EDPB-EIOÚ

Společné stanovisko 5/2021

k návrhu nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci)

18. června 2021

Shrnutí

Dne 21. dubna 2021 představila Evropská komise svůj návrh nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (dále jen „návrh“). Evropský sbor pro ochranu osobních údajů (EDPB) a evropský inspektor ochrany údajů (EIOÚ) vítají zájem normotvůrce řešit otázky používání umělé inteligence (UI) v Evropské unii (EU) a zdůrazňují, že návrh má významné **důsledky v oblasti ochrany osobních údajů**.

EDPB a EIOÚ poznamenávají, že **právním základem** návrhu je v prvé řadě článek 114 Smlouvy o fungování Evropské unie (SFEU). Dále návrh vychází z článku 16 SFEU vzhledem k tomu, že obsahuje zvláštní pravidla ochrany fyzických osob v souvislosti se zpracováním osobních údajů, zejména omezení používání systémů UI pro biometrickou identifikaci na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva. EDPB a EIOÚ připomínají, že v souladu s judikaturou Soudního dvora EU (SDEU) v případě, kdy je ochrana osobních údajů jedním z hlavních účelů nebo jednou z hlavních složek pravidel přijímaných unijním normotvůrcem, poskytuje článek 16 SFEU náležitý právní základ. Použití článku 16 SFEU znamená také **nutnost zajistit nezávislý dohled nad dodržováním** požadavků týkajících se zpracování osobních údajů, jak to vyžaduje i ustanovení článku 8 Listiny základních práv EU.

Pokud jde o **oblast působnosti návrhu**, EDPB a EIOÚ velmi vítají, že se návrh vztahuje i na poskytování a používání systémů UI orgány, institucemi a jinými subjekty EU. **Vyloučení mezinárodní spolupráce v oblasti prosazování práva** z oblasti působnosti návrhu vzbuzuje však u EDPB a EIOÚ vážné obavy, protože představuje významné riziko obcházení právních předpisů (např. v případě třetích zemí nebo mezinárodních organizací provozujících vysoce rizikové aplikace, jejichž funkcí využívají veřejné orgány v EU).

EDPB a EOIÚ **vítají přístup založený na posouzení rizik**, z něhož návrh vychází. Tento přístup by však měl být vysvětlen a pojem „riziko pro základní práva“ by měl být sladěn s obecným nařízením o ochraně údajů (GDPR) a nařízením (EU) 2018/1725 (EUDPR), protože zde do hry vstupují aspekty související s ochranou osobních údajů.

EDPB a EIOÚ jsou dále s tvůrcem návrhu zajedno v tom, že klasifikace **systému UI jako vysoce rizikového** ještě sama o sobě neznamená, že **jeho používání musí být nezbytně zákonné** a uživatel jej může jako takový využívat. Je možné, že správce **bude muset splnit další požadavky vyplývající z právních předpisů EU o ochraně údajů**. Kromě toho by dodržování zákonných povinností vyplývajících z právních předpisů Unie (včetně předpisů o ochraně osobních údajů) mělo být předpokladem pro uvedení produktu s označením CE na evropský trh. V souladu s tím se EDPB a EIOÚ domnívají, že **požadavek na zajištění souladu s GDPR a EUDPR by měl být obsažen v hlavě III kapitole 2.** EDPB a EIOÚ navíc považují za nezbytné upravit postup posuzování shody stanovený v návrhu tak, aby posuzování shody *ex ante* u vysoce rizikových systémů UI prováděly vždy třetí strany.

Vzhledem k vysokému riziku diskriminace návrh zakazuje „hodnocení sociálního kreditu“, pokud je prováděno „v určitém časovém úseku“ nebo „orgány veřejné moci nebo jejich jménem“. Soukromé společnosti, jako jsou provozovatelé sociálních médií a cloudových služeb, ale mohou také zpracovávat obrovské množství osobních údajů a provádět hodnocení sociálního kreditu. **Budoucí nařízení o UI** by proto mělo obsahovat zákaz jakéhokoli druhu hodnocení sociálního kreditu.

Biometrická identifikace jednotlivců na dálku na veřejně přístupných místech představuje vysoké riziko zásahu do soukromého života jednotlivců s vážnými důsledky pro očekávání obyvatelstva, pokud jde o anonymitu na veřejných místech. Z těchto důvodů EDPB a EIOÚ **vybízejí k obecnému zákazu jakéhokoli používání UI k automatizovanému rozpoznávání lidských rysů na veřejně přístupných**

místech – například obličeje, ale také způsobu chůze, otisků prstů, DNA, hlasu, úhozů na klávesnici a dalších biometrických údajů nebo znaků chování, a to bez ohledu na okolnosti. **Zákaz** se doporučuje i v případě **systémů UI, které dělí jednotlivce na základě biometrických údajů do kategorií** podle etnického původu, pohlaví a politické nebo sexuální orientace nebo na základě jiných důvodů diskriminace podle článku 21 Listiny. EDPB a EIOÚ se dále domnívají, že využívání UI k **odvozování emocí fyzických osob je krajně nežádoucí a mělo by být zakázáno.**

EDPB a EIOÚ vítají **jmenování EIOÚ příslušným orgánem a orgánem dozoru nad trhem, pokud jde o dohled nad orgány, institucemi a subjekty Unie.** Úloha a úkoly EIOÚ by však měly být blíže upřesněny, zejména v souvislosti s jeho úlohou jakožto orgánu dozoru nad trhem. Budoucí nařízení o UI by navíc mělo jasně stanovit **nezávislost dozorových úřadů** při plnění jejich úkolů v oblasti dohledu a vymáhání.

Jmenování orgánů pro ochranu údajů jako vnitrostátních dozorových orgánů by zajistilo jednotnější regulační přístup a přispělo by k jednotnému výkladu ustanovení o zpracování údajů a zabránilo rozporům při jejich vymáhání mezi jednotlivými členskými státy. EDPB a EIOÚ se proto domnívají, že **by vnitrostátními dozorovými orgány podle článku 59 návrhu měly být jmenovány orgány pro ochranu údajů.**

Podle návrhu bude mít ústřední postavení v „Evropské radě pro umělou inteligenci“ Komise. To je v rozporu s potřebou nezávislosti evropského orgánu pro UI na jakémkoli politickém vlivu. Návrh by měl **poskytnout větší míru autonomie radě EAIB** v zájmu zajištění její nezávislosti a zajistit, aby mohla jednat z vlastního podnětu.

Vzhledem k rozšíření systémů umělé inteligence na jednotném trhu a pravděpodobnosti, že bude docházet k přeshraničním případům, zde existuje zásadní potřeba harmonizovaného prosazování a řádného rozdělení pravomocí mezi vnitrostátní dozorové orgány. EDPB a EIOÚ navrhují stanovit **mechanismus zaručující jednotné kontaktní místo pro jednotlivce dotčené touto právní úpravou, jakož i pro společnosti, a to v případě každého systému UI.**

Pokud jde o **pískoviště**, doporučují EDPB a EIOÚ **upřesnit jejich působnost a cíle**. Návrh by měl také jasně konstatovat, že právní základ těchto pískovišť by měl být v souladu s požadavky zakotvenými ve stávajícím rámci ochrany údajů.

V případě systému certifikace uvedeného v návrhu **chybí jasný vztah k právním předpisům EU v oblasti ochrany údajů** a dalším právním předpisům EU a členských států, které upravují každou „oblast“ vysoce rizikových systémů UI, a nejsou zde zohledněny **zásady minimalizace údajů a záměrné ochrany osobních údajů** jako jeden z aspektů, které je nutno zohlednit **před získáním označení CE**. EDPB a EIOÚ proto doporučují pozměnit návrh tak, aby byl upřesněn vztah mezi certifikáty vydanými podle tohoto nařízení a osvědčeními, pečetěmi a známkami dokládajícími ochranu údajů. A konečně, na přípravě a zavádění harmonizovaných norem a společných specifikací by se měly podílet orgány pro ochranu údajů.

Pokud jde o **kodexy chování**, považují EDPB a EIOÚ za **nezbytné upřesnit**, zda bude ochrana osobních údajů považována za jeden z „dalších požadavků“, které lze těmito kodexy chování upravit, a zajistit, aby „technické specifikace a řešení“ nebyly v rozporu s pravidly a zásadami stávajícího rámce ochrany údajů EU.

OBSAH

1 ÚVOD 5
2 ANALÝZA KLÍČOVÝCH ZÁSAD NÁVRHU 7
2.1 Oblast působnosti návrhu a vztah ke stávajícímu právnímu rámci 7
2.2 Přístup založený na posouzení rizik 8
2.3 Zakázaná použití UI 10
2.4 Vysoce rizikové systémy UI 13
2.4.1 Nutnost posouzení shody *ex ante* prováděného externími třetími stranami 13
2.4.2 Do oblasti působnosti nařízení musí spadat i systémy UI, které se již používají 13
2.5 Správa a Evropská rada pro umělou inteligenci 14
2.5.1 Správa 14
2.5.2 Evropská rada pro umělou inteligenci 15
3 INTERAKCE s rámcem ochrany osobních údajů 17
3.1 Vztah návrhu ke stávající unijní právní úpravě ochrany osobních údajů 17
3.2 Pískoviště a další zpracování (články 53 a 54 návrhu) 18
3.3 Transparentnost 19
3.4 Zpracování zvláštních kategorií údajů a údajů týkajících se trestných činů 20
3.5 Mechanismy dodržování předpisů 20
3.5.1 Certifikace 20
3.5.2 Kodexy chování 21
4 ZÁVĚR 23

Evropský sbor pro ochranu osobních údajů a evropský inspektor ochrany údajů

s ohledem na čl. 42 odst. 2 nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES[1],

s ohledem na Dohodu o EHP, a zejména přílohu XI a protokol 37 k uvedené dohodě ve znění rozhodnutí Smíšeného výboru EHP č. 154/2018 ze dne 6. července 2018[2],

s ohledem na žádost o společné stanovisko evropského inspektora ochrany údajů a Evropského sboru pro ochranu údajů ze dne 22. dubna 2021 k návrhu nařízení, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci),

PŘIJALI TOTO SPOLEČNÉ STANOVISKO

1 ÚVOD

1. Nástup systémů umělé inteligence („UI“) je zásadním okamžikem ve vývoji technologií a ve způsobu, jakým lidé s technologiemi komunikují. Umělá inteligence představuje soubor klíčových technologií, které ve společenské a hospodářské rovině výrazně změní náš každodenní život. Ve vztahu k UI se v několika příštích letech očekávají průlomová rozhodnutí vzhledem k tomu, jak nám UI pomáhá překonávat některé z největších výzev, před kterými dnes v mnoha oblastech stojíme, zdravotnictvím nebo veřejnou správou počínaje a mobilitou a školstvím konče.

2. Pokrok, který si od ní slibujeme, ale není zcela prostý rizik. A tato rizika jsou velmi závažná vzhledem k tomu, že s dopady systémů UI na jednotlivce a celou společnost máme zatím jen velmi omezené zkušenosti. Tvorba obsahu, prognózování nebo automatizované rozhodování v podání systémů UI pomocí technik strojového učení nebo logiky a pravidel pravděpodobnostního odvozování přinášejí něco zcela nového oproti situacím, kdy tyto činnosti provádějí na základě kreativního nebo teoretického uvažování lidé, kteří nesou plnou odpovědnost za související důsledky.

3. Umělá inteligence přinese větší množství prognóz, které lze provádět v řadě oblastí, počínaje měřitelnými korelacemi mezi údaji, které nejsou postižitelné lidským okem, ale jsou zjistitelné strojem, a tím nám usnadní život a vyřeší velké množství problémů, ale zároveň naruší naši schopnost kauzálního výkladu vzniklých výsledků do takové míry, že bude vážně zpochybněno samotné chápání pojmů transparentnosti, lidské kontroly a odpovědnosti za výsledky.

[1] Úř. věst. L 295, 21.11.2018, s. 39–98.
[2] Pokud se v tomto dokumentu hovoří o „členských státech”, rozumějí se tím „členské státy EHP“.

4. U systémů UI jsou v mnoha případech klíčovým východiskem autonomních rozhodnutí údaje (osobní i neosobní), a to bude mít nevyhnutelně významný dopad na životy jednotlivců hned na několika úrovních. EDPB a EIOÚ proto již v této fázi naléhavě upozorňují na to, že návrh nařízení, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (akt o umělé inteligenci) (dále jen „návrh“)[3] má **zásadní důsledky v oblasti ochrany osobních údajů**.

5. Svěření rozhodování na základě údajů strojům povede ke vzniku rizik pro práva a svobody jednotlivců, bude mít dopad na jejich soukromí a může přivodit újmu skupinám nebo dokonce společnostem jako celku. EDPB a EIOÚ zdůrazňují, že právo na soukromý život a právo na ochranu osobních údajů, které jsou v rozporu s předpokladem rozhodovací autonomie strojů coby základu koncepce UI, jsou pilířem hodnot EU tak, jak jsou tyto uznány ve Všeobecné deklaraci lidských práv (článek 12), Evropské úmluvě o lidských právech (článek 8) a Listině základních práv EU (dále jen „Listina“) (články 7 a 8). Sladění perspektivy růstu, kterou nabízejí aplikace UI, a ústředního a prvořadého postavení lidí ve vztahu ke strojům je velmi ambiciózním, nicméně zcela nezbytným cílem.

6. EDPB a EIOÚ vítají, že do tvorby nařízení byly zapojeny všechny zúčastněné strany hodnotového řetězce UI a že byly zavedeny konkrétní požadavky na poskytovatele řešení, protože ti sehrávají významnou úlohu v případě produktů, které využívají funkcí jejich systémů. Je ale nezbytné jasně vymezit a přiřadit odpovědnosti různých stran – uživatelů, poskytovatelů, dovozců nebo distributorů systémů UI. Zejména při zpracovávání osobních údajů by měla být zvláštní pozornost věnována souladu těchto úloh a odpovědností s pojmy správce a zpracovatel osobních údajů tak, jak jsou zakotveny v rámci ochrany údajů, protože tyto dva právní předpisy nejsou v tomto bodě zajedno.

7. EDPB a EIOÚ hodnotí kladně, že návrh přisuzuje důležitost pojmu lidského dohledu (článek 14). Jak již ale bylo uvedeno, vzhledem k výraznému potenciálnímu dopadu některých systémů UI na jednotlivce nebo skupiny jednotlivců by faktické ústřední postavení člověka mělo spočívat na vysoce kvalifikovaném lidském dohledu a zákonném zpracování, pokud jsou tyto systémy založeny na zpracování osobních údajů nebo v rámci plnění svého úkolu provádějí zpracování osobních údajů tak, aby bylo zajištěno, že bude respektováno právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování.

8. Kromě toho by vzhledem k datové náročnosti mnoha aplikací UI měl návrh prosazovat přijetí přístupu záměrné a standardní ochrany osobních údajů na všech úrovních a vybízet k účinnému provádění zásad ochrany osobních údajů (podle článku 25 GDPR a článku 27 EUDPR) prostřednictvím nejmodernějších technologií.

9. V neposlední řadě EDPB a EIOÚ zdůrazňují, že toto společné stanovisko se předkládá pouze jako předběžná analýza návrhu a nejsou jím dotčena případná další posouzení a stanoviska k dopadům návrhu a jeho slučitelnosti s právními předpisy EU o ochraně údajů.

[3] COM(2021) 206 final.

2 ANALÝZA KLÍČOVÝCH ZÁSAD NÁVRHU

2.1 Oblast působnosti návrhu a vztah ke stávajícímu právnímu rámci

10. Podle důvodové zprávy je **právním základem** návrhu v prvé řadě článek 114 SFEU, který stanoví přijetí opatření nezbytných pro vytvoření a fungování vnitřního trhu[4]. Kromě toho návrh vychází z článku 16 SFEU *vzhledem k tomu, že obsahuje zvláštní pravidla ochrany fyzických osob v souvislosti se zpracováním osobních údajů*, zejména omezení používání systémů UI pro biometrickou identifikaci na dálku „v reálném čase" na veřejně přístupných místech pro účely prosazování práva[5].

11. EDPB a EIOÚ připomínají, že v souladu s judikaturou Soudního dvora Evropské unie je v případě, kdy je ochrana osobních údajů jedním z hlavních účelů nebo jednou z hlavních složek pravidel přijímaných unijním normotvůrcem, poskytuje článek 16 SFEU náležitý právní základ[6]. Použití článku 16 SFEU znamená také nutnost zajistit nezávislý dohled nad dodržováním požadavků týkajících se zpracování osobních údajů, jak to vyžaduje i ustanovení článku 8 Listiny.

12. EIOÚ a EDPB připomínají, že již existuje komplexní rámec ochrany údajů přijatý na základě článku 16 SFEU, který tvoří obecné nařízení o ochraně osobních údajů (GDPR)[7], nařízení o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie (EUDPR)[8] a směrnice o prosazování práva[9]. Podle návrhu lze za založená na článku 16 SFEU, a tedy mající stejný právní základ jako GDPR, EUDPR nebo směrnice o prosazování práva, považovat pouze dodatečná omezení týkající se zpracování biometrických údajů obsažená v návrhu. To má na obecnější úrovni důležité důsledky pro vztah návrhu k GDPR, EUDPR a směrnici o prosazování práva, jak je uvedeno níže.

13. Pokud jde o **oblast působnosti návrhu**, EDPB a EIOÚ velmi vítají, že se návrh vztahuje i na používání systémů UI orgány, institucemi a jinými subjekty Unie. Vzhledem k tomu, že používání systémů UI těmito subjekty může mít rovněž významný dopad na základní práva jednotlivců, podobně jako u jejich používání v členských státech EU, je nezbytné, aby se nový regulační rámec pro UI vztahoval jak na členské státy EU, tak na instituce, úřady, orgány a agentury Unie, aby byl zajištěn soudržný přístup v celé Unii. Jelikož instituce, úřady, orgány a agentury Unie mohou vystupovat jako poskytovatelé i uživatelé systémů UI, považují EIOÚ

[4] Důvodová zpráva. s. 5.
[5] Důvodová zpráva, s. 6. Viz také bod 2 odůvodnění návrhu.
[6] Posudek ze dne 26. července 2017, *PNR Canada*, řízení o posudku 1/15, ECLI:EU:C:2017:592, bod 96.
[7] 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) Úř. věst. L 119, 4.5.2016, s. 1–88.
[8] Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES, Úř. věst. L 295, 21.11.2018, s. 39–98.
[9] Směrnice Evropského parlamentu a Rady (EU) 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, Úř. věst. L 119, 4.5.2016, s. 89–131.

a EDPB zcela za vhodné zahrnout tyto subjekty do oblasti působnosti návrhu na základě článku 114 SFEU.

14. EDPB a EIOÚ ale mají vážné obavy, pokud jde o vyloučení mezinárodní spolupráce v oblasti prosazování práva z působnosti podle čl. 2 odst. 4 návrhu. Tímto vyloučením vzniká významné riziko obcházení právních předpisů (např. v případě třetích zemí nebo mezinárodních organizací provozujících vysoce rizikové aplikace, jejichž funkcí využívají veřejné orgány v EU).

15. Při rozvoji a používání systémů UI bude v mnoha případech docházet ke zpracování osobních údajů. Je nanejvýš důležité upřesnit vztah tohoto návrhu ke stávajícím právním předpisům EU o ochraně osobních údajů. GDPR a EUDPR a směrnice o prosazování práva nejsou nijak dotčeny návrhem, který je doplňuje. Přestože v odůvodnění je objasněno, že využívání systémů UI by mělo být i nadále v souladu s právními předpisy o ochraně osobních údajů, **EDPB a EIOÚ důrazně doporučují v článku 1 návrhu upřesnit,** že pro jakékoli zpracování osobních údajů spadající do oblasti působnosti návrhu budou platit **právní předpisy Unie upravující ochranu osobních údajů**, zejména GDPR a EUDPR, směrnice o soukromí a elektronických komunikacích[10] a směrnice o prosazování práva. Rovněž by mělo být v příslušném bodu odůvodnění upřesněno, že návrh nemá za cíl ovlivnit uplatňování stávajících právních předpisů Unie upravujících zpracování osobních údajů, a to ani úkoly a pravomoci nezávislých dozorových úřadů příslušných k monitorování dodržování těchto nástrojů.

2.2 Přístup založený na posouzení rizik

16. EDPB a EOIÚ **vítají přístup založený na posouzení rizik**, z něhož návrh vychází. Návrh se vztahuje na všechny systémy UI, včetně systémů, u kterých nedochází ke zpracování osobních údajů, ale které i tak mohou mít dopad na zájmy nebo základní práva a svobody.

17. EDPB a EIOÚ poznamenávají, že některá ustanovení návrhu opomíjejí rizika pro skupiny jednotlivců nebo společnost jako celek (např. zvláště významné hromadné dopady, jako jsou skupinová diskriminace nebo vyjadřování politických názorů ve veřejném prostoru). Sbor EDPB a EIOÚ doporučují, aby byla stejným způsobem řešena a zmírněna i společenská/skupinová rizika, která představují systémy UI.

18. EDPB a EIOÚ jsou toho názoru, že by měl být vysvětlen přístup založený na posouzení rizik uvedený v návrhu a že pojem „riziko pro základní práva“ by měl být **sladěn s nařízením GDPR** v případech, kdy přicházejí ke slovu aspekty související s ochranou osobních údajů. Ať jde o koncové uživatele, jednoduše subjekty údajů nebo jiné osoby dotčené systémem UI, slepým místem návrhu se jeví být skutečnost, že v textu chybí jakýkoli odkaz na jednotlivce dotčeného systémem UI. Povinnosti uložené subjektům vůči dotčeným osobám by měly konkrétněji vycházet z ochrany jednotlivce a jeho práv. EDPB a EIOÚ proto naléhají na

[10] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) ve znění směrnice 2006/24/ES a směrnice 2009/136/ES.

normotvůrce, aby se v návrhu výslovně zabýval **právy a prostředky nápravy**, které jsou k dispozici jednotlivcům, kteří podléhají systémům UI.

19. EDPB a EIOÚ berou v potaz rozhodnutí stanovit taxativní výčet **vysoce rizikových systémů UI**. Toto rozhodnutí se může projevit černobíle, nízkou atraktivitou vysoce rizikových situací, což by mohlo podrývat celkový přístup založený na posouzení rizik, který je základem návrhu. Ve výčtu vysoce rizikových systémů UI uvedeném v přílohách II a III návrhu chybí některé případy použití, při kterých vznikají významná rizika, například využívání UI k určení pojistného nebo k posouzení lékařských ošetření nebo pro účely výzkumu v oblasti zdraví. EDPB a EIOÚ rovněž zdůrazňují, že tyto přílohy bude nutné pravidelně aktualizovat s cílem zajistit jejich odpovídající oblast působnosti.

20. V návrhu zaznívá požadavek, aby posouzení rizik prováděli **poskytovatelé** systémů UI. Ve většině případů ale budou správci (údajů) spíše **uživatelé** než poskytovatelé systémů UI (např. uživatel systému rozpoznávání obličejů je „správcem“, a podle tohoto návrhu tedy není vázán požadavky na poskytovatele vysoce rizikových systémů UI).

21. Kromě toho **nebude vždy možné, aby poskytovatel posoudil všechna použití** systému UI. Počáteční posouzení rizik se tedy bude týkat obecnějšího použití než je to, které provádí uživatel systému UI. I když z počátečního posouzení rizik provedeného poskytovatelem nevyplyne, že systém UI je podle návrhu „vysoce rizikový“, nemělo by to vyloučit **následné (podrobnější) posouzení** (posouzení vlivu na ochranu osobních údajů podle článku 35 GDPR, článku 39 EUDPR nebo článku 27 směrnice o prosazování práva), **které by měl provést uživatel systému** s přihlédnutím k podmínkám používání a konkrétním případům použití. Závěr o tom, zda je podle GDPR, EUDPR a směrnice o prosazování práva pravděpodobné, že určitý druh zpracování povede ke vzniku vysokého rizika, bude formulován nezávisle na návrhu. Klasifikace systému UI jako „vysoce rizikového“ vzhledem k jeho dopadu na základní práva však[11] **aktivuje domněnku „vysoké rizikovosti” podle GDPR, EUDPR a směrnice o prosazování práva, pokud dochází ke zpracovávání osobních údajů.**

22. **EDPB a EIOÚ jsou dále s tvůrcem návrhu zajedno v tom, že klasifikace systému UI jako vysoce rizikového ještě sama o sobě neznamená, že jeho používání musí být nezbytně zákonné a uživatel jej může jako takový využívat. Je možné, že správce bude muset splnit další požadavky vyplývající z právních předpisů EU o ochraně údajů.** Dále je třeba se v návrhu zabývat argumentací, na které spočívá článek 5 návrhu a podle které mohou být na rozdíl od zakázaných systémů vysoce rizikové systémy v zásadě přípustné, a odstranit ji zejména proto, že navrhované označení CE neznamená, že související zpracování osobních údajů je zákonné.

23. Dodržování zákonných povinností vyplývajících z právních předpisů Unie (včetně předpisů o ochraně osobních údajů) by však mělo být předpokladem pro uvedení produktu s označením

[11] Agentura Evropské unie pro základní práva (FRA) se již zabývala potřebou provádět posouzení dopadu na základní práva při využívání UI nebo souvisejících technologií. Ve své zprávě z roku 2020 „Správně zvládnutá budoucnost – Umělá inteligence a základní práva” agentura FRA poukázala na „úskalí ve využívání UI, například při prediktivní policejní práci, při formulaci lékařských diagnóz, v sociálních službách a v cílené reklamě“, a zdůraznila, že „soukromé a veřejné organizace by měly provádět posouzení toho, jak by UI mohla poškozovat základní práva“ s cílem omezit negativní dopady na jednotlivce.

CE na evropský trh. Za tímto účelem EDPB a EIOÚ **doporučují, aby byl do hlavy III kapitoly 2 návrhu zařazen požadavek na zajištění souladu s nařízeními GDPR a EUDPR**. Dodržení těchto požadavků musí být před získáním označení CE zkontrolováno (auditem třetí strany) v souladu se zásadou odpovědnosti. V souvislosti s tímto posouzením třetí stranou bude mít zvláštní význam počáteční posouzení dopadu prováděné poskytovatelem.

24. S ohledem na složitosti vyvolané vývojem systémů UI je třeba zdůraznit, že v důsledku technických vlastností systémů UI (např. druhu zastávaného přístupu k UI) mohou vznikat závažnější rizika. Proto by u každého posouzení rizik systému UI měly být **technické vlastnosti** posuzovány společně s **daným případem použití a okolnostmi**, za jakých bude systém nasazen.

25. S ohledem na výše uvedené EDPB a EIOÚ doporučují, aby bylo v návrhu stanoveno, že **poskytovatel** provede počáteční posouzení rizik dotčeného systému UI s **přihlédnutím k případům použití** (které budou upřesněny v návrhu – například doplněním ustanovení přílohy III bodu 1 písm. a), ve kterém nejsou uvedeny případy použití biometrických systémů UI), a že **uživatel** systému UI, (případně) v postavení správce údajů podle právní úpravy EU o ochraně osobních údajů, provede posouzení vlivu na ochranu osobních údajů podle podrobného popisu v článku 35 GDPR, článku 39 EUDPR a článku 27 směrnice o prosazování práva, a to nejen s ohledem na tyto technické vlastnosti a daný **případ použití**, ale **také na konkrétní okolnosti**, za kterých bude UI použita.

26. Kromě toho by měly být upřesněny některé pojmy uvedené v příloze III návrhu, například pojem „základní soukromé služby“ nebo malý poskytovatel využívající systémy UI pro posouzení úvěruschopnosti pro svou vlastní potřebu.

2.3 Zakázaná použití UI

27. EDPB a EIOÚ se domnívají, že **rušivé formy UI** – obzvláště ty, které mohou mít dopad na lidskou důstojnost – budou považovány za zakázané systémy UI podle článku 5 návrhu, namísto toho, aby byly klasifikovány jen jako „vysoce rizikové” podle přílohy III návrhu, jak je tomu například u těch uvedených v bodě 6. Týká se to zejména srovnávání údajů, která ve velkém měřítku postihují také osoby, které nezavdaly žádný nebo téměř žádný důvod k policejnímu sledování, nebo zpracování, u kterého je porušena zásada účelového omezení podle právní úpravy ochrany osobních údajů. Pro využívání UI při policejní práci a prosazování práva je nutné stanovit pravidla, která jsou specifická pro danou oblast, přesná, předvídatelná a přiměřená a která zohledňují zájmy dotčených osob a dopady na fungování demokratické společnosti.

28. Kvůli znění článku 5 návrhu hrozí, že budou tyto „hodnoty“ a zákaz systémů UI, které jsou s těmito hodnotami v rozporu, platit jen zdánlivě. Kritéria uvedená v článku 5, která musí být splněna, aby systém UI bylo možné označit za zakázaný, totiž **omezují rozsah tohoto zákazu** do takové míry, že by se v praxi mohlo ukázat, že nesplňují svůj účel (např. „[…] způsobuje nebo by mohlo způsobit fyzickou nebo psychickou újmu“ v ustanovení čl. 5 odst. 1 písm. a) a b); omezení na orgány veřejné moci v čl. 5 odst. 1 písm. c); vágní formulace v písmenu c)

a jeho bodech i) a ii); omezení výhradně na biometrickou identifikaci na dálku „v reálném čase“ bez jakékoli jasné definice atd.).

29. Zejména používání umělé inteligence pro účely „hodnocení sociálního kreditu“ podle ustanovení čl. 5 odst. 1 písm. c) návrhu může vést k diskriminaci a je v rozporu se základními hodnotami EU. Návrh zakazuje tyto praktiky, pouze pokud jsou prováděny „v určitém časovém úseku“ nebo „orgány veřejné moci nebo jejich jménem“. Soukromé společnosti, zejména provozovatelé sociálních médií a cloudových služeb, mohou zpracovávat obrovská množství osobních údajů a provádět hodnocení sociálního kreditu. **Návrh by proto měl obsahovat zákaz jakéhokoli druhu hodnocení sociálního kreditu**. V souvislosti s prosazováním práva je namístě poznamenat, že článek 4 směrnice o prosazování práva již výrazně omezuje – ne-li fakticky zakazuje – činnosti tohoto typu.

30. **Biometrická identifikace** jednotlivců na dálku na veřejně přístupných místech představuje vysoké riziko zásahu do soukromí jednotlivců. EDPB a EIOÚ se proto **domnívají, že je nutné zvolit přísnější přístup**. Využívání systémů UI může vyvolávat závažné důsledky v oblasti přiměřenosti, protože při něm může docházet ke zpracování údajů neurčitého a nepřiměřeného počtu subjektů údajů za účelem identifikace pouze několika jednotlivců (např. cestujících na letištích a nádražích). **Hladký provoz** systémů biometrické identifikace také vyvolává obavy, pokud jde o transparentnost, a otázky v souvislosti s právním základem zpracování podle práva EU (směrnice o prosazování práva a GDPR a EUDPR a další použitelné právní předpisy). Dosud nebyla upravena problematika řádného informování jednotlivců o tomto zpracování a také otázka efektivního a včasného uplatnění práv jednotlivců. Totéž platí pro **jeho nevratný a závažný dopad na** (důvodné) **očekávání obyvatelstva týkající se zachování anonymity při pobytu na veřejných místech**, což má přímý negativní dopad na výkon svobody projevu, shromažďování, sdružování a svobody pohybu.

31. Ustanovení čl. 5 odst. 1 písm. d) návrhu obsahuje rozsáhlý **seznam výjimečných případů**, ve kterých je povolena biometrická identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva. EDPB a EIOÚ považují **tento přístup za chybný** hned v několika směrech: Za prvé, není zřejmé, co přesně se rozumí „značným zpožděním“ a na jakém základě by značné zpoždění mělo být považováno za polehčující okolnost vzhledem k tomu, že systém hromadné identifikace je schopen během několika hodin identifikovat tisíce jednotlivců. Zásah do soukromí, který toto zpracování představuje, navíc nemusí vždy záviset na tom, zda se identifikace provádí v reálném čase či nikoli. Je pravděpodobné, že následná biometrická identifikace na dálku v souvislosti s politickým protestem bude mít značně odrazující účinek na uplatňování základních práv a svobod, jakými jsou svoboda shromažďování a sdružování a obecněji základní principy demokracie. Za druhé, zásah do soukromí spjatý se zpracováním nemusí nutně záviset na jeho účelu. Použití tohoto systému k jiným účelům, jako je bezpečnost soukromých osob, představuje stejnou hrozbu pro základní práva na respektování soukromého a rodinného života a ochranu osobních údajů. A konečně, i s předpokládanými omezeními bude potenciální počet podezřelých nebo pachatelů trestné činnosti téměř vždy „dostatečně vysoký“, aby bylo odůvodněno nepřetržité používání systémů UI pro zjišťování polohy podezřelých, a to navzdory dalším podmínkám stanoveným v čl. 5 odst. 2 až 4 návrhu. Zdá se, že v odůvodnění návrhu je opomenuto, že při monitorování

otevřených prostor je nutné dodržet povinnosti vyplývající z právních předpisů EU o ochraně údajů nejen v případě podezřelých, nýbrž všech osob, které jsou v praxi monitorovány.

32. Na základě všech těchto skutečností **vybízejí** EDPB a EIOÚ k **obecnému zákazu jakéhokoli používání UI k automatizovanému rozpoznávání lidských rysů na veřejně přístupných místech – například obličeje, ale také způsobu chůze, otisků prstů, DNA, hlasu, úhozů na klávesnici a dalších biometrických údajů nebo znaků chování, a to bez ohledu na okolnosti**. Současný přístup uvedený v návrhu spočívá v určení a výčtu všech systémů umělé UI, které by měly být zakázány. V zájmu důslednosti by tedy měly být podle článku 5 návrhu **zakázány všechny rozsáhlé systémy UI pro identifikaci na dálku v on-line prostorech**. S přihlédnutím ke směrnici o prosazování práva a nařízením EUDPR a GDPR nerozumí EIOÚ a EDPB tomu, jak by tato praxe mohla splňovat požadavky na nezbytnost a přiměřenost, které v konečném důsledku vyplývají z toho, co Soudní dvůr Evropské unie a ESLP považují za přijatelné zásahy do základních práv.

33. EDPB a EIOÚ navíc **doporučují** v případě veřejných orgánů i soukromých subjektů **zákaz používání systémů UI, které podle biometrických údajů (získaných například z rozpoznávání obličeje) rozřazují jednotlivce do skupin podle etického původu, pohlaví a politické či sexuální orientace nebo na základě jiných základů diskriminace zakázaných podle článku 21 Listiny, nebo** systémů UI, které nebyly vědecky ověřeny nebo které jsou v přímém rozporu se základními hodnotami EU (např. polygraf, příloha III bod 6 písm. b) a bod 7 písm. a)). V souladu s tím by měla být **podle článku 5 zakázána** „**biometrická kategorizace**“.

34. **Determinace nebo klasifikace budoucího chování počítačem bez ohledu na svobodnou vůli má důsledky i v oblasti důstojnosti člověka.** Systémy UI určené pro použití donucovacími orgány za účelem provádění individuálního posouzení rizik fyzické osoby s cílem posoudit riziko protiprávního jednání nebo opakovaného protiprávního jednání fyzických osob, srov. příloha III bod 6 písm. a), nebo za účelem předvídání výskytu nebo opětovného výskytu skutečné nebo potenciální trestné činnosti na základě profilování fyzické osoby nebo posuzování povahových vlastností a osobnostních rysů nebo dřívější trestné činnosti, srov. příloha III bod 6 písm. e), pokud budou používány v souladu s jejich zamýšleným účelem, povedou k zásadní podřízenosti rozhodování policejních a soudních orgánů a tím pádem i k objektivizaci dotčeného člověka. Tyto systémy UI, které se dotýkají samotné podstaty práva na lidskou důstojnost, by měly být zakázány podle článku 5.

35. EDPB a EIOÚ se dále domnívají, že **využívání UI k odvozování emocí fyzických osob je krajně nežádoucí a mělo by být zakázáno** s výjimkou některých přesně stanovených případů použití, zejména pro zdravotní nebo výzkumné účely (např. pacienti, u nichž má rozpoznávání emocí důležitý význam), ve kterých je ale nutné zajistit odpovídající záruky a pro které bude samozřejmě platit výhrada dodržení všech ostatních podmínek a omezení souvisejících s ochranou osobních údajů, včetně účelového omezení.

2.4 Vysoce rizikové systémy UI

2.4.1 Nutnost posouzení shody *ex ante* prováděného externími třetími stranami

36. EDPB a EIOÚ vítají, že systémy UI, které představují vysoké riziko, musí být před uvedením na trh nebo jiným uvedením do provozu v EU podrobeny předchozímu posouzení shody. Tento model úpravy je v zásadě žádoucí, neboť vhodně vyvažuje hodnotu vstřícnosti k inovacím a vysokou úroveň proaktivní ochrany základních práv. Aby mohly být systémy UI zprovozněny ve specifických prostředích, jako jsou rozhodovací procesy institucí veřejné služby nebo kritické infrastruktury, musí být stanoveny způsoby zkoumání úplného zdrojového kódu.

37. EDPB a EIOÚ podporují změnu postupu při posuzování shody podle článku 43 návrhu tak, aby **muselo být u vysoce rizikových systémů UI obecně prováděno posouzení shody *ex ante* třetí stranou**. Přestože se v GDPR ani EUDPR posouzení shody třetí stranou v případě vysoce rizikového zpracování osobních údajů nepožaduje, platí zde, že rizika, která představují systémy UI, teprve musíme plně pochopit. Obecné zařazení povinnosti posouzení shody třetí stranou by proto dále posílilo právní jistotu a důvěru ve všechny vysoce rizikové systémy UI.

2.4.2 Do oblasti působnosti nařízení musí spadat i systémy UI, které se již používají

38. Podle čl. 43 odst. 4 návrhu by pro vysoce rizikové systémy UI měl platit nový postup posuzování shody, který se uplatní vždy, když dojde k významné změně. Je správné zajistit, aby systémy UI splňovaly požadavky nařízení o UI v průběhu svého životního cyklu. Systémy UI, které byly uvedeny na trh nebo do provozu před nabytím účinností navrhovaného nařízení (nebo 12 měsíců poté u rozsáhlých systémů IT uvedených v příloze IX), jsou z jeho působnosti vyloučeny, pokud u nich nenastaly „významné změny“ návrhu nebo určeného účelu (článek 83).

39. Není ale jasné, kde se nachází mez, při jejímž překročení se již jedná o „významnou změnu“. Pokud jde o dolní mez, v bodě 66 odůvodnění návrhu se stanoví, že opětovné posouzení shody je nutné provést „pokaždé, když dojde ke změně, která může ovlivnit soulad daného systému“. Podobnou mez by bylo namístě stanovit i v případě článku 83, přinejmenším u vysoce rizikových systémů UI. Dále je s cílem odstranit mezery v ochraně nutné, aby systémy UI, které již byly zavedeny a jsou v provozu – po určité fázi provádění – také splňovaly všechny požadavky nařízení o UI.

40. Bezpečnost systémů UI ovlivňuje i mnohost variant zpracování osobních údajů a vnější rizika. Zaměření článku 83 na „významné změny návrhu nebo určeného účelu“ nezahrnuje odkaz na změny vnějších rizik. Do článku 83 návrhu by proto měl být zahrnut odkaz na změny variant hrozeb vyplývajících z vnějších rizik, např. kybernetických útoků, nepřátelských útoků a odůvodněných stížností spotřebitelů.

41. Navíc vzhledem k tomu, že budoucí nařízení nebude účinnost po uplynutí 24 měsíců od jeho vstupu v platnost, EIOÚ a EDPB nepovažují za vhodné vyjímat z jeho oblasti působnosti systémy UI, které již jsou na trhu ještě delší dobu. Přestože návrh rovněž stanoví, že požadavky nařízení budou zohledněny při hodnocení každého rozsáhlého systému IT, jak stanoví právní

akty uvedené v příloze IX, domnívají se EDPB a EIOÚ, že požadavky týkající se uvádění systémů UI do provozu by měly být použitelné ode dne nabytí účinnosti budoucího nařízení.

2.5 Správa a Evropská rada pro umělou inteligenci

2.5.1 Správa

42. EDPB a EIOÚ vítají jmenování EIOÚ příslušným orgánem a orgánem dozoru nad trhem, pokud jde o dohled nad orgány, institucemi a subjekty Unie, které spadají do oblasti působnosti návrhu. EIOÚ je připraven plnit svou novou úlohu regulátora UI ve veřejné správě EU. Kromě toho však úloha a úkoly EIOÚ nejsou v návrhu dostatečně rozvedeny a měly by být blíže upřesněny, zejména v souvislosti s úlohou EIOÚ jakožto orgánu dozoru nad trhem.

43. EDPB a EIOÚ berou na vědomí rozdělení finančních prostředků podle návrhu, se kterým se počítá v případě rady a EIOÚ, který funguje jako oznámený subjekt. Plnění nových povinností, které návrh předjímá v případě EIOÚ, bez ohledu na to, zda funguje jako oznámený subjekt, by ale vyžadovalo výrazně vyšší finanční a lidské zdroje.

44. Důvodem je zaprvé to, že podle ustanovení čl. 63 odst. 6 evropský inspektor ochrany údajů „jedná jako orgán dozoru nad trhem“ v případě orgánů, institucí a subjektů Unie spadajících do oblasti působnosti návrhu, což nevnáší světlo do toho, zda má být EIOÚ považován za plně ztělesněný „orgán dozoru nad trhem“ podle nařízení (EU) 2019/1020. To v praxi vyvolává otázky týkající se povinností a pravomocí evropského inspektora ochrany údajů. Za druhé, a za předpokladu, že bude na první otázku odpovězeno kladně, není zřejmé, jak by se mohl EIOÚ ve své úloze, jak ji vymezuje EUDPR, zhostit úkolu stanoveného v článku 11 nařízení (EU) 2019/1020, který zahrnuje „účinný dozor nad trhem na svém území u výrobků prodávaných on-line“ nebo provádění „fyzických a laboratorních kontrol na základě odpovídajících vzorků“. Existuje riziko, že převzetím nového souboru úkolů bez dalších vysvětlení v návrhu by mohlo být ohroženo plnění jeho povinností jako inspektora ochrany údajů.

45. EDPB a EIOÚ však zdůrazňují, že některá ustanovení návrhu, která vymezují úkoly a pravomoci různých příslušných orgánů podle nařízení o UI, jejich vztahy, jejich povahu a záruku jejich nezávislosti, se v této fázi zdají být nejasné. Zatímco v nařízení 2019/1020 se stanoví, že orgán dozoru nad trhem musí být nezávislý, v návrhu nařízení se nevyžaduje, aby byly dozorové úřady nezávislé, a dokonce je v něm uveden požadavek, aby Komisi podávaly zprávy o některých úkolech prováděných orgány dozoru nad trhem, kterými mohou být různé instituce. Jelikož se v návrhu také uvádí, že v případě systémů UI používaných pro účely prosazování práva (čl. 63 odst. 5) budou orgány dozoru nad trhem orgány pro ochranu údajů, znamená to také, že na ně bude, případně prostřednictvím jejich vnitrostátních dozorových orgánů, dopadat povinnost podávat zprávy Komisi (čl. 63 odst. 2), což se zdá být neslučitelné s jejich nezávislostí.

46. EDPB a EIOÚ se proto domnívají, že tato ustanovení je nutné upřesnit, aby byla v souladu s nařízeními 2019/1020, EUDPR a GDPR, a návrh by měl jasně stanovit, že dozorové úřady podle nařízení o UI musí být při plnění svých úkolů zcela nezávislé, protože se jedná o zásadní záruku řádného dohledu a prosazování budoucího nařízení.

47. EDPB a EIOÚ také připomínají, že v případě systémů UI, u kterých dochází ke zpracování osobních údajů, již orgány pro ochranu údajů vymáhají GDPR a EUDPR a směrnici o prosazování práva v zájmu ochrany základních práv, tedy konkrétně práva na ochranu údajů. Orgány pro ochranu údajů již tedy mají jistou představu o technologiích UI, zpracování dat a datových výpočtech a základních právech a také disponují odborností při posuzování rizik pro základní práva, která představují nové technologie, jak to návrh u vnitrostátních dozorových orgánů požaduje. Navíc pokud jsou systémy UI založeny na zpracování osobních údajů nebo osobní údaje zpracovávají, dochází k přímému propojení ustanovení návrhu s právním rámcem ochrany osobních údajů, což bude platit pro většinu systémů UI spadajících do oblasti působnosti nařízení. V důsledku toho dojde k propojení kompetencí mezi dozorovými úřady podle návrhu a orgány pro ochranu osobních údajů.

48. V důsledku toho by jmenování orgánů pro ochranu údajů jako vnitrostátních dozorových orgánů zajistilo jednotnější regulační přístup a přispělo by k jednotnému výkladu ustanovení o ochraně osobních údajů a zabránilo rozporům při jejich vymáhání mezi jednotlivými členskými státy. Pro všechny zúčastněné strany hodnotového řetězce v oblasti UI by rovněž bylo přínosem, pokud by existovalo jediné kontaktní místo pro všechny operace zpracování osobních údajů spadající do oblasti působnosti návrhu, a pokud by se omezily interakce mezi dvěma různými regulačními orgány pro zpracování, jichž se návrh a GDPR dotýká. EDPB a EIOÚ se proto domnívají, že **by vnitrostátními dozorovými orgány podle článku 59 návrhu měly být jmenovány orgány pro ochranu údajů.**

49. V každém případě, pokud návrh obsahuje zvláštní pravidla ochrany fyzických osob v souvislosti se zpracováním osobních údajů přijatá na základě článku 16 SFEU, dodržování těchto pravidel, zejména omezení používání systémů UI pro biometrickou identifikaci na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva, **musí podléhat kontrole nezávislých orgánů.**

50. Návrh však neobsahuje žádné výslovné ustanovení, které by svěřovalo pravomoc k zajištění dodržování těchto pravidel nezávislým orgánům. Jediný odkaz na příslušné dozorové úřady pro ochranu údajů podle GDPR nebo směrnice o prosazování práva se nachází v čl. 63 odst. 5 návrhu, ale pouze jako na orgány „dozoru nad trhem“ a případně s některými dalšími orgány. EDPB a EIOÚ se domnívají, že toto nastavení nezajišťuje dodržení požadavku na nezávislou kontrolu podle čl. 16 odst. 2 SFEU a článku 8 Listiny.

2.5.2 Evropská rada pro umělou inteligenci

51. Návrh zřizuje „Evropskou radu pro umělou inteligenci“. EDPB a EIOÚ uznávají potřebu důsledného a harmonizovaného uplatňování navrhovaného rámce a také zapojení nezávislých odborníků do vývoje politiky EU v oblasti UI. Návrh zároveň předpokládá, že rozhodující úlohu bude zastávat Komise. Ve skutečnosti by Komise nebyla pouhou součástí Evropské rady pro umělou inteligenci, nýbrž by byla i v jejím čele a měla by právo veta při přijímání jednacího řádu Evropské rady pro umělou inteligenci. To je v rozporu s potřebou nezávislosti evropského orgánu pro UI na jakémkoli politickém vlivu. EDPB a EIOÚ se proto domnívají, že budoucí nařízení o UI by mělo poskytnout Evropské radě pro umělou inteligenci **větší míru autonomie**,

aby Evropská rada pro umělou inteligenci mohla skutečně zajistit důsledné uplatňování nařízení na celém jednotném trhu.

52. EDPB a EIOÚ rovněž poznamenávají, že Evropské radě pro umělou inteligenci není svěřena žádná pravomoc, pokud jde o prosazování navrhovaného nařízení. Vzhledem k rozšíření systémů umělé inteligence na jednotném trhu a pravděpodobnosti, že bude docházet k přeshraničním případům, zde však existuje zásadní potřeba harmonizovaného prosazování a řádného rozdělení pravomocí mezi vnitrostátní dozorové orgány. EDPB a EIOÚ proto doporučují, aby byly v budoucím nařízení o UI stanoveny mechanismy spolupráce mezi vnitrostátními dozorovými orgány. EDPB a EIOÚ navrhují zavést mechanismus zaručující jednotné kontaktní místo pro jednotlivce dotčené právními předpisy a také pro společnosti v případě každého systému UI a aby mohla Evropská rada pro umělou inteligenci v případě organizací, jejichž činnost zasahuje více než polovinu členských států EU, určit vnitrostátní orgán, který bude odpovědný za prosazování nařízení UI v případě tohoto systému UI.

53. Dále, vzhledem k nezávislosti orgánů, které budou tvořit radu, bude rada oprávněna jednat z vlastního podnětu, a nikoli pouze poskytovat poradenství a pomoc Komisi. EDPB a EIOÚ proto zdůrazňují potřebu rozšíření úkolu přiděleného radě, který navíc ani neodpovídá úkolům uvedeným v návrhu.

54. Aby mohly být tyto účely naplněny, **musí mít Evropská rada pro umělou inteligenci dostatečné a vhodné pravomoci** a mělo by být vyjasněno i její právní postavení. Zejména v zájmu zachování relevantnosti věcné působnosti budoucího nařízení se zdá, že je nezbytné zapojit do jeho změn orgány odpovědné za jeho uplatňování. EDPB a EIOÚ proto doporučují, aby byla Evropská rada pro umělou inteligenci zmocněna navrhnout Komisi změny přílohy I, ve které jsou vymezeny techniky a přístupy UI, a přílohy III, ve které jsou uvedeny vysoce rizikové systémy UI podle čl. 6 odst. 2. Před případnou změnou těchto příloh by Komise měla rovněž konzultovat Evropskou radu pro umělou inteligenci.

55. Ustanovení čl. 57 odst. 4 návrhu předpokládá výměny informací mezi radou a jinými subjekty, úřady, agenturami a poradními skupinami Unie. S ohledem na její předchozí práci v oblasti UI a její odbornost v oblasti lidských práv EDPB a EIOÚ doporučují zvážit jmenování Agentury pro základní práva za jednoho z pozorovatelů rady.

3 INTERAKCE S RÁMCEM OCHRANY OSOBNÍCH ÚDAJŮ

3.1 Vztah návrhu ke stávající unijní právní úpravě ochrany osobních údajů

56. Jasně definovaný vztah mezi návrhem a stávajícími právními předpisy v oblasti ochrany údajů je základním předpokladem pro zajištění a podporu respektování a uplatňování acquis EU v oblasti ochrany osobních údajů. Tyto unijní právní předpisy, zejména GDPR, EUDPR a směrnice o prosazování práva, je nutné považovat za předpoklad, z nějž mohou vycházet další návrhy právních předpisů, aniž by byly dotčeny stávající právní předpisy a aniž by do těchto právních předpisů bylo jakkoli zasahováno, a to i pokud jde o pravomoci dozorových úřadů a správu.

57. Podle mínění EDPB a EIOÚ je proto důležité zcela zamezit tomu, že by byl návrh v jakémkoli bodě neslučitelný s GDPR a EUDPR a směrnicí o prosazování práva nebo že by s nimi byl v rozporu. Nejde zde jen o právní jistotu, ale také o snahu zabránit tomu, aby účinky návrhu znamenaly přímé nebo nepřímé ohrožení základního práva na ochranu osobních údajů podle článku 16 SFEU a článku 8 Listiny.

58. Zejména stroje se schopností samoučení mohou chránit osobní údaje jednotlivců, pouze pokud bude tato činnost koncepčně zakotvena. Zásadní význam má také možnost okamžitého uplatnění práv jednotlivců podle článku 22 (Automatizované individuální rozhodování, včetně profilování) GDPR nebo článku 23 EUDPR, a to bez ohledu na účely zpracování. V tomto ohledu musí být v systémech UI od samého počátku a bez ohledu na zvolený přístup UI nebo technickou architekturu zajištěna i další práva subjektů údajů související s právem na výmaz a právem na opravu podle právních předpisů o ochraně údajů.

59. V důsledku používání osobních údajů pro účely učení systémů UI mohou v jádru systému UI vznikat zkreslené vzorce rozhodování. Proto by měly být požadovány různé záruky a zejména kvalifikovaný lidský dohled nad takovými procesy s cílem zajistit, že budou respektována a zaručena práva subjektů údajů, a zamezit případným negativním dopadům na jednotlivce. Příslušné orgány by rovněž měly mít možnost navrhnout pokyny k posouzení zkreslení v systémech UI a napomáhat při výkonu lidského dohledu.

60. Subjekty údajů by měly být vždy, když jsou jejich údaje použity k učení a/nebo k predikci u systémů UI, informovány o právním základu takového zpracování a měla by jim být obecně vysvětlena logika (postup) a rozsah systému UI. V tomto ohledu by v těchto případech mělo být vždy zaručeno právo jednotlivců na omezení zpracování (článek 18 GDPR a článek 20 EUDPR) a právo na výmaz údajů (článek 16 GDPR a článek 19 EUDPR). Kromě toho by měl mít správce výslovnou povinnost informovat subjekt údajů o příslušných lhůtách pro vznesení námitky, omezení zpracování, výmaz údajů atd. Systém UI musí být schopen splnit všechny požadavky na ochranu údajů prostřednictvím odpovídajících technických a organizačních opatření. Dalším zdrojem transparentnosti by mělo být i právo na vysvětlení.

3.2 Pískoviště a další zpracování (články 53 a 54 návrhu)

61. Je důležité podporovat evropské inovace prostřednictvím nástrojů, jako je pískoviště, a to ve stávajících mezích práva a morálky. Pískoviště poskytuje příležitost k zajištění záruk potřebných k vybudování důvěry v systémy UI. Ve složitých prostředích může být pro odborníky aplikující UI obtížné správně vyvážit všechny zájmy. Zejména u malých a středních podniků s omezenými zdroji může provoz v regulačním pískovišti přinést rychlé poznatky a tím podpořit inovace.

62. V ustanovení čl. 53 odst. 3 návrhu se uvádí, že pískoviště nebudou mít vliv na pravomoci příslušných orgánů v oblasti dohledu a nápravy. Pokud má být toto vysvětlení užitečné, je dále zapotřebí vytvořit pokyny nebo návody, jak dosáhnout rovnováhy mezi tím, jak na jedné straně být dozorovým úřadem a na druhé straně prostřednictvím pískoviště poskytovat podrobné pokyny.

63. V čl. 53 odst. 6 se stanoví, že způsoby a podmínky fungování pískovišť jsou stanoveny v prováděcích předpisech. Je důležité, aby byly vytvořeny konkrétní pokyny k zajištění jednotnosti a podpory při zřizování a fungování pískovišť. Závazné prováděcí akty by však mohly omezit schopnost jednotlivých členských států přizpůsobovat si pískoviště svým potřebám a místním zvyklostem. EDPB a EIOÚ proto doporučují, aby namísto toho stanovila pokyny pro pískoviště rada.

64. Cílem článku 54 návrhu je poskytnout právní základ pro další zpracování osobních údajů pro účely vývoje určitých systémů UI ve veřejném zájmu v rámci regulačního pískoviště UI. Vztah mezi ustanoveními čl. 54 odst. 1 návrhu a čl. 54 odst. 2 a bodu 41 odůvodnění návrhu, a tedy i stávajícími právními předpisy EU o ochraně údajů, však zůstává nejasný. Základ pro „další zpracování“ už byl však stanoven v nařízeních GDPR a EUDPR. Zejména s ohledem na případy, kdy je ve veřejném zájmu povolit další zpracování; vyvažování zájmů správce a zájmů subjektu údajů nemusí nutně bránit inovaci. Článek 54 návrhu v současné době neřeší dvě důležité otázky: i) za jakých okolností a pomocí jakých (dodatečných) kritérií jsou váženy zájmy subjektů údajů a ii) zda se tyto systémy UI budou používat pouze v pískovišti. EDPB a EIOÚ vítají požadavek na unijní právní předpis nebo právní předpis členského státu při zpracování osobních údajů shromážděných podle směrnice o prosazování práva v pískovišti, ale doporučují blíže upřesnit, co se zde předpokládá, a to způsobem, který je v souladu s GDPR a EUDPR, zejména objasněním toho, že právní základ těchto pískovišť by měl být v souladu s požadavky stanovenými v čl. 23 odst. 2 GDPR a článku 25 EUDPR, a upřesnit, že u každého použití pískoviště musí být provedeno důkladné hodnocení. To platí také pro úplný seznam podmínek podle čl. 54 odst. 1 písm. b) až j).

65. Z některých dalších úvah týkajících se opakovaného použití údajů v článku 54 návrhu vyplývá, že provozování pískoviště je náročné na zdroje, a že lze proto realisticky předpokládat, že příležitost zúčastnit se dostane jen malý počet podniků. Z účasti na pískovišti by mohla plynout konkurenční výhoda. Možnost opakovaného použití údajů by vyžadovala pečlivé zvážení toho, jak vybrat účastníky, s cílem zajistit, že tito účastníci spadají do oblasti působnosti, aby nedocházelo k nespravedlivému zacházení. EDPB a EIOÚ se obávají, že umožnění

opakovaného použití údajů v rámci pískoviště bude znamenat odchýlení se od zásady odpovědnosti uvedené v GDPR, kde je odpovědnost svěřena správci údajů, nikoli příslušnému orgánu.

66. EDPB a EIOÚ se dále domnívají, že vzhledem k cílům pískoviště, kterými jsou vývoj, testování a ověřování systémů UI, nemohou pískoviště spadat do oblasti působnosti směrnice o prosazování práva. Zatímco směrnice o prosazování práva umožňuje opakované použití údajů pro účely vědeckého výzkumu, údaje zpracovávané pro tento sekundární účel podléhají GDPR nebo EUDPR, nikoli směrnici o prosazování práva.

67. Není jasné, co vše bude regulační pískoviště zahrnovat. Nabízí se otázka, zda navrhované regulační pískoviště zahrnuje infrastrukturu IT v každém členském státě s několika dalšími právními základy dalšího zpracování, nebo pouze zajišťuje přístup k regulačním odborným znalostem a poradenství. EDPB a EIOÚ naléhavě žádají normotvůrce, aby v návrhu tento pojem vysvětlil a aby jasně uvedl, že z regulačního pískoviště nevyplývá příslušným orgánům povinnost zajistit pro něj technickou infrastrukturu. V každém případě musí být podle tohoto vysvětlení příslušným orgánům poskytnuty odpovídající finanční a lidské zdroje.

68. A konečně by EDPB a EIOÚ chtěli zdůraznit rozvoj přeshraničních systémů UI, které budou k dispozici evropskému digitálnímu jednotnému trhu jako celku. V případě těchto systémů UI by se regulační pískoviště jako nástroj pro inovace nemělo stát překážkou přeshraničního rozvoje. EDPB a EIOÚ proto doporučují koordinovaný přeshraniční přístup, který bude i tak na vnitrostátní úrovni dostatečně dostupný všem malým a středním podnikům a bude nabízet společný rámec v celé Evropě, aniž by byl příliš omezující. Je třeba dosáhnout rovnováhy mezi evropskou koordinací a vnitrostátními postupy, aby nedocházelo ke konfliktnímu provádění budoucího nařízení o UI, které by bránilo inovacím v celé EU.

3.3 Transparentnost

69. EDPB a EIOÚ vítají, že vysoce rizikové systémy UI budou registrovány ve veřejné databázi (uvedené v článcích 51 a 60 návrhu). Na tuto databázi je třeba pohlížet jako na prostředek informování široké veřejnosti o rozsahu aplikace systémů UI a o známých nedostatcích a událostech, které by mohly ohrozit jejich fungování, a o nápravných opatřeních přijatých poskytovateli k jejich řešení a odstranění.

70. Klíčovou demokratickou zásadou je používání brzd a protivah. Skutečnost, že se povinnost transparentnosti nevztahuje na systémy UI používané k odhalování, prevenci, vyšetřování nebo stíhání trestných činů, tedy představuje příliš širokou výjimku. Je třeba rozlišovat mezi systémy UI, které se používají k odhalování nebo prevenci trestných činů, a systémy UI, jejichž cílem je vyšetřování nebo pomoc při stíhání trestných činů. Záruky v případě předcházení trestným činům a jejich odhalování musí být silnější, protože platí presumpce neviny. EDPB a EIOÚ navíc litují, že v návrhu chybí varování, což lze chápat tak, že je povoleno používání i neověřených, vysoce rizikových systémů nebo aplikací UI.

71. V případech, kdy z důvodu utajení není možná žádná transparentnost vůči veřejnosti nebo je možná jen ve velmi omezené míře, a to i v dobře fungující demokracii, by měly být zavedeny

záruky a dotčené systémy UI by měly být registrovány u příslušného dozorového úřadu a měly by být vůči němu transparentní.

72. Je velmi náročné zajistit transparentnost systémů UI. Plně kvantitativní rozhodovací přístup mnoha systémů UI, který se přirozeně liší od lidského přístupu, jenž se z velké části opírá o kauzální a teoretické uvažování, může být neslučitelný s potřebou předchozího podání srozumitelného vysvětlení strojových výsledků. Nařízení by mělo prosazovat nové, proaktivnější a včasnější způsoby informování uživatelů systémů UI o stavu (rozhodování), ve kterém se systém v kterémkoli okamžiku nachází, s podáváním včasných varování před potenciálními škodlivými výsledky, aby jednotlivci, do jejichž práv a svobod mohou autonomní rozhodnutí stroje zasahovat, mohli zareagovat nebo proti danému rozhodnutí podat opravný prostředek.

3.4 Zpracování zvláštních kategorií údajů a údajů týkajících se trestných činů

73. Zpracování zvláštních kategorií údajů v oblasti prosazování práva se řídí ustanoveními unijního rámce ochrany údajů, včetně směrnice o prosazování práva a právních předpisů, které ji provádějí do vnitrostátního práva. V návrhu zaznívá tvrzení, že návrh neposkytuje obecný právní základ pro zpracování osobních údajů, případně včetně zvláštních kategorií osobních údajů, srov. bod 41 odůvodnění. Zároveň podle ustanovení čl. 10 odst. 5 návrhu mohou „poskytovatelé těchto systémů zpracovávat zvláštní kategorie osobních údajů“. V témže ustanovení se navíc vyžadují další záruky a jsou zde uvedeny i příklady. Zdá se tedy, že návrh zasahuje do uplatňování GDPR, směrnice o prosazování práva a EUDPR. Ačkoli EDPB a EIOÚ vítají snahu zajistit dostatečné záruky, je zapotřebí soudržnější regulační přístup, protože se nezdá, že stávající ustanovení jsou dostatečně určitá, aby poskytovala právní základ pro zpracování zvláštních kategorií údajů, a musí být doplněna o další záruky, které ještě bude třeba posoudit. Kromě toho, v případech, kdy byly osobní údaje shromážděny na základě zpracování spadajícího do oblasti působnosti směrnice o prosazování práva, bude třeba vzít v úvahu případné další záruky a omezení vyplývající z vnitrostátních právních předpisů, kterými se provádí směrnice o prosazování práva.

3.5 Mechanismy dodržování předpisů

3.5.1 Certifikace

74. Certifikace je jedním z hlavních pilířů návrhu. Certifikační systém uvedený v návrhu vychází ze struktury subjektů (oznamující orgány/oznámené subjekty/Komise) a mechanismu posuzování shody/certifikace pokrývajícího povinné požadavky použitelné v případě vysoce rizikových systémů UI, a dále z evropských harmonizovaných norem podle nařízení (EU) č. 1025/2012 a společných specifikací, které stanoví Komise. Tento mechanismus se liší od certifikačního systému zaměřeného na zajištění dodržení pravidel a zásad ochrany osobních údajů uvedených v článcích 42 a 43 GDPR. Není však zřejmé, jak lze koordinovat certifikáty vydané oznámenými subjekty podle návrhu s osvědčeními, pečetěmi a známkami dokládajícími ochranu údajů podle GDPR, na rozdíl od toho, co je stanoveno pro jiné typy certifikací (viz čl. 42 odst. 2 s ohledem na certifikace vydané podle nařízení (EU) 2019/881).

75. Pokud jsou vysoce rizikové systémy umělé inteligence založeny na zpracování osobních údajů nebo pokud zpracovávají osobní údaje za účelem plnění své funkce, mohou být tyto nespojitosti

zdrojem právní nejistoty pro všechny dotčené orgány, protože mohou vést k situacím, kdy systémy UI certifikované podle návrhu označením shody CE budou moci být po uvedení na trh nebo do provozu používány způsobem, který není v souladu s pravidly a zásadami ochrany údajů.

76. V návrhu chybí jasný vztah k právní úpravě ochrany údajů i k dalším právním předpisům EU a členských států, které upravují jednotlivé „oblasti“ vysoce rizikových systémů UI uvedené v příloze III. Návrh by měl zejména obsahovat zásady minimalizace údajů a záměrné ochrany údajů jako jedno z hledisek, které je třeba vzít v úvahu před získáním označení CE vzhledem k možné vysoké míře zásahu vysoce rizikových systémů UI do základních práv na soukromí a ochranu osobních údajů a vzhledem k potřebě zajistit vysokou úroveň důvěry v systémy UI. EDPB a EIOÚ proto doporučují pozměnit návrh tak, aby byl upřesněn vztah mezi certifikáty vydanými podle tohoto nařízení a osvědčeními, pečetěmi a známkami dokládajícími ochranu údajů. A konečně, na přípravě a zavádění harmonizovaných norem a společných specifikací by se měly podílet orgány pro ochranu údajů.

77. V souvislosti s článkem 43 návrhu, který se týká posuzování shody, se zdá být odchylka od postupu posuzování shody podle článku 47 velmi široce pojatá, včetně nadměrného počtu výjimek, jako jsou výjimečné důvody veřejné bezpečnosti nebo ochrany života a zdraví osob, ochrany životního prostředí a ochrany klíčových průmyslových a infrastrukturních aktiv. Navrhujeme normotvůrci jejich zúžení.

3.5.2 Kodexy chování

78. Podle článku 69 návrhu Komise a členské státy podporují a usnadňují vypracovávání kodexů chování, které mají podpořit dobrovolné uplatňování požadavků platných pro vysoce rizikové systémy UI a dalších požadavků poskytovateli systémů UI, které nejsou vysoce rizikové. V souladu s bodem 78 odůvodnění GDPR doporučují EDPB a EIOÚ určit a vymezit synergie mezi těmito nástroji a kodexy chování stanovenými v GDPR, které podporují dodržování pravidel na ochranu osobních údajů. V této souvislosti je namístě objasnit, zda se ochrana osobních údajů považuje za jeden z těchto „dalších požadavků“, které mohou být upraveny v kodexech chování podle čl. 69 odst. 2. Rovněž je důležité zajistit, aby „technické specifikace a řešení“, které jsou upraveny v kodexech chování podle čl. 69 odst. 1 a jejichž cílem je podpořit dodržování požadavků uvedených v návrhu nařízení o UI, nebyly v rozporu s pravidly a zásadami GDPR a EUDPR. Dodržování těchto nástrojů poskytovateli systémů UI, které nejsou vysoce rizikové, pokud jsou tyto systémy založeny na zpracování osobních údajů nebo pokud zpracovávají osobní údaje v rámci plnění své funkce, by znamenalo přidanou hodnotu, protože by tím bylo zajištěno, že správce a zpracovatelé budou při používání těchto systémů schopni plnit své povinnosti v oblasti ochrany údajů.

79. Právní rámec pro důvěryhodnou UI by byl zároveň doplněn zapracováním kodexu chování s cílem posílit důvěru v používání této technologie způsobem, který je bezpečný a v souladu s právními předpisy, a to i v otázce respektování základních práv. Návrh těchto nástrojů by však měl být posílen stanovením mechanismů, jejichž účelem by bylo ověřit, zda tyto kodexy poskytují účinné „technické specifikace a řešení“ a stanoví „jasné cíle a klíčové ukazatele

výkonnosti umožňující měřit dosahování těchto cílů“ jako nedílné součásti těchto kodexů. Kromě toho absence jakéhokoli odkazu na (povinné) monitorovací mechanismy v případě kodexů chování, jejichž cílem je ověřit, zda poskytovatelé systémů UI, které nejsou vysoce rizikové, dodržují jejich ustanovení, a možnost, aby jednotliví poskytovatelé vypracovali (a sami zavedli) uvedené kodexy (viz bod 5.2.7 důvodové zprávy) mohou dále podrývat účinnost a vymahatelnost těchto nástrojů.

80. A konečně EDPB a EIOÚ žádají vysvětlení, pokud jde o typy iniciativ, které může Komise vyvíjet, podle bodu 81 odůvodnění návrhu „s cílem usnadnit snižování technických překážek bránících přeshraniční výměně dat pro účely rozvoje UI“.

4 ZÁVĚR

81. Přestože EDPB a EIOÚ vítají návrh Komise a domnívají se, že takové nařízení je nezbytné pro zajištění základních práv občanů a obyvatel EU, mají za to, že návrh je třeba v několika otázkách změnit s cílem zajistit jeho použitelnost a účinnost.

82. Vzhledem ke složitosti návrhu a problémům, které má řešit, zbývá ještě vykonat mnoho práce, než návrh umožní vznik dobře fungujícího právního rámce, který účinně doplní GDPR při ochraně základních lidských práv a zároveň podpoří inovace. EDPB a EIOÚ jsou i nadále připraveni poskytovat tomuto procesu podporu.

V Bruselu dne 18. června 2021

Za Evropský sbor pro ochranu osobních údajů	Za evropského inspektora ochrany údajů
Předseda	Inspektor
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI