2. 4. 2020

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Umělá inteligence ve světle ochrany soukromí – 2. díl

Právní limity pro vývoj a používání umělé inteligence v oblasti marketingu: automatizované rozhodování a práva subjektů údajů

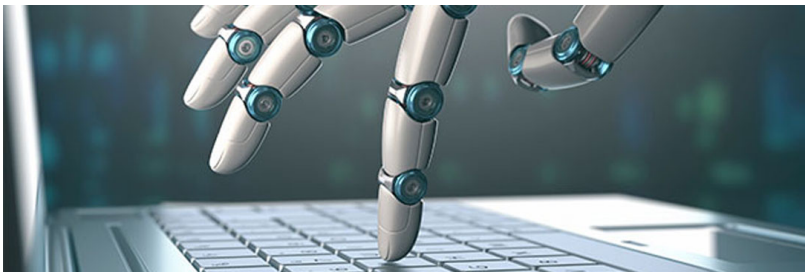
Jedním z nejdiskutovanějších témat v souvislosti s umělou inteligencí jsou dopady z hlediska ochrany soukromí a osobních údajů. V prvním díle [k dispozici >>> zde] jsme se věnovali zejména stádiu vývoje umělé inteligence a faktorům, které musí vývojář jakožto správce osobních údajů vyhodnotit předtím, než ke zpracování osobních údajů přistoupí. V tomto díle analyzujeme dopady nasazování softwaru založeného na algoritmech umělé inteligence v praxi a opatření, které by správci osobních údajů využívající umělou inteligenci měli přijmout, aby zajistili soulad s GDPR.

Za nejzásadnější témata při nasazení umělé inteligence v praxi považujeme (i) obhajitelnost plnění smlouvy a souhlasu pro přípustnost automatizovaného rozhodování, (ii) zajištění naplnění zásady transparentnosti, zejména pro případ uplatnění práva na přístup a ve vztahu k derivovaným údajům a (iii) zajištění efektivního výmazu dat po uplynutí retenčních dob.

PIERSTONE

Umělá inteligence a automatizované rozhodování

Ačkoli se o článku 22 GDPR často hovoří jako o první právní úpravě pro umělou inteligenci, v první řadě je třeba zdůraznit, že nelze klást rovnítko mezi automatizovaným rozhodováním dle článku 22 a umělou inteligencí obecně. Článek 22 GDPR upravuje právo[1] subjektu údajů nebýt předmětem výhradně automatizovaného rozhodování s právními nebo obdobně významnými účinky, nicméně ne každý proces využívající umělou inteligenci bude tyto znaky naplňovat, tj. bude se jednat o *výhradně* automatizované rozhodování, které bude spojeno s účinky podobně závažnými jako jsou účinky právní.



Kdy je zpracování výhradně automatizované?

Kritérium *výhradně* automatizovaného zpracování znamená, že k danému rozhodnutí musí dojít zcela bez lidského zásahu. O automatizované rozhodování se tak nebude jednat, pokud umělá inteligence provede selekci a předloží člověku alternativy nebo zdůvodnění, na základě kterých člověk rozhodnutí učiní. Na druhou stranu však nelze tvrdit, že jakákoli přítomnost či dohled člověka nad zpracováním dat umělou inteligencí postačí, aby dané zpracování osobních údajů bylo vyjmuto z působnosti článku 22.

Vzhledem k tomu, že je umělá inteligence schopná pojmout a posoudit najednou mnohem více faktorů, mnohem rychleji a ve větších souvislostech než člověk, v mnoha případech nebude člověk, který je pověřen dohledem nad zpracováním, schopen reálně proces rozhodnutí ověřit a jeho přítomnost v tomto procesu tak nebude představovat více než pouhé formální schvalování rozhodnutí umělé inteligence. Jestliže je zapojení člověka do procesu rozhodování takto redukováno, je třeba podpořit závěr, že k automatizovanému individuálnímu rozhodování skutečně dochází a článek 22 se uplatní.

Jaké účinky jsou srovnatelné s právními účinky?

Dalším faktorem, který ovlivní, zda se jedná o zpracování podléhající článku 22, jsou konkrétní důsledky zpracování umělou inteligencí. Článek 22 se uplatní na takové automatizované rozhodování, které má pro daný subjekt údajů právní účinky *„nebo se ho obdobným způsobem významně dotýká“*. Příklad takových obdobných účinků nalezneme v recitálu 71 GDPR: *„automatizované zamítnutí on-line žádosti o úvěr nebo postupy elektronického náboru bez jakéhokoli lidského zásahu“*. WP 29 ve svých Pokynech uvádí další příklady: *rozhodnutí ovlivňující finanční situaci určité osoby, její přístup ke zdravotním službám, pracovním příležitostem nebo vzdělávání*. Je otázkou, zda je za obdobně závažné důsledky možné považovat např. cílení reklamy podle chování či předpovídaného chování subjektu údajů nebo rozdílný výpočet ceny služby v závislosti na zpracování údajů prováděném umělou inteligencí.[2]

Na rozdíl od problematiky slučitelnosti účelů, kterou jsme se zabývali v prvním díle [k dispozici >>> zde], nebude úprava automatizovaného rozhodování zpravidla příliš relevantní pro samotné vývojáře umělé inteligence. Samotný vývoj algoritmu nebude mít zpravidla právní nebo obdobné účinky pro konkrétní subjekty údajů. Naopak správce údajů využívající umělou inteligenci pro účely přímého marketingu, zejména za účelem personalizace obchodních nabídek, se bude muset problematikou automatizovaného rozhodování zabývat. Správce údajů tak bude muset vyhodnotit, zda jím prováděné zpracování má pro subjekty údajů účinky podobné právním účinkům.

Jaká ochranná opatření je nutné zajistit při provádění automatizovaného rozhodování?

Pakliže se článek 22 uplatní a bude se jednat o automatizované rozhodování, je nutné, aby zpracování osobních údajů naplnilo některou z výjimek dle odst. 2, kterými jsou plnění smlouvy se subjektem údajů, souhlas subjektu údajů, nebo pokud je automatizované rozhodování povoleno dle práva Evropské unie či členských států. Bez ohledu na to, která z výjimek bude aplikována, je správce povinen přijmout vhodná opatření na ochranu práv a svobod subjektů údajů. GDPR uvádí v odst. 3 článku 22 výčet minimálních opatření, která je správce povinen zajistit: právo subjektu údajů na lidský zásah ze strany správce, právo na vyjádření názoru a právo výsledné rozhodnutí napadnout. Někteří autoři tato základní opatření označují za „algoritmický spravedlivý proces“.[3]

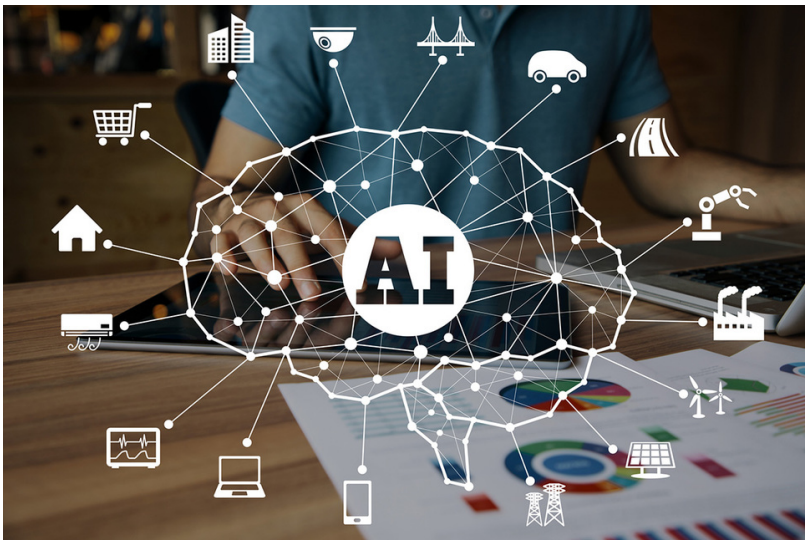
Nejvíce diskutované z těchto tří opatření je právo na lidský zásah. Dle stanoviska WP 29 by správce měl zajistit, že v případě, že o to subjekt údajů požádá, bude rozhodnutí podléhající článku 22 přezkoumáno odpovědnou osobou, která má pravomoc dané rozhodnutí změnit, přičemž při přezkumu musí vzít v potaz všechny relevantní údaje, včetně případných dodatečně poskytnutých údajů ze strany subjektu údajů. Nicméně rychlost, efektivita a kapacita učení umělé inteligence

v mnoha ohledech již v současné době předčí lidské vnímání. Pro efektivní lidský zásah je proto podmínkou transparentnost týkající se vstupujících údajů i principů algoritmu, aby vůbec bylo možné zajistit přezkoumatelnost rozhodnutí. Nejčastěji se v tomto kontextu uvažuje o zavedení paralelního „manuálního" procesu rozhodování, který by osoby přezkoumávající rozhodnutí umělé inteligence měly k dispozici pro ověření, zda umělá inteligence došla ke „správnému výsledku".

V souvislosti s aplikací článku 22 GDPR rovněž bude stále častěji diskutováno, zda a v jakém rozsahu budou skutečně naplněny atributy výše uvedených výjimek pro automatizované rozhodování, tj. plnění smlouvy a souhlasu subjektu údajů. Vzhledem k již existující diskuzi týkající se aplikace těchto titulů dle článku 6 odst. 1 GDPR, bude správce údajů nucen odůvodnit, zda a z jakých důvodů je automatizované zpracování opravdu nezbytné pro plnění smlouvy se subjektem údajů. Pokud bude automatizované rozhodování založeno na souhlasu subjektu údajů, správce bude muset zajistit, že jsou splněny všechny požadavky, které GDPR pro souhlas ukládá, což může být problematické zejména pro splnění informační povinnosti, jak je rozvedeno níže.

Transparentnost a práva subjektů údajů

Vedle principu minimalizace je transparentnost další ze základních pilířů, na kterých GDPR stojí. Tato zásada se projevuje zejména v právech subjektů údajů, zejména v právu obdržet srozumitelné informace dle článků 13, 14 a 15 GDPR. Článek 13 upravuje informační povinnost ve vztahu k vstupním údajům, které správce získá přímo od subjektu údajů, zatímco článek 14 se týká údajů, které správce neobdržel přímo od subjektu údajů, tj. zejména derivovaných osobních údajů. Článek 15 upravuje informace, na které má subjekt údajů právo, pokud vznese požadavek na přístup.



Rozsah povinně poskytovaných informací

Dle výše uvedených ustanovení mají subjekty údajů právo nejen na informace, zda jsou předmětem automatizovaného rozhodování, ale také na *„smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů"*. Je třeba zdůraznit, že se správci nemohou z této povinnosti vyvázat pouhým poskytnutím obecných informací o principech a mechanismech automatizovaného rozhodování či zjednodušených důvodech o výsledku automatizovaného rozhodování. Jestliže jsou informace poskytovány dle článku 15 GDPR, tj. na žádost konkrétního subjektu údajů, měly by se navíc vztahovat ke konkrétnímu subjektu a

konkrétnímu automatizovanému rozhodování, a předpokládají tedy větší míru detailu než informace poskytované před zahájením zpracování dle článku 13 a 14 GDPR.

Jak má správce vysvětlit logiku algoritmu?

Dle stanoviska WP 29[4] je správce povinen srozumitelným způsobem subjektu údajů vysvětlit logiku automatizovaného rozhodování. Někteří správci vyjádřili obavu, že GDPR na základě tohoto ustanovení vyžaduje, aby subjektům údajů byly zpřístupněny zdrojové kódy algoritmu, což by však zasahovalo do obchodního tajemství a autorských práv těchto správců. Nicméně, i kdyby správci zdrojové kódy k algoritmům subjektům údajů poskytli, nepředstavovalo by to pro většinu subjektů údajů relevantní a smysluplné informace. Vzhledem k tomu, že účelem této povinnosti správců je poskytnout subjektům dostatek informací, aby byli schopní uplatnit další ze svých práv, např. udělit souhlas, vyjádřit názor nebo podat námitku proti automatizovanému rozhodování, nebude zdrojový kód pro průměrného člověka příliš významný. Správci tak budou naopak povinni srozumitelně[5] subjektům údajů vysvětlit, jaká vstupní data jsou používána a z jakých zdrojů, jakým způsobem a na základě jakého modelu následně vznikají výstupní data.

Pokud bude automatizované rozhodování implementováno v rámci personalizované reklamy, dobrou praxí bude implementace tlačítka „proč jsem obdržel(a) tuto nabídku“. Prostřednictvím tohoto tlačítka by správce měl vysvětlit, na základě jakých informací týkajících se daného subjektu údajů byla vytvořena konkrétní nabídka, stanovena konkrétní nabídková cena apod., např. z jakých zdrojů byly osobní údaje získány, které kategorie údajů měly na vyhodnocení nabídky a ceny největší vliv atd.

Informační povinnost a data, která umělá inteligence nezávisle „vydedukuje“ ze vstupních údajů

V současné době není zcela jasné, zda jsou správci na základě požadavku subjektu údajů o přístup povinni zpřístupnit pouze vstupní data, nebo zda se toto právo vztahuje také na derivovaná data, která správce o subjektu údajů v průběhu trvání zpracování dovodil, aniž by mu je subjekt údajů sdělil. Jak bylo uvedeno výše, derivovaných dat může být velké množství a mohou se týkat nejrůznějších oblastí zájmu a chování subjektu údajů. Ačkoli to pro konkrétní subjekt údajů může mít značně odrazující psychologický efekt, měl by subjekt údajů získat přístup k veškerým svým osobním údajům, kterými jsou nepochybně i derivovaná data. To však může být v rozporu se zájmy správce, jehož obchodní činností tato data vznikla a jsou tak částečně také výsledkem této činnosti. WP 29 ve svém stanovisku[6] odkazuje na recitál 60 GDPR a dovozuje, že správce je povinen poskytnout subjektu údajů takové informace, které jsou nezbytné *„pro zajištění spravedlivého a transparentního zpracování“*. Lze se tedy domnívat, že správce postupující v souladu s tímto požadavkem bude povinen zpřístupnit subjektu údajů i veškerá derivovaná data.

Dopady výmazu některých vstupních údajů

V souvislosti s umělou inteligencí může být problematické také dodržování retenčních dob a práva na výmaz dle článku 17 GDPR. Jestliže uplyne stanovená doba uchování vstupních údajů nebo subjekt údajů požádá o výmaz svých údajů, je správce povinen dotčené osobní údaje z data setu odstranit, resp. odstranit identifikátory osobních údajů a zpracovávat data derivovaná umělou inteligencí v anonymizované podobě. Ačkoli uplynutí retenční doby či odvolání souhlasu nemá vliv na předcházející zpracování vstupních údajů, úplné odstranění identifikátorů derivovaných dat v rámci umělé inteligence nemusí být možné, resp. nelze zajistit, že umělá inteligence tyto identifikátory zcela „zapomene“.

Zvláště problematické to může být v případě zvláštních kategorií osobních údajů. Jako příklad uvádíme zpracování hlasových údajů prostřednictvím virtuálního asistenta Alexa vyvíjeného

společností Amazon. I když dojde k odstranění původních vstupních údajů, na základě kterých se Alexa naučila rozpoznávat hlasy, jazyky či dialekty, zůstávají poznatky a závěry Alexy nedotčeny a hlas dotčeného subjektu údajů může být pro Alexu nadále rozpoznatelný.

V teoretické rovině se nabízejí dvě potenciální možnosti zajištění celkové anonymizace derivovaných dat, které však v praxi budou zpravidla těžko proveditelné. V první řadě může správce umělou inteligenci „přecvičit" na základě upraveného data setu. To však znamená opakování celých řad zpracovatelských operací, což je ekonomicky velmi náročné, zejména s ohledem na neustálou aktualizaci vstupních data setů v závislosti na běhu retenčních lhůt. Druhou možností je upravení výsledného modelu, tedy odstranění vazeb mezi modelem a vstupními daty (tzv. „machine unlearning"), což však při aplikaci současných technologických postupů zatím ve velkém měřítku není možné. Vývoj postupů pro úpravu výsledných modelů je teprve na začátku a nelze očekávat, že o nich lze uvažovat jako o rychlém řešení pro dodržování retenčních dob.[7]

Vzhledem k výše uvedenému, i přes dodržování retenčních dob a důsledný výmaz osobních údajů ze vstupních data setů, existuje reziduální riziko, že v algoritmech umělé inteligence budou zůstávat stopy po vymazaných vstupních osobních údajích. Tato skutečnost je v současné době diskutována zejména v souvislosti s tzv. inverzními útoky, jejichž účelem je přinutit umělou inteligenci pod nátlakem „vypustit" údaje ze vstupních data setů. Z některých experimentů se zdá, že je možné tímto způsobem z umělé inteligence získat právě výše popsané identifikátory derivovaných dat a bude tak nutné přijmout opatření, aby se umělá inteligence nestala snadným terčem hackerů[8].

Právo na přenositelnost

V neposlední řadě je nutné zmínit, že údajů zpracovávaných umělou inteligencí se zpravidla bude dotýkat i právo na přenositelnost za předpokladu, že je zpracování založeno na plnění smlouvy nebo na souhlasu subjektu údajů. V této souvislosti je zásadní otázkou, zda bude správce v případě požadavku na přenositelnost povinen předat jinému správci také derivovaná data a tím pádem *de facto* potenciálně pomáhat konkurentovi. Dle článku 20 odst. 1 GDPR má subjekt údajů právo na přenositelnost ve vztahu k údajům, které *„poskytl správci"*. V souladu se stanoviskem WP 29[9] však derivovaná data zpravidla nebudou považována za osobní údaje, které subjekt *„poskytl správci"*, jelikož správce údajů tato data získal z jiného zdroje, než je subjekt údajů. Lze tedy podpořit závěr, že právo na přenositelnost se pravděpodobně nebude vztahovat na závěry, které umělá inteligence na základě předvolby zákazníka následně dovodila (např. o možném budoucím nákupním chování zákazníka e-shopu).

Cesta vpřed?

Umělá inteligence a další technologie se v současném světě vyvíjí natolik rychle, že téměř neexistují limity toho, co mohou dokázat. Stále častěji jsou tyto technologie schopny dokázat více, než si běžný subjekt údajů může představit. Měli bychom si proto klást otázku, co chceme, aby tyto technologie dokázaly. Je třeba určit základní směřování a stanovit mantinely, zejména z hlediska respektování základních lidských práv. GDPR v tomto smyslu přinesla mnoho užitečných konceptů, které vývoj umělé inteligence skutečně do jisté míry omezují nebo zpomalují, ale nikoli bezdůvodně. Cenou technologického pokroku a vývoje nemůže být ztráta soukromí a osobnostní sféry člověka. Nejdůležitějšími koncepty, jejichž výklad do budoucna vymezí hranici mezi právem na soukromí a svobodou podnikání, budou obhajitelnost titulů, na kterých je automatizované rozhodování založeno (tj. plnění smlouvy či souhlas subjektu údajů), zásada transparentnosti zajištění efektivního výmazu dat po uplynutí retenčních dob.

Pokud vás problematika umělé inteligence zajímá, sledujte novinky na www.pierstone.com a https://cz.linkedin.com/company/pierstone, kontaktujte nás na jana.pattynova@pierstone.com nebo

teodora.draskovic@pierstone.com nebo se připojte k činnosti Komise pro inovativní sektor v rámci Spolku pro ochranu osobních údajů.

M**gr. Jana Pattynová, LL.M.**

Mgr. Teodora Drašković

PIERSTONE s.r.o., advokátní kancelář

Perlová 371/5
110 00 Praha 1

Tel.: +420 224 234 958

---

[1] V souladu se stanoviskem WP 29 k automatizovanému individuálnímu rozhodování pro účely nařízení 2016/679 ze dne 3. 10. 2017 ve znění naposledy revidovaném a přijatém dne 6. 2. 2018, k dispozici >>> zde, představuje tento článek plošný zákaz takového výhradně automatizovaného rozhodování (nikoli jen právo podat námitku), s výjimkou případů, kdy jsou splněny podmínky stanovené v odst. 2.

[2] Kaminski, M. E., The Right to Explanation, Explained, 34 Berkeley Tech. L.J. 189 (2019)

[3] Kaminski, M. E., The Right to Explanation, Explained, 34 Berkeley Tech. L.J. 189 (2019)

[4] Pokyny WP 29 k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679 ze dne 3. 10. 2017 ve znění naposledy revidovaném a přijatém dne 6. 2. 2018, k dispozici >>> zde.

[5] WP 29 doporučuje např. grafická znázornění.

[6] Pokyny WP 29 k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679 ze dne 3. 10. 2017 ve znění naposledy revidovaném a přijatém dne 6. 2. 2018, k dispozici >>> zde.

[7] Veale M., Binns R., Edwards L, Algorithms that remember: model inversion attacks and data protection law, Royal Society (2018), k dispozici >>> zde.

[8] Veale M., Binns R., Edwards L, Algorithms that remember: model inversion attacks and data protection law, Royal Society (2018), k dispozici >>> zde. Fredrikson M, Jha S., Ristenpart T., Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasure, k dispozici >>> zde.

[9] Pokyny WP 29 k automatizovanému individuálnímu rozhodování a profilování pro účely nařízení 2016/679 ze dne 3. 10. 2017 ve znění naposledy revidovaném a přijatém dne 6. 2. 2018, k dispozici >>> zde.

Další články:

- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše
- Zneužití práva na přístup podle GDPR
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- Právní povaha sítě elektronických komunikací – režim náhrady škody
- Náhrada ušlého nájemného při předčasném ukončení nájemní smlouvy na nebytové prostory
- Jak fungují plánovací smlouvy v reálných situacích (2. díl)
- Nejvyšší soud a forma smlouvy o smlouvě budoucí: krok zpět v ochraně právní jistoty?
- „Za každou kauzou je živý příběh“
- Přehnaná, nebo důvodná prevence? Zajištění a utvrzení závazků v praxi
- Spoluvlastnictví a správa společné věci