13 UMĚLÁ INTELIGENCE

13.1 Technologická regulace strojového učení

Tato kapitola se tematicky liší od zbytku této knihy a systematicky nezapadá ani do struktury práva informačních technologií. Ostatní podobory IT práva reprezentované jednotlivými částmi této publikace mají totiž problémovou podstatu a jsou postaveny na identitě primárního objektu příslušných právních vztahů. Tato kapitola se oproti tomu nezabývá právními problémy, které spojuje identický účel, ale právními souvislostmi vývoje a nasazení konkrétního typu informační technologie souhrnně označovaného jako umělá inteligence (AI).

Nebudeme se na tomto místě zabývat důvodností specifického regulatorního přístupu k umělé inteligenci. Diskuse vhodnosti a potřebnosti právní regulace šité na míru konkrétní technologii již v minulosti proběhla a neměla jednoznačný závěr[1]. Na jedné straně stály argumenty poukazující na specifický charakter této technologie, aktuální a předpokládanou důležitost různých jejích aplikací a s ní spojenou širokospektrální rizikovost pro všechna možná práva a právní zájmy. Na druhé straně zaznívaly stejně relevantní argumenty zpochybňující potřebu regulace technologie, která, na rozdíl například od technologie jaderné, není sama o sobě riziková, a doporučující regulaci její aplikací. Namísto pokračování v této akademické debatě budeme dále konstatovat jen aktuální stav regulace vývoje a aplikací umělé inteligence, který dal, zjednodušeně řečeno, vlastně zapravdu oběma právě uvedeným kontradiktorním argumentům.

Pojem AI je sám o sobě silně metaforický a to činí jeho použití v hypotézách právních norem velmi problematickým[2]. To se projevilo i při konstrukci legislativní definice toho, co má být předmětem právní regulace Aktu o umělé inteligenci. Definice pojmu umělé inteligence doznala od původního návrhu Komise přes stanovisko Evropského parlamentu a Rady až po finální kompromis velmi podstatných změn. Konečné znění vypadá následovně

> „Systémem AI se rozumí strojový systém navržený tak, aby fungoval s různými úrovněmi autonomie, který může po zavedení vykazovat adaptabilitu a který z obdržených vstupů odvozuje pro explicitní nebo implicitní cíle to, jak generovat výstupy, jako jsou predikce, obsah, doporučení nebo rozhodnutí, které mohou ovlivnit fyzické nebo virtuální prostředí."

Tento nepříliš srozumitelný výsledek složitého vyjednávání v sobě skrývá několik typických a pro právo zásadně důležitých znaků technologií založených na strojovém učení. Prvním je autonomie, tj. relativní nezávislost příslušného systému na jeho okolí, včetně člověka. Tato vlastnost je pravým důvodem atraktivity systémů založených na AI, protože mohou působit bez lidského zásahu a nahradit tím lidskou práci.

Především v diskusi týkající se odpovědnostních titulů se pro autonomní systémy sice nabízí řada možných paralel a analogií s právní úpravou situací, kdy je újma způsobená něčím, živým nebo neživým, co funguje relativně nezávisle na lidské vůli, tj. nějakým strojem nebo zvířetem. Autonomní systémy spadající pod shora uvedenou definici se ale oproti například domácím zvířatům liší v tom, že jejich nezávislost na člověku (vlastníkovi nebo zavádějícímu subjektu) může být často pravým účelem jejich pořízení. Zatímco psa si člověk pořídí primárně proto, aby s ním mohl trávit volný čas a auto, aby v něm mohl jezdit, je hlavním smyslem autonomní sekačky na trávu naopak v tom, aby se činila nezávisle na pozornosti a přítomnosti svého vlastníka.

S autonomním fungováním souvisí, rovněž autonomní, adaptabilita. Autonomní systém je schopen sám se učit a přizpůsobovat se vnějšímu prostředí. Tato vlastnost je klíčová pro celou řadu právních otázek, protože bezprostřední vstup člověka při vzniku autonomního systému nespočívá v programování jeho operačního kódu, ale pouze kódu, na jehož základě se takový systém sám učí. Programátor (designér) tedy nekóduje autonomní systém k tomu, aby něco dělal, ale k tomu, aby se něco učil dělat. Na základě instrukce vytvořené programátorem se tedy autonomní systém na vstupních datech sám naučí, jak má fungovat, tzn. sám si vytvoří (naprogramuje) vlastní operační kód.

Se strojovým učením se, byť to není přímo předmětem zákonné definice AI, pojí i další typický rys autonomních systémů, a to absence vysvětlitelnosti[3]. Operační kód autonomního systému je tvořen strojem v procesu jeho samostatného učení a výstupem tohoto procesu je nepřehledná změť nastavení ohromného počtu proměnných. Výsledek se podobá neuronům v lidském mozku, jejichž aktivitu jsme sice schopni zvenčí sledovat, ale nedokážeme kvůli extrémní složitosti určit, jak konkrétně vypadá algoritmus, podle něhož tato složitá soustava zpracuje nějaký podnět a vytvoří určitý výstup. Programátor tedy sice zadá systému instrukci, z čeho a co se má systém učit, nemá už ale kontrolu nad tím, jak systém příslušná vstupní

---

[1] Viz např. SCHERER, M. Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, 2016, č. 29(2), str. 354.

[2] K problému definice AI viz např. FLORIDI, L. On the Brussels-Washington Consensus About the Legal Definition of Artificial Intelligence. *Philosophy & Technology*, 2023, č. 36, str. 87.

[3] K problému vysvětlitelnosti a jeho právním souvislostem viz např. BIBAL, A., LOGNOUL, M. de STREEL, A., FRENAY, B. Legal Requirements on Explainability in Machine Learning. *Artificial Intelligence and Law*, 2021, č. 29(2), str. 149.

data zpracuje, jaký výsledný kód z takového strojového učení vznikne a následně tedy nedokáže ani říci, proč systém fungující na základě nevysvětlitelného autonomně vytvořeného operačního kódu dělá, co dělá.

> Problém autonomie a vysvětlitelnosti dokládá nedávný veřejně známý incident chatbota Tay[4]. Toho zkonstruovala společnost Microsoft s cílem vytvořit automat na autonomní produkci originálních krátkých textových zpráv (tweetů), které měl robot publikovat prostřednictvím známé sociální sítě Twitter[5]. Robot byl naprogramován tak, aby se z této sítě učil produkovat obsah, který bude mít mezi uživateli, pokud možno, co největší popularitu a úspěch. Při svém učení byl tedy robot veden faktorem popularity aktuálního obsahu dostupného na této sociální síti daným počtem sledujících, sdílení a následných reakcí. Zjednodušeně řečeno robot procházel nejpopulárnější tweety a z nich se učil, jaký obsah uživatelé nejvíce oceňují. Kromě toho byl naprogramován tak, aby průběžně vyhodnocoval reakce uživatelů na své vlastní tweety, přizpůsoboval jim další své fungování a díky tomu dále zvyšoval svoji popularitu. Poté, co byl robot uveden do provozu, začal hromadně generovat tweety především s nenávistným, a částečně také manipulativním a zavádějícím obsahem (fake news). Smršť nenávistných zpráv dosáhla takové intenzity, že společnost Microsoft robota odstavila a pokusila se jej opravit. Po následném uvedení do provozu byla situace ohledně nenávistných projevů ještě mnohem horší, takže Microsoft robota vypnul a do prostředí sociální sítě Twitter jej už od té doby nenasadil.
>
> Tento letitý a již dávno zapomenutý případ nemá ani v nejmenším poukázat na možnou technologickou zaostalost společnosti Microsoft nebo neschopnost jejích programátorů. Produkty této firmy jsou na špičkové světové úrovni a její inženýři požívají v IT komunitě velkého respektu. Jeho připomenutí má namísto toho ukázat, že ani dovednosti a schopnosti světové úrovně zde nestačily na to, aby se robot naučený s vysokou mírou efektivity replikovat osvědčené cesty k popularitě na sociální síti Twitter nestal extrémistickým xenofobem, homofobem, militantním náboženským fundamentalistou apod.

Problém vysvětlitelnosti hraje zásadní roli nejen v otázkách souvisejících s odpovědností za újmu způsobenou autonomním systémem, ale také při výkonu různých informačních práv nebo transparenčních povinností souvisejících například s automatizovanými rozhodovacími nebo doporučovacími systémy[6]. Projeví se vždycky, pokud hypotéza právní normy počítá buďto s prokázáním způsobu, kterým příslušný systém funguje, nebo požaduje, aby o takovém způsobu fungování jeho zavádějící subjekt (*deployer*) informoval navenek[7].

Autonomní systém je ve svém fungování, a dokonce i ve své konstrukci, relativně nezávislý na lidské vůli. Je ale naopak velmi závislý na parametrech prostředí, z nichž se učí, resp. na jejichž základě si autonomně vytváří svůj operační kód. Robot Tay ve výše zmíněném příkladu sice dostal od svého programátora instrukci učit se psát tweety a ty následně chrlit za účelem dosažení popularity mezi uživateli sociální sítě, ale to, jak se nakonec choval, bylo kromě základního zadání především výsledkem zpracování dat o tom, jak tato síť funguje a který obsah si na ní získává největší popularitu. Pokud by z příspěvků na Twitteru (nově na službě X) měly největší oblibu ty psané spisovným jazykem a pojednávající o finesách klasické řecké filozofie, projevoval by se Tay jako distingovaný filolog. Diametrální rozdíl mezi strojem na filozofii a strojem na nenávist nebyl v tomto případě ani v nejmenším dílem programátora, ale bezprostředním důsledkem kvality prostředí, z něhož systém čerpal data pro své strojové učení.

13.2 Vývoj specifické právní úpravy umělé inteligence

Vývoj specifické právní úpravy vývoje a nasazení umělé inteligence, který v době psaní této knihy ještě stále probíhá, samozřejmě nepočítáme na stovky ani desítky let. Současně se ale nedá ani říci, že by aktuální legislativní pokrytí této problematiky bylo výsledkem nějaké instantní politické nebo úřednické aktivity. Potřebu regulatorní reakce na rostoucí důležitost autonomních technologií již po více než 10 let intenzivně řeší Evropský parlament, Komise i členské státy.

Trvalý zájem některých poslanců Evropského parlamentu a jejich asistentů o problematiku autonomních technologií doprovázený, to i díky čilé komunikaci s akademickou sférou, nebývale hlubokým porozuměním (bez ironie) této problematiky vyústil v roce 2017 v usnesení, které shrnovalo základní politické pozice a regulatorní otázky[8].

> Usnesení začíná zeširoka odkazem k Frankensteinovi, Pygmalionovi nebo Golemovi a připomíná hned v úvodu i dílo Karla Čapka. Všímá si nebývalého nárůstu komerčních aplikací autonomních technologií a, jak se později ukázalo, správně předvídá jejich zásadní budoucí důležitost pro ekonomiku a život společnost a člověka. Základním motivem dokumentu je civilní odpovědnost za újmu a základní etické zásady vývoje a nasazení autonomních systémů s původem v Asimovových principech. Usnesení předvídá, rovněž správně, brzkou potřebu standardizace a řešení otázek souvisejících s informačními právy, včetně práv duševního vlastnictví, a předvídá domény, kde se autonomní technologie v dohledné době uplatní. Součástí dokumentu je i následující náznak definice toho, co má být předmětem regulatorní pozornosti. Za robota označuje systém, který „je autonomní díky senzorům nebo výměně dat s

[4] Tento příklad je převzat z článku POLČÁK, R. Umělá inteligence v justici. *Soudce*, 2024, č. 1, str. 4.

[5] Podrobněji k případu viz BROWN, N. Bots behaving badly: products liability approach to chatbot-generated defamation. *Journal of Free Speech Law*, 2023, č. 3(2), str. 389.

[6] K pojmu a právním souvislostem doporučovacích systémů viz např. BLOCKX, J., KROOK, J. The EU legal framework for algorithmic recommender systems: I (don't) know it when I see it. Law, *Innovation and Technology*, 2024 (online).

[7] K tomu podrobněji viz výklad poslední podkapitoly k problematice transparentnosti logiky rozhodovacích algoritmů ve smyslu GDPR.

[8] Viz Usnesení Evropského parlamentu ze dne 16. února 2017 obsahující doporučení Komisi o občanskoprávních pravidlech pro robotiku (2015/2103(INL)) (2018/C 252/25).

okolním prostředím (propojenost) a je schopen tato data předávat a analyzovat, má schopnost samostatného učení na základě zkušeností a interakce (volitelné kritérium), má alespoň menší fyzickou strukturu, má schopnost přizpůsobit své jednání a svou činnost okolnímu prostředí a není v biologickém smyslu živý.“ Je až podivuhodné, jak se kompromisní definice AI v Aktu, která byla výsledkem dlouhého a bouřlivého vývoje, nakonec těmto definičním znakům, snad s výjimkou podmínky minimální fyzické struktury, blíží.

V říjnu téhož roku se k potřebě reagovat na rozvoj umělé inteligence stručně vyjádřila i evropská Rada[9]. Na obě iniciativy následně reagovala Komise sdělením označeným jako Umělá inteligence pro Evropu[10]. Tento poziční dokument definoval v reakci na výzvy identifikované ve shora citovaném usnesení Evropského parlamentu strategii Komise v základních oblastech, kterými byly vývoj a investice, socioekonomické změny a etický a právní rámec.

Junckerova Komise v tomto dokumentu vycházela ze své obecné politiky, jejímž hlavním nástrojem byly v té době ekonomické stimuly (nikoli legislativa). Současně zohlednila, i když nikoli úplně explicitně, realitu technologického vývoje, která nevyznívala (tehdy ani dnes) pro Evropu úplně příznivě. Nejdůležitější základní technologie označované dnes jako obecné systémy AI (general purpose AI – GPAI) nebo základní modely (foundational models) měly a mají původ především v USA nebo v Číně.

Komise v tomto směru správně předpokládala, že tím, co může Evropu dostat do hry, jsou především soukromé investice do primárního a aplikovaného výzkumu. Proto je podstatná část sdělení věnována problematice investic a ekonomických pobídek, to i přes skutečnost, že Evropský parlament ani rada ve svých dokumentech neoznačily problém ekonomických souvislostí vývoje AI za kriticky důležité.

Když Junckerova komise zdůraznila ekonomické souvislosti vývoje a nasazení umělé inteligence, nemělo to pouze hospodářský význam. Sdělení totiž poměrně důkladně rozebírá jednak společensko-ekonomické důsledky nasazení autonomních technologií a jednak ve vzájemných souvislostech i problematiku etických principů a ochrany práv. Komise totiž předpokládala, že pokud budou mít dominantní autonomní technologie díky fungujícímu investičnímu prostředí původ v zemích EU, budou jejich vývoj a nasazení přirozeně založeny na hodnotách typických pro EU a bude i jednodušší vůči jejich zavádějícím subjektům vymáhat ochranu těchto hodnot vyjádřených konkrétními právy.

Sdělení Komise si kromě ekonomických a hodnotových otázek všímá i shora zmíněného velmi podstatného aspektu vývoje a provozu autonomních technologií, kterým je dostupnost dat, z nichž se autonomní systémy mohou strojově učit. Jsou to právě data, respektive jejich bezprecedentní rozsah a obsahové bohatství, co činí Evropu výjimečnou v porovnání s největšími konkurenty, tj. USA a Čínou. Například v oblasti kulturních dat, tj. slovesného, výtvarného nebo hudebního kulturního dědictví, se díky bohaté historii, vyspělé civilizaci a jazykové a kulturní rozmanitosti Evropy nemůže s bohatstvím dat spravovaných zdejšími kulturními institucemi nemůže ani vzdáleně srovnávat nic s původem ve kterékoli jiné části světa. Podobné je to i v řadě dalších oblastí jako například ve zdravotnictví, školství, veřejné dopravě, geografii aj.

Základním momentem akcentovaným ve sdělení ve vztahu k datům je jejich dostupnost. Komise si všímá především problému snadného zpřístupnění velkých datových objemů a zvlášť se zaměřuje na překážky ve zpřístupňování dat (informací) veřejného sektoru a dat produkovaných veřejnými institucemi. Poměrně vizionářsky ale zmiňuje i problém dostupnosti soukromých dat, a konkrétně dat označovaných jako „průmyslová“ – těmi se v současné době intenzivně zabýváme a označujeme je nejčastěji jako „neosobní“ nebo „nespecifická“ data[11].

Zajímavé je, že sdělení Komise, jinak pragmatické, logické a v řadě momentů i vizionářské, prakticky ignoruje problematiku majetkových práv autorských. V době, kdy sdělení vzniklo, samozřejmě nebylo možno předvídat nástup generativních technologií, ale už tehdy bylo jasné, že ochrana absolutními právy autorskými patří mezi hlavní regulatorní překážky dostupnosti dat pro účely strojového učení. Komise však na paradoxní situaci, kdy pro všechny možné druhy fyzického zboží sice platí pravidla jednotného trhu, ale pro nehmotná autorská díla stále neexistuje jednotný titul ani jednotný trh, v tomto dokumentu nepoukázala.

Poněkud v pozadí výše diskutovaného sdělení zůstal doprovodný pracovní dokument, v němž Komise rozvedla základní regulatorní teze týkající se problémového okruhu označeného Evropským parlamentem za nejdůležitější – odpovědnosti[12]. Na svou dobu poměrně důkladná analýza zahrnuje různé aspekty fungování autonomních technologií a pragmaticky diskutuje otázky uplatnění nároků na náhradu škody nebo zadostiučinění v případech, kdy bez přímého zavinění člověka dojde v důsledku fungování takových technologií k újmě.

Komise von der Leyenové se v porovnání s Komisí Junckerovou ve své politice méně spoléhá na ekonomické nástroje, a naopak více na legislativu. Lze samozřejmě v této souvislosti diskutovat o tom, do jaké míry lze textem zákona opravdu efektivně řešit systémové problémy související s technologickým vývojem. V každém případě ale se změnou politiky změnilo se i tempo práce na legislativních nástrojích regulujících vývoj a nasazení aplikací založených na umělé inteligenci.

Výsledkem tohoto vývoje jsou dva specifické nástroje, kterými se zabýváme rozebíráme v následujících podkapitolách, a to Akt (nařízení) o umělé inteligenci a směrnice o odpovědnosti umělé inteligence. Byť jde o nejdůležitější právní předpisy,

---

[9] Viz závěry jednání Rady ze dne 19. října 2017, č. EUCO 14/17. Hlavní pozornost tento dokument věnoval aktuálním rizikům souvisejícím s počínající migrační krizí, takže na umělou inteligenci zde vyšlo jen několik odstavců společně věnovaných ještě i problematice blockchain.

[10] Viz Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů č. COM/2018/237, Umělá inteligence pro Evropu.

[11] Vedle těchto pojmů se používá rovněž pojem „průmyslová“ data – blíže k problematice právního režimu tohoto typu dat viz WIEBE, A. Protection of industrial data – a new property right for the digital economy? *Journal of Intellectual Property Law & Practice*, 2017, č. 12(1), str. 62.

[12] Viz Commission staff working document SWD/2018/137 Liability for emerging digital technologies Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe (dokument je k dispozici pouze v angličtině).

které v dohledné době dopadnou na vývoj a nasazení aplikací založených na strojovém učení, zdaleka nejde o předpisy jediné. V následujícím výkladu se tedy zaměříme nejen na tyto dva legislativní návrhy, ale také na další již existující právní předpisy, které tvoří právní rámec ex ante souladnosti (compliance), a ex post odpovědnosti. Třetí ze systematicky provázaných oblastí právní regulace umělé inteligence, právy k datům, se zabýváme převážně ve čtvrté a páté kapitole této knihy.

13.3 Ex ante úprava AI - systematika Aktu a zakázaná užití AI

Když byla v rámci projektu aplikovaného výzkumu Ministerstva průmyslu a obchodu[13] sestavena mezinárodní expertní skupina na vysoké úrovni se zadáním ke kritické reflexi prvního oficiálního návrhu Aktu o AI, očekávalo se, že jedním z hlavních problémových momentů bude smyslu naznačeném v první podkapitole sama věcná působnost aktu, tj. technologie založené na strojovém učení. Kriticky k tomu, že se návrh snaží regulovat technologii, která ale sama o sobě není nebezpečná (a regulovat by si spíš zasloužily její rizikové aplikace), se ale tehdy překvapivě vyjádřil jen jeden z pěti členů komise, zatímco ostatní nepovažovali technologickou regulaci za problémovou.

Důvodem smířlivosti valné většiny členů komise k jinak zřejmě těžko akceptovatelné regulaci konkrétní nikoli per se nebezpečné technologie byla především stratifikace návrhu, v jejímž důsledku byla regulace nejširšího a současně nejméně rizikového okruhu aplikací umělé inteligence silně inkluzivní, tj. splnitelná prakticky kýmkoli bez větších obtíží nebo závazků. Reálně exkluzivní ex ante regulace aplikací založených na strojovém učení byla v původním návrhu provedena až od druhé úrovně rizika, tj. pro aplikace, jejichž nasazení představuje vysoké riziko pro různá práva osob, od vlastnictví přes soukromí nebo spravedlivý proces až po právo na zdraví nebo život. Třetí úroveň původního návrhu zahrnovala aplikace, jejichž rizikovost je v EU neakceptovatelná, a tudíž je třeba je absolutně zakázat.

Původní návrh nařízení[14] se od konečného textu výrazně liší. Vedle velmi rozsáhlé a strukturované politické debaty k tomu přispěl i technologický vývoj a z něj v první řadě nečekaný nástup prakticky použitelných generativních technologií, který odstartovalo uvedení třetí verze velkého jazykového modelu GPT (Generative Pre-trained Transformer) a jeho populární aplikace ChatGPT na podzim roku 2021[15]. Základní regulatorní idea, na které stál původní návrh a která spočívala v rozdělení povinností na inkluzivní (symbolické), exkluzivní (v podobě striktních ex-ante povinností) a restriktivní (zákazy), však zůstala zachována. Jejím prostřednictvím je tedy vhodné nahlížet i na výslednou typologii systémů AI, která se oproti původnímu návrhu zdá být nepoměrně složitější. Ve skutečnosti jde ale pouze o rozvedení prostřední kategorie, tj. kategorie s exkluzivní regulací, a doplnění některých (především transparenčních) povinností do kategorie systémů podléhajících inkluzivní regulaci. Akt tedy ve výsledku pracuje s touto základní typologií systémů založených na umělé inteligenci (ve smyslu výše uvedené definice):

- Zakázané systémy
- Vysoce rizikové systémy
- Ostatní systémy (tj. systémy s nízkým rizikem, resp. s rizikem, které není vysoké)
- Obecné modely AI se systémovým rizikem
- Obecné modely AI bez systémového rizika

Vedle této klasifikace stojí zvláštní kategorie především transparenčních a dokumentačních povinností vztahujících se k systémům s určitým účelem nebo funkcí bez ohledu na jejich zařazení do výše uvedených kategorií:

- Systémy určené k interakci s člověkem
- Generativní systémy
- Systémy generující deep fakes
- Systémy pro rozpoznávání emocí

Absolutní zákaz určitých aplikací AI má dvojí formu. Jednak jde o zákaz uvádět tyto aplikace na trh, který se vztahuje na různé kategorie účastníků trhu, a jednak je to i zákaz tyto aplikace zavádět nebo používat směřující vůči subjektům, které by mohly jejich prostřednictvím zasahovat do práv třetích osob. Nepřípustná míra rizika se tedy v tomto případě projevuje nejen vzhledem k trhu s různými systémy založenými na AI, ale dopadá současně i na všechny formy jejich používání. Zakázané formy užití AI lze rozdělit do následujících základních skupin:

- manipulativní užití zneužívající podvědomé manipulace[16] nebo manipulace založené na systémové zranitelnosti člověka[17],
- hodnocení sociálního kreditu (social scoring)[18] - i v tomto případě jde prakticky rovněž o manipulaci, byť zprostředkovanou nepřímým tlakem na jednání člověka v důsledku skórování,

[13] Viz projekt výzvy Umělá inteligence pro bezpečnější společnost, kód MU 0656/2020.
[14] Viz dokument původně publikovaný 21. dubna 2021 pod číslem 2021/0106 (COD).
[15] K historii technologie GPT viz např. TRAUTMAN, L. J., VOSS, W. G., SHACKLEFORD, S. J. *How We Learned to Stop Worrying and Love AI: Analyzing the Rapid Evolution of Generative Pre-Trained Transformer (GPT) and its Impacts on Law*, ssrn.com, abstrakt číslo 4516154.
[16] Viz čl. 5(1)(a) Aktu.
[17] Viz čl. 5(1)(b) Aktu.
[18] Viz čl. 5(1)(c) Aktu.

- biometrická identifikace v reálném čase pro účely vymáhání práva[19] - původně navržený striktní zákaz byl postupně zmírňován a konečné znění Aktu obsahuje řadu účelem vymezených výjimek např. pro pátrání po hledaných osobách nebo předcházení teroristickým útokům. Úprava výjimek je velmi podrobná a zahrnuje i zásadní[20] podmínku soudního rozhodnutí, notifikační povinnosti nebo povinnosti členských států přijmout národní zákonnou úpravu[21],
- biometrická kategorizace vzhledem k rase, politickým názorům, členství v odborových organizacích, náboženskému vyznání, filozofickému přesvědčení, sexuálnímu životu nebo sexuální orientaci[22],
- prediktivní analýza rizik kriminálního jednání založená na profilování[23],
- systémy pro tvorbu nebo rozšiřování databází pro rozpoznávání obličejů z dat získaných z internetu nebo kamerových záznamů [24] a
- rozpoznávání emocí na pracovišti nebo ve vzdělávacích institucích[25]. Výjimkou jsou případy, kdy je takové technologie použito za účelem ochrany zdraví nebo bezpečnosti (ve smyslu angl. „safety," tj. bezpečnosti práce, požární bezpečnosti apod.) Pozoruhodné rovněž je, že zákaz nepostihuje jiné formy rozpoznávání emocí – typicky takové, které se staly předmětem v poslední době široce diskutovaného velkého množství patentů některých internetových platforem[26].

Především otázka zákazu biometrické identifikace v reálném čase byla po celou dobu přípravy Aktu velmi citlivá a shoda na ní nebyla až do poslední fáze hledání kompromisu mezi Komisí, Radou a Evropským parlamentem[27]. Politická důležitost této otázky byla dokonce tak intenzivní, že absence kompromisu mohla zhatit celé projednávání Aktu Evropským parlamentem v jeho současném volebním období[28].

Výsledné řešení představuje rozumný kompromis, protože přináší na jedné straně zákaz prodeje nebo používání těchto technologií, ale na straně druhé dává možnost členským státům, aby si při vynaložení netriviálního úsilí a splnění různých transparenčních a notifikačních povinností upravily výjimky z tohoto zákazu. Národní úprava přitom musí pro příslušný členský stát představovat věc evidentního politického a společenského zájmu, protože jinak než na základě vzájemné shody moci zákonodárné, výkonné i soudní takovou výjimku prakticky nelze realizovat[29].

Těžkosti, které problematika biometrické identifikace pro účely vymáhání práva přinesla do celého procesu přípravy Aktu, je ale, společně s ostatními postupně bobtnajícímu částmi článku 5, možné chápat i jako projev obecné choroby, kterou Akt v posledních letech přípravy začal trpět. Celý předpis měl totiž v obecné rovině ošetřit ex ante rizika související s vývojem a nasazení různých technologií založených na AI. Namísto toho se ale stal půdorysem (podvozkem), na němž se začaly realizovat různé konkrétní politické představy týkající se nikoli umělé inteligence jako potenciálně rizikové technologie, ale ochrany soukromí a osobních údajů.

Nejde o to, že by si biometrické technologie, rozpoznávání obličejů nebo třeba analýza emocí nezasloužily politickou a legislativní pozornost. Ta by se ale měla soustředit k nástrojům, které v evropském právu a právu členských států k ochraně příslušných práv (zde především práva na soukromí, soukromý život a ochranu osobních údajů) máme systematicky upraveny, tj. ke GDPR, policejní směrnici[30], jejím národním implementacím a případně k národním předpisům upravujícím osobnost v soukromém právu[31]. Výsledkem toho, že se takto konkrétní debata namísto toho vedla nad Aktem, nejsou v tomto případě u nás jinak oblíbené přílepky, ale legislativní útvary, pro které dokonce ani v naší právní terminologii uvyklé jinak na lecjaké formy divoké legislativní tvořivosti, zatím ani nemáme pojmenování.

Úprava Aktu, který na řadě míst materiálně dubluje, rozvádí nebo dokonce mění pravidla založená GDPR, by se možná dala charakterizovat příměrem ke kukaččímu vejci zlomyslně nasazenému do cizího hnízda. Pravidla chránící osobní údaje, částečně převzatá z GDPR a částečně nově vytvořená, budou totiž vymáhána a sankcionována nikoli ve „hnízdě" GDPR, ale v novém „hnízdě" Aktu. Vzhledem k performativní nátuře těchto pravidel lze i čekat, že se záhy stanou předmětem legální interpretace Soudním dvorem EU a lze se jen dohadovat, zda taková interpretace půjde cestou vývoje zcela nové judikatury specificky pro zpracování osobních údajů systémy založenými na umělé inteligenci, nebo k ní SDEU přistoupí jako k rozvoji GDPR a stávající judikatury k němu.

Stejně tak lze jen spekulovat o tom, jak bude vypadat rozhodovací práce národních orgánů předpokládaných Aktem a

---

[19] Viz čl. 5(1)(h) Aktu.

[20] Ze zásady ale existují výjimky, tzn. výjimky z výjimek – typicky v urgentních případech, kdy nelze získat soudní rozhodnutí povolující použití biometrické technologie.

[21] Viz čl. 5(3), 5(4), 5(5), 5(6) a 5(7) Aktu.

[22] Viz čl. 5(1)(g) Aktu.

[23] Viz čl. 5(1)(d) Aktu.

[24] Viz čl. 5(1)(e) Aktu.

[25] Viz čl. 5(1)(f) Aktu.

[26] Srov. MURPHY, H. Facebook patents reveal how it intends to cash in on metaverse. *Financial Times* (ft.com), 18.1.2022 (online).

[27] Viz např. NEUWIRTH, R. Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA). *Computer Law & Security Review*, 2023, č. 48.

[28] Viz např. BORDELON, B. The fight over AI biosecurity risk takes a twist. *Politico.com*, 6. 2. 2024 (online).

[29] Splnění relativně složitých požadavků na výjimku samozřejmě není třeba v oblastech mimo věcnou působnost Aktu, tj. například v obraně nebo národní bezpečnosti – k tomu viz výklad k výjimkám z ex ante ochrany.

[30] Viz směrnici (EU) 2016/680 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV.

[31] Dalším nástrojem měla být např. směrnice „e-privacy" – srov. DEBUSSERÉ, F. The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster? International *Journal of Law and Information Technology*, č. 13(1), str. 70.

jejich konzistentnost s rozhodovací praxí úřadů pro ochranu osobních údajů[32]. Pro oba možné přístupy, tj. konformitu a kontinuitu i diskontinuitu, jsou přitom velmi dobré důvody, a nelze vyloučit ani to, že se orgány moci výkonné vydají jednou cestou, zatímco soudy zvolí druhou.

Dokonce ani právním vědcům, kterým různé překryvy, kontradikce nebo otazníky působnosti právní úpravy obvykle lahodí, nebudou tato legislativní kukaččí vajíčka zřejmě úplně po chuti. Dlouho totiž zřejmě nebude jasno ani o tom, zda literatura nebo judikatura interpretující ustanovení Aktu třeba o lidském dohledu, profilování nebo shora diskutované biometrické identifikaci vlastně patří do nějaké svébytné doktríny Aktu nebo GDPR, a případně jaký je vzájemný poměr těchto doktrín za situace, kdy ani jedna z úprav není vůči té druhé evidentně obecná nebo zvláštní. Podobně bude třeba řešit třeba i otázku, zda je vhodné zabývat se interpretací ustanovení Aktu týkajících se výlučně zpracování osobních údajů v literatuře, včetně komentářové, týkající se Aktu nebo spíše GDPR.

13.4 Ex ante úprava AI – aplikace AI s vysokým rizikem

Samotná definice AI systému s vysokým rizikem je z legislativně-technického hlediska provedena velmi komplikovaným způsobem. Podobně jako v jiných částech Aktu to i zde odráží dlouhý a složitý průběh vyjednávání plný kompromisů a následných kompromisů ke kompromisům. V textu se tak kromě definic vyskytuje nejen řada výjimek, ale i různě řetězených výjimek z výjimek, které by se spíš, než do zákona zřejmě hodily do nějakého Testu studijních předpokladů ověřujícího míru geniality v oblasti logického myšlení uchazečů o studium na vysoké škole.

Za AI systém s vysokým rizikem se podle Aktu považuje jednak systém založený na AI, který sám o sobě spadá do některé z regulovaných kategorií vyčtených v příloze I, nebo který zajišťuje bezpečnost produktu spadajícího do některé z těchto kategorií, a vyžaduje k uvedení na trh ověření shody třetí osobou[33]. Prakticky se jedná buďto o technologicky složitá zařízení, která je standardně k uvedení na trh třeba různými způsoby certifikovat nebo homologovat – např. letadla, motorová vozidla, výtahy apod. - nebo produkty, na kterých ve větší míře závisí život nebo zdraví lidí – např. zdravotnické prostředky nebo ochranné pracovní prostředky.

Druhou základní kategorií systémů AI s vysokým rizikem jsou případy, kdy je AI užito v některé z oblastí se systémově vysokým rizikem zásahu do práv uvedených v příloze III:

- biometrika, včetně systémů, jejichž účelem není ztotožnění ale pouze potvrzení totožnosti
- bezpečnost kritické infrastruktury – příloha konkrétně specifikuje AI systémy zajišťující zabezpečení digitální infrastruktury, silniční dopravy, a infrastruktury pro dodávky vody, plynu, elektřiny a tepla. Výslovně zde není uvedena například infrastruktura pro leteckou nebo drážní dopravu, ale její prvky (včetně bezpečnostních) obvykle spadnou pod první kategorii systémů AI s vysokým rizikem upravených zvláštními předpisy EU obsaženými ve výčtu Přílohy I
- vzdělávání – typicky AI systémy používané při ověřování schopností u přijímacích zkoušek, znalostí v průběhu vzdělávání, nebo pro prevenci disciplinárních deliktů (např. podvádění u zkoušek)
- pracovněprávní vztahy – AI systémy používané pro hodnocení uchazečů o zaměstnání nebo zaměstnanců (typicky pro účely odměn, povýšení apod.)
- základní služby – zde nikoli ve smyslu směrnice NIS, ale služeb zajišťujících základní potřeby člověka, tj. AI systémy používané orgány veřejné moci pro rozhodování o poskytování sociálních služeb nebo služeb krizové intervence (typicky pro rozhodování o prioritách pro vysílání záchranářů, policie apod.) nebo AI systémy používané finančními institucemi pro hodnocení úvěrové spolehlivosti (úvěrové bodování – credit scoring) nebo pro stanovení podmínek pojistných smluv u životního nebo zdravotního pojištění.
- vymáhání práva – AI systémy pro predikci obětí trestných činů, predikci pachatelství trestných činů (zde jsou vedle obecných prediktivních systémů zvlášť zmíněny systémy, které nejsou založeny na profilování, tj. systémy typicky pracující s obecnými modely chování nebo predikcí založenou na příslušnosti člověka k určité skupině), polygrafy (detektory lži) a jiné systémy pro ověřování spolehlivosti důkazů v trestních věcech
- migrace a ochrana hranic – podobně jako u vymáhání práva jsou to polygrafy, prediktivní systémy (zde obecně zaměřené na rizikovost pobytu cizinců, včetně zdravotních nebo bezpečnostních rizik), posuzování žádostí o azyl, víza, trvalý pobyt nebo o jiný ochranný režim. K tomu bylo ještě později doplněno ověřování totožnosti jinak než na základě cestovních dokladů
- justice a demokratické procesy (volby, referenda) – v oblasti justice to má být užití AI pro rešerše a interpretaci práva a skutkového stavu a v oblasti demokratických procesů má jít o systémy určené k ovlivňování názorů voličů. I v tomto případě se v důsledku postupného bobtnání zákonné úpravy na závěr úpravy použití AI v demokratických procesech objevila kazuistická výjimka týkající se „organizace, optimalizace a struktura politických kampaní z hlediska administrativy a logistiky“ za předpokladu, že nemá přímý vliv na fyzické osoby.

Otázka klasifikace určité formy užití AI jako vysoce rizikové ve smyslu Aktu je pro vývojáře a v řadě případů i pro

[32] Na úrovni evropských institucí to zřejmě nebude představovat zásadní problém, protože o sankcích má rozhodovat EDPS (viz čl. 72), ale ve většině členských států nebude agenda Aktu z různých (a povětšinou dobrých) důvodů svěřena úřadům pro ochranu osobních údajů.

[33] Viz čl. 6(1) a 6(2) Aktu.

uživatele takového systému velmi důležitá. Spadne-li totiž nějaký produkt nebo služba do této kategorie, znamená to řadu compliance povinností omezujících možnosti použití AI (a tím i funkční hodnotu příslušného produktu) a generujících dodatečné marginální i transakční náklady[34].

Složitá jednání, která ke konečné úpravě AI systémů vedla, se především točila okolo proporcionality mezi aktuální a potenciální rizikovostí různých forem nasazení AI pro práva člověka nebo veřejný zájem na jedné straně a dodatečnými omezeními a náklady na vývoj a nasazení těchto systémů na straně druhé[35]. Exkluzivita regulace AI systémů s vysokým rizikem by totiž sice měla omezit divoké způsoby nasazení technologií AI v oblastech, kde známe nebo předpokládáme závažná systémová rizika ochrany práv[36], ale neměla by současně vést k tomu, že tyto technologie nebudou v EU vyvíjeny nebo používány. Totální restrikce totiž nemá být účelem právní kategorie systémů AI s vysokým rizikem, ale kategorie zakázaných užití AI, o které píšeme v předchozí podkapitole.

Z právě uvedeného plyne i složitá a v mnoha směrech delikátní úprava výjimek z klasifikace AI systémů jako vysoce rizikových[37]. V případech, kdy je určitá forma užití AI klasifikována podle výše zmíněných kategorií jako vysoce riziková, je totiž z právě uvedených důvodů pravděpodobné, že se vývojáři nebo zavádějící subjekty (deployer) těchto technologií namísto investic do compliance raději uchýlí mimo efektivní jurisdikci EU.

Takové případy má ambici řešit extrateritorialita nařízení[38] koncipovaná obdobně jako v případě ochrany osobních údajů. Reálná zkušenost s doktrínou odpovídající úrovně ochrany ve smyslu GDPR[39] ale ukazuje, že především pro větší poskytovatele nebo obecně pro systémy s reálně vysokým rizikem zásahu do práv je prostě ekonomicky výhodnější usadit se mimo území EU. Podobné riziko, tj. že technologie založené na AI se budou v EU používat a vydělávat zde svým provozovatelům peníze, ale jejich vývojáři, poskytovatelé a zavádějící subjekty budou trvale usazeni mimo EU, je tedy v případě ex ante regulace AI velmi reálné.

Výsledkem výše naznačené delikátní debaty je následující struktura konkrétních skutkových podstat výjimek z klasifikace systémů AI s vysokým rizikem, jejichž generální klauzulí je absence významného rizika pro zdraví, bezpečnost, základní práva nebo svobodu vůle[40]:

- AI systém je určen k úzce vymezeným procedurálním úkonům
- AI systém má pouze vylepšovat výsledky lidské činnosti
- AI systém má detekovat odlišnosti od dřívějších rozhodovacích procesů
- AI systém je určen k přípravným činnostem předcházejícím hodnocení podle přílohy III
- (obecnou výjimkou ze shora uvedených výjimek je profilování. Pokud jej AI systém provádí, nezáleží na tom, zda naplňuje generální klauzuli a některou z výše uvedených skutkových podstat a považuje se vždy za AI systém s vysokým rizikem.)

Z dikce výše uvedených výjimek se zdá, že zřejmě vznikly v lepším případě zobecněním konkrétních kazuistik reagujících na zkušenost s nasazením AI v některé praktické aplikaci. Horší alternativou vysvětlení přítomnosti těchto výjimek je lobbying konkrétních provozovatelů.[41] Ať už je ale geneze těchto výjimek jakákoli, jejich silně metaforický charakter ve spojení se zásadním významem pro ekonomiku vývoje a nasazení technologií založených na AI vytvoří okamžitě po účinnosti Aktu z jejich interpretace ostře sledovanou záležitost.

Akt na to reaguje poměrně neobvyklou procesní úpravou[42] zavazující Komisi nejdéle do 18 měsíců od jeho účinnosti k vydání doporučení k interpretaci výjimek obsahující také „*seznam praktických příkladů použití systémů AI, které jsou a které nejsou vysoce rizikové*“. . Explicitní požadavek na konkrétní praktické příklady užití subsumovatelných pod definice AI systémů s vysokým rizikem i skutkové podstaty výjimek zřejmě odpovídá shora naznačeným dvěma pravděpodobným způsobům postupné formalizace těchto definic a skutkových podstat a ponouká Komisi k tomu, aby srozumitelně sdělila, které konkrétní aplikace nebo produkty inspirovaly formulaci výše uvedených metafor.

Výrazného rozšíření se dočkala i původně velmi stručná úprava podmíněné legislativní kompetence Komise k vydání prováděcích předpisů, která zahrnuje možnost Komise:

---

[34] V některých sektorech se již začaly objevovat předběžné výpočty nákladů na souladnost – viz např. F. HEYMANN, F., PARGINOS, K., BESSA, R.J., GALUS, M. Operating AI systems in the electricity sector under European’s AI Act – Insights on compliance costs, profitability frontiers and extraterritorial effects. *Energy Reports*, 2023, č. 10, str. 4538.

[35] Srov. DUNN, P., De GREGORIO, G. The Ambiguous Risk-Based Approach of the Artificial Intelligence Act: Links and Discrepancies with Other Union Strategies, CEUR Workshop Proceedings, Workshop on Imagining the AI Landscape after the AI Act, *IAIL 2022*, ceur-ws.com.

[36] Srov. NOVELLI, C. CASOLARI, F. ROTOLO, A., TADDEO, M., FLORIDI, L. et al. Taking AI risks seriously: a new assessment model for the AI Act. *AI & Society*, 2023, online na springernature.com.

[37] Viz čl. 6(3) Aktu.

[38] K možné extrateritorialitě Aktu viz např. ROBERTS, H., HINE, E., FLORIDI, L. Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance. In: TIMOTEO, M., VERRI, B., NANNI, R. (eds) Quo Vadis, Sovereignty? *Philosophical Studies Series*, 2023, č. 154, str. 51.

[39] Srov. čl. 45 GDPR a související judikaturu v případech C-362/14 Schrems nebo C-311/18 Schrems II. Zvláštní kategorii pak představují případy, kdy zpracování evropských osobních údajů mimo EU fakticky probíhá mimo zákonné důvody nebo rozhodnutí Komise o odpovídající úrovni ochrany a Komise ani orgány členských států proti němu nezasahují – viz SVANTESSON, D. J. B. Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, *International Data Privacy Law*, č. 5(4), 2015, str. 226.

[40] Nařízení hovoří o ‚obsahovém‘ nezasahování do rozhodování člověka – srov. čl. 6(3), první věta Aktu.

[41] Tento pojem má pro účely Aktu specifický význam a označujeposkytovatele, výrobce produktu, zavádějící subjekt, zplnomocněného zástupce, dovozce nebo distributora. – viz čl. 3(8) Aktu.

[42] Viz čl. 6(5) Aktu.

- rozšířit nebo změnit (včetně zrušení) výčet konkrétních skutkových podstat výjimek ve smyslu čl. 6(3)[43] – tato neobvyklá konstrukce umožňující Komisi přímý zásah do struktury nařízení je ale, na rozdíl od jinak obecného přístupu Aktu založeného na hodnocení rizik, podmíněna prokazatelnou potřebou úpravy (tj. jedná se o uplatnění evidence-based přístupu namísto jinak obvyklého risk-based)
- podobně jako v předchozím případě rozšířit nebo změnit (opět včetně zrušení) výčet systémů AI s vysokým rizikem obsažený v příloze III[44]. Ustanovení čl. 7 je poměrně detailní co do důvodů, pro které Komise může tento typ legislativní kompetence použít – ty ale nejsou v porovnání s předchozím případem založeny na prokazatelnosti ale u většiny postačuje analýza rizik (ať už jde o existenci rizik v případě rozšíření seznamu nebo o neexistenci rizik v případě jeho omezení).

Požadavek na specifikaci výjimek, včetně uvedení konkrétních příkladů, je nařízením formulován kategoricky, zatímco podmíněnou legislativní kompetenci umožňující upravovat definice systémů AI s vysokým rizikem nebo naopak výjimky z těchto definic má Komise upravenu jako fakultativní. Těžko lze tedy předpovídat, jak často a jak vehementně bude mít Komise vůli a motivaci zasahovat do z pohledu provozovatelů zřejmě nejdůležitější části Aktu. Relativně konkrétní úprava Aktu obsahující vedle důvodů i metodu, kterou může Komise tyto legislativní zásahy provádět (typicky risk-based nebo evidence-based), by ale měla být zárukou praktické legitimity a případně i následné transparentní přezkoumatelnosti této delegované právotvorby Soudním dvorem.

Úprava povinností týkajících se systémů AI s vysokým rizikem má podobnou vnitřní logiku jako například GDPR. Nařízení tedy jednak neadresně upravuje obecné povinnosti týkající se (v tomto pořadí):

- správy a řízení rizik – jedná se o typickou abstraktní performativní úpravu povinností typu compliance, jejíž konkrétní realizace bude vždy otázkou typu příslušného AI systému a charakteru rizik[45]. Zvláštní pozornost je věnována problematice testování[46], přičemž povinnost zahrnout testování do systému správy rizik platí i v případech, kdy budou příslušné systémy AI s vysokým rizikem testovány například při certifikaci ze strany orgánů posuzování shody,
- správy dat – podobně jako v případě správy rizik jde o performativní úpravu zakládající povinnost vytvoření systematického řešení zajišťujícího pragmaticky dosažitelnou transparentnost a ověřitelnost dat. Akt se v této části specificky zmiňuje o riziku algoritmické předsudečnosti (bias) a pro účel zjednodušení detekce jejího rizika ve zdrojových datasetech dokonce zavádí výjimku ze zákazu zpracování zvláštních kategorií osobních údajů[47],
- technické dokumentace – tato úprava má behaviorální charakter. Konkrétní formy naplnění povinnosti vytvořit pro systém AI s vysokým rizikem dokumentaci určenou k ověření souladnosti s požadavky Aktu stanoví příloha č. IV, kterou může Komise doplňovat nebo měnit podobně jako ve shora uvedených případech. Narozdíl od definice systémů AI s vysokým rizikem ale v tomto případě nařízení Komisi nijak zvlášť neomezuje účelem ani metodou, když jen obecně říká, že k takové úpravě může komise sáhnout „ve světle technického vývoje“[48]. Poněkud diskutabilní je právo Komise stanovit zjednodušené formuláře použitelné k technické dokumentaci ze strany SME. Nabízí se v této souvislosti otázka, proč by takových formulářů nemohl použít kdokoli, když jejich smyslem je poskytnout různým orgánům členských států dostatečný podklad k ověření souladnosti příslušného systému s požadavky Aktu,
- dokumentace provozu – tato úprava má spíše behaviorální charakter, protože zakládá konkrétní povinnost logovat provoz systémů AI s vysokým rizikem[49],
- informačních povinností vůči zavádějícím subjektům– tato opět behaviorální úprava sice není úplně adresná, ale je z ní zřejmé, že směřuje k typům provozovatelů poskytujících systém AI s vysokým rizikem jiným subjektům jako produkt nebo službu. Akt zde zavádí povinnost dokumentovat příslušný systém tak, aby mohl být adekvátně používán a omezilo se riziko jeho vadného použití nebo dezinterpretace jeho výstupů[50],
- lidského dohledu – toto pravidlo má performativní povahu a směřuje k takovému designu systému AI s vysokým rizikem, který umožní nebo si v určitých případech vyžádá kontrolu nebo zásah člověka (jednoho nebo případně i dvou[51]),
- odolnosti – toto performativní pravidlo zavádí značně metaforickou povinnost provádět návrh a vývoj systémů AI s vysokým rizikem tak, aby v průběhu celého svého životního cyklu dosahovaly „odpovídající úrovně přesnosti, robustnosti a kyberbezpečnosti.“ Oproti např. povinnosti zajistit možnost lidského dohledu jsou ale povinnosti týkající se odolnosti natolik obecně formulované, že bude zřejmě velmi problematické kontrolovat jejich plnění, respektive konstatovat a sankcionovat jejich neplnění. Jediným obecně použitelným důkazem nesplnění této performativní povinnosti bude zřejmě empirické srovnání neodolného systému AI s vysokým rizikem s jiným obdobným systémem, který „odpovídající úrovně“ dosahuje.

Absence konkrétní adresy u výše uvedených povinností má legislativně-technický důvod. Povinnosti definované touto

[43] Viz čl. 6(6) Aktu.
[44] Viz čl. 7 Aktu.
[45] Viz čl. 9 Aktu.
[46] Viz čl. 9(6) až 9(9) Aktu.
[47] Viz čl. 10(5) Aktu.
[48] Viz čl. 11(3) Aktu.
[49] Viz čl. 12 Aktu.
[50] Viz čl. 13 Aktu.
[51] Srov. čl. 14(5) Aktu.

částí Aktu totiž mohou dopadnout na různé druhy subjektů v návaznosti na to, o jaký druh systému AI půjde a jaký bude jeho obchodní model. V nejjednodušších, ale zřejmě nikoli příliš frekventovaných případech, kdy bude systém AI s vysokým rizikem vyvinut a uveden na lokální trh jako zboží určené spotřebiteli, dopadnou všechny tyto povinnosti výlučně na poskytovatele. Zapojí-li se ale do celého řetězce ještě například distributor, nebo bude-li systém AI s vysokým rizikem zaváděn subjektem, který bude jeho prostřednictvím řešit nějaké své činnosti dopadající na třetí osoby (např. škola, orgán veřejné moci apod.), rozšíří se tím i okruh povinných subjektů.

Shora zmíněná společná úprava obecných povinností bez uvedení konkrétního typu povinného subjektu umožňuje, aby pro tyto složitější (a v praxi zřejmě i běžnější) případy Akt v částech, kde specificky upravuje postavení těchto subjektů, na tyto povinnosti jen odkázal. Současně tím dává Akt relativní volnost příslušným národním orgánům v tom, koho budou kontrolovat a sankcionovat za situace, kdy je určitá povinnost založena více subjektům současně.

Druhá část úpravy ex ante povinností dopadajících na provozovatele systémů AI s vysokým rizikem je už vzhledem ke svému charakteru definována pro konkrétní typy subjektů, a to

- Poskytovatele (provider), tj. subjekty, které AI systému uvádějí na trh (ať jde o prodej nebo o službu) nebo je provozují pod svým jménem[52]. Označení, pod kterým je systém uveden na trh nebo zaváděn, je v tomto případě zásadní, protože odlišuje poskytovatele s rozsáhlým katalogem povinností od zavádějícího subjektu, jehož rozsah povinností je nepoměrně užší. Poskytovatel plní většinu z výše uvedených povinností typu compliance, které jsou neadresně specifikovány v čl. 8 až čl. 15 Aktu. Konkrétní definice (u performativních povinností) a realizace organizačních a technických opatření, včetně řízení rizik, se v případě zavádějícího subjektu souhrnně označují jako systém řízení kvality[53]. K tomu přistupují ještě dokumentační povinnosti včetně logování,[54] následný dohled[55] a velmi důležitá registrační povinnost platící i pro případy, že poskytovatel konstatoval a dokumentoval výjimku ve smyslu čl. 6(3)[56]. Stejné povinnosti podle čl. 16 jako poskytovatel má mít výrobce, jehož výrobek spadající do některé z regulovaných kategorií podle přílohy I obsahuje systém AI jako bezpečnostní opatření a je uváděn na trh pod jeho označením[57].
- Dovozce a distributory, tj. subjekty, které zpřístupňují (typicky prodávají nebo je poskytují jako službu) systémy AI na evropském trhu[58]. Rozdíl mezi dovozcem a distributorem spočívá v tom, že dovozce je dovozcem systému AI s původem mimo jednotný trh, zatímco distributorem je každý subjekt odlišný od poskytovatele a dovozce, který uvádí na trh systémy AI bez ohledu na jejich původ. U výrobků obsahujících systém AI s vysokým rizikem a vyrobených v Číně pod značkou americké firmy tedy bude de iure výrobcem čínská firma, poskytovatelem americká firma, dovozcem ten, kdo výrobky doveze na jednotný trh a distributorem každý, kdo bude na jednotném trhu tyto výrobky prodávat. Povinnosti dovozce a distributora se podobají a spočívají především ve formální kontrole a dokumentaci toho, že jejich produkt (výrobek nebo služba) je v souladu s požadavky Aktu.
- Zavádějící subjekty (deployer), tj. všechny možné subjekty, které používají systémy jinak než pro osobní použití[59] – může jít o orgány veřejné moci využívající systémy AI k podpoře rozhodovací činnosti, zaměstnavatele používající takové systémy k personálním rozhodnutím, finanční instituce, které tyto systémy používají např. k rozhodování o úvěrech nebo pojistkách apod. Povinnosti zavádějících subjektů se týkají především dohledu nad fungováním příslušného systému vzhledem k podmínkám Aktu, včetně zajištění lidského dohledu a dokumentace (včetně výročních zpráv). Základním nástrojem compliance je v tomto případě dokument „hodnocení dopadu systému AI s vysokým rizikem“, který má podobný charakter jako například DPIA známý z GDPR[60] a týká se především analýzy rizik a definice opatření k jejich pokrytí. Akt také přímo předpokládá, že Kancelář vydá ke zpracování tohoto hodnocení dopadu snadno použitelný formulář[61]. Zvláštní povinnosti týkající se především identifikačních technologií (včetně těch, na které se vztahují výjimky ze zakázaných forem užití AI diskutované v předchozí podkapitole) pak ještě dopadají na zavádějící subjekty, které jsou orgány veřejné moci.
- Provozovatele (operators) – na rozdíl od předchozích se tato kategorie s ostatními překrývá a tento pojem se používá společně pro různé subjekty vystupující v obchodním řetězci systémů AI bez ohledu na to, zda je obchodní model postaven na jejich prodeji nebo provozu. Jedná se tedy o společné označení pro poskytovatele, výrobce, zplnomocněného zástupce, distributora, dovozce nebo zavádějící subjekt[62]. Obecně lze konstatovat, že Akt pro různé tyto subjekty vyskytující se v distribučním řetězci stanoví povinnosti poskytovatele (viz výše) pro případ, že je příslušný systém AI uveden na trh pod jejich označením nebo významným způsobem zasahují do jeho struktury nebo

[52] Viz definici v čl. 3(3) Aktu.
[53] Viz čl. 17 Aktu.
[54] Viz čl. 18 a čl. 19 Aktu.
[55] Mechanismus následného dohledu (post-market monitoring) se podobá systematickému sběru dat o použití zdravotnických prostředků. Podrobnější srovnání viz v ŽOLNERČÍKOVÁ, V. Autonomous Vehicles Vigilance System: Proposal for a Theoretical Legal Framework. *The Lawyer Quarterly*, č. 11(1), 2021, str. 206.
[56] Viz čl. 49(2) Aktu.
[57] Zavedení výrobce jako poskytovatele ve smyslu čl. 16 je poněkud nesystematicky upraveno v čl. 25(3).
[58] Viz čl. 3(6) a čl. 3(7) Aktu.
[59] Čl. 3(4) používá v anglické verzi nepříliš vhodný výraz „authority,“ a to ve smyslu, že zavádějící subjekt používá systém AI v rámci svých oprávnění. Preambule Aktu v odst. 13 obsahuje trochu srozumitelnější vysvětlení upřesňující, že zavádějícím subjektem může být soukromý i veřejný subjekt a použití systému AI může ovlivnit i jiné osoby než samotný zavádějící subjekt.
[60] Srov. čl. 35 GDPR.
[61] Srov. čl. 27(5) Aktu.
[62] Viz čl. 3(8) Aktu.

fungování. Akt tedy v tomto případě zakládá ex ante povinnosti buďto z důvodu ochrany oprávněného očekávání zákazníka (kterým nemusí být nutně spotřebitel) anebo v důsledku reflexe faktické míry kontroly nad fungováním příslušného systému.

Relativní složitost struktury těchto specifických povinností mají zmírňovat kromě delegované legislativy také doporučené postupy (metodiky) a standardizované (formulářové) nástroje. Ke standardizaci by měly směřovat i smluvní vztahy mezi různými typy provozovatelů účastnících se distribučního řetězce pro určitý systém AI s vysokým rizikem. Akt se v tomto směru poučil ze zkušenosti s náběhem performativní regulace v případě GDPR, kde se ani v řádu let nepodařilo motivovat jednotlivé soukromoprávní nebo veřejnoprávní komunity k tomu, aby vznikly standardní smluvní klauzule, kodexy (neformální nebo oficiálně schválené) a další nástroje, které mají zajistit především středním a malým korporacím plnění často složitě strukturovaných povinností za užití snadno dostupných a srozumitelných typizovaných forem právního jednání. Reálná typizace různých compliance řešení vytvořených na základě požadavků performativních pravidel tak má v případě GDPR stále charakter opisování úspěšných řešení u malých veřejnoprávních korporací typu obcí, nebo opakovaného prodeje téhož osvědčeného komerčního řešení různým zákazníkům ze soukromého sektoru.

Akt díky této nevalné zkušenosti, kdy se různé profesní organizace, sdružení veřejnoprávních korporací, komory apod. namísto tvorby jednoduchých nástrojů zaměřily spíše na veřejný lobbying a další politické aktivity, zavazuje k tvorbě prakticky použitelných formalit povětšinou Kancelář[63]. Otázkou ale je, jak může být takový přístup úspěšný za předpokladu, že bude Kancelář muset tvořit one-size-fits-all nástroje pro typologicky velmi široký okruh systémů AI a jejich provozovatelů (kterými mohou být poskytovatelé, ale také výrobci, distributoři, zavádějící subjekty apod.)

V performativně pojatém regulačním rámci založeném na ex ante compliance vždy existuje přirozená poptávka po mechanismu ex ante ověření souladnosti příslušného řešení vytvořeného a nasazeného regulovaným subjektem. Zákonná povinnost totiž zde nemá konkrétní charakter, ale zavazuje regulovaný subjekt k vytvoření vlastního řešení konkrétních povinností, které sám regulovaný subjekt dokumentuje, dodržuje a interně vymáhá. Fatální nejistota regulovaného subjektu ohledně toho, zda takovým řešením opravdu dostál požadavků metaforické právní úpravy pak logicky generuje zájem po nástroji, kterým by mohlo dojít k oficiálnímu potvrzení nebo vyvrácení souladnosti.

Tradičně základním institutem souladnosti, nikoli jen pro performativní pravidla, je v rámci jednotného trhu shoda. Ta bývá ověřována buďto autonomně, tj. samotný, regulovaným subjektem, nebo v exponovanějších případech formou certifikace nezávislým externím subjektem, tj. orgánem posuzování shody.

S oběma způsoby posuzování shody počítá pro systémy AI s vysokým rizikem i Akt. U produktů spadajících do výčtu podle Přílohy I, kde je certifikace vyžadována jiným předpisem, má být ověření shody s Aktem součástí takové certifikace (tj. neprobíhá paralelně certifikace dle Aktu i zvláštního předpisu)[64]. V ostatních případech akt rozlišuje mezi případy, kdy musí být systém AI s vysokým rizikem certifikován některým z orgánů posuzování shody a případy, kdy shodu ověřuje sám regulovaný subjekt. Specificky je ještě upravena presumpce shody v případech, kdy je systém AI s vysokým rizikem souladný s harmonizovanou technickou normou[65]. Pro tyto účely zavazuje Akt Komisi k podání žádosti o normalizaci tak, aby byla k dispozici konkrétní technická norma (resp. normy) pro systémy AI s vysokým rizikem[66].

Systém certifikací, včetně orgánů posuzování shody, vypadá v Aktu podobně jako například v případě kyberbezpečnosti[67] nebo připravované úpravy kyber-odolnosti[68]. Podstatným rozdílem oproti certifikačnímu systému v oblasti kyberbezpečnosti založenému na relativně oddělených schématech vydávaných Komisí je v tomto případě jednotný charakter zákonných povinností dopadajících na systémy AI s vysokým rizikem (resp. na základní modely – viz dále) doplněný pouze o požadavek na jejich bližší jednotnou specifikaci ze strany Komise[69]. Akt ale stojí na prioritě technických norem, což znamená, že bude-li určitý regulatorní požadavek na systémy AI předmětem harmonizované technické normy, zruší Komise případnou dřívější jednotnou specifikaci a při posuzování shody se bude postupovat podle harmonizované technické normy[70].

Lze očekávat, že posuzování shody a fungování procesu certifikace bude mít pro reálnou praxi vývoje a nasazení systémů AI s vysokým rizikem velký význam. Nejde jen o shora zmíněnou poptávku vyvolanou kombinací performativního charakteru příslušných ex ante pravidel a potenciálně velmi citelných sankcí, ale i o další regulatorní souvislosti shody a především certifikátů.

Zřejmě nejdůležitější z těchto souvislostí se týká otázek ex post regulace systémů AI, tj. odpovědnosti, které se věnujeme dále. Certifikáty a další formy ex ante potvrzené shody budou hrát zásadní roli v přenosu důkazního břemene v případech vymáhání náhrad nebo zadostiučinění. To se pak následně projeví do kalkulace pojistných modelů, které budou mít velký význam v ekonomických úvahách ohledně investic do investičně náročných oblastí vývoje AI. Není v této souvislosti nadsázkou, pokud budeme ceny pojistek považovat v této vysoce rizikové (nejen podle jména) oblasti za klíčový ekonomický faktor investic – a certifikáty, resp. jejich dostupnost a následný význam pro pojistná rizika, budou v tomto případě zřejmě

---

[63] Srov. čl. 25(4) Aktu.
[64] Viz čl. 43(3) Aktu.
[65] Srov. čl. 40(1) Aktu.
[66] Srov. čl. 10 nařízení (EU) č. 1025/2012 evropské normalizaci, změně směrnic Rady 89/686/EHS a 93/15/EHS a směrnic Evropského parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES, a kterým se ruší rozhodnutí Rady 87/95/EHS a rozhodnutí Evropského parlamentu a Rady č. 1673/2006/ES.
[67] Cybersecurity Act
[68] Cyber-resilience Act
[69] Srov. čl. 41 Aktu.
[70] Viz čl. 41(4) Aktu.

hrát rozhodující roli.

13.5 Ex ante regulace obecných modelů AI

Pojem obecných systémů AI (general purpose AI – GPAI) se do struktury návrhu Aktu dostal až relativně nedávno, a to v reakci na masivní nástup generativních technologií. Původně měl označovat základový systém, který je způsobilý provádět samostatně různé druhy zpracování dat a díky tomu je použitelný pro různé konkrétní aplikace. Dalším pojmem, o jehož zavedení do Aktu se původně uvažovalo, a to rovněž v návaznosti na pragmatickou zkušenost s generativními technologiemi, byl základní model (foundation model), a to ve smyslu modelu, který tvoří základ systému obecného určení. Na příkladu známé technologie GPT by taková klasifikace znamenala oddělení samotného modelu, tj. GPT, od jeho aplikace obecného určení, tj. Chat GPT.

Pragmatickou redukcí se nakonec v poslední fázi hledání kompromisu mezi Komisí, Radou a Parlamentem dospělo ke sjednocení kategorie modelu a systému obecného určení do jednotného obecného modelu AI. Takové zjednodušení je postaveno na zřejmě správném předpokladu, že jediným legitimním účelem základního modelu, který si kvůli své důležitosti a potenciální rizikovosti určitě zaslouží regulatorní ošetření, je posloužit jako základ systému AI obecného určení – a pokud se někde projeví defekt nebo jiné riziko takového modelu, je to vždy prostřednictvím systému AI obecného určení, který vadným zpracováním dat zasáhne do práv nebo jiných právem chráněných zájmů. Pokud už tedy dojde k tomu, že jsou model a systém AI obecného určení vyvíjen nebo zaváděn různými subjekty, je z pohledu smyslu a účelu právní regulace lhostejné, na koho z nich dopadnou příslušné regulatorní povinnosti.

Zatímco bylo shora zmíněným výsledkem kompromisu na jedné straně zjednodušení klasifikace GPAI, došlo na druhé straně k vnitřní strukturaci pojmu modelu AI obecného určení do následujících podkategorií:

- Obecné modely AI bez systémového rizika – poskytovatelé těchto modelů mají dokumentační povinnosti týkající se modelu[71] a jeho použití jako základu pro poskytovatele systémů AI založených na takovém modelu[72] a dále zajímavě definovanou povinnost vytvořit korporátní podmínky pro ochranu autorských práv založených právem EU[73]. Poskytovatel modelu, který není usazen v EU, má k tomu povinnost jmenovat a oznámit Kanceláři odpovědného zástupce, jehož prostřednictvím bude plnit povinnosti dle Aktu.
- Obecné modely AI bez systémového rizika poskytované na základě bezúplatné otevřené licence – jejich poskytovatelé mají oproti ostatním poskytovatelům obecných modelů AI katalog povinností omezen o dokumentaci a nutnost jmenovat v EU odpovědného zástupce. Vedle otevřeného a bezúplatného licencování vyžaduje ještě Akt k zařazení do této kategorie ještě transparentní dokumentaci modelu umožňující jeho modifikace.
- Obecné modely AI se systémovým rizikem – jedná se prakticky o původní kategorii modelů, k níž se vážou další povinnosti pro poskytovatele zahrnující nad rámec ostatních výše uvedených obecných povinností především notifikaci[74], relativně rozsáhlé transparenční a evaluační povinnosti a hlášení incidentů[75].

Regulace poskytovatelů obecných modelů AI se sice ve struktuře nařízení objevila až dodatečně, ale můžeme předpokládat, že bude mít na podobu autonomních technologií v Evropě určující dopad. Kvůli velké investiční náročnosti totiž není pravděpodobné, že by s produkty tohoto typu přicházel každou chvíli na trh kdejaký startup. Vývoj modelů v kvalitě, která bude mít šanci uspět na trhu, tedy bude s největší pravděpodobností doménou technologických gigantů a konkurence různých řešení, včetně nenáročných startupových projektů, poroste až o úroveň níže v segmentu, který Akt označuje jakonavazující.

O vhodnosti a potřebnosti regulace poskytovatelů obecných modelů AI se vedla bouřlivá diskuse[76] a výsledná podoba Aktu se v tomto směru zdá být poměrně zdrženlivá – to i v porovnání například s úpravou systémů AI s vysokým rizikem. Oproti vysoce rizikovým aplikacím není v tomto případě ani příliš otevřené pole pro Komisi k dalšímu legislativnímu zpřísňování podmínek[77] a Akt naopak velmi podrobně upravuje proceduru určení obecného modelu AI se systémovým

[71] Viz čl. 53(1) Aktu.

[72] Viz čl. 53(2) Aktu.

[73] Čl. 53(1)(c) explicitně zdůrazňuje, že takové podmínky musí reflektovat výhradu ve smyslu čl. 4(3) směrnice DSM. V této souvislosti je důvod ptát se, proč se Akt nezabývá například právem na život, zdraví nebo třeba základními principy demokratického právního státu a namísto toho se v souvislosti se základními modely specificky soustředí zrovna na majetková práva autorská a strojově čitelné výhrady. Nabízí se spekulativní vysvětlení v tom směru, že zmíněná základní práva nebo principy zřejmě neměly v procesu hledání legislativního kompromisu v porovnání s majetkovými právy autorskými tak silné podporovatele.

[74] Viz čl. 52(1) Aktu.

[75] Specifické povinnosti podle čl. 55 Aktu přistupují v tomto případě k obecným povinnostem všech poskytovatelů modelů podle čl. 53 Aktu.

[76] Viz např. MOREIRA, N. A., FREITAS, P. M., NOVAIS, P. The AI Act Meets General Purpose AI: The Good, The Bad and The Uncertain. In: MONIZ, N., VALE, Z., CASCALHO, J., SILVA, C., SEBASTIÃO, R. (eds) *Progress in Artificial Intelligence*. EPIA 2023, Lecture Notes in Computer Science, č. 14116, str. 157.

[77] Namísto regulace, jejíž parametry by mohla Komise průběžně upravovat v návaznosti na vyhodnocená rizika, počítá Akt pouze s kodexy (srov. čl. 56 Aktu), to navíc za situace kdy se předpoklad, že se kodexy stanou hlavním nástrojem běžné praxe ukázal například v případě GDPR jako vcelku naivní.

rizikem včetně možnosti poskytovatele takové určení zpochybnit[78].

Přísnější regulace poskytovatelů obecných modelů AI se systémovým rizikem přitom mohla přinést jednotnému trhu paradoxně menší regulatorní zátěž a větší efektivitu. Poskytovatelé obecných modelů AI mají totiž díky své velikosti a tržní síle obvykle odpovídající aparát a tím i odbornou a technickou kapacitu ke zpracování různých druhů performativních pravidel a tvorbě vlastních efektivních regulatorních řešení, která kromě samotného poskytovatele dokážou efektivně regulovat chování i dalších subjektů nabízejících návazné aplikace (navazující).

Akt ale namísto toho ale přichází s řešením, které sice zavádí poskytovatelům obecných modelů AI se systémovým rizikem řadu především transparenčních a dokumentačních povinností, ale nenutí je ke komplexnímu regulatornímu ošetření jejich ekosystémů. Namísto toho, aby minimálně část regulatorní zátěže specifických systémů AI (viz dále) nebo i systémů AI s vysokým rizikem vyřešil Akt jednotně a efektivně na úrovni poskytovatele modelu, dopadnou všechny možné povinnosti na každého jednotlivého poskytovatele systému AI, který je na takovém modelu založen. S praktickou jistotou lze předpokládat, že úroveň ochoty a schopnosti dostát takovým povinnostem se bude napříč různými poskytovateli návazných systémů velmi různit a jednoduchou situaci nebudou mít ani orgány členských států, které budou na jejich činnost dohlížet a sankcionovat ji. Byla-li by namísto toho kontrolní a sankční zátěž alespoň zčásti přesunuta na zavádějící subjekt obecného modelu AI, mohla být ochrana práv v návazných systémech jednotnější a její kontrola a vymáhání díky technickým schopnostem poskytovatelů obecných modelů AI i nesrovnatelně efektivnější.

13.6 Ex ante regulace vybraných systémů AI bez ohledu na míru rizika

Původní koncepce Aktu počítala s tím, že pod nějakou formu regulace budou spadat veškeré systémy AI, respektive různé druhy jejich provozovatelů. Tato základní forma regulace ale měla být inkluzivní, tj. naplnění jejích požadavků mělo být relativně snadné a regulace tedy neměla vést k tomu, že by příslušnými požadavky ztěžovala nebo znemožňovala přístup některých systémů AI na trh nebo obecně do aplikační praxe.

Na základě dalších diskusí obsahuje výsledný kompromisní návrh inkluzivní regulaci, která ale dopadá pouze na určité typy systémů AI a řeší tak některá aktuálně známá konkrétní rizika jejich vývoje nebo nasazení. Není ale správnou interpretace v tom směru, že by věcná působnost těchto povinností zahrnovala jen systémy AI s nízkým rizikem. Tyto povinnosti totiž dopadají na všechny AI systémy nebo obecné modely AI bez ohledu na jejich rizikovost a v případě systémů AI s vysokým rizikem tedy doplňují katalog exkluzivních povinností, které jsme rozebrali výše. Inkluzivní povinnosti se tedy týkají:

- poskytovatelů systémů AI určených k interakci s člověkem – ti mají, není-li zjevné, že jde o umělou inteligenci, povinnost informovat o tom jejich uživatele[79].
- poskytovatelů generativních systémů AI pro text, zvuk, obraz (vč. videa) – těm Akt ukládá povinnost zajistit, že z výstupů generovaných těmito systémy bude jasné (včetně strojově čitelné informace), že jde o umělý produkt[80].
- subjektů zavádějících systémů AI generující deep fakes – na rozdíl od poskytovatelů generativních systémů podle odst. 2 jde v tomto případě jednak o zavádějící subjekt a jednak je osobní působnost rozšířena o systémy, které negenerují umělý obsah, ale manipulují existující obsah. Další rozdíl je v tom, že tyto zavádějící subjekty mají na rozdíl od zavádějících subjektů generativních systémů pouze obecně vymezenou povinnost sdělit (disclose), že obsah byl vytvořen nebo změněn generátorem. Pozoruhodné je, že zatímco povinnost sdělit umělost obsahu se uplatní bez omezení pro systémy generující video, obraz a zvuk, dopadá na zavádějící subjekty textových generátorů nebo generátorů deepfakes pouze v případě, je-li takový textový obsah „*zveřejněn za účelem informování veřejnosti o záležitostech veřejného zájmu*.[81]“ Vedle obligátní výjimky pro účely odhalování a stíhání trestné činnosti se také tato transparenční povinnost nevztahuje na situace, kdy generovaný obsah byl „*podroben procesu přezkumu člověkem nebo redakční kontroly a pokud za zveřejnění obsahu nese redakční odpovědnost fyzická nebo právnická osoba*.[82]“
- subjektů zavádějících systémy AI pro rozpoznávání emocí nebo biometrickou kategorizaci – ti mají povinnost informovat o nasazení takových systémů osoby, které jsou vystaveny jejich fungování. Nemusí jít v tomto případě nutně o systémy zpracovávající osobní údaje nebo citlivé osobní údaje a tato povinnost tedy dopadá i na systémy neidentifikující člověka. „Kategorizace“ totiž může znamenat třeba i jen určení pohlaví nebo věku[83].

[78] Komise má v takovém případě relativně exaktně stanovené důvody, pro které může důvody takového zpochybnění odmítnout – ty jsou ale v důsledku různých legislativních úprav stanoveny relativně rigorózně a lze čekat, že se nad nimi budou v brzké budoucnosti odehrávat ostré argumentační bitvy. Je pak docela dobře možné, že v případě agilní argumentace poskytovatele se určení nakonec vyhne i leckterý model, který posloužil jako typický příklad pro definování parametrů této právní úpravy – srov. čl. 52(3) a 52(4).

[79] Výjimkou jsou systémy AI používané na základě zákonného zmocnění při odhalování a stíhání trestné činnosti – viz čl. 50(1) Aktu.

[80] Výjimkou jsou asistenční systémy, které výstup přímo negenerují ale pouze jej upravují, tj. např. jazykové korektory, retušovací systémy apod. – viz čl. 50(2) Aktu.

[81] Viz čl. 50(4) Aktu.

[82] Viz tamtéž.

[83] Výjimkou jsou jako v případě podle odst. 1 systémy používané při odhalování a stíhání trestné činnosti – viz čl. 50(3) Aktu.

13.7 Výjimky z ex ante regulace

Logika výjimek osobní a věcné působnosti Aktu vychází z předpokladu, že Akt je předpisem upravujícím fungování vnitřního trhu, tj. nejde o předpis upravující národní bezpečnost, trestní postih nebo třeba obranu. Zvláštní pozornost si v tomto ohledu žádá především obecná výjimka pro systémy AI používané při zajišťování národní bezpečnosti[84]. Ta je koncipována jako výjimka z věcné působnosti nařízení, protože explicitně nerozlišuje podle subjektů a dopadá tedy například i na soukromé subjekty vyvíjející, poskytující nebo zavádějící (ve smyslu Aktu) systémy AI za účelem zajištění národní bezpečnosti členského státu[85]. Současně to znamená že je tuto výjimku nutno vykládat nikoli paušálně, ale vždy ad hoc vzhledem k typu činnosti příslušného subjektu, soukromého nebo veřejného. Lze tedy sice předpokládat, že například činnost zpravodajských služeb bude obvykle cílena k zajištění národní bezpečnosti – to ale neznamená, že vše, k čemu zpravodajská služba použije systém AI, je automaticky vyňato z působnosti nařízení.

> K interpretaci pojmu národní bezpečnosti a jeho aplikaci na systémy AI a jejich provozovatele lze analogicky použít aktuální judikaturu SDEU ke GDPR. V případu C-33/22[86] posuzoval Soudní dvůr naplnění hypotézy tohoto pojmu při zpracování osobních údajů vyšetřovacím výborem rakouské Národní rady, který se měl zabývat možným politickým ovlivňováním jedné z rakouských zpravodajských služeb. Skutečnost, že byl výbor ustaven za účelem vyšetřování zpravodajské služby, do jejíhož rozsahu činnosti patří především ochrana ústavy a národní bezpečnosti, dle tohoto rozhodnutí nepostačuje sám o sobě k tomu, aby se zde výjimka z věcné působnosti GDPR uplatnila. Soud v této otázce konstatoval, že „výjimka z oblasti působnosti GDPR stanovená v čl. 2 odst. 2 písm. a) tohoto nařízení se vztahuje pouze na kategorie činností, které z důvodu své povahy nespadají do oblasti působnosti unijního práva, a nikoli na kategorie osob bez ohledu na to, zda mají soukromou či veřejnou povahu, ani – pokud je správcem orgán veřejné moci – na okolnost, že úkoly a povinnosti tohoto orgánu jsou přímo a výlučně spjaty s určitou výsadou veřejné moci, aniž tato výsada souvisí s činností, která se každopádně vymyká působnosti unijního práva. Okolnost, že zpracování osobních údajů provádí vyšetřovací výbor zřízený parlamentem členského státu při výkonu jeho kontrolní pravomoci vůči výkonné moci, neumožňuje tedy sama o sobě konstatovat, že toto zpracování je prováděno v rámci činnosti, která nespadá do působnosti unijního práva ve smyslu čl. 2 odst. 2 písm. a) GDPR.[87]“

Další výjimka z věcné působnosti nařízení týká se vědeckého výzkumu a vývoje. Do struktury nařízení byla zařazena až po silném tlaku akademické komunity silně motivované komerčními odběrateli výsledků aplikovaného výzkumu.

Na rozdíl od výše zmíněné národní bezpečnosti nelze v tomto případě úplně použít analogii z GDPR, neboť tam je vědecký výzkum (nemluvě o vývoji – development) pouze důvodem k neaplikovatelnosti zákazu zpracovávat zvláštní kategorie osobních údajů[88] a k omezení některých práv subjektů osobních údajů[89]. Zpracování osobních údajů ale i v případě účelu vědeckého výzkumu spadá pod rozsah věcné působnosti GDPR ve většině oblastí ochrany a je k němu mimo jiné třeba i specifického titulu, kterým vědecký výzkum ani sám o sobě není[90].

První část výzkumné výjimky paušálně dopadá na systémy AI, modely i na jejich výstupy, to za předpokladu, že vznikají výlučné za účelem výzkumu nebo vývoje[91]. Teoreticky by tedy mělo jít o primární nebo experimentální výzkum bez vazby na aplikovaný výstup. Vzhledem k tomu, že tato část výjimky je díky svému paušálnímu charakteru velmi atraktivní, je otázkou, jak bude požadavek výlučnosti výzkumného nebo vývojového účelu odolávat možnému zneužití.

Bez větší nadsázky se dá tvrdit, že žádný, dokonce ani primární, výzkum není důvodné provádět samoúčelně a že všechny výsledky výzkumu a vývoje by v konečném důsledku měly směřovat k nějaké aplikaci – a tomu by měla odpovídat i interpretace výjimky v tom směru, že výlučnost výzkumného účelu nemůže být vykládána absolutně. Na druhé straně ale nelze pominout potenciální pokušení poskytovatelů pracovat s přiřazením jinak právně rizikového výzkumu k nějaké výzkumné instituci jako s alternativou k možná nákladnějšímu a méně komfortnímu pískovišti (sandbox - viz dále).

Druhá část výzkumné výjimky omezuje věcnou působnost Aktu o případy, kdy k výzkumu, vývoji nebo testování systémů AI nebo modelů dochází před jejich uvedením na trh nebo nasazením do provozu[92]. Oproti odst. 6 dopadá v tomto případě výjimka na jakýkoli výzkum a vývoj, tj. včetně takového, na jehož konci stojí komerční produkt. Jedinou výjimkou z výjimky, tj. situací, kdy výzkum, vývoj nebo testování před uvedením na trh nebo do provozu přeci jen spadne pod rozsah povinností stanovených Aktem, je testování v reálných podmínkách[93].

Poslední z obecných výjimek týká se systémů AI šířených pod veřejnými licencemi jako open source. Tato výjimka je ale, podobně jako řada dalších základních ustanovení Aktu, provedena z legislativně technického hlediska poněkud

---

[84] Viz čl. 2(3) Aktu.

[85] Členské státy sice mají autonomii vzhledem k EU v zajišťování své národní bezpečnosti, ale nemají možnost autonomně si stanovit, co je obsahem tohoto pojmu v primárním evropském právu. Naplnění hypotézy takto formulovaných výjimek je tedy otázkou interpretace primárního evropského práva a nikoli autonomního rozhodnutí členského státu ohledně toho, co všechno označí za zájem národní bezpečnosti nebo třeba trestního práva – k tomu srov. Rozhodnutí SDEU C-439/19 Latvijas Republikas Saeima

[86] Viz rozhodnutí SDEU C-33/22 Österreichische Datenschutzbehörde proti WK.

[87] Viz tamtéž, odst. 41 a 42.

[88] Viz čl. 9 GDPR.

[89] Viz např. čl. 14(5)(a) nebo čl. 17(3)(d) GDPR.

[90] Srov. taxativní výčet titulů v čl. 6 GDPR, který vědecký výzkum neobsahuje.

[91] Viz čl. 2(6) Aktu.

[92] Viz čl. 2(8) Aktu.

[93] Srov. čl. 2(8), poslední věta, Aktu.

problematickým způsobem. Obsahuje totiž velmi podstatné výjimky (tj. opět výjimky z výjimky), v jejichž důsledku dopadají na různé druhy provozovatelů takových systémů AI nebo modelů zákazy podle Kapitoly II. a povinnosti podle Kapitoly III. a IV. Jedinou oblastí, na kterou tato výjimka obecně dopadá, jsou tedy základní modely. I v rámci jejich úpravy se ale vyskytuje speciální ustanovení, které poskytovatelům těchto modelů zakládá některé povinnosti (k tomu viz výše), to navíc za užití trochu jiné definiční terminologie[94].

Lze jen těžko odhadovat, do jaké míry se problematická legislativní technika a nejistý smysl obecných výjimek a výjimek z výjimek projeví v reálné praxi. Možností jejich funkčních selhání je celá řada – od jejich zneužití k obcházení ex ante regulace přes fingování výzkumu nebo licenčních podmínek veřejných licencí až po další reálný přesun výzkumu a vývoje do zemí mimo efektivní dosah práva EU a následný pouhý import příslušných produktů.

Možným nástrojem k omezení perverzní interpretační kreativity na straně jedné a prevenci úprku z EU vývojářů a různých typů provozovatelů na druhé straně má být relativně nový typ funkční výjimky z působnosti nařízení souhrnně označovaný jako pískoviště (sandbox). Jedná se o soustavu závazků pro poskytovatele systémů AI, která jim pod zvýšeným dohledem umožní vyvíjet a testovat jejich systémy v reálných podmínkách. Na tento typ výzkumu a vývoje se totiž teoreticky (viz výše problém s interpretací výlučnosti výzkumného účelu) nevztahují výše zmíněné výzkumné výjimky, a i jen experimentální nebo testovací nasazení příslušného systému AI v reálných podmínkách by znamenalo, především u systémů AI s vysokým rizikem, značné regulatorní a transakční výdaje – to navíc v době, kdy vůbec nemusí být jasné, zda má příslušná technologie kýžený tržní potenciál.

Pískoviště bude tedy poskytovat možnost uvést do testovacího provozu v reálných podmínkách systém, k němuž ještě kvůli tomu, že je stále ve vývoji, nejsou splněny všechny ex ante povinnosti, o kterých píšeme výše. Z toho plyne, že by pískoviště mělo být atraktivním nástrojem především pro poskytovatele systémů AI s vysokým rizikem. Namísto požadavku na kompletní analýzy rizik, systém kontroly kvality a další podmínky souladnosti bude možno příslušný systém nasadit v testovacím provozu na základě pískovišťového plánu schváleného příslušným úřadem členského státu, který bude pískoviště zavádět. Zajímavou pobídkou k účasti v pískovišti může být také možnost přístupu k datům, včetně osobních údajů, které se v pískovišti při testovacím provozu systémů AI shromáždí[95].

Nejde ale v tomto případě pouze o nahrazení závazků nebo dokumentace, ale také o způsob, kterým bude úřad příslušný systém AI, respektive jeho poskytovatele, sledovat. Namísto standardního režimu kontroly bude v případě pískovišť uplatňován aktivní dohled a dozor, což na straně poskytovatele vyžaduje daleko větší míru transparentnosti a aktivní komunikace směrem k úřadu. Na straně úřadu to bude vyžadovat rovněž proaktivní působení, včetně permanentní komunikace a poradenské činnosti.

Z právě uvedeného plyne, že pískoviště budou vyžadovat zcela jiný modus operandi na straně příslušných úřadů. Pro případ, že by členské státy neměly k zavedení tohoto zvláštnímu druhu nesrovnatelně náročnějšího způsobu dohledového, dozorového a konzultačního působení svých úřadů dostatek autonomní motivace, zakládá jim Akt přímo povinnost zřídit přinejmenším jedno regulatorní pískoviště[96].

Jednodušší alternativou k pískovišti je pro zájemce o testování systémů AI s vysokým rizikem v reálných podmínkách schválení testovacího plánu. Mohou o něj požádat poskytovatelé systémů AS s vysokým rizikem (resp. budou poskytovatelé) uvedených v příloze III. (tj. systémů nespadajících pod specificky regulované oblasti vypočtené v příloze I).

V porovnání s pískovišti stanoví Nařízení pro možnost testování na základě schváleného plánu řadu relativně rigorózních náležitostí[97]. Tvrdší vstupní podmínky pro tuto alternativu jsou pochopitelné především z toho důvodu, že testování probíhá sice pod kontrolou příslušného orgánu členského státu, ale nikoli pod jeho aktivním dohledem nebo dozorem[98]. Dohledu, na rozdíl od pískoviště, také nepodléhají zpracovaná data a ani se u těchto dat nepředpokládá jejich další užití pro účely vývoje nebo testování jiných systémů AI.

13.8 Ex post regulace AI - újma způsobená autonomním systémem a problém důkazu[99]

Prvním faktorem odlišujícím dokazování v případech, kdy se na skutkovém stavu podílí autonomní technologie, je shora diskutovaná (ne)vysvětlitelnost. Je důsledkem samotné funkční podstaty systému založeného na strojovém učení, který není naprogramován k tomu, aby něco dělal, ale k tomu, aby se to ze zdrojových dat naučil dělat. Výsledný operační kód je nepřehlednou změní nastavení jednotlivých virtuálních neuronů fungujících ve výsledku podobě jako lidská nervová soustava.

---

[94] Čl. 2(12) používá v hypotéze výrazu „s otevřeným zdrojovým kódem“ kumulativně k požadavku na bezplatnou licenci (free license), zatímco čl. 53(2), který poněkud zbytečně vyjímá poskytovatele těchto modelů z některých povinností stanovených tímto článkem (protože tyto modely jsou vyňaty z věcné působnosti Aktu) a některé povinnosti jim naopak zakládá, používá kumulativně k požadavku bezplatné licence už jen „otevřenost“ (pojem „open“ nikoli „open source“). Může ale jít jen o legislativně-technickou chybu – a tomu by ostatně nasvědčovalo, že v preambuli se opakovaně píše výhradně o otevřeném zdrojovém kódu.

[95] Srov. čl. 59(1) Aktu.

[96] Tato povinnost je zmírněna možností podílet se na pískovišti jiného státu – to ale pouze za předpokladu, že bude zajištěno adekvátní pokrytí národního regulatorního prostředí příslušného státu – srov. čl. 57(1), poslední věta, Aktu.

[97] Viz čl. 60(4) Aktu.

[98] Akt předpokládá dohled osob s „odpovídající kvalifikací“ – srov. čl. 60(4)(j) Aktu.

[99] Tato podkapitola vychází z článku POLČÁK, R. Umělá inteligence v justici. *Soudce*, 2024, č. 1, str. 4.

U autonomního systému jsme tedy sice schopni vnějším pozorováním měřit, jak funguje, ale nedokážeme určit, proč dělá to, co dělá[100].

Druhý faktor bezprostředně dopadající na dokazování a skutkovou argumentaci v situacích, kde nějakou roli ve skutkovém stavu hraje systém založený na strojovém učení, přímo vyplývá z problému vysvětlitelnosti a týká se autonomie takového systému[101]. Člověk mu sice dá původní zadání, ale jedinou možností pro člověka, jak kontrolovat jeho další vývoj, je pouze zprostředkovaně dávkováním zdrojových dat. Když pak z nějakého důvodu systém nedělá úplně to, co od něj jeho tvůrce nebo uživatel čeká, nelze jej nějak snadno přeprogramovat, neboť jeho operační kód bezprostředně řídící jeho činnost je pro člověka nejen nečitelný ale také, vcelku logicky, efektivně nezměnitelný.

Diskutabilní zde tedy není jen obligátní otázka zavinění, ale dokonce i samotného způsobení újmy, protože zpracování zdrojových dat má i přes absenci vysvětlitelnosti výsledného systému v podstatě kauzální charakter. To, že systém ve výše zmíněném příkladu chatbota Tay mechanicky produkoval obsah zasahující do cizích práv, totiž nemuselo být jen zaviněno aktivními uživateli, kteří jej v tom zlomyslně podporovali, ale mohlo to být bezprostředně (resp. kauzálně) způsobeno objektivní dostupností nenávistného obsahu, který sociální síť Twitter průběžně označovala (zřejmě rovněž v důsledku fungování nějakého autonomního automatu) jako vysoce populární a amplifikovala jeho dosah mezi různé cílové skupiny[102].

Podobně problematická argumentace jako v případě způsobení a zavinění újmy může se u autonomních systémů týkat i vady[103]. Obecně existuje velmi málo případů, kdy byla škoda nebo jiná újma prokázána ve vztahu k vadě spočívající v nějakém funkčním nedostatku počítačového programu[104]. Lze tedy předpokládat, že pokud se nepodařilo v minulosti prokazovat vady u transparentních a vysvětlitelných algoritmů vytvořených člověkem, tím spíše se to zřejmě nebude dařit u autonomních algoritmů, jejichž definiční vlastností je malá nebo žádná vysvětlitelnost. Je sice víceméně zřejmé, že automat, který produkuje nenávistné tweety, je asi nějak vadný – to ale neznamená, že konkrétní vada půjde identifikovat a prokázat v soudním řízení.

Shora naznačené problémy skutkové argumentace reflektuje i plánovaná evropská právní úprava odpovědnosti za újmu způsobenou autonomními systémy[105], která byla v době psaní tohoto článku stále předmětem složitého politického a odborného jednání. Základ návrhu evropské směrnice stojí na logickém předpokladu, že strana, na níž bude v civilním sporu ležet důkazní břemeno, bude ve velmi obtížné procesní situaci. Kromě stanovení důkazního břemene a důkazních presumpcí[106] zavádí směrnice ještě členským státům závazek upravit ediční povinnosti v soudních řízeních, díky kterým by měla být snadněji řešitelná i jinak extrémně obtížná důkazní situaci v případech, kdy bude vady muset prokazovat žalobce[107].

Otázkou k důkladné celoevropské diskusi je, zda má specifická úprava odpovědnosti napříč jednotným trhem opravdu jen instrumentalizovat důkazní břemeno a předpokládat, že koho toto břemeno v důsledku různých povětšinou formálních skutečností (typicky v důsledku certifikace příslušného systému nebo naopak její absence) zavalí, ten až na výjimky prohraje[108]. Takové řešení totiž sice bude relativně předvídatelné pro dodavatele nebo jejich pojišťovny, ale stranám ani soudům nedá velký manévrovací prostor pro skutkovou argumentaci, která bude vycházet ze specifik konkrétních případů. V situaci, kdy stále nejsme schopní pořádně předvídat, kde a jak se autonomní systémy uchytí, jevil by se vhodnějším přístup založený spíše na zákonné typizaci důkazu a konkretizaci kritérií pro spolehlivost důkazu zohledňujících shora naznačené typické charakteristiky autonomních systémů a umožňující postupný vývoj judikatury na podkladě zkušenosti z konkrétních případů.

Vzhledem k charakteru autonomních systémů běžně užívaných v každodenní praxi lze předpokládat, že se může běžným titulem pro různé nároky plynoucí z jejich činnosti stát diskriminace[109]. V takovém případě nebude nutno prokazovat způsobení újmy, zavinění ani vadu, ale důsledek zpracování dat, tj. že systém rozlišuje ve svých výstupech mezi subjekty bez toho, aby k takovému rozlišení měl legitimní důvod.

Tento typ sporné agendy je populární především ve státech, kde lze využít procesních nástrojů kolektivní ochrany práv, typicky class actions. Výjimkou nejsou případy, kdy vidina vysokých náhrad škody nebo zadostiučinění motivuje žalobce k tomu, aby do věci, resp. do zajištění a práce s důkazy, investovali horentní sumy, díky čemuž mohou být odhaleny a sankcionovány i komplexní případy systémové diskriminace v soukromém nebo veřejném sektoru.

V typických případech, kdy k diskriminaci dojde v důsledku fungování autonomního systému zpracovávajícího např. agendu půjček, pojistek apod., mohou být velikost skupiny zasažené příslušnou újmou, a tím i související nároky na náhrady

---

[100] Problém vysvětlitelnosti projevující se ve výsledku tak, že se autonomní systém jeví zvenčí jako zcela netransparentní ‚black box' popisují např. SHACKLEFORD, S. J., ASARE, I., DOCKERY, R., RAYMOND, A. H., SERGUEEVA, A. Should we trust black box to safeguard human rights?: comparative analysis of ai governance. *UCLA Journal of International Law and Foreign Affairs*, 2022, č. 26(1) str. 35.

[101] Podrobněji viz QUEZADA-TAVÁREZ, K., VOGIATZOGLOU, P., ROYER, S. Legal challenges in bringing AI evidence to the criminal courtroom. *New Journal of European Criminal Law*, 2022, č. 12(4), str. 531.

[102] Podrobněji k mechanismu fungování a amplifikačnímu efektu platforem viz POLČÁK, R. Zákaz cenzury jak zásah do svobody podnikání a svobody projevu internetových platforem. In ŠIMÍČEK, V. (ed.). *Právo svobodně podnikat*, Praha: Leges, 2023. str. 95.

[103] Řešení této otázky nemá primárně právní ale skutkový charakter. Inspirace tím pádem může být i v našem právu brána z jinak nikoli úplně kompatibilních právních systémů – viz např. GRIEMAN, K. Hard drive crash: an examination of liability for self-driving vehicles. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2018, č. 9(3), str. 294.

[104] Srov. ROWLAND, D. Liability for Defective Software. *Cambrian Law Review*, 1991, č. 22, str. 78.

[105] Viz návrh směrnice o přizpůsobení pravidel mimosmluvní občanskoprávní odpovědnosti umělé inteligenci (směrnice o odpovědnosti za umělou inteligenci), č. COM/2022/496.

[106] Nejdůležitější je domněnka příčinné souvislosti upravená v čl. 4 směrnice.

[107] Viz čl. 3 směrnice.

[108] Srov. tamtéž, odst. 3 preambule.

[109] Viz např. důkladně zdokumentovaný případ rasové předsudečnosti v prediktivním systému COMPASS používaném při rozhodování o podmínečném propuštění z výkonu trestu – viz MAYSON, S. G. Bias in, bias out. *Yale Law Journal*, 2019, č. 128(8), str. 2218.

nebo zadostiučinění, ještě násobně větší. Nelze sice předpokládat, že autonomní systém bude přímo naprogramován k tomu, aby diskriminoval nějakou část subjektů např. na základě rasy nebo pohlaví, a diskriminaci bude možno prokázat na základě revize práce programátora. Namísto toho je pravděpodobné, že se takový systém začne diskriminačně projevovat až na základě toho, jak zpracoval dřívější manuální rozhodovací agendu příslušné instituce.

Důkaz diskriminace takovým systémem se tedy může vztahovat nikoli jen na osoby, jejichž případy systém aktuálně vyřizuje, ale může posloužit i k prokázání toho, že k diskriminaci docházelo také v době, kdy bylo rozhodováno člověkem a z níž systém čerpal zdrojová data. Tam, kde se např. bankovní systémy učí z předchozí praxe rozhodování o úvěrech trvající roky nebo i celá desetiletí, tedy může nabýt skupina poškozených (class) obřích rozměrů.

Aby bylo možno tyto nároky vznášet, je třeba mít především k dispozici důkaz diskriminace příslušným systémem umožňující adekvátní skutkovou argumentaci. V evropském právu za tímto účelem existuje institut práva na informaci o logice fungování algoritmu použitého k rozhodnutí o právech subjektu údajů[110]. Člověk, o jehož právech reálně rozhoduje algoritmus, má díky tomuto právu možnost zjistit, jak algoritmus funguje – především proto, aby se mohl bránit právě v situaci, kdy takové fungování vykazuje znaky diskriminace[111]. Skutečnost, že toto právo má v Evropě víceméně virtuální charakter, je způsobena jednak nedostatkem motivace ke vznášení příslušných nároků daných absencí účinných procesních nástrojů pro kolektivní žaloby. Ve Spojených státech, kde by o motivaci k investicím do náročných sporů nebyla nouze, zase naopak chybí konkrétní informační právo zajišťující poškozenému přístup k logice příslušného algoritmu[112].

Nedostatek motivace ale není jediným problémem práva na informaci o logice algoritmů rozhodujících o subjektivních právech. Uplatnění tohoto práva brání i jeho formální neurčitost. Pokud by totiž měl někdo zájem požadovat například po bance informaci o logice algoritmu rozhodujícího o úvěrech a spor o tuto žádost by dospěl k soudu, nebylo by možno formulovat petit a následně ani enunciát prostě jen tak, že banka má povinnost vydat žalobci logiku algoritmu. Takto formulovaný nárok by totiž byl sám o sobě tak metaforický, že by soud nemohl mít konkrétní představu, co přiznává, a ani banka by z něj neměla jasno v tom, co má vlastně vydat. Bylo by to něco podobného, jako kdyby měl soud rozhodnout o tom, že se má žalovaný omluvit žalobci – už by ale v rozsudku neřekl, jak má taková omluva vypadat a kde se má uskutečnit.

Adekvátní rozhodně není názor, že právem na informaci o logice fungování algoritmu rozumí se automaticky právo na samotný algoritmus. Ten může totiž vedle majetkových práv autorských, která by mohla jeho vydání bránit sama o sobě, chránit i obchodní tajemství, a to typicky například u rozhodovacích algoritmů bank. Má-li rozhodovací algoritmus autonomní charakter, nebyla by navíc zájemci o kontrolu jeho nastavení nic platná ani jeho transparentní dostupnost, protože kód autonomního systému je kvůli své nevysvětlitelnosti pro člověka nepochopitelný.

Na druhou stranu se ale nelze spokojit ani s tím, že by požadavku zákona na informaci o logice fungování algoritmu bylo možno vyhovět jen nějakými obecnými řečmi o tom, že algoritmus rozhoduje na základě jakýchsi vstupních dat a ta prostě nějak zpracovává[113]. Informace totiž v tomto případě musí být dostatečně konkrétní na to, aby mohla splnit svůj účel, tj. aby mohl člověk, o jehož právech algoritmus rozhoduje, kvalifikovaně posoudit, zda takové rozhodování není diskriminační.

Dokud nebudeme disponovat obecně uznávanými metodami zajišťujícími vysvětlitelnost autonomních algoritmů, jeví se jako jediné řešení tohoto interpretačního a argumentačního problému reverzní inženýrství[114]. Tento postup spočívá v tom, že se algoritmu dodává velké množství vstupů a následně se podle výstupů snažíme zpětně zrestaurovat podobu původního algoritmu[115], tj. vytvořit nový algoritmus, který není kopií toho původního, ale vykazuje podobné parametry funkčnosti, a přitom je transparentní a vysvětlitelný. Pokud se to s nějakou mírou přesnosti podaří, lze díky tomu prokazovat diskriminační zpracování dat.

Z hlediska následné skutkové argumentace stran a hledání praktické jistoty soudem je ale potřeba v každém případě akceptovat nepřesnost, která takový postup bude vždy provázet. Strany ani soud nemohou očekávat exaktnost, na níž jsou v souvislosti s prokazováním za užití informačních technologií v jiných případech zvyklí, ale musí k autonomním systémům přistupovat podobně, jako když se snažíme prokázat, co se odehrává v mysli člověka.

Na míře toho, jak se nám s tímto relativně novým typem skutkové argumentace podaří naložit, nebude záviset nic menšího než ochrana práv člověka v dnes již velmi frekventovaných případech, kdy jsou tato práva předmětem automatizovaného rozhodování. Nebezpečí, že s nevyhnutně postupující a víceméně žádoucí virtualizací rozhodovacích procesů dojde i k evidentně nežádoucí virtualizaci těchto práv, přitom kvůli shora naznačeným obtížím při skutkové argumentaci není zanedbatelné. Neznamená to sice, že ochranné mechanismy subjektivních práv v takovém případě zcela přestaly existovat. Podobně, jako to už můžeme postupně sledovat v řadě oblastí běžného života informační společnosti[116], by se ale staly

---

[110] V české verzi GDPR je toto právo ve vztahu k algoritmu popsáno nikoli výrazem „logika fungování“ ale metaforičtějím „smysluplné informace týkající se použitého postupu“ – srov. čl. 13(2)(f) GDPR.

[111] K tomuto informačnímu právu viz komentář POLČÁK, R. Transparent information, communication and modalities for the exercise of the rights of the data subject. In KUNER, C., BYGRAVE, L., DOCKSEY, C. *The EU General Data Protection Regulation (A commentary*). Oxford: Oxford University Press, 2020, str. 398.

[112] Podrobněji viz POLČÁK, R. Procedural and Institutional Backing of Transparency in Algorithmic Processing of Rights. *Masaryk University Journal of Law and Technology*. Brno: Masarykova univerzita, 2019, č.13(2), str. 401.

[113] Srov. odst. 63 preambule obecného nařízení o ochraně osobních údajů.

[114] K tomuto informačnímu právu viz komentář POLČÁK, R. 12- Transparent information, communication and modalities for the exercise of the rights of the data subject. In KUNECR, C., BYGRAVE, L., DOCKSEY, C. *The EU General Data Protection Regulation (A commentary)*. Oxford: Oxford University Press, 2020, str. 402.

[115] K dovolenosti reverzního inženýrství viz rozhodnutí SDEU ve věci C-406/10 SAS Institute Inc. v. World Programming Ltd.

[116] Srov. Del DUCA, L. RULE, C., RIMPFEL, K. eBay's De Facto Low Value High Volume Resolution Process: Lessons and Best Practices for ODR Systems Designers. *Arbitration Law Review*, 2014, č. 6, str. 204.

předmětem privatizace.

13.9 Práva k datům jako faktor investiční náročnosti AI

Problematika specifického právního uchopení je v posledních dvou dekádách diskutována především ve vztahu k ochraně osobních údajů, dalšímu užití informací veřejného sektoru nebo různým regulatorním (či spíše deregulatorním) opatřením směřujícím k vytvoření z nepochopitelných důvodů stále neexistujícího jednotného digitálního trhu[117]. Pro autonomní technologie představují data zcela klíčovou oblast, neboť autonomní systém se díky datům orientuje ve svém operačním prostředí a průběžně se vyvíjí. S trochou nadsázky by se dalo říci, že autonomní systémy používají data jako potravu, kterou nezbytně potřebují ke své funkční existenci[118].

Ve využití unikátní evropské datové základny pro potřeby vývoje a nasazení autonomních technologií však v Evropě brání různé právní překážky. Data jsou totiž předmětem celé řady regulatorních režimů, u nichž se přes jejich čistě technickou povahu stále nedaří sjednotit právní úpravy v jednotlivých členských státech. Příkladem může být ochrana některých typů dat autorskými právy nebo právy sui generis k databázím. Přestože je autorskoprávní úprava v jednotlivých členských státech částečně harmonizována a v neharmonizovaných aspektech není politického, ekonomického, sociálního nebo kulturního důvodu ke vzájemným rozdílům, neexistuje doposud nic takového jako jednotný autorskoprávní titul nebo jednotná licenční smlouva[119]. Obdobná byla donedávna též situace v oblasti ochrany osobních údajů – i zde se totiž obecně harmonizované regulatorní režimy v různých členských státech natolik vzájemně lišily, že bylo prakticky pro každý členský stát nutno vytvářet jiný typ smluvní nebo vrchnostenské dokumentace.

Pro právnickou obec se shora popsaná situace naopak jeví jako výhodná, neboť zájemce o využití dat je nucen k vyšším investicím do právních služeb. Při existenci jednotného regulatorního režimu by postačila jedna sada dokumentů vytvořená profesionálním právním servisem kdekoli v Evropě, zatímco současná situace nutní podnikatele najmout si profesionála z každého dotčeného členského státu. Praxe však ukazuje, že ve skutečnosti zájemci o složitější formy užití evropských dat vyžadující profesionální právní ošetření, raději hledají možnosti, jak data vyvézt mimo Evropu a tam je následně zpracovat s daleko menšími obslužnými náklady a rovněž i s nesrovnatelně nižší mírou právního rizika[120]. Evropský profesionální servis v oblasti právní ochrany dat je tedy ve výsledku na stejné lodi jako průmysl autonomních technologií. Pro právníky je přitom situace o to horší, že se na rozdíl od dat nebo inženýrů nemohou jen tak přesunout za oceán.

Adekvátní řešení právních vztahů, jejichž sekundárními objekty jsou data, není ve vztahu k autonomním technologiím žádoucí jen proto, aby mohlo v Evropě existovat v porovnání s Asií nebo Amerikou konkurenční investiční prostředí. Jak bylo naznačeno shora, je adekvátní nastavení regulatorního rámce důležité i k tomu, aby Evropa podobně, jako se to děje v oblasti dalšího užití osobních údajů, nemusela kvůli vývozu dat de facto ustupovat ze svých standardů ochrany informačních práv člověka[121].

Ideálním a teoreticky bezproblémově odůvodnitelným, avšak vzhledem k současné situaci zcela nerealistickým, řešením by bylo vytvoření jednotné právní úpravy zahrnující různé nezávisle existující restriktivní regulatorní režimy informačních práv. Jednotná a vzájemně obsahově sladěná úprava osobních údajů, informačního soukromí, informací veřejného sektoru, majetkových práv autorských, práv sui generis, práv ke zdravotnické dokumentaci aj. by vedle odstranění funkčně nesmyslných omezení daných geografickými hranicemi přinesla i citelné snížení nákladů na právní compliance. Úspory na transakčních nákladech by logicky byly o to větší, čím složitější je současná právní úprava zpracování příslušných dat[122].

V podstatě pochopitelná absence politické vůle k titánskému legislativnímu řešení vnitroevropské a strukturální diverzity různých právních režimů ochrany dat každopádně nemusí být fatální překážkou rozvoje autonomního průmyslu. Pragmaticky vzato totiž různé právní složitosti nemají charakter absolutních omezení, ale pouze generují vysoké transakční náklady. V některých odvětvích jsou navíc tyto náklady relativně zanedbatelné, neboť tvoří jen zlomek celkové hodnoty investic do příslušných technologií. Typicky tak u různých prostředků pro autonomní mobilitu nebo u velkých diagnostických přístrojů, kde vývojové náklady šplhají do miliard EUR, nepředstavuje pro dotyčného investora překážku, musí-li vynaložit statisíce k zajištění celoevropské právní compliance ve vztahu k různým typům dat.

Problém transakční nákladnosti tedy řešíme primárně u autonomních technologií, které jsou z hlediska investic středně nebo méně náročné. Právě této oblasti však je třeba věnovat zvýšenou pozornost, neboť jde o segment, kde, stručně řečeno,

---

[117] Základní parametry jednotného digitálního trhu shrnuje dokument Jednotný evropský digitální trh: Odstraňme regulační překážky a využijme maximálně přínosu online technologií. Lucemburk: Úřad pro publikace Evropské unie, 2016. Dokument též vypočítává současné regulatorní bariéry společného trhu (přitom ve však nezmiňuje o tom, z jakého důvodu tyto bariéry, často rozporné s primárním právem Unie, stále existují).

[118] Srov. např. PROIA, A., SIMSHAW, D. HAUSER, C. Consumer Cloud Robotics and the Fair Information Practice Principles: Recognizing the Challenges and Opportunities Ahead, *2015 Minnesota Journal of Law, Science & Technology*, č. 16, str. 145.

[119] Viz např. podrobnou srovnávací studii EECHOUD, M., HUGENHOLTZ, P. B., GOMPEL, S., GUIBAULT, L. HELBERGER, N. Harmonizing European Copyright Law. *Kluwer Law International*, 2009.

[120] Přičitatelnost datové výměny mezi USA a Evropou jednotlivým dominantním službám informační společnosti jednoznačně ukazuje, že se zajímavá data z Evropy zpracovávají v USA. Srov. např. data o platformách v publikaci HAMILTON, D. S. *The Transatlantic Digital Economy* 2017. Washington, DC: Center for Transatlantic Relations, 2017, str. 44.

[121] Podrobněji viz POLČÁK, R. Getting European data protection off the ground, 2014, *International Data Privacy Law*, Oxford: Oxford University Press, 2014, č. 4(4), str. 282.

[122] Mezi nejvíce zatížené sektory v tomto směru patří například biomedicínský výzkum nebo výzkum autonomních technologií zvyšujících kvalitu života.

očekáváme nečekané. Předpokládáme totiž, že právě tento segment bude v krátké době generovat velké množství zcela nových technologií a služeb, z nichž se postupně vyvinou skutečné pilíře autonomní ekonomiky podobně, jako se to stalo v osmdesátých letech v případě spotřebitelského trhu ICT nebo na konci devadesátých let u datové ekonomiky.

Investice do zcela nových forem spotřebitelského nebo průmyslového využití autonomních technologií se budou s největší pravděpodobností vedle nižších investičních objemů vyznačovat i vyšší mírou rizikovosti. Lze tedy ze zkušenosti s jinými technologickými obory očekávat, že oblasti autonomního průmyslu, od nichž si slibujeme největší budoucí růst, přilákají v první fázi především angel nebo venture kapitál (případně budou předmětem veřejné podpory). Za této situace může vysoká nákladnost právního servisu ohledně dat skutečně znamenat pro Evropu fatální problém. Žádný investiční projekt totiž nebude schopen před investory tohoto typu obhájit vysoké náklady na právní compliance generované pouze potencialitou toho, že data potřebná k vývoji nebo fungování příslušné autonomní technologie mohou být předmětem právní úpravy kteréhokoli státu EU nebo EHP.

Jedno z možných řešení naznačuje poziční dokument britské vlády k problematice autonomní ekonomiky, když hovoří o datových trustech bez právní subjektivity[123]. Myšlenka datového trustu je postavena na premise shora popsané ekonomické poptávky po jednoduchém a funkčním právním řešení sběru a využití velkého množství dat chráněných různými právními instituty a pocházejících z různých jurisdikcí. Datový trust může v tomto směru představovat jednotnou a typizovatelnou formu, jejímž prostřednictvím může být takového cíle dosaženo i jinak než pokoutným vývozem dat z území EU, jejich utajeným zpracováváním nebo technickou ekvilibristikou vedoucí k předstírání, že například osobní údaje ve skutečnosti nejsou osobní údaje[124].

V českém právním prostředí by model datového trustu spadal pod soukromoprávní společnost bez právní subjektivity dříve označované jako sdružení[125]. Primárním objektem (účelem) komplexního právního vztahu vytvořeného na základě společnosti, by bylo využití dat příslušnou autonomní technologií. Sekundární objekt by představovala samotná data, přičemž jejich rozmanitost by se projevila pouze v počáteční složitosti smlouvy, na jejímž základě by příslušná společnost vznikla. Subjektem tohoto komplexního právního vztahu by byl samozřejmě na jedné straně ten, kdo by chtěl předmětná data využívat, tj. například technologická společnost vyvíjející nebo provozující určitou autonomní technologii. Současně by se ale společnosti mohl účastnit též investor, ať už by šlo o fond typu angel či venture, banku nebo třeba orgán veřejné moci poskytující finance formou zvýhodněné půjčky nebo veřejné podpory.

Společnosti by se účastnil též subjekt (nebo spíš subjekty) disponující právy k datům. Mohlo by dokonce jít o jednotlivce, kteří by v rámci smlouvy dávali společnosti možnost jejich data využívat, takže společnost by ve výsledku mohla mít třeba i tisíce nebo miliony členů. V jiných případech by se společnosti mohl účastnit subjekt, který by nositele práv pouze v nějaké formě zastoupil, tj. např. kolektivní správce, pokud by šlo o data chráněná majetkovými autorskými právy. Tam, kde právy k týmž datům disponuje více subjektů zaráz, by takové společnosti mohli být účastni všichni – u dat užívaných pro potřeby biomedicínské autonomní technologie by to tedy mohl být příkladně pacient i zdravotnické zařízení pořizující jeho zdravotnickou dokumentaci.

Lze samozřejmě namítnout, že by takové řešení vyžadovalo v praxi stejně složitou nebo možná ještě složitější strukturu právní compliance, jako kdyby investor uzavíral individuální transferové dohody s jednotlivými subjekty disponujícími právy k datům. Pokud by totiž do společnosti vstupovala data chráněná právem jiného členského státu, bylo by nutno ve vztahu k tomuto právnímu řádu řešit i příslušný transfer subjektivních práv.

První výhodou oproti standardní transferové kontraktaci a compliance by měla společnost v tom, že veškerý transfer práv (převod, licenci, souhlas aj.) by probíhal na základě jednoho právního jednání a měl by kontinuální povahu, tj. trval by současně se členstvím ve společnosti. Nebylo by tedy v případě pochybností o povaze práv nutno spekulovat o jednotlivých subjektivních informačních právech zvlášť, ale využitelnost dat by bylo možno posuzovat en bloc ve vztahu k účasti nebo neúčasti na společnosti.

Druhou výhodou řešení formou společnosti bez právní subjektivity by byla právní identita předmětných dat navenek. Data tvořící prostřednictvím různých subjektivních práv materiální substrát společnosti by tak mohla být de iure posuzována jako jeden kompaktní celek a společnost by s nimi mohla i disponovat navenek. Zatímco například transatlantická výměna dat v biomedicínském výzkumu představuje dnes z právního hlediska skutečný oříšek, mohla by v tomto směru společnost kontrahovat daleko jednodušeji. Datový útvar bez právní subjektivity by navíc byl dostatečně flexibilní i pro případ, že dojde ke změně právní úpravy (evropské nebo národní) nebo vyjde později najevo nepředpokládaná potřeba využití dat.

Smluvní konstrukce společnosti (jakkoli ve své podstatě sama o sobě složitá) by totiž přinesla stejný praktický efekt jako jednotná evropská úprava, tedy by de iure vyzdvihla data z různých regulatorních omezení daných právními řády členských států a umožnila s nimi nakládat bez ohledu na jejich původ nebo bydliště jejich původce jako s kompaktním celkem (to však bez toho, aby byla tato data, jak je dnes běžné, fyzicky nebo právně přesunuta pod jinou než evropskou jurisdikci). Společná právní identita dat by tedy ve výsledku ani při dosažení vysoké ekonomické a technické efektivity nevedla k omezení práv jednotlivých oprávněných osob (subjektů osobních údajů, vykonavatelů majetkových práv autorských apod.)

Třetí výhodou řešení založeného na kompaktním právním útvaru bez právní subjektivity by byla shora konstatovaná možnost jeho typizace. Zatímco totiž existuje nepředstavitelně mnoho způsobů, kterými lze data zužitkovat pro potřeby

---

[123] Viz studii HALL, W., PESENTI, J. *Growing the Artificial Intelligence Industry in the UK*. Londýn: Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy, 2017, str. 46.

[124] Jedním z nástrojů takové ekvilibristiky je například pseudonymizace osobních údajů – srov. např. WALDEN, I. Anonymising Personal Data, 2002, *International Journal of Law and Information Technologies*, č. 10(2), str. 224.

[125] Viz § 2716 a násl. občanského zákoníku.

autonomních technologií, je i přes složitost a diverzitu národních právních úprav jen konečné množství právem uznaných typů dat a s nimi souvisejících práv. Lze tedy formou smluvního vzoru vytvořit několik typových modelů datových společností a k nim přiřadit odpovídající transferová ujednání v souladu s právy jednotlivých členských států EU nebo EHP. Ve výsledku tedy samozřejmě půjde o desítky nebo stovky dokumentů lišících se v míře vzájemných odlišností jednotlivých právních řádů členských států – tentýž model ale bude opakovaně použitelný jako smluvní vzor pro nejrůznější případy, jejichž rozmanitost nedokážeme dnes ani předpovědět.

Z výše uvedeného plyne, že náklady na vytvoření typické datové společnosti budou vyšší, než jsou náklady na zajištění transferu a právní compliance u typického projektu pracujícího s daty z více evropských jurisdikcí. Zatímco je ale každé individuální compliance řešení jen velmi omezeně použitelné v jiných případech, hodí se model datového trustu k obecnému použití bez ohledu na to, jaká data, odkud nebo za jakým účelem budou zpracovávána.

3.10 Shrnutí

V této kapitole jsme se zabývali některými otázkami specifické regulace technologií založených na strojovém učení. Věnovali jsme se v tomto směru především genezi Aktu (nařízení) o umělé inteligenci, který by se měl stát základním pramenem ex ante regulace vývoje a nasazení těchto technologií, o jejichž disruptivním potenciálu jsme již měli možnost se přesvědčit v řadě oblastí společenského života, politiky nebo ekonomiky. Pozitivní je, že se různé regulatorní teze Aktu staly předmětem široké politické debaty a výsledný kompromis má díky tomu velmi solidní demokratickou legitimitu. Za problém jsme ale označili jednak některé vnitřní systematické rozpory v rámci Aktu a jednak skutečnost, že se k technologické regulaci zahnízdila i úprava otázek systematicky patřících do jiné části evropského práva – konkrétně ochrana osobních údajů.

Ex ante regulace ale není jediným způsobem, který bude právo zasahovat do vývoje a nasazení systémů AI v EU. Velmi důležitým faktorem technologického rozvoje, nebo naopak ochrany práv bránící takovému rozvoji, bude nastavení právních nástrojů umožňujících vymáhat nároky z vad nebo různých druhů porušení právních povinností. Z hlediska odpovědnostních titulů to vypadá, že budeme spoléhat, podobně jako u původní úpravy služeb informační společnosti, na civilní úpravu v jednotlivých členských státech. Evropská úroveň úpravy zde ale, na rozdíl od právě zmíněné úpravy ISP, nepředpokládá jednotné omezení odpovědnosti, ale kýženou právní jistotu a efektivitu ochrany práv plánuje ošetřit prostřednictvím určení důkazního břemene a založení skutkových domněnek a presumpcí.

Vedle ex ante regulace směřující k souladnosti a ex post regulace upravující odpovědnost jsou třetím významným regulatorním nástrojem práva k datům. Zdrojová data totiž mají pro systémy založené na strojovém učení z důvodů popsaných výše zásadní důležitost. Jejich dostupnost, právní i faktická, doslova definuje pole pro rozvoj systémů AI. Vedle samotné existence různých druhů vzájemně se překrývajících práv, od ochrany osobních údajů přes soukromí, autorské právo, práva sui generis až třeba po obchodní tajemství, je klíčovým faktorem právní dostupnosti dat v rámci EU také přetrvávající partikularita národních úprav. Poskytovatel systému AI pak musí řešit vedle mnohosti práv i mnohost regulatorních režimů, což celý proces vývoje a nasazení takového systému výrazně komplikuje. V těchto souvislostech jsme se v této kapitole zabývali především možností agregace práv do útvarů bez právní subjektivity (případně i se subjektivitou).

Literatura

BIBAL, A., LOGNOUL, M. de STREEL, A., FRENAY, B. Legal Requirements on Explainability in Machine Learning. *Artificial Intelligence and Law*, 2021, č. 29(2), str. 149.

BLOCKX, J., KROOK, J. The EU legal framework for algorithmic recommender systems: I (don't) know it when I see it. Law, *Innovation and Technology*, 2024 (online).

BORDELON, B. The fight over AI biosecurity risk takes a twist. *Politico.com*, 6. 2. 2024 (online).

BROWN, N. Bots behaving badly: products liability approach to chatbot-generated defamation. *Journal of Free Speech Law*, 2023, č. 3(2), str. 389.

DEBUSSERÉ, F. The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster? International *Journal of Law and Information Technology*, č. 13(1), str. 70.

Del DUCA, L. RULE, C., RIMPFEL, K. eBay's De Facto Low Value High Volume Resolution Process: Lessons and Best Practices for ODR Systems Designers. *Arbitration Law Review*, 2014, č. 6, str. 204.

DUNN, P., De GREGORIO, G. The Ambiguous Risk-Based Approach of the Artificial Intelligence Act: Links and Discrepancies with Other Union Strategies, CEUR Workshop Proceedings, Workshop on Imagining the AI Landscape after the AI Act, *IAIL 2022*, ceur-ws.com.

EECHOUD, M., HUGENHOLTZ, P. B., GOMPEL, S., GUIBAULT, L. HELBERGER, N. Harmonizing European Copyright Law. *Kluwer Law International*, 2009.

F. HEYMANN, F., PARGINOS, K., BESSA, R.J., GALUS, M. Operating AI systems in the electricity sector under European's AI Act – Insights on compliance costs, profitability frontiers and extraterritorial effects. *Energy Reports*, 2023, č. 10, str. 4538.

FLORIDI, L. On the Brussels-Washington Consensus About the Legal Definition of Artificial Intelligence. *Philosophy & Technology*, 2023, č. 36, str. 87.

GRIEMAN, K. Hard drive crash: an examination of liability for self-driving vehicles. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 2018, č. 9(3), str. 294.
HALL, W., PESENTI, J. *Growing the Artificial Intelligence Industry in the UK*. Londýn: Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy, 2017, str. 46.
HAMILTON, D. S. *The Transatlantic Digital Economy* 2017. Washington, DC: Center for Transatlantic Relations, 2017, str. 44.
MAYSON, S. G. Bias in, bias out. *Yale Law Journal*, 2019, č. 128(8), str. 2218.
MOREIRA, N. A., FREITAS, P. M., NOVAIS, P. The AI Act Meets General Purpose AI: The Good, The Bad and The Uncertain. In: MONIZ, N., VALE, Z., CASCALHO, J., SILVA, C., SEBASTIÃO, R. (eds) *Progress in Artificial Intelligence*. EPIA 2023, Lecture Notes in Computer Science, č. 14116, str. 157.
MURPHY, H. Facebook patents reveal how it intends to cash in on metaverse. *Financial Times* (ft.com), 18.1.2022 (online).
NEUWIRTH, R. Prohibited artificial intelligence practices in the proposed EU artificial intelligence act (AIA). *Computer Law & Security Review*, 2023, č. 48.
NOVELLI, C. CASOLARI, F. ROTOLO, A., TADDEO, M., FLORIDI, L. et al. Taking AI risks seriously: a new assessment model for the AI Act. *AI & Society*, 2023, online na springernature.com.
POLČÁK, R. 12- Transparent information, communication and modalities for the exercise of the rights of the data subject. In KUNECR, C., BYGRAVE, L., DOCKSEY, C. *The EU General Data Protection Regulation (A commentary)*. Oxford: Oxford University Press, 2020, str. 402.
POLČÁK, R. Getting European data protection off the ground, 2014, *International Data Privacy Law*, Oxford: Oxford University Press, 2014, č. 4(4), str. 282.
POLČÁK, R. Procedural and Institutional Backing of Transparency in Algorithmic Processing of Rights. *Masaryk University Journal of Law and Technology*. Brno: Masarykova univerzita, 2019, č.13(2), str. 401.
POLČÁK, R. Transparent information, communication and modalities for the exercise of the rights of the data subject. In KUNER, C., BYGRAVE, L., DOCKSEY, C. *The EU General Data Protection Regulation (A commentary*). Oxford: Oxford University Press, 2020, str. 398.
POLČÁK, R. Umělá inteligence v justici. *Soudce*, 2024, č. 1, str. 4.
POLČÁK, R. Zákaz cenzury jak zásah do svobody podnikání a svobody projevu internetových platforem. In ŠIMÍČEK, V. (ed.). *Právo svobodně podnikat*, Praha: Leges, 2023. str. 95.
PROIA, A., SIMSHAW, D. HAUSER, C. Consumer Cloud Robotics and the Fair Information Practice Principles: Recognizing the Challenges and Opportunities Ahead, *2015 Minnesota Journal of Law, Science & Technology*, č. 16, str. 145.
QUEZADA-TAVÁREZ, K., VOGIATZOGLOU, P., ROYER, S. Legal challenges in bringing AI evidence to the criminal courtroom. *New Journal of European Criminal Law*, 2022, č. 12(4), str. 531.
ROBERTS, H., HINE, E., FLORIDI, L. Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance. In: TIMOTEO, M., VERRI, B., NANNI, R. (eds) Quo Vadis, Sovereignty? *Philosophical Studies Series*, 2023, č. 154, str. 51.
ROWLAND, D. Liability for Defective Software*. Cambrian Law Review*, 1991, č. 22, str. 78.
SHACKLEFORD, S. J., ASARE, I., DOCKERY, R., RAYMOND, A. H., SERGUEEVA, A. Should we trust black box to safeguard human rights?: comparative analysis of ai governance. *UCLA Journal of International Law and Foreign Affairs*, 2022, č. 26(1) str. 35.
SCHERER, M. Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, 2016, č. 29(2), str. 354.
SVANTESSON, D. J. B. Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, *International Data Privacy Law*, č. 5(4), 2015, str. 226.
TRAUTMAN, L. J., VOSS, W. G., SHACKLEFORD, S. J. *How We Learned to Stop Worrying and Love AI: Analyzing the Rapid Evolution of Generative Pre-Trained Transformer (GPT) and its Impacts on Law*, ssrn.com, abstrakt číslo 4516154.
WALDEN, I. Anonymising Personal Data, 2002, *International Journal of Law and Information Technologies*, č. 10(2), str. 224.
WIEBE, A. Protection of industrial data – a new property right for the digital economy? *Journal of Intellectual Property Law & Practice*, 2017, č. 12(1), str. 62.
ŽOLNERČÍKOVÁ, V. Autonomous Vehicles Vigilance System: Proposal for a Theoretical Legal Framework. *The Lawyer Quarterly*, č. 11(1), 2021, str. 206.