PRO

OCHRANA OSOBNÍCH ÚDAJŮ V PRAXI

Číslo 3/2023, ročník III. Měsíčník SMS - služby s. r. o. www.dpopro.cz

Je třeba najít balanc mezi potřebami businessu a regulací, aby byly spokojené ideálně obě strany

Rozhovor

Finanční instituce zpracovávají osobní údaje mnoha klientů, a to ve velkém rozsahu. Tyto instituce mají často silné vazby do zahraničí, kam jsou údaje předávány. Jsou také svázány celou řadu dalších právních předpisů a regulací. Monika Kovář Staňková pracuje jako Senior Compliance Advisor v ČSOB skupině. Jak spolu souvisí tato její funkce s činností pověřence pro ochranu osobních údajů a jak najít balanc mezi potřebami businessu a regulací? I na to se jí ptáme v následujícím rozhovoru.

Vážení čtenáři,

s prvními jarními dny je tu i březnové číslo časopisu DPO PRO, měsíčníku pro pověřence pro ochranu osobních údajů. A nejen pro ně. Co se v něm dočtete?

Začínáme tradičně rozhovorem, tentokrát jsem si povídala s Monikou Kovář Staňkovou. Řeč bylo mimo jiné o vztahu mezi compliance a ochranou osobních údajů.

Ve zpravodaji nikdy nechybí aktuální informace o činnosti Spolku pro ochranu osobních údajů, který se zabýval předáváním dat mimo EU a aktuální judikaturou.

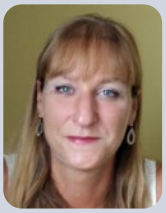
Nejvyšší správní soud předložil Soudnímu dvoru Evropské unie předběžné otázky týkající se legality policejní databáze DNA. Podrobněji se věnujeme úvahám Nejvyššího správního soudu, které vedly k tomuto kroku.

Evropská komise v dubnu 2021 publikovala návrh nařízení o umělé inteligenci. Tímto nařízením se ve svém článku zabývala Jana Andraščiková.

Nad vývojem autonomních systémů řízení s pomocí dat z palubních kamer a ochranou osobních údajů se zamýšlela Ludmila Probstová.

Ptáte se, zda je to vše? Kdepak. Časopis obsahuje mnohem více.

Tak tedy ničím nerušené čtení a mnoho inspirativních podnětů pro vaši práci přeje



Eva Janečková
šéfredaktorka

Pracujete jako Senior Compliance Advisor. Jak spolu souvisí tato funkce a ochrana osobních údajů?

V rámci ČSOB skupiny, kde pracuji již pět let, jsem začínala jako Compliance Advisor a dodávala zároveň služby zajištění ochrany osobních údajů do vícero dceřiných společností. V posledních letech došlo k vytvoření jednoho specializovaného týmu, který zajišťuje ochranu osobních údajů v rámci více entit ve skupině. Pro ty zajišťujeme jak funkci útvaru Compliance, tak i jednotného DPO. Některé menší entity ze skupiny však mají ponechanou funkci Compliance Officera zvlášť.

Takový Compliance Officer u nás má na starost vždy všechny compliance domény, jako je např. ochrana spotřebitele, AML apod., musí mít tedy širší znalost i dalších compliance domén. Pro naši dceřinou společnost Ušetřeno.cz jsem tak vykonávala funkci samostatného Compliance Officera i pověřence pro ochranu osobních údajů. Zároveň nemusí být pravidlem, že Compliance Officer rovná se DPO. Záleží na okolnostech i zkušenostech daného zaměstnance. Vždy však zachováváme společné týmové Data Protection porady, kde si sdílíme otázky k řešení ze všech entit ze skupiny a vzniká krásná společná týmová práce. Aktuálně jsem od ledna zpět na pozici Compliane Advisor Senior pro ČSOB, tedy mým úkolem je řešit otázky týkající se primárně ochrany osobních údajů v mateřské společnosti.

Banky často předávají osobní údaje do zahraničí. V rámci informací poskytnutých podle čl. 13 a 14 obecného nařízení (GDPR) jsou obvykle uvedeny velmi obecné informace o tom, že je vše v souladu s právními předpisy. Jak ve skutečnosti banky řeší tuto mnohdy problematickou činnost?

Souhlasím s vámi, co se týká informační povinnosti. Když jsem si prošla memoranda několika větších finančních institucí, napadlo

mě nejednou, že není řádně splněna informační povinnost vůči subjektům údajů. Záznamy o činnostech zpracování a z nich plynoucí stručné, ale jasné informační memorandum, kdy bude především subjektu údajů jakožto laikovi jasné, kde se jeho osobní údaje zpracovávají, považuji za správný přístup. Osobně nemám ráda složitě pojaté informace o zpracování osobních údajů. Těch, které by měly správný kaskádovitý přístup, v praxi tolik není. A v některých oblastech, jako je například předávání osobních údajů mimo EU, je u některých bank stručnosti až příliš, de facto není ani zřejmé, zda k předání mimo EU dochází. Takže najít zlatou střední cestu je klíčové. V rámci informačního memoranda skupiny ČSOB dáváme tuto informaci pod účel, kde je předání mimo EU, např.: *„Tyto údaje předáváme i do Švýcarska, a to na základě a v souladu s rozhodnutím Komise o odpovídající ochraně osobních údajů ve Švýcarsku, a dále do dalších zemí mimo EU (do UK a USA). Vždy však pečlivě posuzujeme, zda je vašim osobním údajům zajištěna srovnatelná úroveň ochrany jako v EU dle GDPR, případně využíváme další technická a organizační opatření pro její zajištění (např. šifrování).*" Správci osobních údajů obecně by si měli udělat především hlubší analýzu svých dodavatelů, zda dochází k předávání osobních údajů pouze v rámci EU. Např. datovým centrům může být poskytována podpora z míst mimo EU.

Jedním z práv, které obecné nařízení (GDPR) přiznává subjektům údajů, je právo být zapomenut. V praxi se ukázalo, že čím větší je správce, tím větší je problém toto právo realizovat, a to mimo jiné také kvůli různým opatřením v rámci zabezpečení osobních údajů nebo kybernetické bezpečnosti, jako je zálohování. Jak jste se vypořádali s tímto problémem?

Pečlivá implementace GDPR s sebou dokonce u nás přinesla i vznik samostatného útvaru, který jako prvoliniový útvar zajišťuje např. i výkon práv subjektů údajů. Až v interně definovaných případech se zapojuje compliance, tedy běžně s žádostmi o výkon práv do styku nepřijdeme. Jak jsme se konkrétně vypořádali s implementací, odpovědět nemohu, jedná se o interní informaci. Každopádně obecně se dá říct, že u většiny obchodních vztahů musíme provádět opatření podle zákona proti praní špinavých peněz. Ve smyslu tohoto zákona jsme povinni příslušné údaje, tedy zejména identifikační a transakční údaje, archivovat po dobu 10 let od ukončení obchodního vztahu, plus další právní předpisy. Obchodní vztah s bankou, jak všichni víme, trvá po dlouhou dobu, k tomu musíme přičíst zákonnou povinnost, tedy málokdy je v praxi zatím možné vyhovět právu na výmaz osobních údajů. Pokud by k tomu u konkrétního subjektu údajů mohlo dojít, pak samozřejmě dokážeme realizovat výkon práv a bez technických komplikací.

Když už jsme zmínili jedno právo, je nutné zmínit i další, které v praxi přináší značné potíže. Jedná se o právo na přístup k osobním údajům, kdy správce často není schopen dohledat, kde všude se osobní údaje nachází, některé osobní údaje zapomíná uvést do výčtu zpracovávaných údajů (typicky údaje týkající se samotné žádosti). Jak máte nastavené procesy pro realizaci takových žádostí?

Mohu pouze dodat, že už se jedná o zcela běžný proces, kdy prvoliniový útvar přijme žádost subjektu údajů, zpracuje ji a obratem odesílá. Společně jsme před lety definovali, jak k tomuto právu budeme přistupovat a jaký výčet osobních údajů budeme předávat. Primárně tedy je proces nastaven tak, že subjekt údajů

Monika Kovář Staňková

Monika Kovář Staňková pracovala v minulosti v PwC, kde v rámci konzultačního týmu pomáhala s implementací GDPR desítkám společností z různých oborů. Před pěti lety zahájila své působení v ČSOB skupině, kde je součástí Data Protecion týmu.

dostane základní informace, zda vůbec ČSOB jeho osobní údaje zpracovává, následně pak obdrží kategorie dotčených osobních údajů plus další informace dle článku 15 GDPR. Pokud by chtěl subjekt údajů např. konkrétní záznam jeho osoby z kamer, kopii listin apod., je potřeba, aby se s takovou žádostí obrátil na banku zvlášť.

Věnovala jste se ochraně osobních údajů zaměstnanců, včetně problematických aspektů týkajících se získávání zaměstnanců. Jak se díváte na běžnou praxi náborářů, kteří si bez souhlasu uchazeče prověřují údaje uvedené v životopisu, a na bývalé zaměstnavatele, kteří rovněž bez souhlasu poskytují o svých bývalých zaměstnancích informace?

Ano, toto je běžná praxe, setkala jsem se s tím poměrně nedávno u známého, kdy na toto došlo, a ještě se do stávající práce, kde neměli tušení, že by chtěl měnit práci, dotázali na reference a sdělili informaci, že u nich byl na pohovoru, což samozřejmě způsobilo akorát komplikace na obou stranách. Myslím si, že dokud to nebude sankcionováno, tak se praxe nijak nezmění. Když jsem pracovala v konzultační společnosti, setkala jsem se dále u klien-

Další obsah

tů s různými zajímavými databázemi na HR, kde si např. personalisté evidují osobní údaje ze sociálních sítí bez právního titulu apod., a to nemusí jít ještě ani o zaměstnance. Společnosti, které berou ochranu osobních údajů vážně, by se těmto praktikám měly obloukem vyhnout, přinejmenším z reputačního rizika.

Napsala jste článek o rozsudku Evropského soudu pro lidská práva, který se týkal kamerových systémů na pracovišti. Máte zkušenosti, jak se na tuto problematiku dívají čeští správci osobních údajů a zahraniční společnosti? Je rozdíl mezi praxí u nás a v jiných státech?

Zajímavé by bylo podívat se na tuto problematiku i z pohledu dozorových úřadů. V roce 2022 provedl Úřad kontrolu týkající se kamerového monitorovacího systému ve vnitřních a vnějších prostorách kliniky, kde ve vnitřních prostorách měly být kamery dle vyjádření kontrolované osoby podpůrným procesem pro detekci vzniku nežádoucích stavů pacientů a nedílnou součástí celkové léčby pacienta, ke všemu to správce opřel o právní titul zákonnou povinnost dle článku 6 GDPR a zdravotní stav zdůvodněn výjimkou dle čl. 9 odst. 2 písm. i) GDPR, kdy je zpracování nezbytné z důvodu veřejného zdraví. Toto nastavení rozhodně není správné. Dokážu si představit, že v zahraničí by úřad nezůstal u nápravného opatření. Např. v Rakousku tamní dozorový úřad udělil v roce 2018 krátce po účinnosti GDPR několik tisíc eur pokutu soukromému podnikateli, jelikož nepřiměřeně a bez splnění informační povinnosti snímal částečně veřejný prostor.

Myslím, že správci osobních údajů se naučili správně označit, že je prostor monitorován, ale zda je za tím dobře nastavený proces včetně definování účelu a právního titulu, nastavení přiměřené archivační doby, výmazu či přístupových oprávnění, to si netroufnu obecně posoudit, chtělo by to mít více informací z provedených kontrol v rámci ČR a těch bylo zatím podle mého názoru málo.

Trochu osobní otázka… Věnujete se ochraně osobních údajů již několik let, vidíte v této práci pořád smysl?

S ohledem na technický vývoj je to oblast prakticky neustále se rozvíjející a věřím, že nám všem, kdo se v ní pohybujeme, přináší stále zajímavé výzvy. Osobně mám poměrně silný smysl pro spravedlnost. Je však zapotřebí najít balanc mezi potřebami businessu a regulací, kde je mým cílem, aby byly spokojené ideálně obě strany.

Rozhovor vedla Eva Janečková

Spolek v březnu pokračoval v přednáškové činnosti, zabýval se aktuální judikaturou a stal se garantem studentské soutěže

I v březnu Spolek pro ochranu osobních údajů pokračoval ve vzdělávacích aktivitách a osvětové činnosti v oblasti zpracování a ochrany dat. Probíhala rovněž zasedání komisí Spolku a také přednášky na aktuální témata.

Přednášky a semináře

Pokračovala např. série přednášek od expertů z Národního úřadu pro informační a kybernetickou bezpečnost (NÚKIB). Vladěna Saskoá z oddělení regulace soukromého sektoru provedla účastníky základními body nové kyberbezpečnostní směrnice NIS2 a její transpozicí do českého práva. Návrhem transpoziční legislativy, nového zákona a řady vyhlášek, a formováním připomínek k nim se opakovaně zabývala i spolková Komise pro kybernetickou bezpečnost.

Další březnový seminář se týkal vztahu, souvislostí a odlišností ochrany osobních údajů a ochrany bankovního tajemství. S tématem seznámila zájemce Sylvie Milerová, která mj. na toto téma publikovala celou monografii.

Setkání s judikaturou…

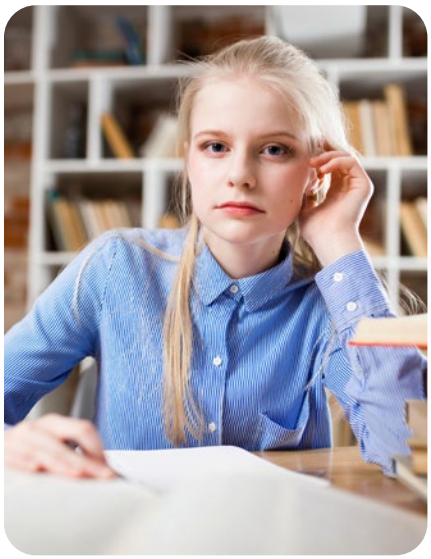
Na počátku měsíce také proběhlo další setkání s judikaturou, kde jsme se věnovali mj. rozsudkům SDEU ve věcech C-205/21, C-453/21 a C-349/21 a také německému rozsudku Zemského soudu Paderborn, sp. zn. 2 O 212/22.

Spolek garantem studentské soutěže

Spolek pro ochranu osobních údajů se stal garantem speciální ceny sekce ICT v rámci XVI. ročníku soutěže Studentské vědecké a odborné činnosti (SVOČ) na Právnické fakultě UK pro akademický rok 2022/2023. Cílem této snahy je probudit mezi studenty větší zájem o problematiku ochrany soukromí a odměnit nejlepšího z těch, kteří se rozhodnou svou studentskou vědeckou a odbornou činnost věnovat právě některému z témat, jež doporučí náš Spolek. Autor/ka nejlepší vědecké práce zaměřené na oblast ochrany soukromí získá díky podpoře Spolku jednorázové stipendium ve výši 10.000 Kč a také bezplatný vstup na tradiční konferenci Spolku, která se i letos uskuteční 5. října v Praze.

Data Privacy Monthly Resume

Pravidelný souhrn zajímavostí a novinek ze světa ochrany osobních údajů je zpět! U příležitosti mezinárodního Dne ochrany osobních údajů, který připadá na 28. leden, český spolek ve spolupráci s partnerským slovenským Spolkom pre ochranu osobných údajov obnovil pravidelnou publikaci Data Privacy Monthly Resume. Každý měsíc se můžete těšit na shrnutí důležitých rozhodnutí a doporučení evropských dozorových úřadů včetně Evropského sboru pro ochranu osobních údajů i příslušných soudů v otázkách týkajících se ochrany soukromí. Měsíční přehledy jsou k dispozici na profilu Spolku na sociální síti LinkedIn, později budou i na našich webových stránkách.



Pověřenec roku 2022

Na konci března Spolek uzavře nominace na pověřence pro ochranu osobních údajů roku 2022. Jedná se již o pátý ročník ocenění těch nejlepších pověřenců od správců a zpracovatelů osobních údajů, kteří působí v České republice. Slavnostní vyhlášení oceněných se bude konat dne 25. května v Praze. Více informací o ocenění i vyhlášení jako takovém je k dispozici na www.dporoku.cz.

Soudní dvůr EU bude posuzovat legalitu policejní databáze DNA

Česká policie vede už řadu let databázi DNA osob, ve většině případů odsouzených za úmyslné trestné činy, někdy i osob dalších. V rámci dlouhodobého sporu mezi Ministerstvem vnitra a Úřadem pro ochranu osobních údajů konstatoval Nejvyšší správní soud, že má pochybnosti o souladu některých aspektů vnitrostátní právní úpravy s právem Unie.

Nejvyšší správní soud proto předložil Soudnímu dvoru Evropské unie následující předběžné otázky:

1) Jakou míru rozlišování mezi jednotlivými subjekty osobních údajů vyžaduje čl. 4 odst. 1 písm. c) či čl. 6 ve spojení s čl. 10 Směrnice č. 2016/680? Je slučitelné s imperativem minimalizace zpracování osobních údajů, stejně jako povinnosti rozlišovat mezi různými kategoriemi subjektů údajů, aby vnitrostátní právní úprava umožňovala odběr genetických údajů s ohledem na všechny osoby podezřelé nebo obviněné ze spáchání úmyslného trestného činu?
2) Je v souladu s čl. 4 odst. 1 písm. e) Směrnice č. 2016/680, pokud je s odkazem na obecný účel předcházení, vyhledávání nebo odhalování trestné činnosti potřebnost pokračujícího uchovávání profilu DNA hodnocena orgány policie na základě jejich interních předpisů, což v praxi často znamená uchovávání citlivých osobních údajů na dobu neurčitou, aniž by byl stanoven jakýkoliv maximální časový limit pro uchovávání těchto osobních údajů? Pokud to v souladu není, s ohledem na jaká kritéria má být případně hodnocena časová přiměřenost uchovávání osobních údajů shromážděných a uchovávaných s tímto cílem?
3) V případě zvláště citlivých osobních údajů spadajících pod čl. 10 Směrnice č. 2016/680, jaký je minimální rozsah hmotně-právních či procesních podmínek získávání, uchovávání, a vymazání těchto údajů, který musí být v právu členského státu upraven „obecně závazným předpisem"? Může mít kvalitu „práva členského státu" ve smyslu článku 8 odst. 2 ve spojení s čl. 10 Směrnice 2016/680 také judikatura soudní?

Vymezení věci a dosavadní řízení

Útvar odhalování korupce a finanční kriminality (stěžovatel), který je útvarem Policie ČR, zahájil trestní stíhání žalobce za přečin porušení povinnosti při správě cizího majetku podle ust. § 220 odst. 1, odst. 2 písm. a), písm. b) zákona č. 40/2009 Sb., trestního zákoníku, kterého se měl žalobce dopustit ve formě spolupachatelství. Skutek měl spočívat v přidělení dotace, přestože žalobce věděl, že posuzovaná žádost nesplňuje náležitosti pro její poskytnutí. [1]

Dne 13. 1. 2016 stěžovatel žalobce v rámci trestního řízení vyslechl a nařídil provedení identifikačních úkonů. Stěžovatel i přes žalobcem vyslovený nesouhlas sejmul daktyloskopické otisky, provedl bukální stěr, z kterého vytvořil profil DNA, pořídil fotografie a popis žalobce, které následně zařadil do příslušných databází Policie ČR. [2]

Žalobou podanou dne 8. března 2016 se žalobce domáhal určení, že provedení identifikačních úkonů, uchovávání vzorků a informací při nich získaných a následné vložení záznamu o provedení těchto úkonů do informačního systému Policie ČR představuje nezákonný zásah ve smyslu § 82 s. ř. s. Městský soud v Praze (dále jen „městský soud"), v této věci místně a věcně příslušný soud, přerušil řízení, aby vyčkal posouzení ústavnosti § 65 zákona o Policii ČR ze strany Ústavního soudu ČR, kterému tuto otázku v jiné právní věci již předložil. Po rozhodnutí Ústavního soudu ze dne 22. března 2022, sp. zn. Pl. ÚS 7/18 (publikován pod č. 119/2022 Sb.), kterým tento soud návrh městského soudu zamítl, pokračoval městský soud v řízení v projednávané věci. [4]

Rozsudkem pak městský soud žalobě vyhověl. Výrokem určil, že zásah stěžovatele vůči žalobci, který spočíval v sejmutí daktyloskopických otisků, provedení bukálního stěru, pořízení fotografií a popisu žalobce, byl nezákonný. Městský soud dále určil, že uchovávání těchto osobních údajů žalobce v databázích Policie ČR, s výjimkou v mezidobí zničeného bukálního stěru žalobce, představuje rovněž nezákonný zásah. Městský soud proto nařídil stěžovateli ve lhůtě třiceti dnů od právní moci rozsudku smazat z databází Policie ČR všechny uchovávané osobní údaje žalobce. [5]

V odůvodnění svého rozhodnutí městský soud předně zdůraznil, že odběr genetického materiálu představuje výrazný zásah do práva na ochranu soukromí, chráněného čl. 8 Evropské úmluvy, stejně jako čl. 10 odst. 3 Listiny základních práv a svobod. Současné znění § 65 zákona o Policii ČR však nedává dostatečná legislativní vodítka pro posouzení přiměřenosti podobného zásahu. Bylo tedy na stěžovateli, aby sám posoudil zásah z hlediska legality, legitimity a proporcionality. Stěžovatel však trval na skutečnosti, že jediné kritérium pro odběr genetického materiálu v těchto případech uvádí § 65 zákona o Policii ČR, a sice naplnění subjektivní stránky trestného činu: tedy že se jedná o osobu obviněnou ze spáchání úmyslného trestného činu nebo osobu, které bylo sděleno podezření ze spáchání takového (tj. úmyslného) trestného činu. Toto kritérium bylo v projednávané věci naplněno: žalobce byl obviněn ze spáchání úmyslného trestného činu. Nic dalšího stěžovateli dle jeho názoru hodnotit nepříslušelo. [6]

Městský soud byl proto nucen posoudit přiměřenost zásahu do práva žalobce sám. Odmítl přitom argument žalobce, že identifikace pomocí biologických vzorků bude smysluplná především u pachatelů násilné trestné činnosti. Akceptoval, že pořizování biologických vzorků může být za určitých okolností vhodné i u trestných činů hospodářských (tzv. trestná činnost „bílých límečků"). S ohledem na skutkové okolnosti projednávané věci však konstatoval, že stěžovatel nedoložil, jaký účel měl být provedením a uchováváním identifikačních úkonů v případě žalobce dosažen. Městský soud zdůraznil, že v okamžiku odběru byl žalobce pouze obviněn z přečinu, tedy trestného činu typově méně závažného; menší společenskou závažnost vytýkaného skutku rovněž potvrdil trestní soud, který výkon trestu odnětí svobody podmíněně odložil; jednalo se o osobu do té doby netrestanou, u které není vysoká pravděpodobnost recidivy; rovněž nebylo jasné, zda trestné činy žalobce patří mezi trestné činy, u kterých pachatelé následně páchají takovou trestnou činnost, k jejímuž odhalení mohou napomo-

ci v databázi uchovávané osobní údaje. Dle městského soudu tak bylo provedení identifikačních údajů v případě žalobce nepřiměřené. Jednalo se proto o nezákonný zásah. [7]

Městský soud se dále rovněž zabýval zákonností dalšího uchovávání osobních údajů žalobce. Zákonnou úpravu § 65 odst. 5 zákona o Policii ČR shledal v tomto ohledu zcela nedostatečnou a v rozporu s čl. 8 Evropské úmluvy a čl. 10 odst. 3 Listiny základních práv a svobod. S odkazem na relevantní judikaturu ESLP zdůraznil, že situace, kdy si má Policie ČR podle § 65 odst. 5 sama vnitřně posoudit, kdy další uchovávání osobních údajů „není nezbytné pro účely předcházení, vyhledávání nebo odhalování trestné činnosti", ve skutečnosti znamená ničím neomezenou úvahu policie a tendenci k nadužívání časově neomezeného uchovávání osobních údajů. Odkazy stěžovatele na obecný rámec a instituty zákona č. 110/2019 Sb., o zpracování osobních údajů, a tam obsažené procesní postupy jsou liché v situaci, kdy neexistuje hmotněprávní zákonná úprava a ani žádná kritéria, podle kterých by vlastně měla Policie ČR o vymazání rozhodnout. Tyto nedostatky nemohou zhojit odkazy na vnitřní předpisy policie, které dané otázky údajně upravují, neboť se jedná o veřejnosti nepřístupné vnitřní akty policie, které nejsou právním předpisem. [8]

Kasační stížnost

Stěžovatel předně zdůraznil, že účel zpracovávání osobních údajů podle § 65 zákona o Policii ČR je jasně vyjádřen v samotné zákonné úpravě: je jím (veřejný zájem na) předcházení, vyhledávání nebo odhalování trestné činnosti. Žalobce byl v době odběru obviněn ze závažné úmyslné trestné činnosti hospodářského charakteru. Identifikačním úkonem získané osobní údaje jsou klíčové při odhalování potenciální budoucí trestné činnosti, kterou nelze zúžit na stejnorodou recidivu. Stěžovatel rovněž zdůraznil, že přiměřenost odběru a uchovávání osobních údajů žalobce hodnotil. Bral přitom v potaz faktor recidivy, stejně jako možnou eskalaci jednání, a konečně i skutečnost, že žalobce v minulosti v několika případech spáchal přestupky, tedy se opakovaně dopouští protiprávního jednání. [9]

S ohledem na právě vymezený skutkový rámec projednávané věci ve spojení s čl. 2 odst. 2 písm. d) Nařízení Evropského parlamentu a Rady ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR") má NSS za to, že na projednávanou věc je aplikovatelná Směrnice Evropského parlamentu a Rady 2016/680 ze dne 27. dubna 2016 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 (dále jen „Směrnice č. 2016/680"). [12]

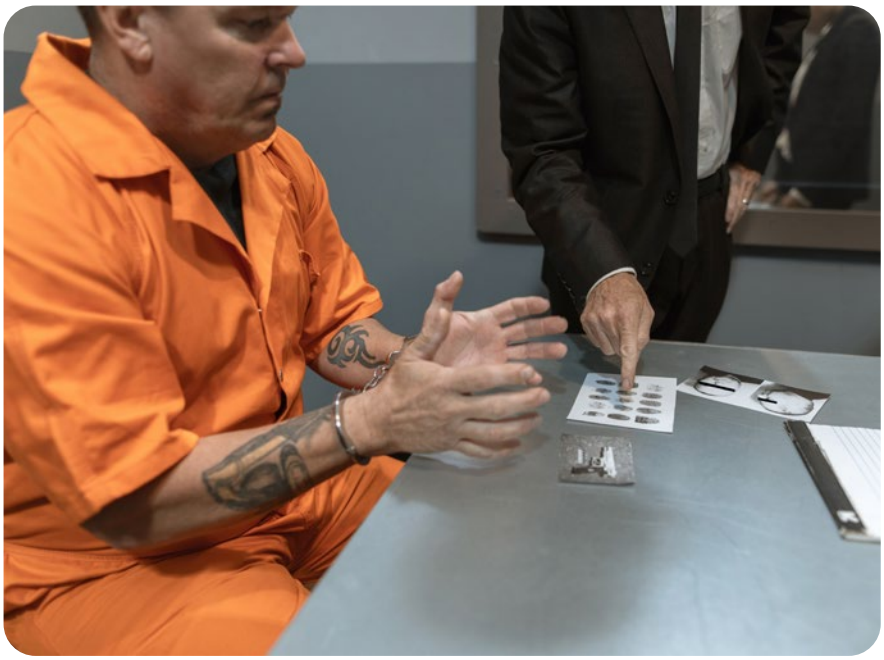
Úvahy Nejvyššího správního soudu

Dne 16. 1. 2018 se Městský soud v Praze obrátil na Ústavní soud s návrhem na zrušení části § 65 zákona o Policii ČR pro jeho protiústavnost. Ústavní soud rozhodl již citovaným nálezem ze dne 22. března 2022, sp. zn. Pl. ÚS 7/18 (publikován pod č. 119/2022 Sb.). Část návrhu městského soudu odmítl pro nepřípustnost, zbytek pak zamítl pro nedůvodnost. Pro předkládané předběžné otázky je podstatné, že Ústavní soud se ve svém přezkumu souladu vnitrostátního práva s českým ústavním pořádkem výkladem Směrnice č. 2016/680 nezabýval. [24]

Nejvyšší správní soud nicméně považuje výklad této směrnice pro rozhodování v projednávané věci za klíčové, neboť otázka přiměřenosti získávání osobních údajů pro účely budoucí identifikace v konkrétních případech je nezřídka předmětem řízení před správními soudy. Děje se tak v situacích, kdy osoba, předvolána policejními orgány k provedení odběru vzorků, se proti tomuto předvolání brání soudně (ochrana ex ante), anebo po provedeném odběru žádá o výmaz již získaného profilu DNA z databází Policie ČR (ochrana ex post, směřující pak nicméně nejenom proti nezákonnosti samotného odběru, ale rovněž proti uchovávání vzorků a DNA profilu), jako je tomu i v projednávané věci. [25]

Novější judikatura NSS v těchto případech zdůrazňuje, že pouhé naplnění formálních znaků § 65 odst. 1 zákona o Policii ČR (že se jedná o úmyslný trestný čin a osoba je podezřelá či obviněná) je nedostatečné pro zákonnost získání či uchovávání osobních údajů v těchto situacích. Orgány policie musí tuto úvahu doplnit testem přiměřenosti odběru v každém konkrétním případě, přičemž mají zohlednit především dosavadní trestnou činnosti dané osoby, či její absenci; typovou individuální závažnost trestné činnosti, pro kterou byla daná osoba předvolána k provedení identifikačních úkonů; osobu a osobnost pachatele; v případě ex post žádosti o výmaz pak dobu, která od spáchání trestného činu uběhla, stejně jako další chování pachatele. [26]

Aplikace těchto kritérií v novější rozhodovací praxi správních soudů vede k situacím, kdy je žalobcům vyhověno buď již jednoduše proto, že při vyhotovení standardizovaných formulářů o předvolání a provedení identifikačního úkonu posuzování přiměřenosti ze strany policejních orgánů naprosto absentuje, případně proto, že v rámci typicky hospodářských či jiných nenásilných trestných činů spáchaných do té doby netrestanými osobami bude obtížné dovodit přiměřenost odběru na základě výše uvedených kritérií. [27]



Společným znakem celé situace nicméně zůstává, za prvé, že kritéria, podle kterých je o neprovedení identifikačních úkonů rozhodováno, či nařízen výmaz již získaných osobních údajů, existují v podobě demonstrativního výčtu pouze v judikatuře soudní. Nemají však jakýkoliv zákonný předobraz. Za druhé, o (ne) přiměřenosti daného odběru bude na základě řady těchto kritérií rozhodováno v praxi pouze se značným zpožděním až správními soudy. Není běžné, aby byl policejní orgán provádějící identifikační úkon typicky v rané fázi vyšetřování sto vyžadovaný typ a rozsah posouzení provést, neboť nemusí mít ani dané informace k dispozici. [28]

Rozbor předkládaných předběžných otázek

V rámci předestřené skutkové a právní situace má Nejvyšší správní soud pochybnosti o souladu některých aspektů vnitrostátní právní úpravy s právem Unie. Před osvětlením pozadí jednotlivých předběžných otázek považuje NSS za vhodné zmínit dva obecné body, které jsou společné všem třem předkládaným otázkám. [29]

Za prvé, Směrnice č. 2016/680 je relativně nový právní instrument Unie, ke kterému doposud relevantní judikatura Soudního dvora chybí. Již existující judikatura k GDPR, či jeho předchůdkyni v podobě Směrnice č. 95/46, jistě poskytuje užitečná výkladová východiska pro řadu zde nastolených otázek. Není však jasné, nakolik je úprava Obecného nařízení o ochraně osobních údajů skutečně bez dalšího analogicky přenositelná do specifického aplikačního rámce Směrnice č. 2016/680. Ostatně, kdyby měly být oba režimy bez dalšího totožné, pak není zřejmé, proč by unijní zákonodárce považoval za nezbytné přijmout komplexní, specifickou úpravu v podobě Směrnice č. 2016/680 coby lex specialis vůči GDPR. Lze tedy vycházet z toho, že ochrana fyzických osob v souvislosti se zpracováním osobních údajů za účelem prevence, vyšetřování či stíhání trestních činů má být v něčem odlišná od obecného režimu ochrany osobních údajů. Společným jmenovatelem všech tří předkládaných otázek je snaha o zjištění, v čem přesně má daná odlišnost spočívat. [30]

Za druhé, předkládaná věc se nalézá v kontextu rozsáhlého shromažďování obzvláště citlivého typu osobních údajů: genetického materiálu a z něj získaného DNA profilu osob. [31]

Na pozadí těchto společných východisek právní a skutkový rámec projednávané věci vznáší následující tři předběžné otázky, s ohledem na které Nejvyšší správní soud žádá Soudní dvůr o výklad relevantních ustanovení Směrnice č. 2016/68: za prvé, zda zásada minimalizace zpracování osobních údajů vyžaduje diferenciaci s ohledem na společenskou závažnost trestného činu (minimalizace věcná); za druhé, jaký dopad má ta samá zásada v rovině časové co do uchování osobních údajů (minimalizace temporální); konečně za třetí, na jaké úrovni a v jaké kvalitě práva musí být stanoveny minimální náležitosti zpracování a uchovávání citlivých osobních údajů typu profil DNA.

K otázce č. 1: zač lze odebrat? [32]

Judikatura Evropského soudu pro lidská práva opakovaně formulovala s ohledem na ochranu práva na soukromí podle čl. 8 Evropské úmluvy požadavek, aby vnitrostátní úprava smluvní strany Evropské úmluvy rozlišovala mezi trestnými činy, v souvislosti s nimiž dochází ke shromažďování vzorků DNA, s ohledem na jejich společenskou závažnost. Dle názoru ESLP nelze přistupovat k pachatelům závažných trestných činů, především těch násilných, u kterých je odběr a skladování vzorků DNA legitimní, stejně jako k pachatelům méně závažných trestných činů. [33] Judikatura Soudního dvora také v obecné rovině, nicméně v kontextu výkladu jiných právních předpisů než Směrnice č. 2016/680, trvá na požadavku přiměřenosti mezi závažností zásahu do základních práv (v podobě získávání osobních údajů) a závažností trestné činnosti, proti kterým je bojováno a které mají za následek omezení základních. [34] Nejasným však zůstává, jaký typ přiměřenosti je zde vlastně zamýšlen, a nakolik lze logiku budování databází (systémové, legislativní přiměřenosti) bez dalšího automaticky nahradit posuzováním jednotlivé přiměřenosti s ohledem na konkrétního pachatele v každém jednotlivém případě (konkrétní, kasuistické přiměřenosti). Odtud otázka, jaký typ a míru přiměřenosti vlastně citované unijní právní předpisy vyžadují co do předpokládané diferenciace mezi subjekty údajů.

Tím však znovu otevírá otázku požadované míry individualizace/diferenciace závažnosti trestné činnosti, pro které by mohly být bez dalšího shromažďovány vzorky DNA a na jejich základě pořizovány identifikační profily. [36]

Z tohoto důvodu je pokládána první předběžná otázka ve znění „Jakou míru rozlišování mezi jednotlivými subjekty osobních údajů vyžaduje čl. 4 odst. 1 písm. c) či čl. 6 ve spojení s čl. 10 Směrnice č. 2016/680? Je slučitelné s imperativem minimalizace zpracování osobních údajů, stejně jako povinnosti rozlišovat mezi různými kategoriemi subjektů údajů, aby vnitrostátní právní úprava umožňovala odběr genetických údajů s ohledem na všechny osoby podezřelé nebo obviněné ze spáchání úmyslného trestného činu?“.

K otázce č. 2: jak dlouho lze uchovávat? [39]

Projednávaná věc pak kromě otázky zákonnosti odebrání identifikačních údajů orgány policie vznáší rovněž otázku přiměřené délky jejich uchovávání. Z čl. 4 odst. 1 písm. e) Směrnice č. 2016/680, stejně jako obecných principů a judikatury Soudního dvora s ohledem na jiné situace ochrany osobních údajů, se podává, že minimalizace zásahů do základních práv má také zřetelný aspekt temporální: osobní údaje mají být uchovávány pouze po dobu nezbytně nutnou s ohledem na účel jejich zpracování. Jak nicméně tuto logiku aplikovat na situaci, kdy je deklarovaným účelem předcházení, vyhledávání nebo odhalování trestné činnosti, které je svojí podstatou prospektivní a časově neomezené? Jasným a naprosto logickým účelem v tomto kontextu je mít maximální datový soubor pro maximální možné časové údobí do budoucna. Aplikací principu přiměřenosti vedoucího k výmazu osobních údajů, které mohou být stále relevantní, není s ohledem na tento účel dosahováno přiměřenosti a rovnováhy. Je spíše popírán samotný účel a smysl existence databáze, která nebude komplexní a nebude proto schopna svůj účel plnit. [40]

Předběžná otázka, která se z této problematiky podává, je, zda je slučitelné s právem Unie, aby vnitrostátní právo žádnou maximální hranici pro možnou délku uchovávání nestanovilo s tím, že na základě periodického vnitřního posouzení se strany orgánů policie bude v praxi docházet spíše k tomu, že získané profily DNA budou uchovávány bez časového omezení. [45] Z tohoto důvodu předklá-

dá NSS Soudnímu dvoru druhou předběžnou otázku ve znění „Je v souladu s čl. 4 odst. 1 písm. e) Směrnice č. 2016/680, pokud je s odkazem na obecný účel předcházení, vyhledávání nebo odhalování trestné činnosti pokračující uchovávání profilu DNA hodnoceno orgány Policie na základě jejich interních předpisů, což v praxi často znamená uchovávání citlivých osobních údajů na dobu neurčitou, aniž by byl stanoven jakýkoliv maximální časový limit pro uchovávání těchto osobních údajů? S ohledem na jaká kritéria má být případně hodnocena časová přiměřenost uchovávání osobních údajů shromážděných a uchovávaných s tímto cílem?".

K otázce č. 3: kvalita „obecné právní úpravy"? [47]

Nejvyšší správní soud nemá pochyb o skutečnosti, že interní předpisy policie v podobě pokynů policejního prezidenta nesplňují podmínky na kvalitu ani publicitu právních předpisů. Nejsou právními předpisy a pojmově nemohou mít kvalitu „práva" ve smyslu čl. 8 odst. 2 Směrnice č. 2016/680. [49] Ustanovení § 65 zákona o Policii ČR kvalitu „práva členského státu" bezpochyby má. Toto ustanovení samo o sobě však není dostatečně určité a podrobné, aby bylo sto naplnit požadavky čl. 8 odst. 2 ve spojení s čl. 10 Směrnice č. 2016/680. Ustanovení § 65 zákona o Policii ČR neobsahuje, mimo jiné, žádnou úpravu konkrétních podmínek uchovávání, typů informací, které smějí být z odebraného vzorku získávány, a co do pokračujícího uchovávání profilů DNA podmínky, za kterých má být přistoupeno k jejich výmazu. Už vůbec pak neobsahuje jakékoliv záruky vyžadované čl. 10 Směrnice č. 2016/680. [49] Jak však v řízení o kasační stížnosti podotkl stěžovatel, zákonná právní úprava co do možnosti omezení základních práv z důvodů zpracování osobních údajů je dotvářena ústavně souladným výkladem a judikaturou soudní. Úvodní bod č. 33 Směrnice č. 2016/680 je v tomto ohledu spíše velkorysý, neboť stanoví, že „Odkazy v této směrnici na právo či právní předpis, právní základ či legislativní opatření členského státu neznamenají nutně legislativní akt přijatý parlamentem, aniž jsou dotčeny požadavky vyplývající z ústavního řádu dotčeného členského státu. Toto právo, právní předpisy, právní základ či legislativní opatření členského státu by však měly být jasné a přesné a jejich použití by mělo být předvídatelné pro osoby, na něž se vztahují, jak to vyžaduje judikatura Soudního dvora a Evropského soudu pro lidská práva." [50] Ze setrvalé judikatury ESLP rovněž plyne, že „právo" v kontextu testu legality omezení základních práv zahrnuje nejenom zákon, ale i judikaturu soudní. [51] Novější judikatura Soudního dvora byla však v tomto ohledu ve znamení vyšších požadavků na kvalitu a publicitu „práva", kterým dochází k omezení základních práv. Dělo se tak především v oblastech práva, kde docházelo k omezení klíčových či základních práv, a kde Soudní dvůr trval na postulátu, že vysokou úroveň ochrany v případě zvlášť závažných omezení základních práv „může požadavky na srozumitelnost, předvídatelnost, dostupnost, a zejména na ochranu před svévolí splňovat jedině obecně závazný právní předpis." K obdobnému závěru Soudní dvůr došel také v řadě případů týkajících se právě ochrany osobních údajů, kdy trval na požadavku, že to musí být nejenom vnitrostátní právní úprava, a nikoliv judikatura, ale že ona právní úprava „musí rovněž stanovit hmotněprávní a procesní podmínky", jimiž se bude jakékoliv využití a přístup k uchovávaným provozním a lokalizačním údajům řídit. [52] Logika striktnějších požadavků co do kvality právního předpisu, kterým jsou vymezeny minimální náležitosti pro sběr, vytěžení, uchovávání a ničení vzorků DNA a z nich pořízených profilů DNA, by měla být patrně aplikovatelná také v projednávané věci. Ostatně sám čl. 10 Směrnice č. 2016/680, ve spojení s úvodním bodem č. 37 směrnice, který tyto osobní údaje řadí do specifické kategorie dat se zvláštní ochranou, by svědčil tomuto závěru. V takovém případě by unijní právo vyžadovalo, aby obecný právní předpis stanovil přinejmenším obecný rámec databáze, otázky přístupu, přesnější typ využití DNA informací včetně bariér jejich využití, ale především, v souladu s čl. 10, vhodné záruky práv a svobod, mimo jiné v podobě jasné diferenciace typů trestných činů, v případě kterých může být DNA profilace pořizována, a podmínek, za kterých může či musí být následně zničena. [53] Nic takového však vnitrostátní právní úprava aplikovatelná v projednávané věci v současnosti neupravuje. Pokud by však byly podobné požadavky bez dalšího aplikovány také v projednávané věci a dalších věcech před správními soudy na půdorysu současného § 65 zákona o Policii ČR, pak následek by byl nezbytně spíše radikální: soud by byl nucen vyhodnotit vnitrostátní úpravu jako neslučitelnou s čl. 8 odst. 2 ve spojení s čl. 10 Směrnice č. 2016/680 a jakékoliv biologické vzorky DNA a na jejich základě pořízené profily DNA automaticky za nezákonné. [54] Než by k podobnému závěru Nejvyšší správní soud byl nucen přistoupit, klade třetí předběžnou otázku, zda: „V případě zvláště citlivých osobních údajů spadajících pod čl. 10 Směrnice č. 2016/680, jaký je minimální rozsah hmotně-právních či procesních podmínek získávání, uchovávání a vymazání těchto údajů, který musí být v právu členského státu upraven „obecně závazným předpisem"? Může mít kvalitu „práva členského státu" ve smyslu článku 8 odst. 2 ve spojení s čl. 10 Směrnice 2016/680 také judikatura soudní?"

Závěr

Nejvyšší správní soud považuje českou úpravu získávání a uchovávání osobních údajů pro účely budoucí identifikace, především tedy citlivých osobních údajů v podobě profilu DNA, ve znění současného § 65 zákona o Policii ČR v řadě ohledů za neslučitelnou s v tomto usnesení citovanou judikaturou Soudního dvora EU a Evropského soudu pro lidská práva. Na druhou stranu však rovněž uznává legitimní důvody pro budování databází podobného typu a logiku jejich fungování, zdůrazňovanou policejními orgány. Společným jmenovatelem všech tří předkládaných předběžných otázek proto zůstává, nakolik lze bez dalšího přenést obecné závěry judikatury Soudního dvora, založené na robustním výkladu čl. 8 Charty základních práv EU a relevantních ustanovení GDPR a vysoké míře ochrany práv subjektů osobních údajů na minimalizaci zpracovávání jejich osobních údajů, včetně jejich práva být po určité době „zapomenut", rovněž do této specifické oblasti právní úpravy. Pokud by k tomu došlo, pak se stává dlouhodobé využívání policejních databází podobného typu obtížné, či spíše nemožné. [56]

Zpracovala Eva Janečková

Evropský legislativní přístup k regulaci umělé inteligence

Dynamický technologický vývoj s sebou v posledních dekádách přináší i množství legislativních výzev. Vzniká potřeba právního vymezení fakticky existujících institutů, jakými jsou třeba blockchain, kryptoměna nebo umělá inteligence (UI).

Zákonodárci na národní, ale i evropské úrovni tak stojí před nelehkým úkolem, jímž je vytvoření proporcionální právní úpravy, která stanoví meze pro aplikaci nových technologií *de facto* a taktéž *de iure*, neboť je třeba zajistit kompatibilitu s již existujícím legislativním rámcem. V neposlední řadě například i s GDPR.

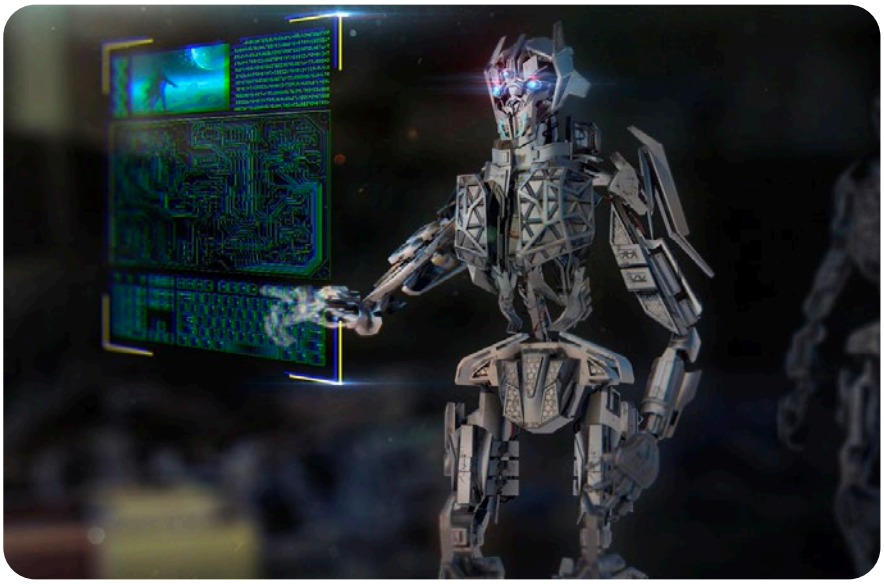
Potenciál do budoucna je enormní

Tato role je nelehká také proto, že nová úprava by neměla být limitující, což by mohlo vést k nežádoucímu zpomalení výzkumu, vývoje a taktéž oslabení konkurenceschopnosti v dotčených jurisdikcích – a tedy celé EU. Dnes je totiž již znatelná transformační kapacita UI, popř. strojového učení. Mezi nejběžnější příklady patří komunikace se zákazníky, např. formou voicebotů, chatbotů nebo virtuálních asistentů. UI se ale stále více aplikuje např. též na zefektivnění procesů, konkrétně při zpracování žádostí, vyhodnocování spokojenosti. Dále se využívají prediktivní analýzy, což vede k hlubší personalizaci produktů a cen. Potenciál do budoucna je však enormní.

Do roku 2025 má dojít k 56násobnému nárůstu

V současném vývojovém stadiu nemá smysl představovat si UI jako humanoidního robota nebo jiné dystopické scénáře. UI chápeme jako sofistikovaný, konektivní, autonomní systém založený na algoritmech, která závisí na datech. Obrovskou byznysovou kapacitu služeb aplikujících UI lze dedukovat z odhadů, podle kterých dojde od roku 2016 do roku 2025 k 56násobnému nárůstu z 644 mil. USD na 35 mld. USD [1]. Potenciál je vázán na existenci a analýzu velkého množství dat splňujících kvalitativní a kvantitativní předpoklady. Revoluce „velkých dat" může otevřít cestu k novým způsobům řízení organizací a přispět k výraznému zvýšení jejich efektivity [2].

Vycházejíc z tohoto stavu Evropská komise v dubnu 2021 publikovala návrh horizontálního nařízení o umělé inteligenci (*Artificial Intelligence Act*, AIA) [3], kterému předcházela veřejná konzultace. Vzhledem k jeho významu v obecné, částečně ideologické neboli proklamační rovině – kdy půjde o vůbec první legislativní úpravu UI globálně, bude toto nařízení významným předpisem zakotvujícím konkrétní požadavky na aplikaci UI napříč spektrem sektorů, jež UI využívají čím dál tím více.



Návrh AIA lze chápat jako nadstavbu GDPR

Jak bylo již naznačeno výše, podmínkou funkční a přínosné právní úpravy je zajistit sémantickou, právní a technickou kompatibilitu s již existující praxí, neustále postupujícím technologickým vývojem a v neposlední řadě stávající právní základnou. Návrh AIA tak lze chápat jako nadstavbu GDPR, a to ze dvou pohledů. Zaprvé, ambicí Evropské komise u AIA je dosáhnout podobného, celosvětově inspirativního minimálního standardu, jako tomu je u GDPR (tzv. „bruselský efekt"). Zadruhé, AIA by měla vycházet ze zásad již zakotvených v GDPR, podmínek a nároků, především v oblastech práv subjektů osobních údajů, včetně práva na lidské posouzení v případě automatizovaného rozhodování.

Legislativní formou je nařízení… Proč?

Co se týká konkrétních aspektů návrhů, jako legislativní forma bylo tedy zvoleno nařízení, a to z důvodu vyšší pravděpodobnosti zajištění unifikace a harmonizace a taktéž naplnění základního cíle nové úpravy. Tím má být kromě podpory konkurenceschopnosti z hlediska zajištění vysoké úrovně práv subjektů údajů hlavně posílení právní jistoty, odstranění národní fragmentace a případných přeshraničních překážek.

Pozastavíme-li se nad dopadem…

Původní návrh Evropské komise obsahuje dělení aplikace UI do tří kategorií dle rizikovosti. Rámec AIA by tedy neupravoval případy aplikace UI, které s sebou nenesou žádné nebo jen minimální riziko pro spotřebitele, což je dle zprávy Zvláštního výboru pro umělou inteligenci v digitálním věku (AIDA) [4] většina případů využití UI.

Rámec by však dopadal na aplikace UI s nízkou úrovní rizikovosti, na něž by se vztahovaly požadavky na informační povinnost a transparentnost (např. konverzační a asistenční UI poskytující informace). Dále by dopadal na aplikace UI s vyšším rizikem, na které by se vztahovaly požadavky vymezené AIA a ex ante posouzení kompatibility (např. *recruitment*). Tyto aplikace mají zvýšené požadavky na testování, risk management, přístup k datům a jejich validaci (s respektem k GDPR), technickou dokumentaci a informační povinnost vůči uživatelům vč. práva na lidský zásah.

1) FELDMAN, Michael. Market for Artificial Intelligence Projected to Hit $36 Billion by 2025. In: Top500.org [online]. 29. 8. 2016 [28. 1. 2023]. Dostupné z: https://www.top500.org/news/market-for-artificial-intelligence-projected-to-hit-36-billion-by-2025/
2) FORD, Martin. *Roboti nastupují – Automatizace, umělá inteligence a hrozba budoucnosti bez práce*. Praha: Rybka Publishers, 2017, s. 199. ISBN: 978-80-87950-46-3.
3) Návrh nařízení o umělé inteligenci Evropské komise dostupný z https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence
4) Evropský parlament. Zpráva o umělé inteligenci v digitálním věku (2020/2266(INI). Dostupné z: https://www.europarl.europa.eu/doceo/document/A-9-2022-0088_CS.html.

Poslední kategorií je aplikace UI nesoucí s sebou neakceptovatelné riziko (např. sociální inženýrství), jejíž využití by proto nebylo přípustné.

Specifická jsou i očekávaní Evropské komise v článku 83 návrhu AIA. Ten se vztahuje také na vysoce rizikové systémy UI, které byly uvedeny na trh nebo do provozu před datem použitelnosti tohoto právního předpisu, pokud u těchto systémů došlo k významným změnám v jejich konstrukci nebo zamýšleném účelu. Avšak zpětné splnění požadavků (například pokud jde o údaje o testování) v situaci, kdy byl systém UI již vyvinut, je velmi nákladné.

Kategorizace rizik a české předsednictví v Radě EU

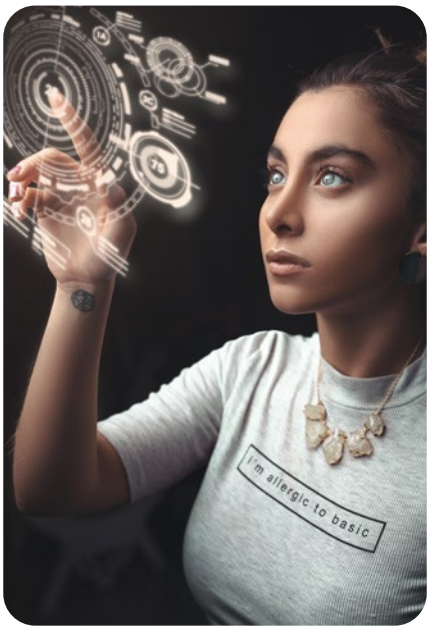
České předsednictví v Radě EU bylo ve věci kategorizace rizik aktivní, když ve druhé polovině minulého roku reagovalo na vzniklou opozici některých členských států ohledně přístupu navrhovaného Evropskou komisí. Ten je obecně považován za příliš široký, a proto může selhat při identifikaci systémů, které *„pravděpodobně nezpůsobí závažné porušení základních práv nebo jiné závažné důsledky"*. Během českého předsednictví v Radě EU došlo k významnému posunu ve vyjednávání, v listopadu minulého roku byla přijata smysluplnější pozice Rady a pomyslné žezlo bylo předáno švédskému předsednictví, které se dalšímu posunu AIA hodlá rovněž aktivně věnovat.

Nadále však zůstávají otevřené některé klíčové otázky

Pro plnohodnotnou funkčnost plánovaného legislativního rámce je (jak bylo již naznačeno výše) relevantní také co nejoptimálnější taxonomie. Co nejdokonalejší formulace definice UI je relevantní nejenom z hlediska dostatečné míry právní jistoty aplikovaného AIA, ale také z důvodu pravděpodobné další navazující evropské (např. v kontextu úpravy odpovědnosti u UI, které se stručně věnuji níže) i globální inspirace.

Evropská komise vycházela v článku 3 z definice UI OECD *„a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments"*, kterou však rozšířila o software. To povede k zahrnutí systémů, technik a přístupů (které by neměly být považovány za UI) do oblasti působnosti a obecně pak i k nejasnostem a nedostatku právní jistoty. I zde by se mělo navázat na dosavadní OECD práci[5], v níž je např. uvedeno že *„Microsoft Excel je systém pro ukládání a analýzu dat. Tento software umožňuje uživatelům ukládat, třídit a provádět základní analýzy zadaných dat. Není to však systém UI."* Totéž platí i pro celou řadu dalších typů softwarů nebo statistických přístupů, které mohou potenciálně spadat pod navrhovanou definici.

Nedojde-li k úpravě této nevhodné formulace, hrozí nebezpečí, že v praxi by se rozsah použití rozšířil na základní informační



technologie, které se dlouhodobě a běžně používají. Regulace UI by pochopitelně neměla obsahovat neodůvodněné překážky současné bezrizikové aplikace a rovněž ani ty, které přinese budoucnost. V nejhorším případě by příliš široká oblast působnosti AIA mohla brzdit vývoj nových systémů a na druhé straně by mohla vést k nutnosti demontáže již existujících systémů.

Původním smyslem AIA je upravovat a zmírňovat rizika

Původní smysl AIA spočívá v upravování a zmírňování rizik „specifických pro UI", jimiž je vznik nových (skrytých a nezamýšlených) předpojatostí, zesílení těchto předpojatostí, jakož i neprůhlednost mnoha systémů UI. Obecné riziko předpojatosti a nespravedlivé diskriminace by se mělo řešit v rámci jiné stávající regulace.

Kdo je poskytovatelem?

Řadu otázek vyvolává také původní definice Evropské komise pojmu „poskytovatele" v článku 3 návrhu AIA. „Poskytovatelem" se rozumí fyzická osoba, právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, jiný než uživatel, který vyvíjí systém UI nebo který si nechává vyvíjet systém UI s cílem uvést jej na trh nebo do provozu pod svým jménem nebo ochrannou známkou, a to za úplatu nebo bezplatně. Návrh textu stanoví řadu povinností jak pro poskytovatele (zejména v článku 16), tak pro uživatele systémů UI. Podle článku 3 může být poskytovatelem někdo, kdo vyvíjí systém UI nebo kdo si nechá systém UI vyvinout. Leč hodně systémů UI není vyvíjeno interně, ale spíše externími vývojáři. Proto existuje riziko, že tyto subjekty budou kvalifikovány jako poskytovatel, protože si nechávají vyvinout systém UI pro sebe, i uživatel podle článku 3 odst. 4 návrhu. Mělo by být proto jasně stanoveno, že veškeré povinnosti poskytovatele podle AIA by se měly týkat vývojáře, neboť právě ten má veškeré potřebné know-how a technické znalosti.

Další nevyjasněné definice…

Dále je potřeba vyjasnit i další definice, jako např. „základní soukromé služby", „negativní dopad na základní práva", „známá nebo předvídatelná rizika pro zdraví a bezpečnost nebo základní práva".

Bez chyb a úplné?

Je rovněž důležité zajistit, aby soubory tréninkových, validačních a testovacích dat podléhaly vhodným postupům správy a řízení dat. Ustanovení článku 10 odst. 3 návrhu Evropské komise však požaduje, aby tyto soubory dat byly „bez chyb a úplné". Ačkoli by mělo být vynaloženo maximální úsilí, aby se chybám předešlo, požadavek, aby údaje byly „bez chyb a úplné", je fiktivním očekáváním, které nezohledňuje realitu používání souborů údajů a možnost lidského pochybení, jak bylo naznačeno v úvodu tohoto článku. Požadavek na „úplnost" datových souborů může být zavádějící i při práci s chybějícími hodnotami. Zmírněna by měla být i formulace týkající se potřeby úplnosti a přesnosti údajů, aby více odpovídala smluvním prohlášením/zárukám, které dostáváme od poskytovatelů údajů třetích stran. Mnozí poskytovatelé údajů ukládají smluvní ustanovení, že jejich údaje budou poskytovány tak, jak jsou, a že mohou obsahovat chyby a opomenutí, a vyžadují prohlášení o vyloučení odpovědnosti, pokud jde o úplnost, přesnost, aktuálnost, vhodnost nebo dostupnost poskytovaných údajů.

Klíčový prvek pro usnadnění lepšího porozumění a důvěry veřejnosti

Zajímavým legislativním oříškem je i požadavek na navržení a vývoj systémů UI určených pro interakci s fyzickými osobami tak, aby byly tyto osoby informovány o tom, že komunikují se systémem UI. Transparentnost zakotvená v článku 52 návrhu AIA je klíčovým prvkem pro usnadnění lepšího porozumění a důvěry veřejnosti, pokud jde o používání a uplatňování UI, což představuje paralelu s GDPR. Zajistit, aby bylo zřejmé, kdy je UI používána a k jakému účelu, pomůže nejen ke zvýšení důvěry spotřebitelů v tuto technologii, ale také k usnadnění jejího celkového přijetí v průmyslu. Poskytování smysluplných a srozumitelných informací rovněž pozitivně přispěje k rozhodování informovanějších spotřebitelů. Požadavky v tomto ohledu by se však neměly ukázat jako zbytečně zatěžující v důsledku příliš širokého výkladu. Není hned srozumitelné, jak vykládat pojmy jako „zřejmé z okolností a kontextu použití", což vyvolává otázky, kdy by se měl požadavek na informace uplatnit. Mělo by být například jasné, že požadavek na transparentnost je relevantní

5) Rámec pro klasifikaci UI OECD. Dostupný zde: https://oecd.ai/en/classification

pouze pro systémy UI, kde dochází k přímé interakci mezi systémem a zákazníkem a systém může plně/částečně ovlivnit volbu a/nebo práva zákazníka. Zde totiž opětovně narážíme nejen na limitovanou vysvětlitelnost, ale i na možnou neprůhlednost zapříčiněnou složitostí algoritmů. To bylo ostatně známo již před 10 lety, kdy vědci konstatovali, že i tvůrci systémů tohoto typu časem ztrácí kontrolu a mají obtíže jim porozumět [6]. Tento samo evolutivní faktor by rozhodně měl být zohledněn v aktuálním evropském legislativním procesu.

Evropský parlament zatím svou pozici nepublikoval

V současné době máme k dispozici původní návrh Evropské komise a postoj Rady. Evropský parlament zatím svou pozici nepublikoval. To může být ovlivněno také tím, že vzhledem ke komplexnosti problematiky úpravy UI, jakožto disruptivní technologie ovlivňující vývoj mnoha sektorů, je spoluzodpovědných několik výborů (IMCO, LIBE, JURI, ITRE, CULT). Z dostupných informací však plyne, že na kompromisních návrzích aktivně pracují především výbory IMCO a LIBE. Plenární hlasování Evropského parlamentu je prozatím avizováno na duben 2023, poté mohou začít trialogy. Vzhledem ke komplexnosti problematiky lze ale předpokládat složitá vyjednávání. V následujících měsících snad bude ze strany evropských institucí zohledněno, že nové podmínky a povinnosti k aplikaci UI je vhodné formulovat v souladu se zásadou proporcionality tak, aby vznikl na zásadách založený horizontální rámec požadavků, aniž by nepřiměřeně omezoval nebo bránil technologickému vývoji a inovacím.

Návrh AIA v návaznosti na evropské diskuze o modernizaci odpovědnostního rámce

Kromě toho je návrh AIA vhodné vnímat nejenom v souvislostech se stávající legislativou, ale také v návaznosti na evropské diskuze o modernizaci odpovědnostního rámce. Evropská komise již létě 2021 zveřejnila konzultaci k plánu přizpůsobení pravidel odpovědnosti digitálnímu prostředí a UI [7], která je součástí jejího postupného přístupu k rozvoji ekosystému důvěryhodnosti pro UI a bude doplňovat AIA a pravděpodobně vést k revizi směrnice o obecné bezpečnosti výrobků (*Product liability directive, PLD*) a/nebo návrhu nového předpisu regulujícího odpovědnost v kontextu UI.

Zaprvé: zastaralé pojmy

Bylo zjištěno, že je obtížné aplikovat směrnici na výrobky v digitálním a oběhovém hospodářství, a to zaprvé kvůli zastaralým pojmům. Např. v kontextu insurtechu už de *facto* není určujícím bodem pro hodnocení odpovědnosti uvedení výrobu do oběhu. Taxonomická nejednotnost může vést k budoucí právní nejistotě a limitaci vývoje. Nejednotným vnímáním terminologie se zaobírá i Smejkal [8], který popisuje absenci právních definic relevantních pojmů. Odkazuje na Občanskoprávní pravidla pro robotiku [9], kterými Evropský parlament vyzval Evropskou komisi k navržení jednotných definic, což se snad povede právě v AIA.

Zadruhé: získávání odškodnění spotřebitelů

Zadruhé je obtížné získávání odškodnění spotřebitelů, zejména pokud jde o prokazování, že složité výrobky byly vadné a způsobily škodu. Jedná se např. o zakomponovaný software, který je-li považován za produkt, spadá pod PLD, je-li ale považován za službu, tak nikoli. Odškodnění a důkazní břemeno souvisí i s problematikou spletitostí dodavatelského řetězce. Hardware, software a služby tvoří technologické ekosystémy, což je ještě komplexnější u IoT, kde dochází k interakcím mnoha propojených zařízení, služeb a subjektů (designér, programátor, výrobce, poskytovatel, poskytovatel připojení, poskytovatel finální služby atd.). Zároveň se jedná o vyvíjející se systémy, takže modernizace může zamíchat kartami k posuzování původní a aktualizované verze.

Zatřetí: složitost algoritmů

Zatřetí lze za obtížné považovat načrtnutou složitost algoritmů, jež naráží nejen na limitovanou vysvětlitelnost, ale i na možnou neprůhlednost. To nemusí být závislé pouze na primárně vložených datech (když vycházím z předpokladu, že se jedná o data, u kterých nehrozí riziko diskriminačního posouzení), ale jak hodnotí i Evropská komise ve Zprávě k bezpečnosti a odpovědnosti umělé inteligence, IoT a robotiky, na základě efektu samostatného učení UI se může stát, že stroj učiní rozhodnutí odlišné od původně zamýšleného výrobcem nebo očekávaného uživatelem. Vede to k důsledku, že ex ante je omezena předvídatelnost UI a ex post je omezena vysvětlitelnost. Což nás opětovně dostává k důkaznímu břemenu. To je na straně subjektu osobních údajů dle mého názoru v praxi velmi těžce realizovatelné, a to jak z hlediska samotného pochopení fungování algoritmu, tak z hlediska ochrany obchodního tajemství apod. Jako průchodnější variantu vnímám kauzální odpovědnost za chybné chování UI, které vede ke vzniku škody.

Čeho chce dosáhnout Evropská komise?

Cílem Evropské komise je modernizovat pravidla odpovědnosti tak, aby zohledňovala vlastnosti a rizika insurtechu, komplexních digitálních a obchodních modelů, včetně produktů a služeb vybavených UI. Navazující konkrétní návrh Evropské komise však zatím nebyl předložen. U legislativního podchycení těchto složitých fenoménů je důležité zohlednění toho, že prvotním krokem k řádnému praktickému fungování UI je dostatečný datový vzorek, přičemž pro analýzu dat je nezbytná jednotná metodologie sběru. Z hlediska právní jistoty je pak nezbytností jasný rámec vycházející z principů proporcionality, rizikové založenosti, transparentnosti a vysvětlitelnosti složitého řetězce UI, možnosti lidského zásahu a prevence diskriminace, zajištění kybernetické bezpečnosti, rámce GDPR atd.

Zajímá vás více?

Další legislativní vývoj AIA a navazujících iniciativ by tak ani v nejbližších měsících neměl uniknout naší pozornosti. V případě že vás problematika UI zajímá, ať už z lásky k sci-fi nebo z praktičtějších pohnutek, dovolím si upozornit na bezplatný online kurz k UI „Elements of AI" [10], který již v roce 2018 spustila Helsinská univerzita a který je nyní k dispozici taktéž v češtině.

Jana Andraščiková
Autorka je právník, koordinátor evropské agendy a gestor kybernetické bezpečnosti v České asociaci pojišťoven.

6) JOHNSON, Neil, ZHAO, Guannan, HUNSADER, Eric, QI, Hong, JOHNSON, Nicolas, MENG, Jing a TIVNAN, Brian. Abrupt rise of New Machine Ecology Beyond Human Response Time. Nature [online]. 11. 2. 2023. Dostupné z: https://www.nature.com/articles/srep02627
7) Směrnice o odpovědnosti za vadné výrobky – přizpůsobení předpisů digitálnímu věku, oběhovému hospodářství a globálním hodnotovým řetězcům. Dostupné zde: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence_en
8) SMEJKAL, Vladimír. Kybernetická kriminalita. Druhé, rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018, s. 88. ISBN 978-80-7380-720-7.
9) Usnesení Evropského parlamentu ze dne 16. února 2017 obsahující doporučení EK o občanskoprávních pravidlech pro robotiku (2015/2103[INL]). In: *Úřední věstník* [online], C252/239, 18. 7. 2018, s. 239–257 [cit. 22. 2. 2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52017IP0051
10) Kurz je dostupný z: https://www.elementsofai.cz/

Právo na sdělení konkrétních příjemců podle čl. 15 GDPR

Soudní dvůr Evropské unie (SDEU) vydal letos v lednu rozsudek C 154/21 ve věci RW proti Österreichische Post AG, přinášející výklad čl. 15 odst. 1 písm. c) GDPR, tedy práva subjektu údajů, aby mu na jeho žádost správce poskytl informace o příjemci nebo kategoriích příjemců, kterým osobní údaje byly nebo budou zpřístupněny. Podstatou sporu bylo, zda má správce povinnost poskytnout informace o konkrétních příjemcích nebo stačí, pokud subjekt údajů bude informován pouze o kategoriích příjemců.

Pan RW využil své právo na přístup k údajům podle čl. 15 GDPR a požádal Rakouskou poštu (Österreichische Post), aby mu umožnila přístup k osobním údajům, které o něm uchovává nebo které uchovávala v minulosti. Pokud byly osobní údaje předány třetí osobám, požadoval RW, aby mu Österreichische Post sdělila totožnost osob, kterým byly osobní údaje předány.

Österreichische Post se při odpovědi na žádost omezila pouze na sdělení, že osobní údaje nabízí obchodním klientům pro marketingové účely a odkázala pana RW na internetové stránky. Konkrétní názvy a totožnost příjemců údajů Österreichische Post panu RW nesdělila. Rakouský nejvyšší soud požádal SDEU o zodpovězení předběžné otázky. Podstatou této otázky bylo, zda je třeba, aby správce sdělil subjektu údajů v rámci práva na přístup informace o příjemcích osobních údajů, pokud již byly těmto příjemcům předány.

Konkrétní příjemci mají přednost

SDEU odpověděl na tuto otázku kladně. Subjekt údajů má právo znát, až na výjimky, totožnost příjemců údajů. Podle SDEU není možné ze znění čl. 15 odst. 2 písm. c) vyvodit, zda má při vyřizování žádosti o práva na přístup přednost pojem „příjemci", nebo „kategorie příjemců". Nicméně je podle SDEU třeba zohlednit i bod odůvodnění 63 GDPR, ve kterém se uvádí, že každý subjekt údajů by měl mít právo vědět a být informován mimo jiné o tom, kdo jsou příjemci osobních údajů.

Zpracování osobních údajů musí být v souladu se zásadami zakotvenými v čl. 5 GDPR. Jednou ze zásad je zásada transparentnosti zpracování. Zásada transparentnosti vyžaduje, aby byly subjektům údajů poskytovány informace o tom, jak jsou jejich osobní údaje zpracovávány, a aby tyto informace byly snadno dostupné a srozumitelné.

SDEU upozorňuje na to, že pokud má mít subjekt údajů skutečné právo na přístup, musí to být on, kdo si vybírá, zda požaduje informace o konkrétních příjemcích nebo pouze jejich kategoriích. Není to správce, kdo má právo volby mezi těmito alternativami.

Informace k uplatnění dalších práv

Podle SDEU musí právo na přístup subjektu údajů umožnit ověřit, zda jsou jeho údaje správné a jsou nebo byly zpracovávány zákonným způsobem. Toto zjištění umožňuje subjektu údajů následně uplatňovat i další práva jako právo na opravu, na výmaz nebo omezení zpracování, právo vznést námitku nebo právo podat žalobu na náhradu škody. Pro účinný výkon těchto práv musí mít subjekt údajů informace o totožnosti konkrétních příjemců, pokud jim byly osobní údaje zpřístupněny.

SDEU zmiňuje i čl. 19 GDPR, podle kterého správce oznamuje jednotlivým příjemcům, jimž byly osobní údaje zpřístupněny, veškeré opravy nebo výmazy osobních údajů nebo omezení zpracování a informuje subjekt údajů o těchto příjemcích, pokud to subjekt údajů požaduje.

Kdy stačí i kategorie příjemců

Správce se může omezit na kategorie příjemců údajů, pokud není možné poskytnout informace o konkrétních příjemcích, zejména pokud nejsou ještě známi. Správce může žádost subjektu údajů na přístup odmítnout podle obecných pravidel čl. 12 GDPR, tedy v případě, kdy je žádost zjevně nedůvodná nebo nepřiměřená.

Rozsudek SDEU neobsahuje vodítka pouze pro výklad čl. 15 odst. 1 písm. c), tedy co má obsahovat odpověď správce na žádost subjektů údajů o právo na přístup. SDEU zmiňuje i čl. 13 a čl. 14 GDPR, které obsahují téměř totožnou formulaci. Správce musí podle čl. 13 odst. 1 písm. e) a čl. 14 odst. 1 písm. e) informovat subjekt údajů o případných příjemcích nebo kategoriích příjemců. SDEU na rozdíl od ustanovení, jehož výklad byl předmětem předběžné otázky, u výše uvedených článků neuvádí, že by měla informace o příjemcích osobních údajů přednost před informací o kategoriích příjemců nebo že by měl subjekt údajů právo volby mezi poskytnutím informací o konkrétních příjemcích nebo jejich kategoriích.

Závěr

Pro správce z tohoto rozsudku vyplývá povinnost evidovat, komu osobní údaje subjektů údajů předává, aby mohl v případě žádosti podle čl. 15 subjektu údajů sdělit totožnost všech příjemců jeho údajů. Spolu s evidencí příjemců by si měl správce zaznamenávat i důvod, pro jaký byly osobní údaje těmto správcům předány, kdyby subjekt údajů např. namítal protiprávnost zpracování. Naopak při informování subjektů údajů podle čl. 13 a 14 má (zatím) možnost volby, zda subjekt údajů informuje o příjemcích nebo jejich kategoriích.

Eva Fialová
Autorka je právnička se specializací na ochranu osobních údajů a právo ICT. Působí v advokátní kanceláři PRK Partners.

Vývoj autonomních systémů řízení s pomocí dat z palubních kamer

Samotná instalace palubních kamer ve vozidlech není již žádnou novinkou. Jejich využití za účelem získání důkazního materiálu pro případ dopravní nehody je v České republice legální (z hlediska bezpečnosti provozu i ochrany soukromí dotčených osob) a zřejmě i poměrně obvyklou praxí. S tím, jak se do výbavy vozidel prosazují stále pokročilejší asistenční systémy a vývoj směřuje k plně autonomním vozům, získává však shromažďování a další využívání dat z palubních kamer zcela jiné rozměry a význam. Právě díky masivnímu zpracování dat můžeme v dohledné budoucnosti očekávat na našich silnicích vozidla, která se doteď objevovala pouze jako rekvizita ve sci-fi filmech.

Moderní vozidla jsou již dnes běžně vybavena množstvím senzorů, které získávají data jak o provozu vozidla samotného, tak i o jeho interakci s okolím, a které takto získaná data ukládají pro budoucí využití nebo i přímo předávají zpět výrobcům, servisům apod.[1] Veškeré informace „zevnitř" vozu (vypovídající o způsobu řízení nebo o využívání bezpečnostních a asistenčních systémů) i „zvenku" (týkající se např. dopravního značení a dopravních situací) jsou totiž zcela zásadní z hlediska další optimalizace stávajících asistenčních systémů i pro vývoj nových, včetně autonomních.

Množství dat, která jsou a nadále budou zapotřebí k vývoji a dalšímu zdokonalení („učení") systémů autonomního řízení, je přitom takové, že jen s malou nadsázkou lze říci, že vozidla budoucnosti budou ke svému pohonu data potřebovat stejnou měrou jako palivo, resp. energii.

Osobním údajům se nelze vyhnout

Kamery snímající dění v okolí vozidla jsou jedním z klíčových prvků při vývoji autonomních systémů řízení, neboť jejich prostřednictvím lze získat komplexní data o interakci vozidla s okolím v mnoha nejrůznějších situacích a za nejrůznějších okolností. Kamery slouží k rozpoznávání překážek, chodců, zvířat, jiných vozidel, dopravních značek nebo detekci jízdních pruhů. Tato data jsou pak základem pro algoritmy autonomních systémů řízení i jejich další vývoj. S ohledem na to, že tyto algoritmy se strojově učí na základě předchozích dat, je přesnost a spolehlivost (a tedy bezpečnost) autonomních systémů řízení přímo závislá na množství, kvalitě a různorodosti dat, která získávají.

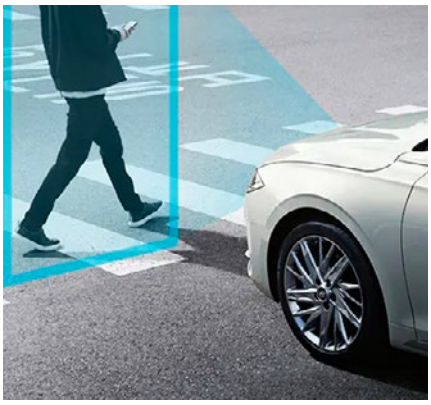
Z uvedeného je zřejmé, že získávání dat např. pouze pomocí testovacích vozů nemůže být dostačující. Naopak je žádoucí zapojení co největšího počtu vozidel účastnících se reálného provozu, a to v co nejrozmanitějším prostředí. A je tedy logické, že společnosti podílející se na vývoji autonomních systémů řízení mají, ve snaze získávat co největší objemy dat, zájem o spolupráci s provozovateli větších vozových parků, případně i se soukromými uživateli, kteří jim umožní ve svých vozech kamery instalovat.

Nejpozději v této fázi přichází na řadu také otázky spojené s plněním povinností vyplývajících z GDPR,[2] neboť jistě není zapotřebí detailně vysvětlovat, proč je na informace získané z palubních kamer nutno pohlížet jako na osobní údaje ve smyslu čl. 4 odst. 1) GDPR. Vždy bude možné přiřadit tyto informace alespoň k řidiči či provozovateli daného vozidla, případně i k třetím osobám zachyceným v okolí. Ve vztahu k posledně zmíněné skupině osob pak platí, že konkrétní obsah záběru, a tedy to, zda dojde k zaznamenání určitých identifikačních prvků, např. podoby anebo registrační značky jiného vozidla, nelze předem ovlivnit, a shromáždění těchto údajů proto není možné zcela vyloučit.

Zpracování osobních údajů „zevnitř" vozu

Základní otázkou u každého zpracování osobních údajů je, zda je předmětná činnost vůbec legální a legitimní, tj. zda pro ni lze aplikovat některý z právních základů v čl. 6 odst. 1 GDPR. Přičemž v tomto směru je možné odlišit dva základní úhly pohledu, tj. zpracování dat z pohledu řidiče, resp. vlastníka či provozovatele vozidla, a z pohledu třetích osob náhodně zachycených v okolí.

Již samotnou instalaci kamery logicky nelze provést bez souhlasu vlastníka či provozovatele vozidla. Jestliže se jedná o fyzickou osobu, pak také zpracování osobních údajů vypovídajících o provozu tohoto vozidla, které se k této osobě vztahují, bude probíhat s jejím souhlasem ve smyslu čl. 6 odst. 1 písm. a) GDPR. V této souvislosti je potřeba vyzdvihnout zásadní roli informací o všech podstatných parametrech zpracování, bez nichž nebude souhlas platně udělen. Půjde zejména o to, kam budou získaná data předávána (s kým budou sdílena), jak dlouho budou využívána v původní (neanonymizované) podobě nebo jakým způsobem budou případně dále upravována.



Pokud vlastník vozidla a jeho řidič nejsou tatáž osoba, platí požadavek na získání souhlasu se zpracováním osobních údajů i pro řidiče. Taková situace nastane zejména u vozidel provozovaných právnickými osobami, určených k užívání jejich zaměstnanci. V případě tzv. referentských vozů (které nevyužívá trvale pouze jeden konkrétní zaměstnanec) je pak vhodné spíše přijmout technické řešení umožňující např. kameru dočasně vypnout.

Důvodem, proč není možné získávat data z kamer bez souhlasu zaměstnance, který vozidlo využívá, je fakt, že spojením informací pořízených kamerou s identitou řidiče lze docílit poměrně komplexního přehledu o jeho pohybu i způsobu chování v provozu. Takové informace přitom nejsou nezbytné pro plnění zákonných povinností správce, tj. neexistuje právní předpis, k jehož splnění by takové zpracování bylo zapotřebí. Argumentace oprávněným zájmem zaměstnavatele či vývojáře autonomních systémů pak narazí kromě zmíněného rozsahu dat i na problematiku slabšího postavení zaměstnanců ve vztahu k zaměstnavateli. Požadovaný balanční test by tedy v tomto případě jen stěží vyzněl tak, že práva a právem chráněné zájmy subjektu údajů – zaměstnance nepřevažují nad zájmy správce či třetích osob.[3]

1) Zpracování osobních údajů získaných v souvislosti s provozem vozidla, příp. propojením s dalšími zařízeními, a sdílených s třetími stranami (výrobci, pojišťovnami, servisy) je předmětem stanoviska EDPB č. 1/2020 (Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications; https://edpb.europa.eu).
2) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (Obecné nařízení o ochraně osobních údajů).
3) Otázka, kdo je v uvažované situaci správcem a kdo zpracovatelem, příp. zda jde o společné správce, může mít zřejmě více vyústění s ohledem na to, jak konkrétně je nastavena spolupráce mezi všemi zainteresovanými subjekty. Závěr o nevhodnosti uvedených právních titulů platí nicméně ve všech konstelacích.

Kromě výše zmíněné podmínky v podobě dostatečně podrobné a srozumitelné informace o zpracování je pro získání souhlasu samozřejmě zásadní, aby bylo možné zpracování skutečně svobodně a bez následků odmítnout, což se týká zejména popsané situace se služebními či referentskými vozy.

Zpracování osobních údajů „vně" vozu

Jak bylo již uvedeno, snímáním veřejného prostoru se nelze vyhnout zpracování osobních údajů třetích osob. Tuto část zpracování je pak možné pokrýt pouze oprávněným zájmem správce a dalších zainteresovaných osob. Aplikace právního základu podle čl. 6 odst. 1 písm. f) GDPR přitom není možná bez provedení tzv. balančního testu, tedy srovnání oprávněných zájmů výrobců a vývojářů s právy a zájmy dotčených osob, zde tedy těch, kdo mohou být na záběru zachyceni.

Východiskem pro argumentaci ve prospěch shromažďování těchto údajů je fakt, že (alespoň v současné době), nejsou k dispozici srovnatelné metody získání potřebného množství dat v potřebné kvalitě, které by současně představovaly menší či nulový zásah do práv subjektů údajů. Dále, že zákonné požadavky na zajištění bezpečnosti jsou v oblasti automobility natolik přísné a specifické, že bez dlouhodobého a podrobného tréningu založeného na reálných datech není možné jim dostát.

Pro zajištění maximální míry ochrany práv subjektů údajů je dále nutné garantovat především opatření směřující k minimalizaci shromážděných dat. Není např. nutné získávat nonstop záznam veškerého provozu a dění v okolí. Na základě již získaných dat lze zařízení před-programovat tak, že bude pořízen vždy jen krátký záznam anebo sekvence fotografií předem indikované situace. Dále lze vhodně nastavit míru rozlišení pořízených záběrů, která umožní spolehlivě a bezchybně interpretovat zachycené dopravní situace, avšak bez dalších (nadbytečných) detailů. Je také možné implementovat filtrační mechanismy, které získaná data protřídí a vyberou jen ta skutečně použitelná, a další, jimiž se odstraní staré záběry, které se pro vývoj a trénování již nevyužívají.

Důležitým prvkem je i oddělení identity provozovatele či vlastníka konkrétního vozidla od předávaných dat tak, aby nebylo možné např. zpětné trasování či profilování. Pro sledovaný účel lze záznamy z jednotlivých kamer odesílat bez bližšího určení např. registrační značky či typu vozidla, ze kterého pochází. Opatření zavedená na poli minimalizace získaných dat pak mohou správci posloužit jako argument spočívající v tom, že zpětná identifikace osob zachycených na záznamech by byla spojena s nemalými dodatečnými náklady bez přínosu pro jeho cíle.

Jistým limitem pro minimalizaci rozsahu dat jsou již zmíněné bezpečnostní požadavky – autonomní systémy řízení musí být schopné detekovat např. i směr pohledu či gesta účastníků provozu, aby bylo možné předvídat jejich chování (např. úmysl chodce přejít ulici). Zásadnější následná manipulace s pořízenými záběry např. ve formě rozmazání či pixelace je proto neúčelná, neboť tím dochází ke snížení kvality snímků, a tedy bezpečnosti výsledného algoritmu. Obdobně nebude možné pořízené záznamy likvidovat v relativně krátkých lhůtách, které se vžily např. pro standardní kamerové systémy, neboť zde není účelem ad hoc odhalení a doložení určitého incidentu, ale naopak dlouhodobé využití záznamu k vývoji a dalšímu zdokonalování příslušných algoritmů.

Uvedená negativa (z pohledu subjektů údajů) bude proto nezbytné vyvážit zvýšeným důrazem na vyhodnocení rizik a přijetí opatření k jejich eliminaci. Stěžejní jsou v tomto ohledu opatření bezpečnostní, tj. organizační, fyzické i technické prostředky určené k zamezení přístupu neoprávněným osobám. Samozřejmostí je omezení přístupových oprávnění na limitovaný okruh osob, včetně zavedení interních kontrolních mechanismů.

Za těchto okolností by následně bylo možné označit shromažďování a další zpracování dat získaných pomocní palubních kamer i vně vozu za oprávněný zájem správce či třetí osoby, při jehož realizaci nedochází k zásahu do práv subjektů údajů v míře vyšší než nezbytné (tj. oprávněné zájmy subjektu údajů nepřevažují nad zájmy správce).

Co na to umělá inteligence?

Tématu tohoto příspěvku se přímo nevěnuje žádné stanovisko EDPB[4] a nezabývá se jím ani český dozorový úřad (ÚOOÚ).[5] Je však samozřejmě možné využít stanoviska a vodítka zabývající se obecně požadavky na souhlas a balančními testy publikovaná EDPB nebo národními dozorovými úřady.[6]

Shrnutí tématu můžeme nicméně nechat na umělé inteligenci samotné. Co odpoví na otázku, jaký můžeme očekávat další vývoj v oblasti sběru dat pro vývoj autonomních systémů?

„Další vývoj v oblasti sběru dat pro vývoj autonomních systémů bude pravděpodobně směřovat k vyšší kvalitě a přesnosti dat. Výrobci a vývojáři autonomních systémů se budou snažit získat co nejvíce kvalitních dat z různých zdrojů a tato data budou analyzovat a využívat k trénování svých algoritmů. Můžeme také očekávat vývoj nových technologií a senzorů, které budou schopny získat nové typy dat s vyšší přesností a rozlišením. Například lze očekávat pokrok v oblasti senzorů pro rozpoznávání hloubky, které mohou poskytnout detailnější informace o okolním prostředí a umožnit vozidlům lépe rozlišovat překážky. Zároveň by mělo docházet k dalšímu zdokonalování technologií pro ochranu soukromí, aby byla zajištěna co největší ochrana osobních údajů při sběru dat pro vývoj autonomních systémů. To může zahrnovat využití technologií pro anonymizaci a pseudonymizaci dat, zpřísnění pravidel pro sběr a ukládání dat a další opatření pro ochranu soukromí."

Ludmila Probstová
Autorka je GDPR specialistka ve společnosti Bosch.

4) Ve výše zmíněném stanovisku EDPB č. 1/2020 jsou kamery zmíněny spíše okrajově a výslovně je z jeho předmětu vyňato monitorování veřejných prostranství.
5) Stanovisko ÚOOÚ č. 1/2015, Provozování kamery v motorovém vozidle se záběrem mimo toto vozidlo, není již na webových stránkách tohoto úřadu dostupné. Z dohledatelných informací je však zřejmé, že se zabývalo výhradně kamerami instalovanými za účelem doložení okolností a průběhu dopravních nehod.
6) Např. stanovisko EDPB č. 5/2020, k souhlasu podle nařízení 2016/679. K balančním testům např. přehledný návod vypracovaný dozorovým úřadem pro Velkou Británii (Information Commissioner, https://ico.org.uk/).
7) OpenAI, (2023), ChatGPT, https://openai.com/blog/chatgpt/ k dotazu: Jaký můžeme očekávat další vývoj v oblasti sběru dat pro vývoj autonomních systémů? Odpověď ze dne 24. února 2023.

DPO PRO. Ročník III, číslo 3. Vychází každého 28. dne v měsíci v Praze. Cena ročního předplatného činí 1 990 Kč bez DPH. Vydávají SMS-služby s. r. o. se sídlem V Rovinách 40, 140 00 Praha 4-Podolí, IČ: 067 84 771. Adresa redakce: Národní 41, 110 00 Praha 1-Staré Město. Webové stránky: https://www.dpopro.cz. Minimální rozsah 12 stran A4. Evidenční číslo: MK ČR E 24123. ISSN 2695-1363. Šéfredaktorka: JUDr. et Mgr. Eva Janečková, eva.janeckova@sms-sluzby.cz. Redakční rada: JUDr. et Mgr. Eva Janečková, Ing. Mgr. Oldřich Kužílek, Ing. Michal Merta, MBA, MSc., LL.M., JUDr. Adam Furek. Jazyková redakce: Marie Machačová. Předplatné: Magdalena Komárková, magdalena.komarkova@sms-sluzby.cz, tel.: +420 723 644 867. Grafické práce: Studio Matrix. Redakční uzávěrka: 25. 3. 2023. Autorská práva vykonává vydavatel.