důvodů ochrany údajů, soukromí a osobnosti jednotlivce, zejména v souladu s pravidly ochrany údajů*“, protože nevíme, co je *režimem přístupu* míněno.

3. 2. 5 Návrh Aktu o datech

Dalším připravovaným legislativním aktem je *Nařízení Evropského parlamentu a Rady o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání (Akt o datech)* (dále jen „Návrh Aktu o datech“)), který je nyní (v srpnu 2023)

[63] Pozn. autorky: Směrnice Evropského parlamentu a Rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru (přepracované znění)

v prvním čtení u Evropského parlamentu.[64] O tomto pramenu se zmiňuje mimo jiné i důvodová zpráva Aktu o správě dat, jemuž se věnujeme v předcházející kapitole. Z oné zprávy vyplývá i zamýšlená materie Aktu o datech. Dle důvodové zprávy Aktu o správě dat totiž má Akt o datech *„udělovat, měnit či rušit významná práva týkající se přístupu k údajům a jejich používání*".[65] Aktu o datech se dotýká také usnesení Evropského parlamentu o evropské strategii ze dne 25. 3. 2021, kde je řečeno, že cílem onoho aktu má být „*větší a spravedlivější sdílení dat*" napříč odvětvími, veřejnou správou a podniky.[66] Podívejme se tak na akt o datech detailněji, abychom posoudili, zda byly tyto předpoklady naplněny.

Návrh Aktu o datech vychází z Evropské strategie pro data z února roku 2020[67] a má napomoci vytvoření jednotného datového trhu stejně jako Akt o správě dat, který doplňuje. Právním základem je i zde čl. 114 Smlouvy o fungování Evropské unie. Podle Evropské komise, jež stojí za Návrhem Aktu, má být cílem Aktu podpora zpřístupnění dat, jejich využití a zužitkování ekonomickými subjekty. Jeho souvislost s umělou inteligencí je vysvětlena v důvodové zprávě Návrhu Aktu. Akt o datech totiž navazuje na průmyslovou strategii, a zabývá se tak systémy umělé inteligence. [68] Ovšem není zcela jasné, zda se toto nařízení bude vztahovat na všechny technologie založené na umělé inteligenci. Toto tematizujeme v následující kapitole, která pokrývá působnost nařízení.

Návrh Aktu o datech se člení do jedenácti kapitol.

3. 2. 5. 1 Definice a působnost Návrhu Aktu o datech z hlediska výrobku

První kapitola definuje předmět úpravy návrhu, působnost a pojmy v návrhu užívané. Na úvod zmiňme čl. 1 odst. 3 Návrhu Aktu, podle něhož se na osobní údaje

[64] Přehled postupu legislativního procesu Aktu o datech. Online. Dostupné z: EUR-Lex - 52022PC0068 - EN - EUR-Lex (europa.eu). [cit. 2023-08-24].
[65] Návrh Nařízení Evropského Parlamentu a Rady o evropské správě dat (akt o správě dat) – důvodová zpráva. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020PC0767. [cit. 2023-08-24].
[66] Návrh Nařízení Evropského Parlamentu a Rady o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání (Akt o datech) – důvodová zpráva. Online. Dostupné z: EUR-Lex - 52022PC0068 - EN - EUR-Lex (europa.eu). [cit. 2023-08-24].
[67] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů – Evropská strategie pro data COM/2020/66 final
[68] Návrh Nařízení Evropského Parlamentu a Rady o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání (Akt o datech) – důvodová zpráva. Online. Dostupné z: EUR-Lex - 52022PC0068 - EN - EUR-Lex (europa.eu). [cit. 2023-08-24].

zpracované v souvislosti s tímto nařízením uplatní zejména GDPR a směrnice o soukromí a elektronických komunikacích[69]. Čl. 2 Návrhu Aktu definuje termíny, z nichž jsou pro naše téma relevantní ty, které vysvětluje čl. 2 Návrhu Aktu o datech v prvních čtyřech bodech. Tentokrát jich zmíníme více v důsledku nejasné působnosti diskutované níže.

Daty se dle čl. 2 bodu 1 Návrhu Aktu rozumí „*veškeré digitální záznamy jednání, skutečností nebo informací a všechny soubory takových jednání, skutečností nebo informací, včetně v podobě zvukové, vizuální nebo audiovizuální nahrávky*". Definice je tak totožná jako v případě Aktu o správě dat, kterému se věnuje předchozí kapitola.

Výrobek je v čl. 2 bodě 2 Návrhu Aktu definován jako „*hmotný movitý předmět, i jako součást nemovitého majetku, který získává, vytváří nebo shromažďuje data o svém použití nebo prostředí, je schopen přenášet data prostřednictvím veřejně dostupné služby elektronických komunikací a jehož hlavní funkcí není uchovávání a zpracování da*t".

Související službu Návrhu Aktu v čl. 2 bodě 3 vymezuje jako digitální službu „*včetně softwaru, která je součástí výrobku nebo je s ním propojena takovým způsobem, že v případě neexistence této služby by výrobek nemohl plnit některé ze svých funkcí*".

Virtuální asistenti jsou v čl. 2 bodě 4 vymezeni jako „*software, který dokáže zpracovávat požadavky, úkoly nebo otázky, a to i na základě zvukových, písemných vstupů, gest nebo pohybů, a na základě těchto požadavků, úkolů nebo otázek poskytuje přístup k vlastním službám a službám třetích stran nebo ovládá vlastní zařízení a zařízení třetích stran*".

Co se týče působnosti, není zcela zřejmé, zda se toto nařízení bude vztahovat na všechny technologie založené na umělé inteligenci, respektive na které technologie se vztahovat bude, a na které už naopak dopadat nebude. Působnost nařízení vymezuje čl. 1 návrhu nařízení v druhém odstavci tak, že se vztahuje na: *„a) výrobce výrobků a poskytovatele souvisejících služeb uvedených na trh v Unii a uživatele těchto výrobků*

[69] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)

nebo služeb; b) držitele dat, kteří zpřístupňují data příjemcům dat v Unii; c) příjemce dat v Unii, kterým jsou data zpřístupněna; d) subjekty veřejného sektoru a orgány, instituce nebo jiné subjekty Unie, které žádají držitele dat o zpřístupnění dat, pokud je to výjimečně zapotřebí pro vykonání úkolu ve veřejném zájmu, a držitele dat, kteří tato data poskytují v reakci na takovou žádost; e) poskytovatele služeb zpracování dat, kteří tyto služby nabízejí zákazníkům v Unii.“

Vezměme si tedy za příklad soukromoprávní právnickou osobu, jež vyvíjí konverzační aplikace, případně virtuální asistenty, využívající principy umělé inteligence. Z této perspektivy je relevantní pouze písm. a) zmíněného odstavce čl. 1 Návrhu Aktu a je třeba si zodpovědět otázku, zda výše vymezená právnická osoba naplňuje definici buď *výrobce výrobků*, nebo *poskytovatele souvisejících služeb*.

Začněme s virtuálním asistentem ovládaným lidským hlasem, kterého jsme se dotkli již v kapitole 2. 4 Podoba umělé inteligence v každodenním životě jako jednoho z elementů tzv. *smart home*. V tomto ilustračním případě tak půjde o fyzický výrobek ve tvaru malého reproduktoru, který je vybaven konverzační aplikací a jehož jediným účelem je vést s uživatelem nezávaznou konverzaci, případně zodpovědět jeho faktické dotazy. V takovém případě se zřejmě bude jednat o „*hmotný movitý předmět (…) který získává, vytváří nebo shromažďuje data o svém použití nebo prostředí, je schopen přenášet data prostřednictvím veřejně dostupné služby elektronických komunikací*“, jak zní první část definice *výrobku* v čl. 2 bodě 2 Návrhu. Co však již činí větší potíže, je poslední část definice, která stanoví, že hlavní funkcí *výrobku* není uchovávání a zpracování dat. Jestliže je jedinou rolí hlasového asistenta vést s uživatelem konverzaci, dalo by se očekávat, že je jednou z jeho hlavních funkcí mimo jiné uchovávání a zpracování dat. Proto se nabízí podřadit tento příklad pod související služby, jež jsou definovány v čl. 2 bodě 2 Návrhu Aktu. Parametry tohoto bodu by měl námi vymezený virtuální asistent naplnit, poněvadž se jedná o software umožňující konverzaci s uživatelem, což představuje jedinou funkci reproduktoru, bez níž by výrobek postrádal smysl. Zůstává otázkou, zda by se nařízení vztahovalo na výrobce fyzického nosiče, tedy reproduktoru, nebo na tvůrce softwaru, tedy poskytovatele souvisejících služeb. Nejspíš půjde o to, kdo má k datům, jež vznikají užíváním *výrobku*/*služby*, přístup.

Dalším naším ilustračním případem jsou virtuální asistenti, kteří také mají podobu malého reproduktoru, ale jejichž jediným účelem není konverzace s uživatelem, nýbrž přijímání pokynů např. v souvislosti se zmíněnou chytrou domácností. Ani v tomto případě není zřejmé, zda není hlavní funkcí takového virtuálního asistenta právě „*uchovávání a zpracování da*t“ vzhledem k tomu, že data pocházející z interakce s uživatelem musejí být dále zpracována, aby se předmětná součást chytré domácnosti zachovala podle uživatelových instrukcí. I v tomto případě je třeba zvažovat, zda případ nespadá spíše pod *související služby*. Tomuto případu se věnuje čl. 7 odst. 2 kapitoly II Návrh Aktu, podle něhož „*[o]dkazy na výrobky nebo související služby v tomto nařízení zahrnují rovněž virtuální asistenty, pokud jsou používáni pro přístup k výrobku či související službě nebo ovládání výrobku či související služby*“. Z toho vyplývá, že virtuální asistent, jímž ovládáme prvky chytré domácnosti, jistě spadá pod čl. 1 odst. 2 návrhu aktu o datech, což je mimo jiné v souladu s bodem 22 recitálu Návrhu Aktu[70].

Třetím a zároveň posledním ilustračním příkladem je mobilní konverzační aplikace, kterou si lze do mobilního telefonu stáhnout v příslušném internetovém obchodě. V prvé řadě je třeba se zamyslet, zda takto vymezená aplikace vůbec naplňuje parametry virtuálního asistenta. Dle našeho přesvědčení aplikace virtuálním asistentem být může, jelikož v souladu s čl. 2 bodu 4 Návrhu Aktu umožňuje aplikace prostřednictvím hlasových, případně psaných inputů člověka přístup k vlastním službám aplikace, kterými mohou být např. seznámení s určitým obsahem, poskytnutí psychologické podpory a vlastně cokoliv, o čem lze vést konverzaci. Co se týče zařazení aplikace pod pojmy *výrobek* či *související* služba, aplikace jistě nenaplňuje definici výrobku, poněvadž není *movitý hmotný předmět*, ani *součást nemovitého majetku*. Naopak by tvůrci aplikace mohli spadat pod termín *poskytovatelé souvisejících služeb*, přičemž by se jednalo o službu, jež je součástí výrobku, jímž by se v této situaci mínil mobilní telefon.

[70] *„(…) Virtuální asistenti mohou fungovat jako jediná brána například v inteligentním domácím prostředí a zaznamenávat značné množství příslušných dat o tom, jak uživatelé interagují s výrobky připojenými k internetu věcí, včetně výrobků vyrobených jinými stranami, a mohou nahradit používání rozhraní poskytovaných výrobcem, jako jsou dotykové obrazovky nebo aplikace pro chytré telefony. Uživatel může chtít tato data zpřístupnit výrobcům, kteří jsou třetími stranami, a umožnit nové inteligentní domácí služby. Na takové virtuální asistenty by se mělo vztahovat právo na přístup k datům stanovené v tomto nařízení (…).*“

Vzhledem k tomu, že otázka působnosti není vůbec jednoduchá, a to především v případě mobilních konverzačních aplikací, podívejme se raději i na další body nezávazného recitálu, jehož úloha tkví právě v nápomoci v případě interpretačních pochybností, abychom se ujistili, že náš výklad obstojí i v jeho světle. Kromě bodu 15 recitálu Návrhu Aktu o datech, který se zabývá omezením platnosti nařízení, zmiňme pro celistvost a dokreslení kontextu také předcházející bod č. 14 recitálu, jenž naopak definuje výrobky, na něž se nařízení vztahuje:

„*(14) Toto nařízení by se mělo vztahovat na fyzické výrobky, které prostřednictvím svých součástí získávají, vytvářejí nebo shromažďují data o své výkonnosti, použití nebo prostředí a které jsou schopny tato data předávat prostřednictvím veřejně dostupné služby elektronických komunikací (často označované jako internet věcí). Služby elektronických komunikací zahrnují pozemní telefonní sítě, televizní kabelové sítě, satelitní sítě a bezdrátové komunikační sítě krátkého dosahu (NFC). Tyto výrobky mohou zahrnovat vozidla, vybavení pro domácnost a spotřební zboží, zdravotnické prostředky nebo zemědělské a průmyslové stroje. Data představují digitalizaci činností a událostí uživatele, a proto by k nim měl mít uživatel přístup, zatímco informace získané nebo odvozené z těchto dat, pokud jsou drženy zákonným způsobem, by neměly být do oblasti působnosti tohoto nařízení zahrnuty. Taková data jsou pro uživatele potenciálně cenná a podporují inovace a rozvoj digitálních a jiných služeb na ochranu životního prostředí, zdraví a oběhového hospodářství, zejména tím, že usnadňují údržbu a opravy dotčených výrobků.*

(15) Toto nařízení by se naopak nemělo vztahovat na některé výrobky, které jsou primárně určeny k zobrazování nebo přehrávání obsahu nebo k zaznamenávání a přenosu obsahu, mimo jiné pro použití on-line službou. Mezi takové výrobky patří například osobní počítače, servery, tablety a chytré telefony, fotoaparáty, webové kamery, systémy pro záznam zvuku a textové skenery. K vytváření různých forem obsahu, jako jsou textové dokumenty, zvukové soubory, videosoubory, hry či digitální mapy, vyžadují lidské vstupy“.

V třetí větě bodu 14 recitálu jsou výrobky demonstrativně vymezeny. Mezi nimi nalezneme třeba i vybavení pro domácnosti, které uvádíme jako jeden z našich tří

ilustračních příkladů. Je tedy zřejmé, že na virtuálního asistenta, který slouží pro ovládání zařízení chytré domácnosti (tzn. náš první ilustrační příklad), nařízení dopadá.

Pokud vezmeme v úvahu náš druhý ilustrační příklad (reproduktor, který je vybaven virtuálním asistentem, jehož jedinou úlohou je vést s uživatelem konverzaci), pak můžeme zmínit bod 16 recitálu Návrhu Aktu, podle něhož akt dopadá na výrobky, „*které zahrnují službu nebo jsou s ní propojeny, a to takovým způsobem, že by neexistence služby bránila výrobku v plnění jeho funkcí*“, což významově odpovídá čl. 2 bodu 2 Návrhu Aktu. Ani u druhého ilustračního případu tak není pochyb, že se na něj Návrh Aktu vztahuje.

Zbývá nám tak osvětlit situaci pouze ve spojitosti s mobilní konverzační aplikací, a právě z toho důvodu výše citujeme bod 15 recitálu, podle něhož se nařízení nevztahuje na výrobky typu „*osobní počítače (...) a chytré telefony (...)*“. Proto zřejmě nelze o mobilních konverzačních aplikacích uvažovat ani v kontextu *souvisejících služeb*, které jsou dle definice v čl. 2 bodě 3 nařízení dostupné právě na *výrobku*, protože mobilní aplikace je součástí chytrého telefonu.

Z výše uvedeného tak vyplývá, že stěžejní je nosič neboli *výrobek*, který je vybaven konverzačním softwarem, nikoliv samotný software, což může zapříčinit řadu problémů. Pokud například budu mít konverzační aplikaci, kterou mohu užívat buď v podobě mobilní aplikace, nebo přes fyzický reproduktor jako hlasového asistenta, Návrh Aktu o datech se podle všeho uplatní pouze na hlasového asistenta, nikoliv na mobilní aplikaci, přestože se jedná o tutéž technologii, která je však implementována ve dvou podobách.

Na okraj upozorňujeme na ne zcela zřejmý vztah poslední věty bodu 16 recitálu ke zbytku textu. Zmiňme tak i anglickou verzi tohoto bodu, z níž je patrnější, že se poslední věta citovaného bodu recitálu vztahuje k větě předchozí, a určitým způsobem tak *výrobky*, na něž se nařízení neuplatní, specifikuje: „*In contrast, certain products that are primarily designed to display or play content, or to record and transmit content, amongst others for the use by an online service should not be covered by this Regulation. Such products include, for example, personal computers, servers, tablets and smart phones, cameras, webcams, sound recording systems and text scanners.* ***They***

require *human input to produce various forms of content, such as text documents, sound files, video files, games, digital maps*“. Tato pasáž by mohla být vyložena tak, že příčinou, že se na určité *výrobky* nařízení nevztahuje, je právě to, že vyžadují lidský input, což však nekoresponduje se zbytkem textu nařízení, z něhož plyne, že se nařízení uplatní na hlasové asistenty, k jejichž fungování je rovněž třeba hlasový input člověka. Každopádně situace, kdy není jasné, jaký konkrétní prvek „vyvazuje“ výrobek z působnosti nařízení, je příčinou nejasné působnosti návrhu.

3. 2. 5. 2 Působnost Návrhu Aktu o datech z hlediska dat

Data, na něž se Akt o datech má aplikovat, nejsou v závazné části Návrhu Aktu nijak specifikována kromě toho, že Návrh Aktu dle čl. 1 odst. 1 Návrhu Aktu má upravovat „*zpřístupňování dat vytvořených používáním výrobku nebo související služby*“. Nezbývá nám tak nic jiného než se podívat do nezávazného recitálu.

V tomto ohledu je relevantní pouze již zmíněný bod 22 recitálu, který se věnuje přímo virtuálním asistentům[71]. Podle tohoto bodu recitálu vznikají dvě skupiny dat – data, jež souvisejí s používáním výrobku, a data nesouvisející s používáním výrobku. Co je již méně srozumitelné, je působnost nařízení. Na jednu stranu se má nařízení uplatnit pouze na data, jež vznikla během užívání virtuálního asistenta, na druhou stranu se má právo na přístup k datům vztahovat i na data vzniklá mimo užívání asistenta. Z prostého jazykového výkladu vyplývá, že ono právo dopadá na širší okruh dat než nařízení, ovšem toto právo je stanoveno právě v onom nařízení.

V případě hlasového asistenta, jenž slouží výhradně nezávazné konverzaci, není jasné následující: Uživatel aktivuje asistenta aktivačním slovem a vede s ním konverzaci. Během ní však uživatel řekne něco, co hlasový asistent zachytí a uloží, ovšem tento input není namířen vůči hlasovému asistentu (např. pokyn uživatele hlasového asistenta vůči jinému členu domácnosti, nikoliv vůči hlasovému asistentovi). Spadá tento příklad do užívání asistenta, nebo nikoliv? Dle bodu 17 recitálu taková data

[71] „(…) *Na takové virtuální asistenty by se mělo vztahovat právo na přístup k datům stanovené v tomto nařízení, a to i pokud jde o data zaznamenaná před aktivací virtuálního asistenta prostřednictvím aktivačního slova a data vytvářená, když uživatel interaguje s výrobkem prostřednictvím virtuálního asistenta poskytnutého jiným subjektem, než je výrobce výrobku. Do oblasti působnosti tohoto nařízení však spadají pouze data pocházející z interakce mezi uživatelem a výrobkem prostřednictvím virtuálního asistenta. Data vytvořená virtuálním asistentem, která nesouvisejí s používáním výrobku, nejsou předmětem tohoto nařízení.*“

nespadají pod data vzniklá užíváním *výrobku/služeb*, protože dle něj „*data vytvářená používáním výrobku nebo související služby zahrnují data záměrně zaznamenaná uživatelem*“. Z hlediska podstaty práva přístupu k datům ale nedává smysl, aby měl uživatel tímto nařízením garantován přístup ke konverzaci s hlasovým asistentem, při níž data pro hlasového asistenta „vědomě“ vytváří, ale neměl přístup k datům, která asistent zachytí, aniž by to uživatel věděl. Nehledě na to, že tato data, která jsou hlasovým asistentem zachycena „omylem“, mohou mít zpravidla „citlivější“ povahu než data záměrně sdílená s asistentem při konverzaci s ním. Situaci nenapomáhá ani fakt, že recitál neuvádí žádný konkrétní legislativní pramen, který se vztahuje právě na data „*nesouvisející s používáním výrobku*“. Pouze se omezuje na obecné konstatování v bodě 30 recitálu, že „[*p*]*odle tohoto nařízení má uživatel, který je fyzickou osobou, dále právo na přístup ke všem osobním i neosobním údajům vytvořeným výrobkem*“.

3. 2. 5. 3 Další obsah Návrhu Aktu o datech

Kapitola II upravuje výše již zmíněné právo uživatele na zpřístupnění dat, jež vznikají užitím *výrobku* či *služby*. Na druhé straně práva uživatele na zpřístupnění dat stojí povinnost data uživateli zpřístupnit. Tato povinnost přísluší držiteli dat, jímž bude klasicky *výrobce* případně *poskytovatel souvisejících služeb*. Dále je zde zakotveno právo uživatele sdílet data se třetími stranami a z toho plynoucí povinnosti pro dané strany. Za zmínku stojí také čl. 7 odst. 1 nařízení, který z těchto povinností vyvazuje mikropodniky a malé podniky ve smyslu čl. 2 přílohy 2 doporučení 2003/361/ES[72].

Kapitola III stanovuje povinnosti, kterými jsou držitelé dat, vymezení v čl. 1 bodě 6 Návrhu, vázáni v souvislosti s povinností data zpřístupnit. Čtvrtá kapitola chrání výše uvedené mikropodniky a malé podniky před nepřiměřenými smluvními podmínkami a pátá kapitola, která se na mikropodniky a malé podniky nevztahuje, reguluje zpřístupnění dat subjektům veřejného sektoru. Pro téma této rigorózní práce je relevantní ještě kapitola VII, která nese název *Záruky pro neosobní údaje v mezinárodním kontextu*, která dokládá, že se návrh nařízení neomezuje jen na osobní údaje, a ukládá v návaznosti na to poskytovatelům služeb zpracování dat povinnost řídit

[72] Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků (text s významem pro EHP)

se unijním právem. Nařízení se tak v tomto ohledu drží obecné roviny a nezmiňuje konkrétní unijní právní předpisy, jež se neosobními údaji a jejich zpracování zabývají.

3. 2. 5. 4 Shrnutí Aktu o datech

Z pohledu ochrany dat zakotvuje Akt o datech uživatelovo právo na zpřístupnění dat a jejich sdílení s třetími stranami. Držitelé a zpracovatelé dat jsou vázáni povinnostmi, které navazují na toto uživatelovo právo a zároveň se neomezují pouze na osobní údaje.

Co však činí při aplikaci návrhu nařízení problémy, je jeho první kapitola, která způsobuje potíže v porozumění působnosti samotného nařízení a také některých definic, jak nastiňujeme v předchozích kapitolách. Pokud jsme text nařízení vyložili správně, znamená to, že největší roli hraje podoba, v níž je technologie „zhmotněna“. Zatímco se na technologii v jedné podobě tento předpis neuplatní, v jiné podobě předpis na tutéž technologii dopadne. S velkou pravděpodobností totiž závisí na druhu nosiče, v němž je technologie implementována. Konverzační software, který bude zakomponován do fyzického hlasového asistenta, bude pod nařízení spadat, zatímco tentýž software zasazený do rozhraní mobilní aplikace bude z působnosti nařízení vyňat. Tato skutečnost podle nás může vést k nejasnostem a nekalým jednáním v praxi, kdy se tvůrci budou o „podobě vnějšího zhmotnění“ softwaru rozhodovat na základě toho, jaká legislativa se na jaký případ vztahuje.

Zcela jasno není ani v případě druhu dat, na něž se nařízení uplatní. Ze závazné části textu vyplývá, že se užije pouze na data, která plynou z užívaní *výrobku* či *služby*. Není však zřejmé, ke které z těchto kategorií se řadí případ, kdy člověk během konverzace s hlasovým asistentem řekne něco, co je v daném kontextu konverzace irelevantní (například se obrátí na jiného člena domácnosti, přijme hovor na svém mobilním telefonu apod.). Tato otázka je přitom stěžejní nejen s ohledem na ono právo uživatele mít k datům přístup, ale také s ohledem na možnost držitelů dat s těmito daty dále nakládat.

3. 2. 6 Návrh Směrnice o odpovědnosti za umělou inteligenci

V rámci připravované legislativy spjaté s umělou inteligencí nesmíme opomenout Návrh směrnice Evropského parlamentu a Rady o přizpůsobení pravidel

mimosmluvní občanskoprávní odpovědnosti umělé inteligenci (směrnice o odpovědnosti za umělou inteligenci), COM(2022) 496 final. V rámci řádného legislativního procesu nyní, tedy na začátku října 2023, probíhá první čtení v Radě EU.[73]

Právním základem této směrnice je i v tomto případě čl. 114 SFEU. Úlohou této směrnice je doplnit vnitrostátní pravidla občanskoprávní odpovědnosti a směrnici o odpovědnosti za vadné výrobky[74], čímž má být zaplněna nynější legislativní mezera. Směrnice o odpovědnosti za vadné výrobky upravuje objektivní odpovědnost výrobce za vady jeho výrobků a s tím související náhradu škody a navazuje tím na vnitrostátní pravidla odpovědnosti, která jsou však často provázána s prvkem zavinění. Institut zavinění, který spočívá v prokázání nedbalostního, či úmyslného jednání, nebo opomenutí konkrétní osoby, je však v kontextu umělé inteligence zcela nevhodný. Proces rozhodování umělé inteligence je pro nás často skrytý a obtížně vysvětlitelný (tzv. efekt „černé skříňky“). Dohledání konkrétní osoby, která by byla odpovědna za konkrétní krok systému umělé inteligence, a současně prokázání, že je to právě ona, kdo nese odpovědnost za daný úkon umělé inteligence, se jeví jako velmi náročný, zdlouhavý a zřejmě i nákladný proces, který navíc nemusí vést k jasnému výsledku. Hlavním cílem směrnice o odpovědnosti za umělou inteligenci je proto zmírnit důkazní břemeno, které je u požadavku na náhradu škody v případě vad na straně poškozeného.[75]

Směrnice o odpovědnosti za umělou inteligenci má zvýšit právní jistotu. Z perspektivy poškozeného by měla zharmonizovat a zjednodušit postup při vzniku škody a z pohledu výrobců systémů umělé inteligence by měla vytvořit ucelený soubor pravidel, která reflektují specifika umělé inteligence. Vedle Aktu o umělé inteligenci, GDPR, Aktu o digitálních službách a Aktu o datech tak rozšiřuje (navrhovanou) evropskou úpravu umělé inteligence o další oblast, kterou je odpovědnost. Zároveň je ale třeba zdůraznit, že se tato směrnice nedotýká povinnosti řádné péče a odpovědnosti

[73] Přehled postupu legislativního procesu Směrnice o odpovědnosti za umělou inteligenci. Online. [cit. 2023-10-7]. Dostupné z: EUR-Lex - 52022PC0496 - EN - EUR-Lex (europa.eu)
[74] Návrh Směrnice Evropského parlamentu a Rady o odpovědnosti za vadné výrobky, COM(2022) 495 final. Online. Dostupné z: EUR-Lex - 52022PC0495 - EN - EUR-Lex (europa.eu). [cit. 2023-10-7].
[75] Návrh Směrnice Evropského parlamentu a Rady o přizpůsobení pravidel mimosmluvní občanskoprávní odpovědnosti umělé inteligenci (směrnice o odpovědnosti za umělou inteligenci) – důvodová zpráva. Online. Dostupné z: EUR-Lex - 52022PC0496 - EN - EUR-Lex (europa.eu). [cit. 2023-10-7].

subjektů, které upravují předpisy zmíněné v předchozí větě. Jedinou materií směrnice je tak ulehčení důkazního břemene na straně poškozeného v případě, že mu vznikla škoda, jež byla způsobena systémem umělé inteligence.[76]

3. 2. 6. 1 Obsah Návrhu Směrnice o odpovědnosti za umělou inteligenci

Samotná Směrnice o odpovědnosti za umělou inteligenci se člení pouze na jednotlivé články, nikoliv hlavy či díly a oddíly. Dohromady se jedná pouze o devět článků.

Článek 1 vymezuje předmět úpravy této směrnice, jímž je vedle výše zmíněného důkazního břemene poškozeného v kontextu náhrady škody také zpřístupnění důkazů o vysoce rizikových systémech umělé inteligence. Vysoce rizikové systémy však nejsou pro nás relevantní vzhledem k tomu, že se tato práce zaměřuje na konverzační hlasové asistenty a konverzační mobilní aplikace. Proto se nebudeme věnovat ustanovením, která se dotýkají právě vysoce rizikových systémů. Článek 1 dále výslovně omezuje působnost směrnice na oblast občanskoprávní odpovědnosti. Na trestní odpovědnost se tak směrnice vůbec neuplatní.

Článek 2 vymezuje definice, přičemž se u čtyř termínů (např. *poskytovatel*) omezuje na odkaz na návrh Aktu o umělé inteligenci, kde jsou termíny již definovány. Je třeba vzít v úvahu, že návrh směrnice nepracuje s pojmem *poškozený*, nýbrž s pojmem *žalobce*, kterým je osoba, jež uplatňuje nárok na náhradu škody a zároveň splňuje jednu z podmínek uvedených v čl. 2 bodě 6 návrhu směrnice.

Článek 4 upravuje vyvratitelnou domněnku příčinné souvislosti mezi zaviněním žalovaného a výstupem vytvořeným systémem umělé inteligence, případně absencí takového výstupu. Tím, že se jedná o domněnku vyvratitelnou, má žalovaný právo ji vyvrátit, jak konstatuje čl. 4 odst. 7 směrnice. Vzhledem k tomu, že tento článek směrnice činí výkladové potíže, uvádíme první odstavec pro jistotu v celém jeho znění:

„*S výhradou požadavků stanovených v tomto článku vnitrostátní soudy pro účely použití pravidel odpovědnosti na nárok na náhradu škody předpokládají příčinnou*

[76] Návrh Směrnice Evropského parlamentu a Rady o přizpůsobení pravidel mimosmluvní občanskoprávní odpovědnosti umělé inteligenci (směrnice o odpovědnosti za umělou inteligenci) – důvodová zpráva. Online. Dostupné z: EUR-Lex - 52022PC0496 - EN - EUR-Lex (europa.eu). [cit. 2023-10-7].

souvislost mezi zaviněním žalovaného a výstupem vytvořeným systémem UI nebo tím, že systém UI takový výstup nevytvořil, pokud jsou splněny všechny následující podmínky: a) žalobce prokázal nebo soud podle čl. 3 odst. 5 předpokládal zavinění žalovaného nebo osoby, za jejíž chování žalovaný odpovídá, spočívající v nedodržení povinnosti řádné péče stanovené unijním nebo vnitrostátním právem, jejímž přímým účelem je ochrana před vzniklou škodou; b) na základě okolností případu lze považovat za přiměřeně pravděpodobné, že zavinění mělo dopad na výstup vytvořený systémem UI nebo na to, že systém UI takový výstup nevytvořil; c) žalobce prokázal, že výstup vytvořený systémem UI nebo to, že systém UI takový výstup nevytvořil, vedlo ke vzniku škody."

Lze tak usoudit, že se příčinná souvislost obecně předpokládá za kumulativního splnění všech tří podmínek stanovených v prvním odstavci tohoto článku. Pro systémy umělé inteligence, jež nejsou vysoce rizikové, však platí ještě čl. 4 odst. 5 směrnice, podle něhož „*[v] případě nároku na náhradu škody týkajícího se systému UI, který není vysoce rizikovým systémem UI, se domněnka stanovená v odstavci 1 uplatní pouze tehdy, pokud vnitrostátní soud považuje za příliš obtížné, aby žalobce mohl prokázat příčinnou souvislost uvedenou v odstavci 1*". Znamená to tedy, že se u systémů umělé inteligence, jež nejsou vysoce rizikové, uplatní domněnka příčinné souvislosti mezi zaviněním žalovaného a výstupem systému[77] jen tehdy, kdy je pro žalobce příliš obtížné prokázat příčinnou souvislost. Jakou příčinnou souvislost je ale pro žalobce příliš obtížné prokázat? Směrnice stanovuje pouze „*příčinnou souvislost uvedenou v odstavci 1*". V čl. 4 odst. 1 směrnice jsou ovšem uvedeny příčinné souvislosti dvojího druhu – příčinná souvislost mezi zaviněním a výstupem (uvedena v návětí odstavce) a příčinná souvislost mezi výstupem a vzniklou škodou (uvedena pod písm. c).

Jestliže by byla myšlena první zmíněná příčinná souvislost, pak by to doslova znamenalo, že se domněnka příčinné souvislosti mezi zaviněním žalovaného a výstupem systému uplatní u nevysoce rizikových systémů umělé inteligence tehdy, je-li pro žalobce příliš obtížné prokázat tuto příčinnou souvislost. Bylo by k aplikaci této domněnky ještě třeba splnění všech tří podmínek uvedených pod písmeny *a)-c)* čl. 4

[77] Z důvodu úspornosti a přehlednosti je v tomto a následujících odstavcích této kapitoly užíván pouze termín „výstup systému umělé inteligence", přestože se tím míní také absence tohoto výstupu.

odst. 1 směrnice? Zřejmě nikoliv, protože tyto podmínky právě upravují prokázání oné příčinné souvislosti, které je v tomto případě považováno za *příliš obtížné*.

Jestliže by byla myšlena druhá zmíněná varianta, pak by se domněnka příčinné souvislosti mezi zaviněním žalovaného a výstupem systému uplatnila u nevysoce rizikových systémů umělé inteligence, jestliže by bylo pro žalobce příliš obtížné prokázat příčinnou souvislost mezi výstupem systému a škodou. Není však zřejmé, zda by bylo k aplikaci domněnky ještě nezbytné splnit podmínky uvedené v prvním odstavci pod písmeny *a)* a *b)*, tzn. prokázání zavinění a přiměřená pravděpodobnost, že zavinění mělo na výstup systému umělé inteligence dopad.

K zodpovězení otázky, jaká příčinná souvislost je v čl. 4 odst. 5 směrnice míněna a případně zda je třeba k aplikaci domněnky splnit (některé) podmínky uvedené v čl. 4 odst. 1 směrnice pod písm. *a)-c)*, nám nepomůže ani důvodová zpráva[78]. Tato otázka tak zůstává směrnicí nezodpovězena.

Podle čl. 4. odst. 6 směrnice se vyvratitelná domněnka za určitých podmínek aplikuje také v případě, že žalovaný systém umělé inteligence užíval při *osobní neprofesionální činnosti*. Podmínky, jež postačuje naplnit alternativně, představují zaprvé podstatný zásah žalovaného do podmínek provozu a zadruhé neurčení podmínek provozu žalovaným, přestože k tomu byl povinen a byl toho schopen. Ani v této souvislosti není jasné, zda je k uplatnění vyvratitelné domněnky třeba, aby byly splněny podmínky čl. 4 odst. 1 písm. a)-c) směrnice.

3. 2. 6. 2 Shrnutí Směrnice o odpovědnosti za umělou inteligenci

Přestože je směrnice obsahově velmi krátká, není její znění zcela srozumitelné. První nedostatek lze spatřit již v definici řádné péče, která je v kontextu vyvratitelné domněnky příčinné souvislosti mezi zaviněním žalovaného a jednáním systému umělé inteligence stěžejní. Povinnost řádné péče je totiž vymezena jen jako určitý standard chování, který je definován vnitrostátním nebo unijním právem. Nezbývá nám tak nic jiného než spoléhat na kvalitní transpozici směrnice jednotlivými státy, z níž bude patrné, jak je záhodno tento pojem chápat.

[78] *„[v] případě systémů UI, které nejsou vysoce rizikové, stanoví čl. 4 odst. 5 podmínku pro uplatnění domněnky příčinné souvislosti, podle níž je tato domněnka podmíněna tím, že soud zjistí, že je pro žalobce příliš obtížné prokázat příčinnou souvislost*“

Další slabinu můžeme vidět ve formulaci oné vyvratitelné domněnky, jejíž úskalí detailně vymezujeme již v předchozí kapitole. „Ulehčení“ důkazního břemena, které u náhrady škody nese poškozený, se navíc týká pouze vybraných případů. Směrnice se tak omezuje na pouhou výseč a prokazování příčinné souvislosti neupravuje komplexně. Není zcela jasné, jaké právní předpisy se uplatní v případech, na něž se zmíněná domněnka vztahovat nebude. Bude to Směrnice o vadných výrobcích, jež je stále v legislativním procesu, společně s příslušnými vnitrostátními předpisy? Nejspíše ano. Pokud vezmeme v úvahu náš demonstrativní příklad – konverzační hlasový asistent, případně mobilní konverzační aplikace – pak se jistě jedná o systémy umělé inteligence, které nejsou vysoce rizikové. Vzhledem k problematickému znění ustanovení čl. 4 odst. 5 směrnice, které se týká právě takových systémů, lze jen stěží říci, zda je v těchto případech pro poškozeného *příliš obtížné* prokázat příčinnou souvislost. Z tohoto důvodu se našim ilustrativním příkladům v tomto kontextu více nevěnujeme.

3. 2. 7 Další relevantní legislativa

Výše zmíněná legislativa souvisí s naším tématem ve velké míře, a proto jí je věnována patřičná pozornost. Nelze však dospět k závěru, že jsou v této práci analyzovány všechny relevantní prameny. V této souvislosti upozorňujeme, že ambicí předmětné rigorózní práce není dopodrobna popsat veškerou legislativu, jež se tématu technologií založených na umělé inteligenci a související ochraně dat a soukromí dotýká. U následujících předpisů se tak omezujeme na jejich pouhou zmínku, případně velmi stručné představení v případě, že název pramenu jeho obsah dostatečně nevysvětluje.

Relevantním pramen pro naše téma by mohlo být *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)*, které je účinné od 16. listopadu 2022 a které se uplatní na zprostředkovatelské služby v tomto nařízení definované, či *Směrnice Evropského parlamentu a Rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru*. Tuto směrnici jsme již okrajově zmínili v kontextu Aktu o správě dat, poněvadž je také její úlohou podpořit opakované použití dat.

Dále je třeba v kontextu komunikačních technologií založených na umělé inteligenci zmínit *Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti")*, jež nabylo účinnosti částečně již v červnu roku 2019 a ve zbytku pak o dva roky později. V oblasti kybernetické bezpečnosti stojí za zmínku také *Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (Text s významem pro EHP)*, která bude v následujících měsících transponována, a *Návrh Nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020*, který je v říjnu 2023 v prvním čtení v Radě Evropské unie.

Z plánované legislativy uveďme ještě *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)*, kterého jsme se již dotkli v kapitole věnující se GDPR (3. 2. 1. 1 Shrnutí GDPR z perspektivy tvůrce a uživatele konverzačního asistenta a konverzační aplikace). Tento pramen má stanovit pravidla ochrany dat a soukromí v případě mobilních aplikací s důrazem na aspekt důvěrnosti obsahu komunikace uživatele.[79]

3. 3. Soft law

3. 3. 1 Umělá inteligence pro Evropu

Jeden z vůbec prvních oficiálních dokumentů Evropské Unie, který upozorňuje na rozmach umělé inteligence a s tím související potřebu umělou inteligenci zakomponovat do legislativy, je Sdělení Evropské komise *Umělá inteligence pro Evropu* ze dne 25. 4. 2018[80], které je též někdy označováno jako *Strategie pro umělou*

[79] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. *Privacy and data protection in mobile applications: a study on the app development ecosystem and the technical implementation of GDPR*. 2017, 8. ISBN 9789292042424.

[80] Sdělení Komise Evropskému Parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů Umělá inteligence pro Evropu. Online. Dostupné z:

inteligenci. Na toto sdělení jsme již narazili v druhé kapitole, která se věnuje definici umělé inteligence.

Sdělení se především zaměřuje na zajištění konkurenceschopnosti Unie prostřednictvím investic, spolupráce soukromého a veřejného sektoru a zajištění velkého objemu dat, a právním aspektům tak dává jen omezený prostor. Zmiňuje ochranu osobních údajů, která se v té době dočkala účinnosti své zásadní právní úpravy v podobě GDPR, a připravovanou regulaci volného pohybu neosobních údajů. Vedle závazných pramenů upomíná sdělení na pokyny ohledně odpovědnosti za jednání umělé inteligence, etické pokyny a Koordinovaný plán v oblasti umělé inteligence. Posledním dvěma zmíněným se věnují samostatné kapitoly. Dostatečná právní úprava by měla vedle právní jistoty vést také k posílení důvěry občanů EU v technologie. Dle přesvědčení Komise totiž budou lidé více důvěřovat zařízením, na něž bude doléhat evropská legislativa, poněvadž tato zahrnuje i bezpečnostní standardy.[81]

3. 3. 2 Koordinovaný plán v oblasti umělé inteligence

Vedle sdělení *Umělá inteligence pro Evropu* uvedeného v předcházející kapitole vydala Evropská komise tentýž rok ještě další sdělení související s umělou inteligencí, a to Sdělení Evropské komise ze dne 7. 12. 2018 související s umělou inteligencí, jehož přílohu tvoří Koordinovaný plán v oblasti umělé inteligence.[82]

Ani v tomto případě není legislativní stránka věci stěžejním bodem, ale i přesto se jí částečně věnuje. Regulační rámec by měl vedle etických a bezpečnostních aspektů zohledňovat i stránku inovací. To znamená, že by je měl aktivně podporovat a usnadňovat jim cestu, aby Unie byla konkurenceschopná. Vedle bezpečnosti a kyberbezpečnosti klade důraz na úpravu v oblasti ochrany dat a soukromí.[83]

---

https://www.vlada.cz/assets/evropske-zalezitosti/umela-inteligence/Sdeleni-EK-k-AI.PDF. [cit. 2023-04-23].

[81] Sdělení Komise Evropskému Parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů Umělá inteligence pro Evropu. 3-4,6,11,15-17 Online. Dostupné z: https://www.vlada.cz/assets/evropske-zalezitosti/umela-inteligence/Sdeleni-EK-k-AI.PDF. [cit. 2023-04-23].

[82] Sdělení Komise Evropskému Parlamentu, Evropské radě, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Koordinovaný plán v oblasti inteligence. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018DC0795. [cit. 2023-04-23].

[83] Sdělení Komise Evropskému Parlamentu, Evropské radě, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Koordinovaný plán v oblasti inteligence. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018DC0795. [cit. 2023-04-23].

Koordinovaný plán byl v roce 2021 aktualizován Sdělením komise *Podpora evropského přístupu k umělé inteligenci*.[84] V tomto dokumentu konstatuje Komise jistý legislativní posun od roku 2018, a to především v podobě nezávazných etických pokynů či Bílé knihy nebo připravovaných aktů o umělé inteligenci a o správě dat.[85]

3. 3. 3 Etické pokyny pro zajištění důvěryhodnosti umělé inteligence

Tento dokument se také řadí mezi tzv. soft law, tedy tu část právních pramenů, jež nejsou právně závazné. Za vznikem *Etických pokynů pro zajištění důvěryhodnosti umělé inteligence* (dále také „Pokyny“) v roce 2019 stojí Odborná skupina na vysoké úrovni pro umělou inteligenci známá také pod anglickou zkratkou *AI HLEG* (*High-level Expert Group on Artificial Intelligence*). Pokyny byly sepsány v návaznosti na sdělení Evropské komise ze dne 25. 4. 2018 a 7. 12. 2018, jemuž se věnuje předchozí kapitola.[86] Jedná se o jednu z prvních prací na úrovni Evropské unie, která se umělé inteligenci věnuje podrobněji a která v tomto kontextu zmiňuje problematiku ochrany a správy dat, proto je jí tady věnována větší pozornost.

Zmíněná odborná skupina byla zřízena Komisí za účelem jednotného evropského přístupu v oblasti umělé inteligence, jak už napovídá samotný název skupiny. Práce skupiny byla stěžejní pro první kroky EU v právní úpravě umělé inteligence a jednou z jejích prvních počinů jsou právě Pokyny.[87]

Cílem Pokynů je definovat rámec pro důvěryhodnou umělou inteligenci a podpořit ji. A jak je důvěryhodná umělá inteligence vymezena? Umělá inteligence musí disponovat třemi aspekty, aby mohla být pokládána za důvěryhodnou. Prvním aspektem je legalita, která spočívá v souladu umělé inteligence s platným právem. Detailněji se jí Pokyny nevěnují, protože se jí zabývá jiný dokument Odborné skupiny, a sice

[84] Sdělení Komise Evropskému Parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Podpora evropského přístupu k umělé inteligenci. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021DC0205. [cit. 2023-04-23].
[85] Sdělení Komise Evropskému Parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Podpora evropského přístupu k umělé inteligenci. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021DC0205. [cit. 2023-04-23].
[86] Evropské pokyny pro zajištění důvěryhodnosti umělé inteligence, 2. Online. Dostupné z: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_CS.pdf. [cit. 2023-04-02].
[87] *Skupina odborníků na vysoké úrovni pro umělou inteligenci*. Online. Evropská komise. 2022. Dostupné z: https://digital-strategy.ec.europa.eu/cs/policies/expert-group-ai. [cit. 2023-04-02].

dokument Policy and Investment reccomendation for trustworthy Artificial Intelligence uvedený v následující kapitole. [88]

Druhou složkou důvěryhodné umělé inteligence je etika, respektive dodržování čtyř etických zásad, jimiž jsou respektování lidské autonomie, předcházení újmám, spravedlnost a vysvětlitelnost. Tyto zásady vycházejí ze základních práv, mezi něž se mimo jiné řadí lidská důstojnost. S ohledem na umělou inteligenci ji lze vymezit tak, že by neměla být lidská osobnost degradována na pouhý objekt, s jehož daty je dále nakládáno, ale stále bychom měli mít na paměti, že se jedná o subjekt, s nímž bychom měli zacházet v souladu s morálními principy a úctou. Zásada lidské autonomie odráží tzv. přístup zaměřený na člověka. Člověk by měl stát vždy nad technologií a dohlížet na ni. Umělá inteligence by tak s ním neměla nijak manipulovat či ho klamat. Zásada předcházení újmám akcentuje důstojnost a nedotknutelnost člověka. Zásada spravedlnosti spočívá jednak v prevenci diskriminace, jednak v možnosti procesně se bránit proti následkům činnosti systémů umělé inteligence. Poslední zásada, zásada vysvětlitelnosti, přispívá důvěryhodnosti umělé inteligence tím, že stanoví maximální možnost transparentnosti procesů systémů umělé inteligence a z nich plynoucích rozhodnutí. Pokyny přitom neopomíjejí ani systémy, jejichž procesy a rozhodnutí vysvětlit nelze. V případě takovýchto systémů známých také jako tzv. „černé skříňky" je třeba přistoupit k prostředkům, jakými jsou např. sledovatelnost a transparentní vymezení schopností systému, jež alespoň částečně absenci vysvětlitelnosti systémových rozhodnutí kompenzují. [89]

Třetí složkou je robustnost, která je založena na bezpečnosti, spolehlivosti a prevenci újmy a negativních dopadů. Všechny tři složky se navzájem doplňují a v případě, že si odporují, je třeba usilovat o to, aby byly v souladu, a tím byla zajištěna důvěryhodnost.[90]

---

[88] Evropské pokyny pro zajištění důvěryhodnosti umělé inteligence, 2, 6. Online. Dostupné z: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_CS.pdf. [cit. 2023-04-02].

[89] Evropské pokyny pro zajištění důvěryhodnosti umělé inteligence, 8, 10-13. Online. Dostupné z: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_CS.pdf. [cit. 2023-04-02].

[90] Evropské pokyny pro zajištění důvěryhodnosti umělé inteligence, 5, 7. Online. Dostupné z: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_CS.pdf. [cit. 2023-04-02].

Kritéria důvěryhodnosti jsou tedy již známa, ale co vše je zapotřebí k tomu, aby takto vymezená důvěryhodná umělá inteligence mohla být realizována v praxi? Pokyny tyto podmínky sepisují vedle technických i netechnických metod také v podobě sedmi požadavků, které nemíří pouze na vývojáře systémů, ale také na koncové uživatele. Jsou jimi lidský faktor a dohled, technická robustnost a bezpečnost, ochrana soukromí a správa dat, transparentnost, rozmanitost společně se spravedlností a zákazu diskriminace, dobré sociální a enviromentální podmínky a odpovědnost. Z těchto požadavků se skládá také pilotní verze hodnotícího seznamu, jež je součástí Pokynů a která má subjektům pracujících na systémech umělé inteligence poskytnout určité vodítko, jaké všechny aspekty mají vzít při své činnosti v úvahu a jaké otázky by si měli být schopni zodpovědět.[91] Tento hodnotící seznam byl zmíněnou Odbornou skupinou na vysoké úrovni pro umělou inteligenci zrevidován na základě zpětné vazby účastníků připomínkového řízení a v roce 2020 byl seznam vydán ve své finální podobě.[92]

Třetí požadavek se týká ochrany soukromí a správy dat, jež úzce souvisí s výše zmíněnou zásadou předcházení újmám. Správa dat by totiž měla sloužit k tomu, aby soukromí uživatelů nebylo bezdůvodně narušeno. Ochrana soukromí a dat se přitom vztahuje na data poskytnutá uživatelem na začátku používání systému (typicky „vstupní“ údaje, které musí uživatel sdělit, aby mohl systém používat), ale rovněž na údaje, které systém získá během interakce s uživatelem. Data by měla být dostatečně zabezpečena před případnými útoky a úniky a přístup k nim by měl regulovat tzv. přístupový protokol, který stanoví, kdo a za jakých podmínek může k datům získat přístup, přičemž platí, že okruh osob, jež mají k datům konkrétních uživatelů přístup, by měl být omezený. V souvislosti s tímto požadavkem je zmíněna také kvalita dat, na nichž se systémy učí. Tato data by měla projít důkladnou kontrolou, aby se eliminovalo

[91] Evropské pokyny pro zajištění důvěryhodnosti umělé inteligence, 14-15. Online. Dostupné z: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_CS.pdf. [cit. 2023-04-02].

[92] *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*. Online. European Commission. 2020. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment. [cit. 2023-04-16].

riziko, že budou zahrnovat společenské stereotypy, diskriminační prvky či faktické nesprávnosti.[93]

3. 3. 4 Policy and Investment Recommendations for trustworthy AI

Jak bylo zmíněno v předchozí kapitole, jeden ze tří aspektů důvěryhodné umělé inteligence je legalita. Na rozdíl od dalších dvou atributů důvěryhodné umělé inteligence není legalitě v Pokynech zmíněné Odborné skupiny Komise věnována větší pozornost. Tuto skutečnost napravuje další dokument oné Odborné skupiny, a sice *Policy and Investment Recommendations for trustworthy Artificial Intelligence* z roku 2019, který se na ni zaměřuje v rámci své předposlední části.[94]

Dokument obsahuje dohromady 31 doporučení, která by měla být zohledněna při vytváření regulačního rámce umělé inteligence. Jednotlivá doporučení jsou uspořádána do čtyř skupin. Hlavním mottem první skupiny je rozlišovat různou míru rizik, která umělá inteligence může způsobovat. Vysoce rizikové systémy by měly být regulovány více než systémy s nižším rizikem. Druhá skupina doporučení se týká revize stávající právní úpravy nejen na úrovni EU, ale také v rámci jednotlivých členských států, kde se může EU inspirovat. Jedno doporučení v této skupině explicitně míří na oblast ochrany dat, kde Odborná skupina doporučuje zamyslet se nad tím, zda je ochrana poskytnutá prostřednictvím GDPR dostatečná, nebo je třeba ji doplnit, a zda jsou data z veřejného sektoru otevřená, a tím využitelná v rámci výzkumu. Třetí skupina se zaměřuje na rizikové systémy, čtvrtá na revizi dosavadní institucíální struktury a pátá akcentuje harmonizaci předpisů a spolupráci mezi jednotlivými členskými státy.[95]

3. 3. 5 Bílá kniha o umělé inteligenci – evropský přístup k excelenci a důvěře

Dne 19. 2. 2020 vydala Evropská komise Bílou knihu o umělé inteligenci. Její obsah se dělí na dva základní „ekosystémy“, a to tzv. ekosystém excelence a ekosystém

[93] Evropské pokyny pro zajištění důvěryhodnosti umělé inteligence, 18. Online. Dostupné z: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_CS.pdf. [cit. 2023-04-02].
[94] Policy and Investment Recommendations for trustworthy Artificial Intelligence. Online. Dostupné z: https://digital-strategy.ec.europa.eu/cs/node/1694. [cit. 2023-04-23].
[95] Policy and Investment Recommendations for trustworthy Artificial Intelligence. 37-43. Online. Dostupné z: https://digital-strategy.ec.europa.eu/cs/node/1694. [cit. 2023-04-23].

důvěry. První z nich je reprezentován zejména výzkumem a inovacemi, druhý se týká právního rámce Unie.[96]

V rámci ekosystému důvěry shrnuje Bílá kniha dosavadní úsilí na legislativním poli v souvislosti s umělou inteligencí a otázky, které je třeba si při tvorbě právního rámce klást a zodpovídat. Také je zde například konstatováno, že občan EU očekává od výrobku, jenž je spjat s umělou inteligencí, stejné bezpečnostní a spotřebitelské standardy jako od výrobku prostého, ovšem umělá inteligence disponuje vlastnostmi, které toto narušují. Za všechny lze zmínit již několikrát uvedenou neprůhlednost ať už rozhodovacích či jiných mechanismů umělé inteligence.[97]

Právní rámec umělé inteligence by měl především reflektovat a minimalizovat rizika užívání umělé inteligence, která vyplývají pro bezpečnost a dodržování základních práv, jakým je ochrana soukromí. Otázku, zda dosavadní evropská právní úprava aspoň některé z těchto rizik plně pokrývá, či nikoliv, Bílá kniha nezodpovídá. Ostatně to ani není její úloha. Upozorňuje také na to, že bude třeba jasně stanovit působnost právního rámce, resp. zda se omezí na výrobky, nebo se bude vztahovat i na služby podpořené umělou inteligencí, jako jsou např. služby finanční, a detailněji rozvádí sedm požadavků na důvěryhodnou umělou inteligenci představených Etickými pokyny výše.[98]

3. 4 Shrnutí legislativy EU v oblasti umělé inteligence

Úlohou třetí kapitoly této práce je představit relevantní legislativu Evropské unie v kontextu umělé inteligence. Je třeba znovu zdůraznit, že kapitola nepokrývá veškeré předpisy, které se umělé inteligence dotýkají. Výběr legislativy byl stanoven na základě tématu práce a zaměření práce na případ virtuálních (konverzačních) asistentů a aplikací

[96] Bílá kniha o umělé inteligenci – evropský přístup k excelenci a důvěře. Online. Dostupné z: https://eur-lex.europa.eu/legal-. content/CS/TXT/?uri=CELEX%3A52020DC0065&lang1=CS&from=EN&lang3=choose&lang2=choose&_csrf=212f314d-7b1d-4d1f-9a71-c1a5f0e092fc. [cit. 2023-04-23].
[97] Bílá kniha o umělé inteligenci – evropský přístup k excelenci a důvěře. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52020DC0065&lang1=CS&from=EN&lang3=choose&lang2=choose&_csrf=212f314d-7b1d-4d1f-9a71-c1a5f0e092fc strana 11. [cit. 2023-04-23].
[98] Bílá kniha o umělé inteligenci – evropský přístup k excelenci a důvěře. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52020DC0065&lang1=CS&from=EN&lang3=choose&lang2=choose&_csrf=212f314d-7b1d-4d1f-9a71-c1a5f0e092fc. [cit. 2023-04-23].

založených na umělé inteligenci. Z tohoto důvodů v přehledu nenalezneme prameny zabývající se autonomními vozidly, zbraněmi či mechanismy v prostředí internetu a marketingu.

Zmíněnou legislativu můžeme rozdělit do dvou základních skupin. Jedna skupina pramenů jsou ze své podstaty obecné a nezaměřují se pouze na umělou inteligenci. Naopak se na ni vztahují, aniž by ji explicitně zmiňovaly. K těmto pramenům se bezpochyby řadí obecné nařízení o ochraně osobních údajů (GDPR), jemuž se kromě podkapitoly 3. 2. 1 věnujeme také v následující části práce, kde jsou podrobně rozvedena některá práva v něm zakotvená. Dále je to Nařízení o rámci pro volný tok neosobních údajů v EU či návrhy Aktu o datech a Aktu o správě dat. Druhý soubor předpisů vztahující se výlučně na zařízení, jež využívají principy umělé inteligence, tvoří Akt o umělé inteligenci a Směrnice o odpovědnosti za umělou inteligenci, přičemž legislativní proces obou pramenů není ještě u konce.

Mezi hlavní nedostatky rozebírané legislativy patří beze sporu ne vždy srozumitelné definice nově zavedených legislativních termínů a nejasné formulace, které však pro aplikaci předpisu hrají zásadní roli. Jako příklad uveďme Směrnici o odpovědnosti za umělou inteligenci a v ní zakotvenou vyvratitelnou domněnku příčinné souvislosti mezi zaviněním žalovaného a výstupem systému umělé inteligence, který způsobil poškozenému újmu (kapitola 3. 2. 6. 1 Obsah Návrhu Směrnice o odpovědnosti za umělou inteligenci). Další slabinu lze shledat v nedostatečném vymezení působnosti např. v případě Aktu o datech (kapitoly 3. 2. 5. 1 Definice a působnost Návrhu Aktu o datech z hlediska výrobku a 3. 2. 5. 2 Působnost Návrhu Aktu o datech z hlediska dat) či absenci vytyčení vztahu předpisu s jiným předpisem (kapitola 3. 2. 4. 4 Shrnutí Návrhu Aktu o správě dat z perspektivy ochrany dat). Situaci neulehčuje ani recitál pramenů, jehož úkolem je přitom primárně napomoci výkladu závazné části předpisu. Recitál se totiž také velice často uchyluje k obecným, těžce uchopitelným frázím, a navíc nejednou užívá termíny, které dále nedefinuje, čímž vzbuzuje další otázky a dosavadní ponechává nezodpovězené (např. kapitola 3. 2. 4. 4 Shrnutí Návrhu Aktu o správě dat z perspektivy ochrany dat).

Jestliže se na uvedené prameny podíváme optikou soft law, lze vidět, že předpisy v zásadě reflektují jeho zásady. Jako ilustrační případ zmiňme Směrnici o

odpovědnosti za umělou inteligenci, která v souladu se zásadou spravedlnosti vytyčenou v Pokynech umožňuje poškozenému se procesně bránit proti výsledkům činnosti systémů umělé inteligence (kapitola 3. 2. 6. 1 Obsah Návrhu Směrnice o odpovědnosti za umělou inteligenci). Zůstává však otázkou, zda stávající, případně zmíněná plánovaná, legislativa podporuje svým zněním inovace, výzkum a s tím související konkurenceschopnost EU na mezinárodním poli, jak stanovuje Koordinovaný plán v oblasti umělé inteligence (kapitola 3. 3. 2 Koordinovaný plán v oblasti umělé inteligence). Vedle toho, že se touto problematikou zabýváme v následující části práce, by nám v tomto ohledu jistě mohla pomoci komparace legislativy EU s jiným právním řádem, ovšem pro takové srovnání nemáme v naší práci prostor.

4. Ochrana dat a soukromí v kontextu umělé inteligence

Poté, co byla shrnuta legislativa relevantní pro umělou inteligenci, je třeba se zaměřit úžeji na téma ochrany dat a soukromí. Na to, jak systém umělé inteligence zachází s daty, má vliv několik faktorů. Vedle samotné funkcionality systému umělé inteligence a jeho způsobu zpracování dat to je také přesnost, s jakou pracuje, účel, pro nějž jsou data systémem sbírána, či prostředí, v němž se nachází. Nesmíme zapomenout ani na samotné tvůrce/vývojáře takového systému, protože i jejich postoj a hodnoty ovlivňují skutečnost, zda takový systém funguje v souladu s platným právem a zásadami, mezi něž spadá např. zákaz diskriminace.[99]

4. 1 Pojem dat a soukromí

V souvislosti s umělou inteligencí se nehovoří pouze o datech uživatelů, jež je třeba chránit, ale také o datech, která jsou nezbytná pro vývoj umělé inteligence. Vedle dat uživatelů tak můžeme rozlišit trénovací data, na nichž se umělá inteligence učí. Typicky se jedná o tzv. big data (velká data), která se od klasických dat odlišují svým objemem a rychlostí generování, zahrnují více typů a pochází z více zdrojů.[100] Jde tak o objemné množství komplexních dat, které vyžaduje speciální nástroje včetně nástrojů analytických. Jejich význam je pro vývoj umělé inteligence klíčový. Právě kvalita trénovacích dat má totiž velký dopad na výstup systému umělé inteligence. Jestliže nejsou trénovací data dostatečně reprezentativní a přesná, mohou mít za následek, že dojde ke zkreslení výstupu (tzv. *bias*), jehož obsah nese diskriminační prvky.[101]

Ukažme si význam kvality trénovacích dat na našem příkladu konverzačních technologií. Zaprvé je třeba myslet na to, že asistent či aplikace „mluví“. Jedná se tak o mluvenou formu jazyka, nikoliv písemnou, která s sebou nese určitá specifika. Co snese písemná forma, neunese mluvená forma, a naopak. Z tohoto důvodu je vhodné, aby trénovací data alespoň částečně pocházela například z přepisů konverzace, jazykových

[99] CORRALES COMPAGNUCCI, Marcelo. *AI in eHealth: human autonomy, data governance and privacy in healthcare*. New York, NY: Cambridge University Press, 2022, 185. ISBN 9781108921923.
[100] LEE, Joseph a DARBELLAY, Aline. *Data Governance in AI, FinTech and LegalTech*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 171. ISBN 9781800379954.
[101] ABBOTT, Ryan. *The reasonable robot: artificial Intelligence and the law*. Cambridge: Cambridge University Press, 2020, viii, 31. ISBN 9781108459020.

korpusů, kde je zastoupena i mluvená forma jazyka, či případně z takových zdrojů, kde se jazyk vyskytuje v ne zcela knižní podobě. Zadruhé je nezbytné mít na paměti i onu reprezentativnost, aby nedocházelo ke zkreslení dat. Reprezentativnosti docílíme dostatečnou robustností a různorodostí trénovacích dat.

4. 1. 1 Vztah mezi ochranou soukromí a ochranou dat

V dnešní době si běžný člověk ani neuvědomuje, v jaké míře nechává technologie každý den nahlédnout do svého soukromí. Různorodé aplikace a zařízení však o nás sbírají rozličná data, která otevírají dveře do našeho soukromí. Již z této skutečnosti je zřejmé, že s ochranou dat úzce souvisí také ochrana soukromí.[102]

Soukromí je jednou ze základních hodnot, jejíž ochrana je garantována nejednou mezinárodní úmluvou či ústavním pramenem. I přesto, nebo možná právě proto, je velmi těžké tento koncept definovat a většina dokumentů se jeho vymezení zdržuje.[103] Přese všechno lze říci, že má tento koncept dvě základní úrovně. Soukromí totiž můžeme vnímat v obecné rovině jako ochranu jednotlivce před zásahy okolí, ať už je jím míněn stát či jiný jednotlivec. Pak lze soukromí a jeho ochranu „konkretizovat" v podobě práv, která střeží určitý dílčí aspekt soukromí. V tomto smyslu se jedná např. o zásadu nedotknutelnosti obydlí či právo na ochranu listovního tajemství.[104]

Jak již bylo naznačeno výše, ochrana soukromí a ochrana dat se navzájem prolínají. Průsečíkem těchto dvou práv je ochrana autonomie jednotlivce.[105] Pokud se budeme držet teorie „dvou úrovní soukromí", kterou jsme představili v předchozím odstavci, můžeme na ochranu dat nazírat jako na jednu z „konkrétních" dimenzí ochrany soukromí.[106]

---

[102] DE BRUYNE, Jan a VANLEENHOVE, Cedric (ed.). *Artificial Intelligence and the Law.Intersentia*, 2021, 126. ISBN 9781839701047.
[103] ŠTĚDROŇ, Bohumír. *Právo a umělá inteligence*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020, 52. ISBN 9788073808037.
[104] KOLAŘÍKOVÁ, Linda, HORÁK, Filip. *Umělá inteligence & právo*. Praha: Wolters Kluwer ČR. 2020, 61. ISBN 9788075987839.
[105] LEE, Joseph a DARBELLAY, Aline. *Data Governance in AI, FinTech and LegalTech*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 16. ISBN 9781800379954.
[106] BARFIELD, Woodrow a PAGALLO, Ugo. *Research handbook on the law of artificial intelligence*. Cheltenham, UK: Edward Elgar Publishing, 2018, 282. ISBN 9781786439048.

4. 1. 2 Osobní údaje

Přestože se na první pohled může zdát, že je zcela zřejmé, co jsou osobní údaje a jaké všechny typy informací se k nim vážou, jedná se o pojem, jehož vymezení není triviální. V kapitole 3. 2. 1 Obecné nařízení o ochraně osobních údajů (GDPR) jsme uvedli definici osobních údajů stanovenou čl. 4 bodem 1 GDPR.

4. 1. 2. 1 Čtyři elementy osobních údajů

Poměrně širokou definici zakotvenou v GDPR můžeme shrnout tak, že osobním údajem je „*jakákoliv informace, jež se vztahuje k identifikované či identifikovatelné osobě*“ s tím, že je vždy nezbytné vzít v úvahu kontext, v němž jsou informace sbírány a zpracovány.[107] Z originální definice v GDPR i její zkrácené varianty vyplývá, že osobní údaje se vyznačují čtyřmi hlavními elementy. Musí jít o informaci (první element), která se vztahuje k určité osobě (druhý element), přičemž se jedná o fyzickou osobu (třetí element), která je identifikována či ji lze identifikovat (čtvrtý element). Právě čtvrtý prvek činí interpretační potíže. Nabízí se totiž otázka, kdy je ještě osoba *identifikovatelná*, a kdy již nikoliv.[108] Její zodpovězení je přitom z pohledu působnosti GDPR zcela zásadní. Pokud se totiž informace vztahuje k osobě, kterou nelze identifikovat, jedná se o anonymní informaci, na níž GDPR nedopadá.

Podle čl. 4 bodu 1 GDPR je osoba identifikovatelná, pokud ji lze „*přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby*“. Ustanovení tak obsahuje demonstrativní výčet identifikačních znaků, které z fyzické osoby činí osobu identifikovatelnou. Co však nám toto ustanovení a ani další jiná neříkají, je to, zda se ona „*identifikovatelnost*“ odvíjí výlučně od znalosti správce dat, nebo může pramenit ze znalosti třetí osoby. Ptáme se tak, zda osobu činí identifikovatelnou skutečnost, že její určitý identifikátor zná správce

[107] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. *Privacy and data protection in mobile applications: a study on the app development ecosystem and the technical implementation of GDPR.* 2017, 14. ISBN 9789292042424.
[108] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 78. ISBN 9783748930952.

daných dat, nebo skutečnost, že si k ní identifikátor přiřadí jakákoliv třetí osoba odlišná od správce dat.[109]

Jako ilustrační příklad nám pro lepší představitelnost může posloužit případ z medicínského prostředí. Představme si systém založený na umělé inteligenci, který má lékařům napomoci při identifikaci nádorů. Jako trénovací data poslouží krevní obrazy a obrazy tkáně zdravých osob a osob s nádorem. Tyto obrazy neobsahují žádné identifikátory v podobě jména, data narození či adresy trvalého bydliště a jsou doplněny pouze o údaje věku a pohlaví osoby. Je na základě těchto informací (pohlaví, věk, krevní obraz a obraz tkáně) osoba identifikovatelná, nebo ne? Provozovatel takového systému nedokáže na základě takových dat osobu identifikovat. Z jeho pohledu se tak jedná o neidentifikovatelnou osobu, a tudíž anonymní informace, na něž se GDPR nevztahuje. Pokud se však na věc podíváme z perspektivy např. kliniky, která tato data na trénování systému poskytla, dojdeme k jinému závěru. Tato klinika totiž jistě bude mít u daných snímků ve své vlastní databázi další identifikační údaje příslušné osoby, pomocí kterých bude schopna identifikovat konkrétní osobu. V případě kliniky se tedy jedná o osobní údaje ve smyslu GDPR.[110] U konverzačních aplikací by podle této logiky byla situace obdobná. Jestliže by byla uživatelská data pocházející z konverzace předána třetí osobě a zároveň očištěna o identifikátory, z perspektivy třetí osoby by se o osobní údaje nejednalo. Z pohledu správce dat aplikace by však data charakter osobních údajů neztratila, protože správce má stále k dispozici identifikátory, díky nimž může data znovu přiřadit ke konkrétní osobě.

Určité vodítko k zodpovězení otázky, zda postačuje, aby byla osoba identifikovatelná osobou odlišnou od správce dat, nám v tomto případě poskytuje recitál GDPR ve svém bodě 26. Podle něj se totiž má u identifikovatelnosti přihlédnout „*ke všem prostředkům, (...) o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použijí pro přímou či nepřímou identifikaci dané fyzické osoby*“. Z tohoto důvodu lze dospět k závěru, že spíše bude postačovat schopnost identifikace osoby prostřednictvím osoby odlišné od správce dat. Dle judikatury Soudního dvora Evropské unie se však

[109] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 79. ISBN 9783748930952.
[110] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 80-81. ISBN 9783748930952.

nemůže jednat o jakoukoliv třetí osobu, ale pouze o takovou, u níž lze předpokládat kontakt se správcem dat. Pro náš ilustrativní příklad představený v předchozím odstavci to tedy znamená, že údaje nebudou klasifikovány jako osobní, pokud nejsou správci dat systému umělé inteligence k dispozici s dalšími informacemi, které spravuje klinika. Lze však předpokládat, že pokud by se jednalo o klinický obraz, jenž vykazuje velmi vzácná specifika, snižuje se tím úsilí přiřazení obrazu ke konkrétní osobě, a proto již s největší pravděpodobností půjde o osobní údaje. To samé platí pro případ konverzačních dat, která obsahují nějakou jedinečnou informaci, díky níž jsme schopni osobu identifikovat, aniž by byly přítomné další běžné identifikátory. Uživatel se může například svěřit, že trpí velice vzácnou nemocí. Jestliže jsme na základě této skutečnosti zasazené do dalšího kontextu konverzace schopni uživatele identifikovat, půjde nejspíš o osobní údaj. Nezbývá tak než konstatovat, že vždy bude záležet na daném kontextu věci. [111]

4. 1. 2. 2 Zvláštní kategorie osobní údaje

V kontextu našich ilustrativních příkladů hlasových asistentů a aplikací, jejichž primárním úkolem je vést s uživatelem nezávaznou konverzaci, je třeba zmínit zvláštní kategorii osobních údajů, které představují tzv. citlivé údaje. Podle čl. 9 odst. 1 GDPR se jedná např. o údaje vypovídající o náboženském vyznání či zdravotním stavu uživatele. Zpracování takových informací je v zásadě zakázáno, ovšem odstavec 2 předmětného článku nabízí způsoby jak onen zákaz prolomit.

Tento článek 9 tak bude pro poskytovatele výše vymezených asistentů/aplikací nejspíše relevantní, přestože není primární úlohou asistenta/aplikace získat informace tohoto charakteru. Do hry nám tady totiž opět vstupuje fakt, že uživatel může během konverzace zmínit cokoliv, a právě v souvislosti s tím pak stojí správce dat před otázkou, jak s daty nakládat, jak jsme již zmínili v kapitole 3. 2. 1. 1 Shrnutí GDPR z perspektivy tvůrce a uživatele konverzačního asistenta a konverzační aplikace. Častým příkladem takového „cokoliv“ mohou být emoce.

Ze závazné části ani recitálu není zřejmé, zda emoce spadají pod působnost čl. 9 GDPR, poněvadž ani v jednom případě nejsou explicitně zmíněny. V úvahu tak připadá

[111] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 82-83. ISBN 9783748930952.

jejich podřazení pod kategorii údajů o zdravotním stavu, ovšem to, zda tam opravdu spadají, jasné není.[112] Lze si také položit otázku, zda se vůbec jedná o osobní údaje.

4. 1. 2. 3 Způsob zpracování osobních údajů

Zpracování osobních údajů můžeme chápat vzhledem k jeho definici zakotvené v čl. 4 bodě 2 GDPR, kterou v plném znění zmiňujeme v kapitole 3. 2. 1 Obecné nařízení o ochraně osobních údajů (GDPR), jako „*jakékoliv nakládání s osobními údaji*“[113]. Takové nakládání podléhá zásadám, jež jsou vyjádřeny čl. 5 GDPR a jejichž úkolem je stanovit určité minimální standardy, které je třeba v rámci zpracování následovat, a garantovat tím určitou míru ochrany subjektům údajů. Některým zásadám se věnujeme podrobněji v samostatné kapitole 4. 2 Vybrané zásady zpracování osobních údajů, poněvadž jejich dodržování v oblasti umělé inteligence může činit značné potíže. Zpracování lze také za určitých okolností stanovených čl. 18 GDPR omezit.

Mezi techniky zpracování dat patří mimo jiné anonymizace a pseudonymizace. Tyto dvě metody se v kontextu technologií založených na umělé inteligenci objevují poměrně často, a proto se jim věnujeme v následujících odstavcích.

Jak již bylo uvedeno výše, systémy umělé inteligence mnohdy pracují s velkým objemem dat. Právě dostatečné množství dat je jednou z podmínek, aby systém fungoval přesně takovým způsobem, jak je zamýšleno.

Takový soubor dat nevyhnutelně zahrnuje i osobní údaje. Zpracování osobních údajů však musí být vázáno na určitý účel, jak rozebíráme v kapitole 4. 2. 1 Zásada účelového omezení. Vzhledem k tomu, že nelze účel zpracování omezit na pouhé trénování a vývoj umělé inteligence, může se pro vývojáře systému jednat o těžce překonatelnou překážku. Z tohoto důvodu může připadat v úvahu anonymizace dat, tedy proces, na jehož závěru již nebude možné nalézt jakoukoliv spojitost mezi daty a

[112] DIMATTEO, Larry A.; PONCIBÒ, Cristina a CANNARSA, Michel. *The Cambridge handbook of artificial intelligence: global perspectives on law and ethics*. New York, NY: Cambridge University Press, 2022, 277. ISBN 9781009072168. ISBN 9781009072168.
[113] KOLAŘÍKOVÁ, Linda, HORÁK, Filip. *Umělá inteligence & právo*. Praha: Wolters Kluwer ČR. 2020, 74-75. ISBN 9788075987839.

konkrétní fyzickou osobu. Soubor dat tím bude očištěn od osobních údajů, a tak se vyváže z působnosti ustanovení GDPR.[114]

Metoda anonymizace má ovšem i své nevýhody. Vedle toho, že s ohledem na již zmíněný velký objem dat není tato metoda ve většině případů vůbec možná, nevyplatí se ani ve výzkumu, poněvadž reprezentativnost takto „očištěných" dat prudce klesá. Kromě toho je zde přítomné riziko tzv. reidentifikace, kdy data nejsou anonymizována řádně, a lze je znovu propojit s konkrétní fyzickou osobou. Je proto úlohou správce, aby toto riziko dostatečně eliminoval.[115] Proto se místo anonymizace nabízí jít cestou pseudonymizace.

Co se týče techniky pseudonymizace, je vymezena v čl. 4 bodě 5 GDPR. Výsledkem tohoto postupu jsou údaje, které nyní již nelze přiřadit ke konkrétní fyzické osobě bez použití dodatečných informací. Tyto dodatečné informace tak musí být uloženy na odděleném místě a pomocí organizačních a technických opatření je třeba zabezpečit, aby nebyly propojeny s původně osobními údaji.[116]

Tímto způsobem upravená data jsou velmi dobře využitelná ve výzkumu, poněvadž procesem pseudonymizace nedochází k jejich degradaci. I v tomto případě sice zůstává riziko reidentifikace, ovšem ta může být právě z pohledu výzkumů někdy žádoucí. Příkladem může být studie na poli medicíny, kdy na základě výsledků je možné kontaktovat probandy a například je informovat o nežádoucích vedlejších účincích.[117]

Vzhledem k tomu, že reidentifikace je v případě pseudonymizace poměrně jednoduchá, jsou pseudonymizovaná data stále klasifikována jako osobní údaje, a proto spadají do působnosti GDPR. Správce si tak pseudonymizací nijak neulehčí od povinností stanovených GDPR. Navíc není proces pseudonymizace jednoduchý.

---

[114] DIMATTEO, Larry A.; PONCIBÒ, Cristina a CANNARSA, Michel. *The Cambridge handbook of artificial intelligence: global perspectives on law and ethics*. New York, NY: Cambridge University Press, 2022, 140-141. ISBN 9781009072168.
[115] CORRALES COMPAGNUCCI, Marcelo. *AI in eHealth: human autonomy, data governance and privacy in healthcare*. New York, NY: Cambridge University Press, 2022, 188, 257. ISBN 9781108921923.
[116] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 217-218. ISBN 9783748930952.
[117] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 218. ISBN 9783748930952.

Nemálo vědců tak může mít potíže data odpovídajícím způsobem pseudonymizovat, poněvadž jim chybí k tomu potřebné znalosti a zdroje.[118]

Inspirací může být jihokorejská novela z roku 2020[119], která umožňuje využívat pseudonymizovaná data ve výzkumu, aniž by k nim byl nutný souhlas subjektu údajů.[120] Vědci tak mají výhodnější pozici v porovnání s evropskými kolegy, jelikož nejsou povinni si opatřit ex ante souhlas s užitím dat pro výzkum, a mohou proto využít i data původně sbíraná pro jiný výzkum/účel. Taková legislativa může vést k podpoře výzkumu, který se zakládá na reálných datech. Například mohou být data získána interakcí mezi uživatelem a hlasovým asistentem využita pro lingvistický výzkum. Zůstává ovšem otázkou, zda tímto nedochází k narušení práv subjektu údajů, poněvadž ten netuší, že jeho data, sic pseudonymizovaná, poslouží konkrétní studii. Úskalí hledání rovnováhy mezi ochranou soukromí a podporou výzkumu se věnujeme v kapitole 4. 4 Základní výzvy pro legislativu v oblasti ochrany dat a umělé inteligence.

4. 1. 3 Neosobní údaje

Neosobní údaje jsou definovány nařízením o rámci pro volný tok neosobních údajů v EU, kterému věnujeme samostatnou kapitolu v části mapující legislativu EU. Podle tohoto nařízení se jedná o údaje odlišné od osobních údajů dle GDPR. Taková data jsou z pohledu GDPR anonymními informacemi, které z hlediska zpracování nepožívají žádné ochrany.

Typicky se může jednat třeba o data pocházející ze senzorů zabudovaných v automobilu či v případě konverzačních aplikací o informace, které uživatele neidentifikují (např. počet sourozenců, pracovní pozice). V rámci neosobních údajů můžeme rozlišit dvě kategorie, jak to činí Evropská komise. Zaprvé se jedná o data, která jsou anonymní „per se“, tedy ze své podstaty. Druhou skupinu pak tvoří data, jež

[118] CORRALES COMPAGNUCCI, Marcelo. *AI in eHealth: human autonomy, data governance and privacy in healthcare*. New York, NY: Cambridge University Press, 2022, 257. ISBN 9781108921923.
[119]Personal Information Protection Act, Act No. 16930; Act on the Protection and Utilization of Credit Information, Act No. 16957; Act on the Promotion of Information and Communications Network Utilisation and Information Protection, Act No. 16955
[120] YEW, Gary Chan Kok a YIP, Man (ed.). *AI, Data and Private Law*. Hart Publishing, 2021, 25. ISBN 9781509946860.

byla v minulosti osobními údaji, ale v průběhu času došlo k jejich anonymizaci, čímž ztratila svůj identifikační charakter.[121]

Přestože na základě neosobních údajů nedokážeme ztotožnit konkrétní osobu, představuje manipulace s takovými údaji potenciální hrozbu. Vezměme si za příklad filtry založené na umělé inteligenci, které se zaměřují na specifický nebezpečný obsah a fungují již např. na sociálních sítích. Umělá inteligence může nějakou myšlenku chybně vyhodnotit jako zakázaný obsah a tato data nahlásit. Příslušná osoba se pak s daty, která pochází ze soukromé konverzace, seznámí a má povinnost vyhodnotit, zda se o zakázaný obsah opravdu jedná, či nikoliv. I kdyby se nakonec zakázaný obsah nepotvrdil, byla už část konverzace zpřístupněna, čímž bylo dotčeno soukromí dané osoby.

4. 2 Vybrané zásady zpracování osobních údajů

Jak již bylo zmíněno výše, nakládání dat podléhá určitým zásadám, jejichž přehled nám poskytuje čl. 5 GDPR. Vzhledem k tématu této rigorózní práce se zaměříme pouze na vybrané zásady, které v souvislosti s přítomností umělé inteligence mohou činit potíže. Tyto nesnáze se dotýkají realizace určitých zásad v praxi a také interpretační roviny, kdy ne vždy je znění nařízení srozumitelné a jednoznačné.

4. 2. 1 Zásada účelového omezení

Zásada účelového omezení je stanovena čl. 5 odst. 1 písm. b) GDPR a zakotvuje, že osobní údaje mohou být shromažďovány jen pro jasně vymezený účel. Zásadu můžeme rozdělit na tři části. První část definuje atributy účelu, pro nějž jsou osobní údaje sbírány. Druhou část zásady tvoří zákaz dalšího zpracování údajů způsobem, který je s původním účelem neslučitelný. Poslední část se vztahuje k třetí části definice a stanovuje, že některé vyjmenované účely se nepovažují za neslučitelné s původními účely. Tuto třetí část definice analyzujeme detailněji v kapitole 4. 4. 3 Ochrana soukromí a dat vs. podpora výzkumu, proto se ve stávající kapitole koncentrujeme pouze na první dva úseky zásady.

[121] KOLAŘÍKOVÁ, Linda, HORÁK, Filip. *Umělá inteligence & právo*. Praha: Wolters Kluwer ČR. 2020, 63. ISBN 9788075987839.

Účel, pro který jsou osobní údaje shromažďovány, má být určitý, výslovně vyjádřený a legitimní. Právě konkretizace účelu může činit potíže pro systémy umělé inteligence či pro společnosti, které se soustředí na sběr velkého objemu dat. V době shromažďování dat nemusejí mít konkrétní představu, k čemu data v budoucnu využijí. Zpravidla postupují opačně, tedy nejprve sesbírají dostatečné množství dat, a až poté si vymezí účel, pro který jej budou analyzovat.[122]

Obdobně je tomu i u systémů umělé inteligence, které k trénování využívají velká množství dat. Ne vždy už v době trénování tušíte, k čemu přesně systém umělé inteligence využijete. Navíc čím rozličnější budou trénovací data, tím bude systém s větší pravděpodobností schopnější. Specifikace účelu zpracování dat tak může být ve spojitosti s umělou inteligencí kamenem úrazu. Kromě toho nám GDPR neposkytuje pro konkretizaci účelu žádné mantinely. Není proto jasné, co je dostatečně konkrétní, a co nikoliv. Lze ale předpokládat, že opřít účel pouze o trénování umělé inteligence postačovat nebude.[123]

Druhá část zásady otevírá otázku, za jakých podmínek je účel dalšího zpracování slučitelný s účely původními. Již ze samotného znění této otázky je patrné, že GDPR zaprvé umožňuje zpracovávat data pro více účelů a že zadruhé počítá s možností, že budou osobní údaje zpracovány i později za účelem jiným. Právě druhá implikace je pro vývojáře systému umělé inteligence pozitivní zprávou, neboť umožňuje „recyklovat" již dříve nasbíraná data (samozřejmě stále za předpokladu, že účel této „recyklace" bude vymezen v souladu s GDPR).[124] Zpracování údajů za „pozdějším" účelem je vedle slučitelností účelů limitováno také povinností správce údajů data vymazat v návaznosti na právo subjektu údajů na výmaz dat zakotvené v čl. 17. GDPR.[125]

Co ovšem zakládá onu slučitelnost účelů? Čl. 6 odst. 4 GDPR nám poskytuje určité vodítko v podobě demonstrativního výčtu okolností, které je při otázce

[122] LEE, Joseph a DARBELLAY, Aline. *Data Governance in AI, FinTech and LegalTech*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 64. ISBN 9781800379954.
[123] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 153-154. ISBN 9783748930952.
[124] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 154. ISBN 9783748930952.
[125] DIMATTEO, Larry A.; PONCIBÒ, Cristina a CANNARSA, Michel. *The Cambridge handbook of artificial intelligence: global perspectives on law and ethics*. New York, NY: Cambridge University Press, 2022, 136. ISBN 9781009072168.

slučitelnosti třeba zvážit. Žádné jasné mantinely slučitelnosti tady ani v recitálu však nenajdeme, což vede k právní nejistotě, která se promítá také do oblasti umělé inteligence.[126] Z toho důvodu je třeba zdůraznit, že další zpracování pro jiný účel je možné i v případě, kdy slučitelnost nového a původního účelu dána není. Tuto situaci upravuje návětí čl. 6. odst. 4 GDPR, z něhož vyplývá, že je k takovému zpracování třeba buď souhlasu subjektu údajů, nebo právo Unie či členského státu.[127] V této souvislosti podotýkáme, že v české verzi GDPR došlo v onom návětí[128] zřejmě k předkladatelské chybě. Pasáž zvýrazněná autorkou práce v poznámce pod čarou se totiž s největší pravděpodobností vztahuje k *právu*. Pro tento výklad vedle bodu 40 recitálu GDPR hovoří také anglická[129] a německá[130] verze textu.

Lze shrnout, že zásada účelového omezení s sebou přináší pro systémy umělé inteligence jednu nelehkou překážku v podobě povinnosti konkrétně vymezit účel zpracování dat před samotným zahájením zpracování. Tím může dojít ke snížení výsledné kvality systému umělé inteligence, k jehož trénování jsou data zapotřebí. Navíc podle všeho nepostačuje vymezit účel pouze jako trénování systému umělé inteligence, protože takový účel nesplňuje požadavek na konkrétnost účelu. V této souvislosti je ale třeba upozornit na to, že není jasné, co již lze považovat za konkrétní, a co už naopak nikoliv. Zásada účelového omezení ovšem umožňuje využít data pro pozdější účely a využít i data pocházející od třetí osoby, což je jistě pro umělou inteligenci pozitivní. Na druhou stranu je třeba dodat, že dané je možné pouze za určitých podmínek, jejichž naplnění nemusí být vždy lehké nehledě na nejednoznačný závazný text GDPR.

---

[126] DIMATTEO, Larry A.; PONCIBÒ, Cristina a CANNARSA, Michel. *The Cambridge handbook of artificial intelligence: global perspectives on law and ethics*. New York, NY: Cambridge University Press, 2022, 137. ISBN 9781009072168.

[127] KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research handbook on EU data protection law*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 401. ISBN 9781800371675.

[128] *Pokud zpracování pro jiný účel (…) není založeno na souhlasu subjektu údajů nebo na právu Unie či členského státu,* ***který v demokratické společnosti představuje nutné a přiměřené opatření k zajištění cílů uvedených v čl. 23 odst. 1****, zohlední správce (…)*

[129] *Where the processing for a purpose (…) is not based on the data subject's consent or on a Union or Member State* ***law which constitutes*** *a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall (…)*

[130] *Beruht die Verarbeitung zu einem anderen Zweck (…) nicht auf der Einwilligung der betroffenen Person oder* ***auf einer Rechtsvorschrift*** *der Union oder der Mitgliedstaaten,* ***die*** *in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche (…)*

A jaký účel zpracování by byl dán v případě konverzačních aplikací či asistentů? Jedním z primárních účelů je beze sporu zvýšení kvality konverzačních schopností asistenta na základě již uskutečněných konverzací. Tím by mělo dojít také ke zkvalitnění uživatelského prožitku neboli *user experience*. Je ale takový účel dostatečný, respektive dostatečně konkrétní? Odpověď na tuto otázku nám nepomáhá nalézt ani závazný text GDPR, ani jeho recitál.

4. 2. 2 Zásada transparentnosti

Zásada transparentnosti je zavedena čl. 5. odst. 1 písm. b) GDPR a promítá se do článků 12, 13 a 14 GDPR, které stanovují pro správce dat informační povinnost. Podle této zásady musí být osobní údaje zpracovány transparentním způsobem a správce dat je povinen informovat subjekt údajů o zpracování, *stručným, transparentním, srozumitelným, snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků*.

Zásada má eliminovat neprůhlednost či nesrozumitelnost systémů. Je faktem, že někteří vývojáři navrhují systémy úmyslně tak, aby bylo jejich chování stěží čitelné. Za těchto okolností dává smysl ustanovit pravidlo, které úmyslnou nesrozumitelnost systému zakáže. V případě umělé inteligence však může být zásada transparentnosti zcela fatální. Systémy umělé inteligence jsou na rozdíl od dosavadních systémů tak komplexní, že určitá neprůhlednost vyvěrá z jejich přirozené povahy.[131] Proto se v kontextu umělé inteligence často objevuje fenomén *black box*.

Systém umělé inteligence, který pracuje na základě tzv. hlubokého učení a který lze označit za *black box*, funguje obdobně jako lidský mozek. Dokáže se sám učit a naučené informace si pospojovat tak, že si vytvoří vlastní pravidla, na jejichž základě je způsobilý rozhodnout. Je zde jen jediný prvek, který jej odlišuje od lidského mozku, a to je právě absence schopnosti vysvětlit své pochody. Z tohoto důvodu zůstane příčina

[131] DIMATTEO, Larry A.; PONCIBÒ, Cristina a CANNARSA, Michel. *The Cambridge handbook of artificial intelligence: global perspectives on law and ethics*. New York, NY: Cambridge University Press, 2022, 30. ISBN 9781009072168.

učiněného rozhodnutí zastřena. Je však nezbytné doplnit, že méně transparentní metody dosahují velmi často lepších výsledků než postupy, které lze vysvětlit.[132]

Jak již bylo naznačeno výše, může dodržení transparentnosti bránit i skutečnost, že jsou procesy systému natolik komplikované, že jejich vysvětlení je značně obtížné, i když možné (čímž se liší od případu *black box*). Algoritmy mohou být natolik složité, že jejich pochopení laikem se zdá být takřka nemyslitelné, a natolik jedinečné, že se je vývojář rozhodne chránit prostřednictvím obchodního tajemství. Nejinak je tomu v případě konverzační umělé inteligence. Do jaké míry je tedy třeba být transparentní?[133]

GDPR nám v tomto ohledu neposkytuje jednoznačnou odpověď a na potřebné míře transparentnosti se neshoduje ani akademická obec. Není tak jasné, co vše *smysluplné informace týkající se použitého postupu* zmíněné v rámci práv subjektu údajů[134], zahrnují.[135] Tato nejasnost je spjata s další sporným ustanovením GDPR, a to článkem 22, který poskytuje právo nebýt předmětem rozhodnutí založeného na automatizovaném zpracování. Shoda nepanuje ani v tom, zda toto právo implikuje existenci práva na vysvětlení učiněného rozhodnutí. V případě, že je právo na vysvětlení rozhodnutí garantováno, dávalo by smysl, aby byly subjektu údajů poskytnuty takové informace, na jejichž základě je schopen dospět k závěru, zda bylo rozhodnutí chybné, a případně se proti němu bránit. Taková „kvalita" informací by z tohoto pohledu mohla postačovat také k naplnění zásady transparentnosti.[136]

Na okraj podotýkáme, že není zcela zřejmé, co dělat, pokud by ono minimum informací, které postačuje k naplnění zásady transparentnosti a které je třeba k pochopení rozhodnutí systému, obsahovalo také trénovací data s osobními údaji. Tady pak dochází ke střetu transparentnosti a práva na soukromí osoby, k níž se osobní údaje

[132] LEE, Zhao Yan; KARIM, Mohammad Ershadul a NGUI, Kevin. Deep learning artificial intelligence and the law of causation: application, challenges and solutions. Online. *Information & Communications Technology Law*. 2021, 30 (3), 257, 260. ISSN 13600834. Dostupné z: https://doi.org/10.1080/13600834.2021.1890678. [cit. 2023-11-18].
[133] KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research handbook on EU data protection law*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 164, 168. ISBN 9781800371675.
[134] Čl. 13 odst. 2 písm. f) GDPR, čl. 14 odst. 2 písm. g) GDPR, čl. 15 odst. 1 písm. h) GDPR.
[135] KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research handbook on EU data protection law*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 164, 168. ISBN 9781800371675.
[136] DIMATTEO, Larry A.; PONCIBÒ, Cristina a CANNARSA, Michel. *The Cambridge handbook of artificial intelligence: global perspectives on law and ethics*. New York, NY: Cambridge University Press, 2022, 32. ISBN 9781009072168.

v trénovacích datech vážou.[137] Skutečnost, že si byl tohoto potenciálního střetu zákonodárce vědom, dokládá bod 63 recitálu[138], ovšem nijak ho dále neřeší a k jeho řešení neposkytuje ani žádné vodítko.

Můžeme tak konstatovat, že zásada transparentnosti představuje pro systémy umělé inteligence velké úskalí. Z příslušných ustanovení vyplývá, že zákonodárce vůbec nezohlednil samotnou podstatu umělé inteligence, která spočívá v procesu „samoučení" a inherentní snížené, případně nulové transparentnosti rozhodovacích mechanismů. Není proto jasné, jak má správce dat postupovat v rámci informačních povinností reflektujících onen požadavek transparentnosti, když ani sám vývojář mnohdy nedokáže popsat, jak algoritmus funguje.[139] Kromě toho je v GDPR opomenuto vymezení potřebné míry transparentnosti, která má být naplněna, a nařízení tak pracuje pouze s abstraktním dále nespecifikovaným pojmem transparentnosti.

4. 2. 3. Zásada zákonnosti

Zásada zákonnosti je zakotvena v čl. 5 odst. písm. a) GDPR a podrobněji rozvedena v čl. 6 GDPR. Zpracování osobních údajů je v souladu se zákonem, pokud je odpovídajícím způsobem splněna alespoň jedna z podmínek uvedených v čl. 6 odst. 1 GDPR. V této práci se zaměříme hned na první zmíněnou podmínku, a to je souhlas se zpracováním údajů udělený subjektem údajů, neboť právě tato okolnost je typická pro mobilní aplikace, k nimž se řadí jeden z našich ilustrativních případů v podobě konverzační aplikace využívající prvky umělé inteligence.

4. 2. 3. 1 Souhlas se zpracováním osobních údajů

Podmínky souhlasu upravuje vedle čl. 8 GDPR, který se zaměřuje na souhlas dítěte, také čl. 7 GDPR. Vedle povinnosti správce údajů být schopen doložit udělený souhlas a práva subjektu údajů souhlas odvolat stanovuje ustanovení ve svém druhém odstavci, že v případě písemného prohlášení musí být souhlas se zpracováním osobních

[137] ABBOTT, Ryan. *The reasonable robot: artificial Intelligence and the law*. Cambridge: Cambridge University Press, 2020, viii, 136. ISBN 9781108459020.
[138] *Tímto právem* (pozn. autorky práce: právem na přístup ke shromážděným osobním údajům) *by neměla být nepříznivě dotčena práva ani svobody ostatních, například obchodní tajemství nebo duševní vlastnictví a zejména autorské právo chránící programové vybavení. Zohlednění těchto skutečností by ovšem nemělo vést k tomu, že by subjektu údajů bylo odepřeno poskytnutí všech informací.*
[139] CORRALES COMPAGNUCCI, Marcelo. *AI in eHealth: human autonomy, data governance and privacy in healthcare*. New York, NY: Cambridge University Press, 2022, 156. ISBN 9781108921923.

údajů jasně oddělitelný od dalších skutečností zmíněných v prohlášení. Pro mobilní aplikace to tak v praxi znamená, že by měl být souhlas se zpracováním separován od dalších informací, které jsou uživateli obvykle sdělovány při prvotním spuštění aplikace.[140] Typicky se jedná o souhlas s podmínkami společnosti.

Dále čl. 7 GDPR ve čtvrtém odstavci rozvíjí, k čemu je třeba přihlédnout při posuzování, zda je souhlas svobodný. Podle něj se mimo jiné zohlední, zda je poskytnutí předmětné služby *podmíněno souhlasem se zpracováním osobních údajů, které není pro plnění dané smlouvy nutné*[141]. Máme za to, že u konverzačních aplikací je souhlas se zpracováním osobních údajů nezbytný pro chod aplikace, jelikož uživatel může kdykoliv během konverzace uvést osobní údaj. Jak by pak měl správce údajů postupovat, kdyby tento uživatel neposkytl či odvolal již udělený souhlas? Z tohoto důvodu se jeví podmíněnost fungování aplikace udělením souhlasu se zpracováním údajů jako jediná možnost.

S tím souvisí fakt, že souhlas udělujeme ke zpracování údajů, které o sobě vědomě sdělíme. Ovšem co se bude dít v případě „nevědomky sdělených údajů"? Například z fotky zveřejněné na sociální síti plyne poskytovateli sítě také množství metadat, o jejichž existenci nemusíme mít vůbec tušení.[142] Obdobně můžeme nahlížet na náš ilustrační příklad konverzačních aplikací, kdy se uživatel může do komunikace tak vžít, že si neuvědomuje, co vše o sobě s aplikací sdílí. Vztahuje se souhlas i na tyto údaje, které uživatel sdílí nevědomky? GDPR nám na to neposkytuje jasnou odpověď. Podobné úskalí je u domácích hlasových asistentů. Jak jsme již vícekrát zmínili, mohou tito asistenti zachytit i údaje, které nejsou namířeny vůči nim. Vztahuje se na ně

[140] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. *Privacy and data protection in mobile applications: a study on the app development ecosystem and the technical implementation of GDPR.* 2017, 17. ISBN 9789292042424.

[141] V této souvislosti poukazujeme na zřejmě nepřesnou českou variantu textu. Z nynějšího českého znění vyplývá, že obecně zpracování osobních údajů není nezbytné pro poskytnutí služeb. Anglická verze textu nám v tom příliš nepomůže (*consent to the processing of personal data that is not necessary for the performance of that contract*: slovo *that* se může vztahovat jak k datům, tak ke zpracování), za to německá ano. Z ní totiž vyplývá, že jsou to konkrétní osobní údaje, které nejsou pro poskytnutí služeb třeba (*von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind*). Tato interpretace by však vedla k závěru, že je nezbytné subjekt údajů v souhlasu informovat, jaké konkrétní osobní údaje budou správcem zpracovány. V případě konverzačních aplikací se jeví jako jediná možnost vymezit osobní údaje jako „všechny osobní údaje, které budou uživatelem aplikace sděleny", jelikož nelze říci, co vše nám uživatel během konverzace poví.

[142] KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research handbook on EU data protection law*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 452. ISBN 9781800371675.

souhlas? A co pak v případě třetích osob? Souhlas se zpracováním údajů totiž uděluje jedna osoba. Ale co když asistent zaznamená i input od jiné osoby? V ideálním případě by mělo zařízení podle hlasu detekovat, že se jedná o jinou osobu, která souhlas se zpracováním ještě neudělila, a k udělení souhlasu ji vyzvat. Pokud ale není technologie dostatečně pokročilá a schopna detekce hlasu, není jasné, jak má poté správce zjistit, že se nasbíraná data vztahují k jiné osobě, než je primární uživatel asistenta.[143]

Jakými atributy by měl souhlas disponovat? Dle definice uvedené v čl. 4 bodě 11 GDPR má být *svobodný, konkrétní, informovaný a jednoznačný projev vůle*. Z tohoto výčtu je zřejmé, že je souhlas jako jedna z podmínek zákonnosti zpracování údajů spjat s dalšími zásadami zpracování, konkrétně se zásadami účelového omezení a transparentnosti. Především prvek informovanosti odráží požadavky na jasně vymezený účel zpracování a srozumitelnost procesu zpracování. I u souhlasu proto budeme narážet na to, kdy je souhlas dostatečně informovaný.

U informovanosti navíc narážíme na trend, že uživatelé tyto klauzule vůbec nečtou a automaticky klikají na tlačítko souhlasu. V dnešní době, kdy odsouhlasíte podmínky dané společnosti a podmínky zpracování dat u aplikací i několikrát denně, se není čemu divit. Kromě zahlcení těmito podmínkami jsou zde další faktory. Jsou služby, které chtějí či potřebují uživatelé využívat tak jako tak, i když se třeba podivují nad tím, k čemu potřebuje daná služba příslušný údaj. Navíc v některých případech jsou klauzule souhlasu formulovány tak zdlouhavě a nesrozumitelně, že jejich čtením uživatelé jednoduše nechtějí ztrácet čas. Částečným řešením by mohlo být postavit klauzuli tak, aby byla jasná, srozumitelná a zároveň ideálně stručná. Nehledě na to, jak náročná úloha to může být v případě aplikací fungujících na bázi komplikovaných algoritmů, je třeba poznamenat, že ani jednodušší verze klauzulí nezaručuje, že si ji uživatelé poctivě přečtou. Vždy totiž v prvé řadě záleží na motivaci uživatele a jeho zájmu o to, jak je s jeho daty nakládáno.[144]

Souhlas by měl být také svobodný. U mobilních aplikací však nezřídka narazíme na klauzuli souhlasu, u níž už je políčko souhlasu předem zaškrtnuto. To však není

[143] DE BRUYNE, Jan a VANLEENHOVE, Cedric (ed.). *Artificial Intelligence and the Law.Intersentia*, 2021, 186. ISBN 9781839701047.
[144] LEE, Joseph a DARBELLAY, Aline. *Data Governance in AI, FinTech and LegalTech*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 66-73. ISBN 9781800379954.

v souladu s požadavky na svobodný souhlas stejně jako situace, kdy je souhlas se zpracováním údajů presumován a pokud ho uživatel udělit nechce, musí vyvinout speciální úsilí.[145]

Další potíž může pro poskytovatele aplikace představovat právo subjektu údajů na odvolání souhlasu se zpracováním. Pokud na něj dojde, *není* dle čl. 7 odst. 3 *dotčena zákonnost zpracování vycházejícího ze souhlasu*. Ovšem to nejspíš neznamená, že tyto „dřívější" údaje může správce nadále uchovávat. Naopak by mělo dojít k jejich výmazu v souladu s čl. 17odst. 1 písm. b) GDPR. To může být v kontextu systému umělé inteligence, která se z takových dat již „učila", a s tím spjatým velkým objemem dat poněkud problematické, a může tím ohrozit fungování celého systému. Proto by měl správce zvážit variantu, zda se neopřít o jinou skutečnost, která naplňuje zásadu zákonnosti a nepředstavuje takové riziko.[146]

Na závěr podotýkáme, že ze závazné části nikde explicitně nevyplývá, že by měl být souhlas se zpracováním osobních údajů udělen před samotným zpracováním. Někteří tuto povinnost odvozují z čl. 24 odst. 1 GDPR, kde je zakotvena odpovědnost správce za zpracování údajů v souladu s GDPR. Dle našeho názoru se však jedná o tak obecné ustanovení, z něhož povinnost obstarat si souhlas před zahájením samotného zpracování lze dovodit jen stěží.[147] Tím však nepopíráme, že dává smysl, aby bylo třeba si souhlas se zpracováním údajů obstarat před zpracováním.

4. 2. 4 Zásada minimalizace údajů

Zásada minimalizace údajů je zakotvena v čl. 5 odst. 1 písm. c) GDPR. Podle této zásady mají být osobní údaje *přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány*.

Tato zásada představuje pro umělou inteligenci určitou výzvu vzhledem k tomu, že se fungování systémů umělé inteligence zakládá na velkém objemu dat. Čím více dat má umělá inteligence k dispozici, tím lépe pro její kvalitu, protože se z těchto dat může

[145] KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research handbook on EU data protection law*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 464. ISBN 9781800371675.
[146] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 91-92. ISBN 9783748930952.
[147] DIMATTEO, Larry A.; PONCIBÒ, Cristina a CANNARSA, Michel. *The Cambridge handbook of artificial intelligence: global perspectives on law and ethics*. New York, NY: Cambridge University Press, 2022, 139. ISBN 9781009072168.

umělá inteligence dále učit. Tuto rovnici ale GDPR nenásleduje, protože množství údajů omezuje na *nezbytný rozsah*. [148]

Jak však vypadá *nezbytný rozsah* údajů u systému umělé inteligence? GDPR tento rozsah nijak nespecifikuje a není se čemu divit. *Nezbytný rozsah* se totiž bude lišit případ od případu.[149] Na druhou stranu tím, že zákonodárce tento pojem nijak nepřiblížil, přenesl břemeno interpretace na adresáty právní úpravy.

V případě virtuálních či hlasových asistentů může být tato zásada obzvlášť problematická. Jak už jsme v práci zmínili, může u nich dojít i k nahrávání inputu uživatele, aniž by uživatel daná slova mířil právě na asistenta. Další obtíže nalezneme u ryze konverzačních asistentů či aplikací. V tomto případě je každý input uživatele pro konverzaci důležitý, a proto se nabízí, že *nezbytný rozsah* v tomto případě zahrnuje veškeré údaje.

4. 3 Vybraná práva subjektu údajů

GDPR reflektuje jednotlivé zásady, kterými se zabýváme v předešlé kapitole, také v podobě ustanovení konkrétních práv, která slouží k ochraně zájmů subjektu osobních údajů. Jedná se zejména o právo subjektu údajů na přístup k osobním údajům (čl. 15), právo na opravu (čl. 16), právo na výmaz (čl. 17), právo na omezení zpracování (čl. 18), právo na přenositelnost údajů (čl. 19), právo vznést námitku (čl. 21) a právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování (čl. 22). Právě posledně zmíněnému právu a právu na výmaz věnujeme dílčí samostatné kapitoly, poněvadž mohou činit v případě umělé inteligence potíže.

4. 3. 1 Právo na výmaz (právo být zapomenut)

Hojně zmiňovaným právem zavedeným GDPR je právo na výmaz neboli „právo být zapomenut“ v čl. 17 GDPR. Za podmínek stanovených v čl. 17 odst. 1 GDPR je správce povinen na žádost subjektu údajů smazat veškeré jeho osobní údaje. Jednou z těchto podmínek je odvolání souhlasu, na jehož základě bylo zpracování zákonné. Jak

[148] BARFIELD, Woodrow a PAGALLO, Ugo. *Research handbook on the law of artificial intelligence*. Cheltenham, UK: Edward Elgar Publishing, 2018, 299. ISBN 9781786439048.
[149] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 162. ISBN 9783748930952.

jsme již zmínili v kapitole 4. 2. 3. 1 Souhlas se zpracováním osobních údajů, činí toto ustanovení v kontextu umělé inteligence nemalé potíže. Tím, že se umělá inteligence včetně umělé inteligence konverzační z dat učí „ihned“ a tyto osobní údaje jsou součástí velkého objemu dat, zdá se na první pohled velice náročné, v některých případech až nemožné, vyhovět požadavku subjektu údajů a údaje smazat, aniž by byla dotčena kvalita fungování systému umělé inteligence.

Upozorněme ještě na třetí odstavec článku 17 GDPR, který je pro umělou inteligenci významný na poli výzkumu. Podle čl. 17 odst. 3 písm. d) GDPR totiž správce není povinen požadavku subjektu na výmaz dat vyhovět, jestliže je zpracování nezbytné pro vědecký výzkum. Jedná se tak o další ze vstřícných kroků úpravy vůči výzkumu, kterým se detailněji věnujeme v kapitole 4. 4. 3 Ochrana soukromí a dat vs. podpora výzkumu.

4. 3. 2 Právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování

Jak jsme již v práci nejednou zmínili, GDPR se umělé inteligenci a jejím specifikům nijak zvlášť nevěnuje. Na systémy umělé inteligence tak dopadají všeobecná ustanovení. Jedinou výjimku tvoří čl. 22 GDPR, který se zaměřuje na tzv. automatizované individuální rozhodování.[150]

4. 3. 2. 1 Pojem automatizované individuální zpracování

Už samotný pojem *automatizované individuální rozhodování* představuje interpretační oříšek. Není totiž zcela zřejmé, co vše pod něj můžeme podřadit. GDPR ho ve svém čl. 22 odst. 1 GDPR rozvádí jako *rozhodnutí založené výhradně na automatizovaném zpracování, včetně profilování, které má pro subjekt údajů právní účinky nebo se ho obdobným způsobem významně dotýká*.

Ne všechna rozhodnutí systému umělé inteligence mají na subjekt takto vymezený významný dopad. Např. systém, který reguluje v domácnosti subjektu údajů teplotu na základě vytyčených parametrů, sem jistě spadat nebude. Naopak pokud systém umělé inteligence objedná pro subjekt údajů výrobek či službu pouze na základě

[150] DIMATTEO, Larry A.; PONCIBÒ, Cristina a CANNARSA, Michel. *The Cambridge handbook of artificial intelligence: global perspectives on law and ethics*. New York, NY: Cambridge University Press, 2022, 133. ISBN 9781009072168.

svého vyhodnocovacího procesu, bude se jednat o rozhodnutí, které má pro subjekt právní účinky.[151]

Kde však leží ona hranice, která dělí rozhodnutí významně se dotýkající subjektu údajů od těch, která se subjektu dotýkají, ale nikoliv významně? GDPR nám neříká, co je tím komponentem, který činí rozhodnutí pro subjekt údajů významné.[152] Jedná se přitom o zásadní skutečnost, neboť druhá zmíněná skupina rozhodnutí (tzn. rozhodnutí, která nemají na subjekt významný dopad) nebude čl. 22 GDPR dotčena, a bude tak a priori povolena. Tak jako tak můžeme konstatovat, že v případě konverzačních aplikací, jejichž účelem je uživatele pouze zabavit prostřednictvím nezávazného rozhovoru, se o rozhodování s významným dopadem jednat nebude.

Další otázkou je, zda musí být rozhodování prosté jakéhokoliv podílu člověka na něm. Podíl člověka na rozhodování může hrát s ohledem na výsledek rozhodování různou roli, ale vždy musí být alespoň v určité nezbytné míře přítomný, jinak by systém vůbec nebyl schopen rozhodnout. Je totiž třeba, aby člověk systém zásoboval dostatkem příslušných dat a systém nastavil tak, že má rozhodnutí učinit.[153] Vedle toho může člověk rozhodnutí, které učinil na základě vlastního vyhodnocení systém umělé inteligence, implementovat, aniž by do něj jakkoliv zasáhl. V těchto případech je asi nesporné, že účast člověka na finálním rozhodnutí je minimální, na jeho obsahu je zcela nulová, a proto lze rozhodnutí klasifikovat jako automatizované.[154]

Můžeme tak dojít k závěru, že určitý zásah člověka je v případě automatizovaného rozhodování nezbytný. Pokud se jedná pouze o nezbytné formální kroky, které neovlivňují rozhodnutí v jeho obsahu, pak se na rozhodování stále vztahuje čl. 22 GDPR.

Co se týče judikatury, vyložil Soudní dvůr EU čl. 22 GDPR pouze jedinkrát, a to teprve v prosinci roku 2023 ve věci C-634/21 OQ v. Land Hessen. Společnost SCHUFA

[151] BARFIELD, Woodrow a PAGALLO, Ugo. *Research handbook on the law of artificial intelligence*. Cheltenham, UK: Edward Elgar Publishing, 2018, 299-300. ISBN 9781786439048.
[152] KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research handbook on EU data protection law*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 448. ISBN 9781800371675.
[153] KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research handbook on EU data protection law*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 439. ISBN 9781800371675.
[154] CORRALES COMPAGNUCCI, Marcelo. *AI in eHealth: human autonomy, data governance and privacy in healthcare*. New York, NY: Cambridge University Press, 2022, 151. ISBN 9781108921923.

Holding AG poskytuje svým smluvním partnerům informace o úvěrové bonitě osob. Každé osobě tak přiřadí určitou hodnotu, tzv. *Score-Wert*, jež se vypočítává automatizovaně, a tu poskytne smluvnímu partnerovi, který se na jejím základě rozhodne úvěr dané osobě poskytnout, nebo neposkytnout. Kvůli této negativní hodnotě nebyl úvěr poskytnut společnosti OQ. Společnost OQ proto požadovala, aby jí společnost SCHUFA sdělila veškeré údaje, které se jí týkají. Obdržela ovšem pouze svou *Score-Wert* a obecné principy výpočtu této hodnoty, nikoliv jednotlivé údaje, na jejichž základě se *Score-Wert* vypočítává, poněvadž to je dle mínění společnosti SCHUFA předmětem obchodního tajemství. Soudní dvůr tak stál před otázkou, zda takový výpočet *Score-Wert* lze podřadit pod pojem automatizované individuální rozhodování. Usnesl se, že i takový výpočet lze podřadit pod pojem *rozhodování*, protože tento pojem je třeba vykládat extenzivně. Činnost, kterou společnost SCHUFA provádí, lze chápat jako *profilování*, tudíž i tato podmínka je naplněna. Navíc je výsledek této činnosti východiskem pro rozhodnutí, zda osobě bude úvěr poskytnut, či nikoliv, takže se osoby *významně dotýká*. Z toho vyplývá, že pod pojem rozhodování nespadá pouze „finální akt“, který má právní účinky či významný dopad, ale také pouhý „mezistupeň“ rozhodování, který má na konečné rozhodnutí vliv.[155]

4. 3. 2. 2 Právo, nebo zákaz?

Ačkoliv je v čl. 17 odst. 1 GDPR stanoveno, že má subjekt údajů *právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování*, a také recitál ve svém bodě 71 hovoří o právu subjektu, lze na celé ustanovení nahlížet také jako na zákaz, jak činí například Pracovní skupina pro ochranu údajů zřízená podle čl. 29[156]. Pokud by se nejednalo o právo, ale o striktní zákaz, u něhož jsou možné výjimky pouze na základě čl. 22 odst. 2 GDPR, pak by pravidlo nečinit subjekt údajů předmětem onoho rozhodování platilo paušálně, a nikoliv až po uplatnění práva subjektem údajů.[157] Tento výklad byl nakonec podpořen také Soudním dvorem EU

[155] *Shrnutí rozsudku Soudního dvora (prvního senátu) ze dne 7. prosince 2023 ve věci C-634/21 OQ v. Land Hessen*. Online. InfoCuria. 2023. Dostupné z: https://curia.europa.eu/juris/document/document.jsf;jsessionid=136B3A5CC22DA3F5C460B325C9E33C36?text=&docid=280437&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=1762372. [cit. 2024-02-01].

[156] Tato pracovní skupina byla zřízena směrnicí 95/46/ES a byla nahrazena Evropským sborem pro ochranu osobních údajů.

[157] DE BRUYNE, Jan a VANLEENHOVE, Cedric (ed.). *Artificial Intelligence and the Law.Intersentia*, 2021, 196. ISBN 9781839701047.

v rozsudku ve věci C-634/21 OQ v. Land Hessen, který je představen v předchozí kapitole. V bodě 52. rozsudku konstatuje, že čl. 22 odst. 1 GDPR „*stanoví obecný zákaz, jehož porušení se taková osoba nemusí dovolávat individuálně*“.[158]

Další související důsledek takového výkladu by spočíval v tom, že by takový proces podléhal zásadě zákonnosti ustanovené v čl. 6 GDPR, a musel by se proto opírat o jednu ze skutečností zakládajících zákonnost zpracování údajů.[159]

Tak jako tak je třeba mít stále na paměti, že se čl. 22 GDPR vztahuje pouze na taková rozhodnutí, která mají na subjekt údajů negativní dopad, přestože ani v tom nepanuje v literatuře stoprocentní shoda. Převažuje však názor, že se čl. 22 GDPR na rozhodnutí s ryze pozitivními účinky neuplatní. Opačný závěr by totiž byl v rozporu se samotným smyslem práva, který má sloužit k bránění zájmů subjektu údajů.[160]

4. 3. 2. 3 Zakotvení práva na vysvětlení

Jak jsme již naznačili v kapitole 4. 2. 2 Zásada transparentnosti, souvisí s čl. 22 GDPR a subjektovým právem na informace (čl. 13, 14 a 15 GDPR) otázka, zda z nich lze odvodit právo na vysvětlení procesu, kterým systém umělé inteligence došel ke konečnému rozhodnutí.

Ze znění samotného čl. 22 GDPR takové právo vydedukujeme jen stěží. Právo subjektu údajů na přístup ke *smysluplným informacím týkajícím se použitého postupu* je zakotveno právě v čl. 13., 14. a 15 GDPR. Jak jsme uvedli v kapitole o zásadě transparentnosti, není jasné, co vše takové informace mají zahrnovat.

---

[158] *Rozsudek Soudního dvora (prvního senátu) ze dne 7. prosince 2023 ve věci C-634/21 OQ v. Land Hessen*. Online. InfoCuria. 2023. Dostupné z: https://curia.europa.eu/juris/document/document.jsf;jsessionid=136B3A5CC22DA3F5C460B325C9E33C36?text=&docid=280426&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=1762372. [cit. 2024-02-01].

[159] KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research handbook on EU data protection law*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 449. ISBN 9781800371675.

[160] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 125, 127. ISBN 9783748930952.

To, co otázku existence práva na vysvětlení podnítilo především, je recitál GDPR, konkrétně bod 71, který zmiňuje *právo na získání vysvětlení o rozhodnutí učiněném po takovém posouzení a na napadnutí tohoto rozhodnutí*.[161]

Není ani jasné, zda se má právo na vysvětlení vztahovat pouze na to, jak bylo dosaženo konkrétního rozhodnutí, anebo zda mají být jeho předmětem obecné principy fungování procesu automatizovaného zpracování dat.[162]

Proti zakotvení práva na vysvětlení svědčí vedle výše uvedených nejasností také právo duševního vlastnictví či obchodní tajemství, jejichž úkolem je chránit podstatu fungování těchto algoritmů. Pokud i přesto dojdeme k přesvědčení, že právo na vysvětlení z GDPR vyplývá, nejsou pak jasné jeho hranice ani na co přesně se vztahuje, což vzbuzuje právní nejistotu.[163]

Na závěr této kapitoly připomínáme, že vysvětlitelnost je také jednou z etických zásad důvěryhodné umělé inteligence, které se věnují Etické pokyny analyzované v kapitole 3. 3. 3 Etické pokyny pro zajištění důvěryhodnosti umělé inteligence. Již tento dokument připouští, že v některých případech může být vysvětlení rozhodnutí, k němuž dospěla umělá inteligence, velice náročné či zcela nemožné. Dokument v této souvislosti zmiňuje jiné nástroje, které mohou nevysvětlitelnost „černé skříňky" alespoň částečně kompenzovat. Jedná se například o transparentní vymezení toho, čeho je systém umělé inteligence schopen. Jak vidno, platná legislativa však tyto alternativy zmíněné nezávaznými pokyny nereflektovala.

4. 4 Základní výzvy pro legislativu v oblasti ochrany dat a umělé inteligence

Vzhledem k tomu, že umělá inteligence se neustále vyvíjí, představuje už sama o sobě pro zákonodárství nemalou výzvu. Pokud k tomu přidáme ještě problematiku ochrany dat, stojí tvůrci legislativy před nemalým úkolem.

[161] KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research handbook on EU data protection law*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 171.
[162] KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research handbook on EU data protection law*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 552. ISBN 9781800371675.
[163] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 179, 181, 185, 186. ISBN 9783748930952.

Nehledě na věcnou složitost oblasti, kterou míní zákonodárce regulovat, by měly být na počátku tvorby legislativy zodpovězeny dvě otázky, a to zda již nastal čas danou materii regulovat, a případně jakou formu úpravy zvolit.

4. 4. 1 Otázka načasování

Umělá inteligence je dynamický fenomén. Netušíme tak, kdy bude zakončen její vývoj a do jakého stadia v rámci něj vůbec dospěje. Nabízí se proto otázka, zda již nastal čas umělou inteligenci ošetřit na legislativní úrovni. Pokud ano, přistoupila Evropská unie k regulaci včas, pozdě, nebo příliš brzy? Nebo naopak měla zatím ponechat umělou inteligenci stran jakékoliv úpravy?

Podle některých je třeba umělou inteligenci regulovat co nejdříve. Podle jejich názoru není jasné, jak by mohlo být vyčkávání s legislativou prospěšné pro inovace a vývoj. Přestože jsou inovace a priori vnímány jako přínos pro lidstvo, nemusí vždy znamenat krok vpřed.[164] Již dnes můžeme pozorovat, že se některé formy umělé inteligence rozvíjí tak rychle a nepředvídatelně, že jejich výstup nemusí být v souladu se základními lidskými hodnotami a svobodami. Jako příklad mohou posloužit systémy založené na umělé inteligenci, které se chovají diskriminačním způsobem, čemuž se věnujeme v samostatné kapitole 4. 5. 2 Diskriminace a předpojatost.

Již teď nasvědčuje vše tomu, že v budoucnu nás systémy založené na umělé inteligenci zastoupí v některých pracích. Je proto třeba počítat se snížením počtu pracovních míst v příslušných oblastech a s tím souvisejícím nárůstem nezaměstnanosti a toto zrcadlit v právních předpisech.[165]

Přívrženci časné regulace jsou přesvědčeni, že brzká zákonná úprava umožní již na začátku vytyčit určité mantinely pro technologie založené na umělé inteligenci, a ty pak v závislosti na pokroku ve výzkumu aktualizovat. Od počátku tak bude možné legislativní cestou podpořit využití předností, jimiž umělá inteligence disponuje, a zároveň podchytit negativa, která jsou uvedena v předchozích odstavcích. Je jasné, že vývoj v reálném světě bude vždy napřed před psanými pravidly, jejichž ustanovení

[164] BARFIELD, Woodrow a PAGALLO, Ugo. *Research handbook on the law of artificial intelligence*. Cheltenham, UK: Edward Elgar Publishing, 2018, 157, 162, 165. ISBN 9781786439048.
[165] BARFIELD, Woodrow a PAGALLO, Ugo. *Research handbook on the law of artificial intelligence*. Cheltenham, UK: Edward Elgar Publishing, 2018, 176. ISBN 9781786439048.

předchází analýza stavu, diskuze a po většinou řádný legislativní proces, proto by měl zákonodárce vynaložit veškeré úsilí, aby byla tato časová prodleva co nejmenší.[166]

Oproti tomuto proudu se formuje skupina lidí, podle jejichž názoru brání raná legislativa technologickému růstu. Brzká regulace se nemůže opírat o zkušenosti s danými technologiemi, a právě v tom tkví jádro jejího nedostatku, které může vést ke dvěma rizikovým scénářům. První variantou je, že pravidla budou příliš obecná, a nedokážou tak reflektovat specifika technologie. Vysoká míra obecnosti úpravy jde navíc často ruku v ruce se sníženou srozumitelností textu. V případě druhého rizikového scénáře se sice zákonodárce bude snažit reagovat na novou technologii co nejkonkrétněji, ovšem tím, že nemá dostatek zkušeností s touto technologií, hrozí, že bude úprava trpět zásadními vadami. Často uváděnými příklady, na nichž se demonstruje prospěšnost takřka nulové počáteční regulace, jsou internet a související výdobytky v podobě e-mailu, webových stránek a prohlížečů. Na druhou stranu je třeba říci, že kromě toho, že je umělá inteligence diametrálně odlišná technologie, se ani internet ve svých počátcích neobešel bez jakékoliv úpravy.[167]

Když se nad otázkou načasování zamyslíme z perspektivy evropského práva, je třeba konstatovat, že jde Evropská unie spíše cestou brzké regulace. Zásadní předpis v oblasti ochrany dat, GDPR, se vztahuje na systémy umělé inteligence takřka od začátku, jelikož se nejedná o legislativu šitou na míru umělé inteligenci. Co se týče speciálních předpisů zaměřujících se výhradně na systémy umělé inteligence, jsou tyto k dnešnímu dni ve fázi legislativního procesu, jak pojednává kapitola mapující legislativu relevantní pro téma předmětné rigorózní práce. Už dnes se však objevují kritické hlasy, že Evropská unie svými stávajícími i plánovanými pravidly brzdí v oblasti umělé inteligence výzkum a inovace. Drtivá většina technologických gigantů vzniká a sídlí mimo území EU, kde se také koncentruje výzkum. Stojí však za úvahu, zda je toto opravdu důsledek (brzkého) načasování legislativy, a nikoliv její formy a obsahu. Otázkou, zda má GDPR negativní vliv na výzkum v oblasti umělé inteligence, se zaobíráme v kapitole 4. 4. 3. Ochrana soukromí a dat vs. podpora výzkumu.

[166] BARFIELD, Woodrow a PAGALLO, Ugo. *Research handbook on the law of artificial intelligence*. Cheltenham, UK: Edward Elgar Publishing, 2018, 162. ISBN 9781786439048.
[167] BARFIELD, Woodrow a PAGALLO, Ugo. *Research handbook on the law of artificial intelligence*. Cheltenham, UK: Edward Elgar Publishing, 2018, 163-165. ISBN 9781786439048.

4. 4. 2 Otázka formy regulace

V situaci, kdy se již rozhodne, že je třeba přistoupit k právní úpravě určité materie, je třeba si zodpovědět otázku, jaká forma regulace se v daném případě jeví jako nejefektivnější. Zároveň je dobré si uvědomit, že příliš velký důraz na ochranu dat může vést k redukci inovací, a naopak vysoká míra inovace často probíhá na úkor ochrany.[168]

Jaké formy tedy vůbec přicházejí v úvahu? Základní varianta, k níž se přistupuje velmi často, je forma závazného předpisu. V rámci státu se jedná o zákon, v rámci Evropské unie je to pak nařízení, nebo směrnice. Vedle toho ale máme k dispozici i další nástroje, jako jsou technické normy (např. ISO), odvětvové standardy, povolenky, s nimiž lze obchodovat, stanovení informační povinnosti či daně. Je tak pouze na předních představitelích státu a daného odvětví, aby společně zvážili pro a proti každého druhu úpravy a vybrali tu, která konkurenceschopnost tamních hráčů posílí, a nikoliv oslabí. Z toho vyplývá, že pokud je zvolena správná forma, nedochází regulací ke zpomalení technologického rozmachu.[169]

Tvůrce úpravy by přitom měl mít na paměti tři rizikové situace, kterých by se měl pokusit vyvarovat. První takovou situaci představuje nekonzistentní regulace, která je v některých aspektech nepatřičně neúměrná, poněvadž upravuje i záležitosti, u nichž to není zapotřebí, a v jiných aspektech naopak nedostatečná, protože opomíjí významné otázky. Druhé riziko spočívá v příliš obecné úpravě, kterou lze jen velmi stěží aplikovat na konkrétní případy v reálném světě. Poslední nebezpečí souvisí částečně s časem, a proto jsme se ho dotkli již v předcházející kapitole. Tkví totiž v nedostatku flexibility. Legislativa není v tomto případě schopná reagovat na vnější změny a přizpůsobovat jim svůj obsah.[170] Je třeba přiznat, že všechny tři zmíněné nedostatky se povětšinou týkají státní/nadnárodní legislativy, a nikoliv jejich alternativ zmíněných v předchozím odstavci. Ani tam však nejsou výjimkou.

V případě ochrany dat můžeme zmínit i dvě formy úpravy aplikované právě v této doméně. Jedná se o tzv. „*privacy by design*“ a datový trust. První z nich spočívá

[168] YEW, Gary Chan Kok a YIP, Man (ed.). *AI, Data and Private Law*. Hart Publishing, 2021, 117. ISBN 9781509946860.
[169] BARFIELD, Woodrow a PAGALLO, Ugo. *Research handbook on the law of artificial intelligence*. Cheltenham, UK: Edward Elgar Publishing, 2018, 165. ISBN 9781786439048.
[170] YEW, Gary Chan Kok a YIP, Man (ed.). *AI, Data and Private Law*. Hart Publishing, 2021, 54-55. ISBN 9781509946860.

v prevenci. Zakládá se na myšlence, že je efektivnější myslet na soukromí již v procesu designu technologie a při jejím provozu než technologii přizpůsobovat jednotlivým zásadám ex post. To je také případ GDPR. Datový trust naopak funguje tak, že ten, kdo data sbírá, předá kontrolu nad daty jiné zákonem regulované entitě, která stanoví pro data závazná pravidla reflektující okolnosti konkrétního případu. Díky tomu, že se pravidla odvíjí vždy od konkrétního případu, není těžké je flexibilně přizpůsobovat dle potřeby.[171]

Z hlediska obsahu jen na okraj podotýkáme, že velkým nedostatkem mnoha legislativ, které se uplatní i na systémy umělé inteligence, je předpoklad, že za každým počínáním programu či stroje stojí člověk, což ale v případě umělé inteligence neplatí.[172] V tomto ohledu je třeba vyzdvihnout čl. 22 GDPR, který potírá automatizované rozhodnutí.

4. 4. 3 Ochrana soukromí a dat vs. podpora výzkumu

Jak jsme již nastínili v kapitole 4. 1. 2. 3 Způsob zpracování osobních údajů, je jednou z výzev, kterým zákonodárci při tvorbě legislativy beze sporu čelí, stanovení pravidel takovým způsobem, aby nebránila inovacím, ale naopak je podporovala. Legislativa, jež v rámci vůdčí hodnoty ochrany soukromí zakotvuje mantinely pro nakládání s daty, totiž může představovat pro vědu určitou komplikaci. Ne vždy si totiž zákonodárci uvědomují, že některá ustanovení mohou brzdit či ztěžovat inovace, které v dnešní době vyžadují velký objem dat (*big data*). Již v předchozí kapitole jsme zmínili, že nadměrná regulace může inovace právě zpomalit. Nejinak je tomu v oblasti technologií založených na umělé inteligenci. Při tvorbě předpisů v oblasti ochrany dat je tak třeba myslet na využití dat ve výzkumu a poměřovat na miskách vah na straně jedné práva jednotlivce, mezi něž můžeme vedle primárního práva na ochranu dat zařadit také právo na informovanost ohledně užití dat a způsobu jejich zpracování, a na straně druhé podporu vědy a výzkumu. To je totiž první krok k tomu, aby legislativa nestála vůči inovacím přímo v opozici.

[171] YEW, Gary Chan Kok a YIP, Man (ed.). *AI, Data and Private Law*. Hart Publishing, 2021, 56-57, 125. ISBN 9781509946860.
[172] BARFIELD, Woodrow a PAGALLO, Ugo. *Research handbook on the law of artificial intelligence*. Cheltenham, UK: Edward Elgar Publishing, 2018, 159. ISBN 9781786439048.

Výzkum často pracuje s osobními, případně již dříve zmíněnými pseudonymizovanými údaji. Na oba druhy dat se vztahují pravidla GDPR, jak uvádíme v kapitole 4. 1. 2. 3 Způsob zpracování dat, která mimo jiné stanovují, že zpracování dat musí naplňovat alespoň jednu podmínku uvedenou v čl. 6 GDPR, aby bylo zákonné, a musí se vázat ke konkrétnímu účelu. Zásadami zákonnosti a vázanosti dat k určitému účelu se zabývá následující kapitola.

Jedním z účelů, s nímž GDPR pracuje, je vědecký výzkum. Na otázku, co vše spadá pod tento pojem, nenalezneme odpověď v závazné části nařízení, ale v bodě 159 recitálu, který obsahuje demonstrativní výčet, kde je zmíněn i technologický vývoj.

To však neznamená, že se vědec při zpracování dat může při vymezení účelu omezit na konstatování „vědeckého výzkumu". I na tento účel totiž dopadá čl. 5 odst. 1 písm. b) GDPR, podle něhož má být účel co nejvíce specifikován. Nejčastěji tak bude vytyčení účelu zhruba odpovídat znění výzkumné otázky. Vedle dostatečného upřesnění účelu má správce dat ještě další povinnost, a to informovat subjekt údajů o účelu ještě před samotným zpracováním dat. To může činit v případě vědy značné potíže, protože ne vždy je možné účel zpracování dat konkretizovat ještě před začátkem výzkumu.[173] Za příklad si můžeme vzít lingvistický výzkum konverzačních dat nasbíraných prostřednictvím hlasového asistenta. V rámci účelu si stanovíme, že se zaměříme na konkrétní jazykový jev. Když ale posléze data analyzujeme, můžeme dojít k závěru, že by bylo příhodnější se koncentrovat na jiný jev. I s tímto případem GDPR počítá. Z již zmíněného čl. 5 odst. 1 písm. b) GDPR vyplývá, že nelze osobní údaje dále zpracovávat způsobem, který je s vytyčeným účelem neslučitelný, přičemž je zde explicitně stanoveno, že se další zpracování pro účely vědeckého výzkumu nepovažuje za neslučitelné s původními účely. Lze tedy usoudit, že je další zpracování pro účely vědeckého výzkumu *vždy* slučitelné s původními účely, nebo pouze *zpravidla*? Pokud by měl zákonodárce na mysli první variantu, proč by nevolil jasnější formulaci, že *je další zpracování pro účely vědeckého výzkumu slučitelné s původními účely*, a uchýlil by se k dvojímu záporu (není neslučitelný), který se objevuje i v anglické (*not incompatible*) a německé verzi (*nicht unvereinbar*).

[173] CORRALES COMPAGNUCCI, Marcelo. *AI in eHealth: human autonomy, data governance and privacy in healthcare*. New York, NY: Cambridge University Press, 2022, 210, 226. ISBN 9781108921923.

K tomu, že se jedná o slučitelnost jen *zpravidla*, se přiklání také Indra Spiecker a Genannt Döhmann.[174] GDPR nám však neposkytuje žádné „výjimky z výjimky". Nejsme proto schopni říci, jaké atributy má vědecký výzkum, který s původními účely slučitelný není. Jisté ale je, že i slučitelný vědecký výzkum musí respektovat pravidla zakotvená v čl. 89 GDPR.

Další „ulehčení" vědeckého výzkumu lze spatřit v čl. 14 GDPR, který upravuje podmínky pro případ, kdy osobní údaje nebyly získány přímo od subjektu údajů, ale od třetí strany.[175] Můžeme si tak představit výzkum, který proběhne na datech, jež si výzkumník neopatřil sám, ale obdržel je od třetí strany. Za takových okolností není dle čl. 14 odst. 5 písm. b) GDPR výzkumník povinen poskytnout subjektu údajů informace o takovém výzkumu a jeho účelu. Z toho vyplývá, že data shromážděna třetí osobou v souladu s GDPR může vědec bez dalšího užít pro účely svého výzkumu.

Dvě výše uvedené výjimky, které spočívají zaprvé v ustanovení slučitelnosti vědeckého výzkumu s původním účelem a zadruhé v možnosti užít pro výzkum data třetí strany bez přidružených povinností, značně usnadňují vědcům práci, a je tak třeba konstatovat, že GDPR na výzkum a jeho podporu pamatuje. Nesmíme ovšem opomenout fakt, že v případě první výjimky není zcela jasné, jaké parametry vyvazují vědecký výzkum z pravidla čl. 5 odst. 1 písm. b) GDPR, podle něhož je vědecký výzkum obvykle slučitelný s původními účely.

GDPR také neposkytuje jednoznačnou odpověď na otázku, zda lze pod vědecký výzkum zahrnout trénování systému umělé inteligence či analýzu velkého objemu dat, který je pro vývoj umělé inteligence potřebný. Na základě dikce čl. 5 odst. 1 písm. b), čl. 89 a bodu 159 recitálu GDPR je třeba se přiklonit spíše k závěru, že na trénování

[174] *As art. 6(4) GDPR still applies the data processing for these purposes typically, but not always, is considered to be compatible* in DIMATTEO, Larry A.; PONCIBÒ, Cristina a CANNARSA, Michel. *The Cambridge handbook of artificial intelligence: global perspectives on law and ethics*. New York, NY: Cambridge University Press, 2022, 138. ISBN 9781009072168.
[175] CORRALES COMPAGNUCCI, Marcelo. *AI in eHealth: human autonomy, data governance and privacy in healthcare*. New York, NY: Cambridge University Press, 2022, 210, 223. ISBN 9781108921923.

systému umělé inteligence a související analýzu velkého množství dat uvedená zvýhodnění nedopadají.[176]

4. 5 Etické výzvy v kontextu umělé inteligence

S rozvojem umělé inteligence a zvyšováním jejího významu v našem každodenním životě jdou ruku v ruce nejen výzvy pro zákonodárce, ale také výzvy etického charakteru. Právo na ně často reaguje prostřednictvím nezávazného soft law, poněvadž právě soft law nevyžaduje žádný náročný legislativní proces ani specifickou formu. Obvykle tak k němu legislativa přistupuje jako k prvnímu kroku na cestě za závaznou regulací, neboť umožňuje poměrně rychle vydat první pokyny a upozornit na největší rizika spjatá s danou materií.[177] Unijnímu soft law proto věnujeme samostatnou kapitolu v třetí části práce, kde se detailněji zaobíráme především Etickými pokyny, které jsou v oblasti umělé inteligence stěžejní.

Etické výzvy u umělé inteligence mají základ buď v morálce člověka, který stojí za jejich vznikem, nebo už přímo v chování samotného systému.[178] Mimo jiné souvisí s využitím velkého objemu dat či nelehkou otázkou, kdo má nést za jejich chování odpovědnost. Také se v kontextu stále většího zapojení umělé inteligence hovoří o tom, jak posílit důvěru člověka v ní, o zavedení právní osobnosti pro systémy umělé inteligence či o nutné restrukturalizaci pracovního trhu, poněvadž je jen otázkou času, kdy umělá inteligence nahradí člověka v některých pracovních pozicích.

Vzhledem k rozsahu práce se zaměřujeme pouze na největší etické výzvy, které představují naše ilustrativní příklady mobilní konverzační aplikace a konverzačního hlasového asistenta v domácnosti.

[176] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 155-156. ISBN 9783748930952.
[177] GUTIERREZ, Carlos Ignacio; MARCHANT, Gary E. a MICHAEL, Katina. Effective and Trustworthy Implementation of AI Soft Law Governance. Online. *IEEE Transactions on Technology and Society*. 2021, 2(4), 169. ISSN 2637-6415. Dostupné z: https://doi.org/10.1109/TTS.2021.3121959. [cit. 2023-11-22].
[178] CORRALES COMPAGNUCCI, Marcelo. *AI in eHealth: human autonomy, data governance and privacy in healthcare*. New York, NY: Cambridge University Press, 2022, 256. ISBN 9781108921923.

4. 5. 1 Nedostatek objektivity a neutrality

Odpůrci umělé inteligence uvádějí jako jednu z jejich slabin nedostatečnou objektivitu a neutralitu. Je však člověk sám o sobě vždy neutrální a objektivní? Není. Za každým systémem umělé inteligence a algoritmem stojí (alespoň zatím) člověk, jehož názory se mohou do nastavení systému promítnout.[179]

I přesto jsou v případě umělé inteligence kladeny daleko vyšší požadavky na objektivitu než u člověka. Jako argument zaznívá absence libovůle u umělé inteligence, protože umělá inteligence nedokáže k zadaným úlohám přistupovat s osobním nasazením.[180] Jak již ale bylo řečeno v předchozím odstavci, nelze zapomínat na to, že systémy umělé inteligence programuje člověk, který na rozdíl od umělé inteligence má na věci názor, a záleží jen na tom, zda ho bude schopen při své práci upozadit, či nikoliv.

Jak je patrné i z následující kapitoly, můžeme se s nedostatečnou neutralitou setkat na různých úrovních. Vedle algoritmu, na jehož základě celý systém funguje a do nějž programátor promítá své postoje, to mohou být také trénovací data, z nichž se umělá inteligence učí. Za výběrem trénovacích dat opět nestojí nikdo jiný než člověk. Jestliže je tak umělá inteligence neobjektivní, zrcadlí pouze neobjektivitu člověka.

4. 5. 2 Diskriminace a předpojatost

V návaznosti na nedostatečnou neutralitu a objektivitu umělé inteligence se u ní můžeme setkat s diskriminačním chováním a předpojatostí.

Diskriminaci můžeme rozlišit na dvou úrovních. První úroveň je tzv. procesní úroveň, která zahrnuje veškeré úkony nezbytné k tomu, aby systém umělé inteligence učinil rozhodnutí. Pokud dojde k diskriminaci již na této úrovni, jsou její příčinou buď trénovací data, která vykazují právě prvky diskriminace či předpojatosti, nebo interní proces umělé inteligence opírající se o informace, které jsou spojeny se strukturální

[179] CORRALES COMPAGNUCCI, Marcelo. *AI in eHealth: human autonomy, data governance and privacy in healthcare*. New York, NY: Cambridge University Press, 2022, 288. ISBN 9781108921923.
[180] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 67. ISBN 9783748930952.

diskriminací. Z těchto důvodů je třeba nepodcenit sběr trénovacích dat a jejich kontrolu.[181]

Druhou úroveň, kde může k diskriminaci dojít, představuje úroveň klasifikace. V této fázi pracuje systém umělé inteligence s jednotlivými atributy informací (např. gender či věk) a jejich významem neboli váhou. Tím, že je atributů neskutečné množství, musí nezbytně dojít k určitému zjednodušení a zobecnění. A právě tady může dojít k eliminaci určité skupiny atributů, která vede v konečném důsledku ke zkreslení výstupu systému umělé inteligence.[182]

Stěžejním problémem v tomto ohledu je, že je velice těžké zjistit, že se systém chová diskriminačně. Samotná data nejsou anotována takovým způsobem, který by nám mohl prozradit, že s nimi umělá inteligence nakládá neadekvátně. Navíc ne vždy máme přístup ke všem datům.[183]

Když už je diskriminace detekována, je systém obvykle již v produkční verzi dostupný širokému okruhu uživatelů a také už dost pozdě na to ji jednoduše odstranit.[184]

A jaké jsou příklady diskriminace v souvislosti s umělou inteligencí? Některé z nich se dočkaly také mediální pozornosti, jako např. kauza technologického gigantu Google, jehož algoritmus na rozpoznání fotek a obličejů identifikoval osoby tmavé pleti jako gorily.[185] Diskriminace může mít i závažné důsledky v medicíně. Ve Spojených státech amerických byl do procesu přidělování transplantovaných orgánů zapojen systém umělé inteligence, který znevýhodňoval Afroameričany v důsledku vyššího rizika selhání transplantátu, které bylo u nich shledáno.[186]

---

[181] DE BRUYNE, Jan a VANLEENHOVE, Cedric (ed.). *Artificial Intelligence and the Law.Intersentia*, 2021, 138. ISBN 9781839701047.
[182] DE BRUYNE, Jan a VANLEENHOVE, Cedric (ed.). *Artificial Intelligence and the Law.Intersentia*, 2021, 140. ISBN 9781839701047.
[183] KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research handbook on EU data protection law*. Northampton, MA, USA: Edward Elgar Publishing, 2022, 167. ISBN 9781800371675.
[184] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 70. ISBN 9783748930952.
[185] VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022, 68. ISBN 9783748930952.
[186] CORRALES COMPAGNUCCI, Marcelo. *AI in eHealth: human autonomy, data governance and privacy in healthcare*. New York, NY: Cambridge University Press, 2022, 291. ISBN 9781108921923.

V případě konverzačních technologií může dojít například k tomu, že hlasový asistent řekne vtip, který je nevhodný a např. rasistický motivovaný. Na vině zde bude především původ a kvalita trénovacích dat. Také se můžeme setkat s určitými formami diskriminace na úrovni tzv. ASR neboli automatického rozpoznávání řeči, kdy ne všechny přízvuky jsou rozeznávány se stejnou úspěšností. Tady navíc často narazíme na to, že poskytovatel služby aplikace nebo hlasového asistenta často k ASR využívá externí služby třetí strany, a je třeba pak řešit komplikovanou otázku odpovědnosti.

5. Závěr

Rigorózní práce pojednává o technologiích založených na principech umělé inteligence a jejich právní úpravě na poli Evropské unie s důrazem na ochranu osobních údajů. První část je věnována představení fenoménu umělé inteligence. Vedle stručného shrnutí jejího vývoje je pozornost zaměřena na úskalí její definice, která je pro právní úpravu zcela stěžejní. Navazující část nám poskytuje přehled pramenů práva zásadních pro umělou inteligenci, přičemž nejsou opomenuty ani prameny, které jsou teprve v legislativním procesu, a ani soft law, jež v oblasti umělé inteligence hraje nezastupitelnou roli. Poslední část se zaměřuje na ochranu dat a soukromí v souvislosti s umělou inteligencí. Zde jsou mimo jiné analyzovány vybraná práva subjektu údajů a nesnáze ve spojitosti s některými zásadami zpracování dat, které vyvěrají ze specifických rysů umělé inteligence. Práci uzavírají hlavní etické výzvy, které užívání umělé inteligence nastoluje.

V rámci části mapující legislativu Evropské unie a části zaměřené na ochranu dat je průběžně poukazováno na nedostatky stávající i plánované úpravy, které lze shrnout do dvou základních skupin. Charakteristickým znakem první skupiny jsou nesrozumitelné definice a vágní formulace, které jsou však pro výklad předmětných ustanovení významné, protože se týkají například působnosti některých pramenů. V mnoha případech navíc interpretaci nepomůže ani recitál či důvodová zpráva, které bývají součástí právního předpisu, přestože je jejich hlavním úkolem právě interpretační opora. Nejasnost lze spatřit také v některých zásadách Obecného nařízení o ochraně osobních údajů, mimo jiné v případě zásady transparentnosti. Z úpravy neplyne, co vše je k jejímu naplnění nezbytné, a není tak zřejmé, kam až sahá povinnost transparentnosti a kde již začíná právní ochrana v podobě obchodního tajemství.

Druhou skupinu nedostatků spojuje skutečnost, že daná legislativa nereflektuje charakter umělé inteligence, přestože se na umělou inteligenci vztahuje, což může zásadním způsobem ztížit uvedení systému umělé inteligence na trh. Jako příklad může posloužit skutečnost, že umělá inteligence potřebuje ke svému fungování velký objem dat, na němž je třeba ji natrénovat. Podle platného práva ale nejspíš nepostačuje vymezit účel zpracování dat jako natrénování umělé inteligence, čímž je natrénování systému ztíženo. Nedostatečné zohlednění specifik umělé inteligence navíc může vést až

k absurdním situacím, kdy správce dat, která shromáždil systém umělé inteligence, nemůže splnit povinnost, kterou mu unijní předpis stanoví, ani kdyby se snažil sebevíc. Právní úprava totiž například nereaguje na to, že umělá inteligence je mnohdy nepředvídatelná a její vnitřní procesy, které předchází výstupu, jsou „černou skříňkou“, tedy neumožňují, aby je člověk identifikoval, natož vysvětlil. Je tak třeba konstatovat, že se s etickými výzvami, jež vlastnosti umělé inteligence představují, nedokázala právní úprava dosud popasovat.

Z těchto legislativních vad pak plynou určitá rizika. Jestliže nelze splnit povinnosti stanovené ustanovením, není údajům poskytnuta žádná ochrana. Navíc riziko pro ochranu soukromí lze spatřit již v některých vlastnostech umělé inteligence, jakými jsou již zmíněná nepředvídatelnost, neprůhlednost či diskriminace. U posledně jmenovaného rysu je třeba podotknout, že umělá inteligence nejedná diskriminačně „sama od sebe“. Nejčastěji se tak děje z důvodů nevhodného výběru trénovacích dat. Tak jako tak by měla legislativa usilovat o eliminaci těchto rizik efektivnějším způsobem, než je vymezení povinností, kterým v některých případech nelze dostát.

Nejinak je tomu v případě konverzačních asistentů a aplikací založených na umělé inteligenci. Je třeba konstatovat, že připravovaný Akt o umělé inteligenci na ně v současné podobě dopadá minimálně, jelikož se Akt soustředí především na vysoce rizikové systémy umělé inteligence, k nimž se konverzační aplikace neřadí. Stěžejní úpravou tak pro ně zůstává již zmíněné Obecné nařízení o ochraně osobních údajů, které skýtá úskalí hned v několika zásadách zpracování. U zásady účelu zpracování dat se potýkáme s problematikou, jaký účel je dostatečně konkrétní. Může jim být pouhé zvýšení kvality konverzačních schopností aplikace? Přestože se od těchto schopností odvíjí uživatelský prožitek, není jisté, že by takto formulovaný účel obstál. Ani zásada zákonnosti zpracování realizovaná prostřednictvím souhlasu subjektu se neobejde bez potíží. Vedle možného odvolání souhlasu a s ním spjatých komplikací u výmazu dat se potýkáme s možností, že jsou zpracována data, která uživatel sdělil asistentovi nevědomky. Například zařízení nahrálo input uživatele, který však nemířil vůči asistentovi. Co pak? Vztahuje se souhlas i na tato data? To z onoho nařízení nevyplývá.

Jak naznačuje předchozí odstavec, specifikem konverzačních technologií je možnost uživatele sdělit aplikaci nebo asistentovi cokoliv. Ono „cokoliv“ ani nemusí

souviset s předmětem konverzace či funkcí technologie. Správce dat tak nikdy dopředu netuší, jaká všechna data mohou být předmětem zpracování. Proto se nabízí otázka, jak má správce dat v takovém případě postupovat. Obecné nařízení o ochraně osobních údajů nám bohužel neposkytuje odpověď ani sebemenší vodítko. Jestliže tak uživatel dobrovolně v konverzaci uvede své politické přesvědčení nebo jiný osobní údaj zvláštní kategorie dle čl. 9 GDPR, není zcela zřejmé, zda je zpracování takového údaje zakázáno, nebo zda se na tuto situaci aplikuje výjimka spočívající ve zveřejnění údaje subjektem. Extenzivním výkladem lze dojít k závěru, že lze situaci, kdy subjekt sdělí zvláštní osobní data, která nejsou vyžadována, podřadit pod zveřejnění, a zpracování těchto dat zakázáno není. Otázkou ale zůstává, zda je taková interpretace záměrem zákonodárce. Vzhledem k tomu, že jsou konverzační technologie na vzestupu, nebylo by od věci explicitně tuto záležitost legislativně upravit, aby byla eliminována právní nejistota.

Seznam použitých zdrojů

Seznam použité literatury

ABBOTT, Ryan. The *reasonable robot: artificial Intelligence and the law*. Cambridge: Cambridge University Press, 2020, viii. ISBN 9781108459020.

BAKER, Dennis J., ROBINSON, Paul. H. *Artificial Intelligence and the Law: Cybercrime and Criminal Liability*. Routledge. 2020. ISBN 9781000210644.

BARFIELD, Woodrow a PAGALLO, Ugo. *Research handbook on the law of artificial intelligence*. Cheltenham, UK: Edward Elgar Publishing, 2018. ISBN 9781786439048.

CORRALES COMPAGNUCCI, Marcelo. *AI in eHealth: human autonomy, data governance and privacy in healthcare*. New York, NY: Cambridge University Press, 2022. ISBN 9781108921923.

DE BRUYNE, Jan a VANLEENHOVE, Cedric (ed.). *Artificial Intelligence and the Law*. Intersentia, 2021. ISBN 9781839701047.

DIMATTEO, Larry A.; PONCIBÒ, Cristina a CANNARSA, Michel. *The Cambridge handbook of artificial intelligence: global perspectives on law and ethics*. New York, NY: Cambridge University Press, 2022. ISBN 9781009072168.

EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. *Privacy and data protection in mobile applications: a study on the app development ecosystem and the technical implementation of GDPR.* 2017. ISBN 9789292042424.

KOLAŘÍKOVÁ, Linda, HORÁK, Filip. *Umělá inteligence & právo*. Praha: Wolters Kluwer ČR. 2020. ISBN 9788075987839.

KOSTA, Eleni; LEENES, Ronald a KAMARA, Irene. *Research handbook on EU data protection law*. Northampton, MA, USA: Edward Elgar Publishing, 2022. ISBN 9781800371675.

LEE, Joseph a DARBELLAY, Aline. *Data Governance in AI, FinTech and LegalTech*. Online. Northampton, MA, USA: Edward Elgar Publishing, 2022. ISBN 9781800379954.

LUI, Alison a RYDER, Nicholas. *Fintech, artificial intelligence and the law: regulation and crime prevention*. New York, NY: Routledge, 2021. ISBN 9781032012469.

ŠTĚDROŇ, Bohumír. *Právo a umělá inteligence*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2020, 201 s. ISBN 9788073808037.

TOMÁŠEK, Michal, TÝČ, Vladimír. *Právo Evropské unie*. 1. vydání Praha: Leges. 2013. ISBN 9788087576533.

VOGEL, Paul. *Künstliche Intelligenz und Datenschutz*. Nomos Verlagsgesellschaft mbH & Co., 2022. ISBN 9783748930952.

YEW, Gary Chan Kok a YIP, Man (ed.). *AI, Data and Private Law*. Hart Publishing, 2021. ISBN 9781509946860.

Seznam použitých internetových zdrojů

AI Act: Parliament and Council Reach Provisional Agreement on World's First AI Rules. Online. Eucrim. 2024. Dostupné z: https://eucrim.eu/news/ai-act-parliament-and-council-reach-provisional-agreement-on-worlds-first-ai-rules/

Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment. Online. European Commission. 2020. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

BENCH-CAPON, T, M ARASZKIEWICZ, K ASHLEY, et al. A history of AI and Law in 50 papers: 25 years of the international conference on AI and Law. *Artificial intelligence and law* [online]. Dordrecht: Springer Netherlands, 2012, 20(3), 215-319. ISSN 15728382. Dostupné z: doi:10.1007/s10506-012-9131-x

Česká republika vstoupila do Globálního partnerství pro umělou inteligenci. Online. Ministerstvo zahraničních věcí České republiky. 2022. Dostupné z:

https://mzv.gov.cz/jnp/cz/udalosti_a_media/archiv_zprav/rok_2022/ceska_republika_vstoupila_do_globalniho.html

Data Governance Working Group Report: November 2022 - GPAI Tokyo Summit. Online. The Global Partnership on Artiificial Intelligence. 2022. Dostupné z: https://www.gpai.ai/projects/data-governance/gpai-data-governance-wg-report-2022.pdf

European Network of AI Excellence Centres. Online. European Network of AI Excellence Centres. Dostupné z: https://www.elise-ai.eu/

Evropské centrum excelence v umělé inteligenci. Online. Národní portál pro evropský výzkum. 2020. Dostupné z: https://www.evropskyvyzkum.cz/cs/novinky/evropske-centrum-excelence-v-umele-inteligenci

GERLOCH, Aleš. Legální definice. HENDRYCH, Dušan a kol. Právnický slovník. 3. vydání. Praha: C. H. Beck, 2009. Dostupné z: https://app-beck-online-cz.ezproxy.is.cuni.cz/bo/document-view.seam?documentId=nnptembqhfpw64zrguxgyzlhmfwg42k7mrswm2lonfrwk

GUTIERREZ, Carlos Ignacio; MARCHANT, Gary E. a MICHAEL, Katina. Effective and Trustworthy Implementation of AI Soft Law Governance. Online. *IEEE Transactions on Technology and Society*. 2021, 2(4), 168-170. ISSN 26376415. Dostupné z: https://doi.org/10.1109/TTS.2021.3121959

LEE, Zhao Yan; KARIM, Mohammad Ershadul a NGUI, Kevin. Deep learning artificial intelligence and the law of causation: application, challenges and solutions. Online. *Information & Communications Technology Law*. 2021, 30 (3), 257, 260. ISSN 13600834. Dostupné z: doi:10.1080/13600834.2021.1890678

MCKEOWN, Tara, Jamila MUSTAFINA, Rustem MAGIZOV a Camila GATAULLINA. AI in Law Practices. Online. *2020 13th International Conference on Developments in eSystems Engineering (DeSE)*. IEEE, 2020, 27-32 . Dostupné z: doi:10.1109/DeSE51703.2020.9450780

M. THORNBERRY, WILLIAM. *National Defense Authorization Act for Fiscal Year 2021: Conference Report to Accompany H.R. 6395*. Online. 2020, 1210. Dostupné z: https://www.congress.gov/116/crpt/hrpt617/CRPT-116hrpt617.pdf#page=1210

Národní strategie v umělé inteligenci v České republice. Online. Vláda České republiky. 2019. Dostupné z: https://www.vlada.cz/assets/evropske-zalezitosti/umela-inteligence/NAIS_kveten_2019.pdf

National Artificial Intelligence Initiative. Online. AI.GOV. 2023. Dostupné z: https://ai.gov/

Přehled postupu legislativního procesu Směrnice o odpovědnosti za umělou inteligenci. Online. 2023. Dostupné z: EUR-Lex - 52022PC0496 - EN - EUR-Lex (europa.eu)

Přehled postupu legislativního procesu Aktu o datech. Online. 2023. Dostupné z: EUR-Lex - 52022PC0068 - EN - EUR-Lex (europa.eu)

Přední české univerzity spouští projekt Evropského centra excelence v umělé inteligenci. Online. Ministerstvo průmyslu a obchodu. 2020. Dostupné z: https://www.mpo.cz/cz/rozcestnik/pro-media/tiskove-zpravy/predni-ceske-univerzity-spousti-projekt-evropskeho-centra-excelence-v-umele-inteligenci--253258/

Shrnutí rozsudku Soudního dvora (prvního senátu) ze dne 7. prosince 2023, OQ v. Land Hessen, OQ v. Land Hessen, C-634/21, EU:C:2023:957. Online. InfoCuria. 2023. Dostupné z: https://curia.europa.eu/juris/document/document.jsf;jsessionid=136B3A5CC22DA3F5C460B325C9E33C36?text=&docid=280437&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=1762372

Skupina odborníků na vysoké úrovni pro umělou inteligenci. Online. Evropská komise. 2022. Dostupné z: https://digital-strategy.ec.europa.eu/cs/policies/expert-group-ai

The European Commission's High-level Expert Group on Artificial Intelligence. *A Definition of AI: Main Capabilities and Scientific Disciplines*. Online. Futurium. 2018. Dostupné z:

https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf

The Global Partnership on Artificial Intelligence. Online. The Global Partnership on Artiificial Intelligence. Dostupné z: https://www.gpai.ai/community/

The Global Partnership on AI (GPAI). Online. The Global Partnership on AI (GPAI). Dostupné z: https://oecd.ai/en/gpai

Umělá inteligence. Online. Vláda České republiky. 2021. Dostupné z: https://vlada.gov.cz/cz/evropske-zalezitosti/umela-inteligence/umela_inteligence/umela-inteligence-192765/#N%C3%A1rodn%C3%AD%20strategie%20%C4%8CR%20pro%20um%C4%9Blou%20inteligenci

WALKER-OSBORN, Charlotte, CHAN, Christopher. Artificial intelligence and the law. *ITNow*. 2017, 59(1), 36-37. Online. ISSN 17465702. Dostupné z: doi:10.1093/itnow/bwx017

Working Group on Data Governance. Online. The Global Partnership on Artificial Intelligence. Dostupné z: https://www.gpai.ai/projects/data-governance/

Seznam použitých pramenů práva a dalších právních dokumentů

Bílá kniha o umělé inteligenci – evropský přístup k excelenci a důvěře. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A52020DC0065&lang1=CS&from=EN&lang3=choose&lang2=choose&_csrf=212f314d-7b1d-4d1f-9a71-c1a5f0e092fc

Evropské pokyny pro zajištění důvěryhodnosti umělé inteligence, 2. Online. Dostupné z: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_CS.pdf

Konsolidované znění Smlouvy o fungování Evropské unie. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX:12012E/TXT

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) (Text s významem pro EHP). Online. Dostupné z: https://eur-lex.europa.eu/eli/reg/2016/679/oj

Návrh Nařízení Evropského Parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:52021PC0206

Návrh Nařízení Evropského Parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci) a mění určité legislativní akty Unie – důvodová zpráva. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:52021PC0206

Návrh Nařízení Evropského Parlamentu a Rady o evropské správě dat (akt o správě dat) – důvodová zpráva. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52020PC0767

Návrh Nařízení Evropského Parlamentu a Rady o harmonizovaných pravidlech pro spravedlivý přístup k datům a jejich využívání (Akt o datech) – důvodová zpráva. Online. Dostupné z: EUR-Lex - 52022PC0068 - EN - EUR-Lex (europa.eu)

Návrh Směrnice Evropského parlamentu a Rady o přizpůsobení pravidel mimosmluvní občanskoprávní odpovědnosti umělé inteligenci (směrnice o odpovědnosti za umělou inteligenci) – důvodová zpráva. Online. Dostupné z: EUR-Lex - 52022PC0496 - EN - EUR-Lex (europa.eu)

Policy and Investment Recommendations for trustworthy Artificial Intelligence. Online. Dostupné z: https://digital-strategy.ec.europa.eu/cs/node/1694

Rozsudek ze dne 7. prosince 2023, OQ v. Land Hessen, C-634/21, EU:C:2023:957. Online. Dostupné z: https://curia.europa.eu/juris/document/document.jsf;jsessionid=136B3A5CC22DA3F5C

460B325C9E33C36?text=&docid=280426&pageIndex=0&doclang=CS&mode=req&dir=&occ=first&part=1&cid=1762372

Sdělení Komise Evropskému Parlamentu, Evropské radě, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Koordinovaný plán v oblasti inteligence. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52018DC0795

Sdělení Komise Evropskému Parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Podpora evropského přístupu k umělé inteligenci. Online. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52021DC0205

Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Umělá inteligence pro Evropu. Online. Dostupný z: https://eur-lex.europa.eu/legal-content/CS/ALL/?uri=CELEX:52018DC0237

The National Security and Investment Act 2021 (Notifiable Acquisition) (Specification of Qualifying Entities) Regulations 2021. Online. 2021. Dostupné z: https://www.legislation.gov.uk/uksi/2021/1264/schedule/3/made

Technologie založené na umělé inteligenci: právní aspekty ochrany dat a soukromí

Abstrakt

Práce se soustředí na technologie založené na principech umělé inteligence a jejich právní úpravě na poli Evropské unie s důrazem na ochranu dat. Je rozdělena do tří částí. Nejprve je pozornost zaměřena na samotný termín umělé inteligence, jehož definice není jednoduchá, ovšem pro právní úpravu zcela nepostradatelná.

Druhá část práce pojednává o legislativě Evropské unie, jež je pro umělou inteligenci relevantní, přičemž opomenuty nezůstávají ani soft law, které právě v oblasti umělé inteligence má svou nezastupitelnou roli, ani právní úprava, která je teprve v legislativním procesu. Již v této části jsou demonstrovány legislativní nedostatky, jež lze rozdělit do dvou skupin. Pro první skupinu nedostatků je charakteristická nesrozumitelnost definic či přílišná vágnost formulací, jež zapříčiňují interpretační potíže i v zásadních skutečnostech, mezi něž se bezpochyby řadí působnost předpisu. Společným rysem druhé skupiny legislativních nedostatků je neúplná reflexe specifik umělé inteligence, která může v nejzazším případě vést k absurdní situaci, kdy nelze povinnost stanovenou právním předpisem splnit.

Poslední část práce se věnuje oblasti ochrany dat a soukromí v kontextu umělé inteligence. V této části práce je představena problematika zpracování dat společně se zásadami zpracování dat, která mohou na poli umělé inteligence činit určité nesnáze. Obdobně jsou zde analyzována vybraná práva subjektu dat, jejichž realizace může být v souvislosti s umělou inteligencí nelehká. V obou případech vyvěrají na povrch nedostatky dané legislativy, jež jsou podrobeny kritice. Tyto slabiny souvisí mimo jiné se skutečností, že evropská legislativa se dosud nedokázala úspěšně vypořádat s etickými výzvami, které charakter umělé inteligence přináší. Mezi tyto výzvy lze zařadit vedle nebezpečí diskriminačního jednání také nepředvídatelnost výstupu umělé inteligence a s tím spjatou neprůhlednost vnitřních procesů, které výstupu předcházejí.

Klíčová slova

umělá inteligence, ochrana dat, právo umělé inteligence, zásady zpracování dat v souvislosti s umělou inteligencí

Technology Based on Artifical Intelligence: Legal Aspects of Data and Privacy Protection

Abstract

The thesis focuses on technologies based on the principles of artificial intelligence and their regulation in the field of the European Union with an emphasis on the data protection. It is divided into three parts. Firstly, the focus is on the term artificial intelligence itself, the definition of which is not simple, but quite indispensable for legal regulation.

The second part of the thesis deals with the European Union legislation relevant to artificial intelligence, leaving aside neither soft law, which has an indispensable role in the field of artificial intelligence, nor legislation that is still in the legislative process. This section already demonstrates the legislative shortcomings, which can be divided into two groups. The first group of shortcomings is characterised by incomprehensibility of definitions or excessive vagueness of formulations, which cause interpretative difficulties even in essential facts, which undoubtedly include the scope of the regulation. A common feature of the second group of legislative shortcomings is the lack of reflection on the specifics of artificial intelligence, which can, in the most extreme case, lead to an absurd situation where the obligation laid down by the legislation cannot be fulfilled.

The last part of the thesis deals with data protection and privacy in the context of artificial intelligence. In this part of the thesis, the issues of data processing are introduced along with the principles of data processing that may pose some difficulties in the field of artificial intelligence. Similarly, selected rights of the data subject are analysed here, the implementation of which may not be easy in the context of artificial intelligence. In both cases, the shortcomings of the legislation in question are highlighted and criticised. These weaknesses are related, among other things, to the fact that European legislation has so far failed to successfully address the ethical challenges posed by the nature of AI. These challenges include, in addition to the risk of discriminatory behaviour, the unpredictability of the output of AI and the associated opacity of the internal processes that precede the output.

Keywords

artificial intelligence, data protection, AI law, principles relating to data processing in the context of artificial intelligence