Český rozhlas

Příloha č. 6 - Pravidla pro externí dodavatele Českého rozhlasu pro využívání umělé inteligence

Čl. 1 Předmět a důvod úpravy

1. Předmětem těchto pravidel pro využití umělé inteligence (dále jen jako „AI“) je stanovení povinností a zásad použití AI, které využití AI v ČRo má a které jsou externí dodavatelé povinni dodržet a brát v úvahu. Tato pravidla dále definují možná rizika, která použití AI představuje, a která musí brát externí dodavatelé v úvahu.

2. ČRo si je vědom toho, že AI umožňuje poskytovat veřejnosti více služeb a profesionálům ČRo pracovat efektivněji, ale rovněž si je vědom i toho, že AI představuje i nezanedbatelná rizika, která nelze s ohledem na specifické postavení ČRo jako média veřejné služby podceňovat.

3. V souladu se závazkem ČRo nabízet posluchačům služby v maximální možné kvalitě a s vědomím hodnot, na kterých je činnost ČRo postavena, považuje proto ČRo za nezbytné stanovit pravidla pro využití AI na činnosti externích dodavatelů, kteří se podílí na poskytování veřejné služby s ČRo.

4. Výklad těchto pravidel a samotné využití AI v praxi je nutno činit způsobem, který minimalizuje rizika používání AI a bude v souladu s hlavními zásadami jejího využití dle těchto pravidel.

5. AI dělíme na dvě skupiny:

   a) analytickou (označovaná též negenerativní) AI

   b) generativní AI.

6. Zapojení nástrojů analytické AI při dodržení všech dosud platných zásad práce v ČRo nepředstavuje pro činnost ČRo významné riziko. Kreativní potenciál algoritmů a povaha tréninkových dat generativní AI ale významná rizika přinášejí a jsou popsány dále. S ohledem na provázanost a souběžné využití obou typů AI v jednotlivých nástrojích se rizika a zásady pro využití AI vztahují na oba typy AI, především však na generativní AI.

Čl. 2 Výklad pojmů

1. **Umělou inteligencí (AI)** se rozumí počítačová technologie založená na struktuře tzv. umělých neuronových sítí, která analyzuje a klasifikuje existující data, vyhledává v nich objekty nebo vzory. Může sloužit pro automatizaci procesů a vytváření nových dat. Algoritmy umělé inteligence nejsou naprogramované do posledního detailu jako běžné počítačové programy, ale učí se z tréninkových dat (zpravidla se jedná o data z internetu).

2. **Analytická (negenerativní) AI** slouží k rozpoznávání skrytých vzorů, k analýze obrázků (například vyhledání obrázků, na kterých je kočka), rozpoznávání textů v obrázcích, k převodu textu do mluveného slova a naopak, k indexaci a doporučování souvisejícího obsahu podle definovaných algoritmů.

3. **Generativní AI** umožňuje vytvářet nový obsah (např. texty, obrázky, zvuk, hudbu, videa nebo počítačové kódy), a to na základě požadavků jednotlivých uživatelů. Tyto požadavky lidé zadávají umělé inteligenci většinou prostřednictvím tzv. textových promptů (příkazů či pokynů). Prompty by měly být formulovány co nejpřesněji, aby byly výsledky co nejlepší. Generativní AI funguje na

principu pravděpodobnosti, neboť se snaží předpovědět, jaký prvek (např. slovo) se bude s největší pravděpodobností vyskytovat v blízkosti předchozího prvku na základě analýzy tréninkových dat. Kromě generování textů, grafiky či hudby dokáže umělá inteligence také provádět analýzu generovaného obsahu nebo kombinovat kreativní práci s texty a obrázky apod. I když funguje na základě složitých umělých neuronových sítí a matematických algoritmů, přesto může vytvářet chybné nebo zkreslené výstupy (tzv. halucinovat).

Čl. 3 Hlavní zásady použití AI

1. Externí dodavatelé jsou povinni znát obchodní podmínky konkrétního užitého nástroje AI a tyto podmínky dodržovat.

2. Externí dodavatelé se zavazují v oblasti umělé inteligence postupovat v souladu s nařízením Evropského parlamentu a Rady (EU) 2024/1689 o umělé inteligenci (dále jen „nařízení o AI“) a dodržovat veškeré postupy a povinnosti, které jim nařízení o AI stanoví, ať už jsou v dodavatelském řetězci dle nařízení o AI v jakémkoli postavení. Externí dodavatelé jsou povinni správně klasifikovat dodávaný systém AI v souladu s nařízením o AI a poskytnout ČRo informace k zhodnocení této klasifikace. Externí dodavatelé jsou povinni poskytnout dokumentaci (vč. technické dokumentace a návodu k použití) a informace o fungování (vč. úlohy systému AI v rozhodovacím procesu) procesu trénování dodávaného systému AI a obsahu pro trénováni systému AI.

3. Žádná zodpovědnost nemůže být z principu přenesena na AI. Základní odpovědnost za využití nástroje AI nese externí dodavatel.

4. ČRo při využití AI dbá na dodržení následujících zásad:

   - **Transparentnost** – Tato zásada je důležitá pro budování důvěry mezi ČRo, posluchači a uživateli služeb ČRo. Externí dodavatel je povinen transparentně informovat ČRo vždy o tom, že konkrétní výstupy byly vytvořeny za pomoci nástrojů generativní AI, a to zejména pokud jsou použity k vytvoření obsahu, který je prezentován jako autorský. Externí dodavatel je povinen předem informovat ČRo vždy o tom, že k plnění bude použit nástroj generativní AI, o jaký konkrétní nástroj generativní AI se jedná a jakým přesně způsobem bude užíván. Externí dodavatel je povinen zajistit, aby syntetický obsah vytvořený jím dodaným AI systémem byl vždy označen ve strojově čitelném formátu a zjistitelný jako uměle vytvořený, případně uměle manipulovaný. U systémů AI přímo interagující s fyzickými osobami je povinen systémy AI upravit tak, aby dotčené fyzické osoby byly vždy vyrozuměny o tom, že komunikují se systémem AI.

   - **Osobní odpovědnost** – Pokud externí dodavatel použije při své práci nástroje AI, je za výsledky práce zodpovědný stejně jako v případě využití jiných technologických prostředků či bez jejich použití. Současně si externí dodavatel musí být vědom základních podmínek fungování AI a rizik spojených s použitím nástroje umělé inteligence alespoň v rozsahu těchto pravidel. Externí dodavatelé musí vždy ověřovat a provádět kontrolu kvality výstupu generovaných AI.

   - **Společenská odpovědnost při využití AI** – V ČRo platí i při používání nástrojů AI zásada vždy jednat v nejlepším zájmu veřejnosti. ČRo a prostřednictvím něj i jeho externí dodavatelé musí zkoumat, jak tyto nástroje využít pro posílení veřejné služby, zároveň má povinnost využívat AI tak, aby užití bylo ve shodě se základními etickými hodnotami a lidskými právy a byla minimalizována rizika, která s použitím AI souvisejí. I při použití AI nese konečnou odpovědnost za veškerý obsah a služby, které posluchačům a uživatelům poskytuje ČRo, který vyžaduje plnění těchto povinností od svých externích dodavatelů.

   - **Informovanost a sdílení zkušeností z využití AI –** Externí dodavatelé jsou povinni být dobře informováni o používání nástrojů AI před jejich užíváním, o obchodních podmínkách a rizicích, která konkrétní nástroj představuje a jsou povinni poučit o rizicích a zásadách v těchto pravidlech uvedených svoje zaměstnance a subdodavatele. Externí dodavatelé

jsou povinni zajistit, aby jejich zaměstnanci vyvíjející či užívající AI systém byli v oblasti využití AI řádně proškoleni. Dále jsou povinni transparentně a přesně informovat ČRo o fungování takových systémů a poskytnout veškerou potřebnou dokumentaci k dodávanému systému AI.

- **Úcta k lidské práci** – Vždy je třeba upřednostňovat talent a oceňovat autentické lidské vyprávění moderátorů, respondentů a tvůrců před výstupy AI. Žádná technologie nemůže plně nahradit lidskou kreativitu a lidskou práci. Externí dodavatelé jsou povinni při používání AI vždy brát ohled na práva tvůrců a držitelů práv. Pro tvorbu autorských děl v Českém rozhlase upřednostňujeme spolupráci s autory na úkor obsahu generovaného umělou inteligencí, ať již pro ad hoc příležitost nebo tvořeného systémově.

- **Bezpečnost** – Modely AI mohou pracovat s osobními údaji, proto je nutné dbát zejména na ochranu soukromí a dodržování příslušných zákonů, zejména nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně osobních údajů. Do nástrojů AI, které slouží k dalšímu trénování AI a mají do nich přístup třetí strany, se nesmí vkládat citlivá, tajná nebo obchodní data ČRo apod. Všechny informace, které se sdílejí v nástrojích AI, musí být považovány za veřejné. Tyto povinnosti musí dodržovat i externí dodavatelé. Osobní údaje, jichž je ČRo správcem a dodavatel je zpracovatelem či osobní údaje, ke kterým v rámci plnění dodavatel získá jinak přístup, nesmí dodavatel poskytnout k trénování umělé inteligence.

- **Obecný soulad s pravidly a hodnotami ČRo** – Externí dodavatelé jsou povinni využívat AI tak, aby užití bylo ve shodě se všemi pravidly uplatňovanými v ČRo a hodnotami a zásadami ČRo jako média veřejné služby, zejména Kodexem Českého rozhlasu a dalšími předpisy. Na obsah vytvořený AI se použijí stejná pravidla jako na veškerý jiný obsah vytvářený v ČRo.

- **Autenticita a důvěryhodnost** – Je nutné dbát na to, aby užití umělé inteligence nevedlo k podkopávání důvěryhodnosti Českého rozhlasu a autenticity jeho obsahu. Užití umělé inteligence může ušetřit finanční náklady spojené s výrobou obsahu, nadměrné či neuvážené užití umělé inteligence však může mít za následek snížení důvěryhodnosti v očích veřejnosti. Je nezbytné vždy dobře zvážit, zda benefity z užití umělé inteligence převažují nad riziky s tím spojenými, zda je takové užití vhodné a není v hrubém nepoměru k naplňováním veřejné služby. Tyto zásady platí i pro externí dodavatele.

Čl. 4 Hlavní rizika spojená s využitím generativní AI a související opatření

Výčet rizik, která souvisejí s využitím generativní AI, není vyčerpávající, neboť s ohledem na samotnou podstatu a rychlý vývoj generativní AI nelze všechna do detailu popsat a předvídat. Externí dodavatelé si musí být těchto rizik vědomi a zavazují se věnovat úsilí jejich minimalizaci a předcházení jim, i za pomocí transparentní komunikace, řádné informovanosti vůči veřejnosti a ČRo.

1. **Etická rizika**

Etická rizika související s využitím generativní AI zahrnují zejména:

a) Riziko zkreslení a zaujatosti z důvodu algoritmických předsudků modelů generativní AI.

b) Předsudky, které typicky vedou k diskriminaci určitých osob nebo skupin osob, se mohou v inteligentním modelu projevit buď z důvodu samotného designu tohoto modelu, který odráží určité chápání světa samotným vývojovým pracovníkem (přitom se může jednat o nevědomý předsudek), nebo z důvodu zakotvení a následné automatické identifikace předsudků z tréninkových dat jako vzorců chování do budoucna.

c) Častá netransparentnost ve využití tréninkových dat, která v kombinaci s jejich masovým používáním může vést k negativním důsledkům pro společnost. U inteligentních systémů nelze zaručit jejich nezávislost a nezaujatost, proto nelze jejich závěry např. považovat za spravedlivé. Modely mohou také produkovat nekvalitní nebo nepřesné výstupy.

2. **Rizika porušení práv duševního vlastnictví, neoprávněné využívání dat**

a) Rizika při využívání nástrojů generativní AI z pohledu práv duševního vlastnictví lze rozdělit do dvou hlavních kategorií:

- **Riziko porušení autorských práv:** Generativní AI lze použít k vytvoření obsahu, který je podobný stávajícím autorským dílům, rovněž obsah s kterým AI při vytváření výstupů pracuje, může být nejasný. To může vést k porušení autorských práv, a je potřeba proto vždy pečlivě individuálně posuzovat podmínky užití generativní AI i z hlediska vloženého obsahu a podmínky užití výstupů a autorství výstupů.

- **Riziko porušení jiných práv duševního vlastnictví:** Generativní AI lze také použít k vytvoření obsahu, který obsahuje prvky, které jsou chráněny jinými právy duševního vlastnictví, například ochrannými známkami, průmyslovými vzory nebo patenty. To může vést k porušení těchto práv, a je potřeba proto vždy pečlivě individuálně posuzovat podmínky užití generativní AI i z hlediska vloženého obsahu a podmínky užití výstupů.

b) Generativní AI je v současné době předmětem mnoha sporů v oblasti zneužití práv duševního vlastnictví, a to kvůli užití děl chráněných autorským právem bez řádného svolení autorů. Tato skutečnost může znamenat riziko budoucích soudních sporů z důvodů užití chráněných děl ve výstupech vytvořených těmito technologiemi.

c) Stávající autorské právo neposkytuje právní jistotu ohledně autorství k výstupům generativní AI. Autorem může být v souladu s naším právním řádem pouze fyzická osoba. Je třeba vzít na vědomí, že všechny výstupy generativní AI nejsou chráněny autorským právem. Vyvstává tedy otázka, kdy může být systém AI považován za pouhý nástroj k vytvoření díla a kdo je v takovém případě autorem dle svého jedinečného tvůrčího vkladu do výstupu generativní AI, nebo kdy na konkrétním výstupu generativní AI není dostatečný jedinečný tvůrčí vklad ani uživatele AI ani tvůrce AI a výstup generativní AI není autorským dílem. Toto je nutné vždy individuálně posoudit.

d) I vzhledem k dosud vyvíjející se právní úpravě užití generativní AI a jejich výstupů a právní nejistotě ohledně autorství výstupů generativní AI musí externí dodavatelé používat nástroje AI způsobem, který minimalizuje rizika v oblasti porušení autorských práv a jiných práv duševního vlastnictví.

e) Externí dodavatelé se zaručují, že při vývoji a trénování dodávaných AI systémů a modelů neporušili/nebyla porušena autorská práva, práva související s právem autorským, práva průmyslového vlastnictví či jiná práva duševního vlastnictví třetích osob.

3. **Rizika v oblasti ochrany osobních údajů**

a) Rizika v oblasti ochrany osobních údajů při využívání nástrojů generativní AI lze rozdělit do dvou hlavních kategorií:

- **Riziko úniku osobních údajů ze strany ČRo resp. ze strany externích dodavatelů:** Toto riziko úzce souvisí s rizikem v oblasti informační bezpečnosti a nastupuje v okamžiku, kdy prostřednictvím nástrojů AI sdílíme informace (zejm. prostřednictvím promptů) obsahující osobní údaje, které se tímto způsobem mohou dostat do nepovolaných rukou.

- **Riziko porušování pravidel ochrany osobních údajů ze strany poskytovatelů nástrojů AI:** Toto riziko souvisí s využíváním tréninkových dat, které obsahují osobní údaje, k čemuž příslušné fyzické osoby nemusely dát souhlas. Nástroje generativní AI byly a stále jsou předmětem šetření lokálních dozorových úřadů, neboť ohledně režimu zajištění dostatečné ochrany osobních údajů panují pochybnosti.

b) Vývoj a zejména testování a vylepšování algoritmu umělé inteligence vyžaduje, aby měl její vývojový pracovník k dispozici dostatečné množství testovacích dat. Pokud testovací data zahrnují osobní údaje, musí je vývojovým pracovníkem nejen shromáždit, ale zároveň i v

souladu s platnými právními předpisy odůvodnit jejich zpracování pro účely vývoje algoritmu umělé inteligence. Zároveň je nutné dostát všem dalším povinnostem v oblasti ochrany osobních údajů, což v současné době je pro některé společnosti vyvíjející nástroje umělé inteligence problém.

c) Externí dodavatelé musí používat, vyvíjet a trénovat nástroje AI způsobem, který respektuje soukromí třetích osob, platné právní předpisy a povinnosti Českého rozhlasu jako správce osobních údajů, který je zodpovědný za jejich ochranu. Osobní údaje, jichž je ČRo správcem a dodavatel je zpracovatelem, nesmí dodavatel poskytnout či užít k trénování umělé inteligence.

4. **Redakční rizika**

a) Hlavní redakční rizika v médiích veřejné služby při použití nástrojů AI lze rozdělit do následujících kategorií:

- **Riziko zkreslení a zaujatosti:** Generativní AI je trénována na datech, která mohou obsahovat předsudky a stereotypy. Pokud nejsou tato data pečlivě vybrána a vyčištěna, může to vést k tomu, že generované výstupy budou také obsahovat tyto předsudky. To může mít negativní dopad na důvěryhodnost a objektivitu média veřejné služby, pokud by výstup nebyl podroben řádné kontrole.

b) Umělá inteligence může výrazně urychlit a zefektivnit procesy probíhající při redakční činnosti. Uplatňuje se při přepisování, shrnutí delšího textu a klasifikaci obsahu. Je třeba si však neustále uvědomovat, že se jedná jen o pracovní nástroje, které používají lidé s určitou odborností a jsou za výstupy AI zodpovědní, jako by výstup vytvořili sami.

c) Největší riziko, které v redakční oblasti s využitím AI souvisí, spočívá v tom, že AI produkuje chybné či zavádějící informace, které je s ohledem na nedostatky v oblasti uvádění zdrojů obtížné odhalit. Zdroj informace také často není vůbec nikde uveden, protože se při procesu AI nedá přesně detekovat.

d) U chatbotů založených na AI existuje tendence k tzv. halucinacím, kdy výsledky, které jsou prezentovány jako pravdivé, jsou zcela vymyšlené nebo věcně nesprávné. To je způsobeno procesem učení generativní AI: modely rozumějí jazyku, ale nerozumějí tomu, co se v něm skrývá. Výstupy AI mohou také trpět nepřesnostmi a zaujatostmi: od kulturních a geografických slepých míst kvůli tréninkovým datovým souborům, které jsou většinou severoamerické, až po historické zkreslení, ale mohou trpět i politickou zaujatostí, demografickou zaujatostí, sexismem, rasismem apod. V případě interakce systému AI s fyzickými osobami musí být fyzické osoby vyrozuměni, že komunikují se systémem AI.

e) Užití nástrojů generativní AI v žurnalistice s sebou nese ještě další specifické etické otázky týkající se důvěryhodnosti zpravodajských příspěvků doprovázených ilustracemi vytvořenými pomocí AI a vlivu AI na kvalitu novinářských výstupů.

f) Externí dodavatelé musí používat nástroje AI způsobem, který minimalizuje rizika zaujatosti a zkreslení, nepřenáší na AI zodpovědnost za publikovaný obsah a nepodrývá důvěryhodnost ČRo. Dále jsou povinni vyvíjet systémy AI tak, aby v případě syntetického obsahu byly výstupy označeny ve strojově čitelném formátu a zjistitelné jako uměle vytvořené nebo uměle manipulované. V případě chatbotů, musí být dotčené fyzické osoby vyrozuměny o tom, že komunikují se systémem AI,

5. **Riziko informační a kybernetické bezpečnosti**

a) Hlavní rizika spojená s užíváním nástrojů AI z pohledu informační bezpečnosti lze rozdělit do následujících kategorií:

- **Riziko kybernetických útoků:** Nástroje AI mohou být cílem kybernetických útoků, které mohou vést k úniku dat, poškození systémů nebo dokonce k zastavení provozu.

- **Riziko bezpečnostní zranitelnosti:** Nástroje AI mohou obsahovat bezpečnostní díry, které mohou být zneužity k útokům.

b) Generativní AI využívá poskytnutá data uživatelů k tréninku a získávání nových zkušeností, což s sebou nese značná rizika v oblasti informační bezpečnosti. Interní informace, které např. chatbot využívá ke svému tréninku, mohou být zpřístupněny skrze dobře mířené prompty i dalším uživatelům.

c) Stejně jako každý jiný software, může i AI obsahovat bezpečnostní chyby, které mají potenciál být zneužity k úniku dat nebo neoprávněnému přístupu k záznamům konverzací, uživatelským informacím nebo jiným citlivým údajům, což může v konečném důsledku vést ke krádeži identity, zneužití dat či ohrožení soukromí.

d) Kybernetická rizika se mohou objevit i v případě, že bude generativní AI využita pro tvorbu zdrojového kódu k programům/aplikacím použitého v intranetu ČRo, eventuálně s přesahem do internetu (webové servery a služby). I v takovém případě nese za spolehlivost a bezpečnost kódu odpovědnost pracovník, resp. oddělení, které jej s použitím generativní AI vytvořilo, a to v souladu s principem odpovědnosti dle těchto pravidel.

e) Z pohledu kybernetické bezpečnosti jsou proto externí dodavatelé povinni zabezpečovat své účty na nástrojích AI pomocí unikátních silných hesel, dvoufaktorového ověřování a pravidelně je aktualizovat o bezpečnostní záplaty.

f) Externí dodavatelé se zaručují, že dodávaný AI systém splňuje náležitou úroveň přesnosti, spolehlivosti a kybernetické bezpečnosti s ohledem na účel jeho užití.

6. **Celospolečenská rizika**

a) Hlavní celospolečenská rizika spojená s užíváním nástrojů AI lze rozdělit do následujících kategorií:

- **Riziko ztráty pracovních míst:** AI může být použita k automatizaci úloh, které jsou v současné době vykonávány lidmi. To může vést k ztrátě pracovních míst a k sociální nestabilitě.

- **Riziko nerovnosti:** AI může být použita k posílení existujících nerovností, například mezi bohatými a chudými, nebo mezi lidmi s různým vzděláním nebo sociálním postavením.

- **Riziko ztráty kontroly:** AI může být použita k tomu, aby lidé byli řízeni nebo ovládáni bez jejich vědomí. To může vést k ztrátě svobody a demokracie.

- **Riziko závislosti na AI:** Generativní AI může být velmi užitečným nástrojem, ale může také vést k závislosti na něm. To může být problematické, protože AI může být chybná nebo může být použita k vytvoření obsahu, který je škodlivý nebo nebezpečný.

b) Nástroje AI se hodí k automatizaci konkrétních úkolů, rozhodnutí nebo pracovních postupů prováděných jednotlivými fyzickými osobami, což pravděpodobně v budoucnu ovlivní dostupnost a povahu pracovních míst a způsob, jakým je vnímána lidská práce v oblasti médií i mimo ně.

c) S ohledem na povahu generativní AI, která má potenciál významně zefektivnit lidskou práci, je nutné vnímat i další celospolečenská rizika, která s jejím využitím souvisejí. Generativní AI snižuje náklady pro generování obsahu a produkci zpráv, což umožňuje vstup nových poskytovatelů obsahu na trh. Tito noví konkurenti však mohou mít diametrálně odlišné cíle a úroveň vnímání etiky.

d) ČRo by měl používat umělou inteligenci způsobem, který je prospěšný společnosti a který pomáhá řešit celospolečenská rizika. Měl by poskytovat informace o rizicích spojených s nástroji AI, podporovat výzkum a vývoj bezpečných nástrojů a spolupracovat s dalšími

organizacemi, které se zabývají snížením celospolečenských rizik. Tyto principy jsou závazné i pro externí dodavatele ČRo.

7. **Rizika týkající se dětí – zvláštní ohled na děti**

a) Při generování obsahu určeného dětem jsme povinni brát ohled na to, že tyto skupiny obyvatel jsou zvláště zranitelné z důvodu jejich věku, čímž jsou více náchylné k manipulacím a dochází u nich snáze ke zkreslení skutečnosti a vyvolání zmatených představ.

b) Český rozhlas by měl používat umělou inteligenci způsobem, který je bezpečný a který chrání děti. Tyto principy jsou závazné i pro externí dodavatele ČRo.

Čl. 5 Zakázané postupy v oblasti AI

V souladu s nařízením o AI jsou v ČRo zakázané následující systémy umělé inteligence:

a) systémy AI, které používají podprahové techniky a manipulují s chováním osob;

b) systémy AI, které zneužívají zranitelnosti osob (věk, zdravotní stav, ekonomická situace) k manipulaci;

c) systémy AI sociálního bodování, hodnotící sociální chování osob, které vedou k nepřiměřenému zacházení nebo diskriminaci;

d) systémy predikující riziko spáchání trestného činu na základě osobnostních znaků bez objektivních důkazů;

e) systémy AI, které vytvářejí nebo rozšiřují databáze rozpoznávání obličeje prostřednictvím necíleného získávání zobrazení obličeje z internetu nebo kamerových záznamů;

f) systémy, které hodnotí emoce osob na pracovištích a ve školách, s výjimkou lékařských nebo bezpečnostních důvodů;

g) systémy biometrické kategorizace, které kategorizují osoby na základě citlivých biometrických údajů (např. rasa, náboženství, politické názory) za účelem predikce jejich chování;

h) systémy biometrické identifikace na dálku v reálném čase ve veřejně přístupných prostorech pro účely vymáhání práva, bez nezbytných záruk a podmínek.

Externí dodavatelé se zavazují tento zákaz dodržovat.