



Brusel 12. září 2022
(OR. en)

12302/22

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

**Interinstitucionální spis:
2021/0106(COD)**

STANOVISKO PRÁVNÍ SLUŽBY¹

Odesílatel:	Právní služba
Předmět:	Návrh nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci – Vhodnost článků 114 a 16 SFEU jako právních základů ve vztahu k ustanovením vztahujícím se na donucovací a justiční orgány

I. ÚVOD

1. Navrhované nařízení stanoví harmonizovaná pravidla pro uvádění systémů umělé inteligence (dále jen „systémy UI“) na trh a do provozu v Unii (dále jen „navrhované nařízení“)².

¹ Tento dokument obsahuje právní poradenství, na které se vztahuje ochrana podle čl. 4 odst. 2 nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise a které Rada Evropské unie nezpřístupnila veřejnosti. Rada si vyhrazuje veškerá práva podle zákona ohledně jakéhokoli nepovoleného zveřejnění.

² Dokument 8115/21.

2. Na zasedání Pracovní skupiny pro telekomunikace a informační společnost dne 7. dubna 2022 se právní služba Rady vyjádřila k otázce vhodnosti dvojího právního základu (články 16 a 114 Smlouvy o fungování Evropské unie) pro navrhované nařízení o systémech UI. Podaná vysvětlení potvrdila, že články 16 a 114 Smlouvy o fungování Evropské unie (dále jen „SFEU“) jsou správnými právními základy návrhu a že použití čl. 87 odst. 2 SFEU namísto článku 114 SFEU není vhodné. Na žádost pracovní skupiny toto stanovisko v písemné podobě zachycuje a dále rozvádí příspěvek, který na uvedeném zasedání přednesl zástupce právní služby.
3. Systémy UI jsou definovány v čl. 3 odst. 1 navrhovaného nařízení. Obecně řečeno odpovídají určitým druhům softwaru. Navrhované nařízení se vztahuje jak na poskytovatele uvádějící systémy UI na trh, tak na poskytovatele uvádějící systémy UI do provozu. Rovněž se vztahuje i na uživatele. Poskytovatelem může být fyzická nebo právnická osoba, orgán veřejné moci/subjekt, které vyvíjí nebo nechávají vyvíjet systém UI za účelem jeho uvedení na trh nebo do provozu pod svým vlastním jménem nebo ochrannou známkou. Uživatelem může být jakákoli fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, které v rámci své pravomoci využívají systém UI.

4. Podle definic v článku 3 by donucovací a justiční orgány mohly být považovány za poskytovatele nebo uživatele systému UI. Systémy UI, jejichž zamýšleným účelem, jak je definován poskytovatelem, je prosazování práva nebo výkon spravedlnosti, jsou podle přílohy III klasifikovány jako vysoce rizikové. Jako takové podléhají základním požadavkům (řízení rizik, testování, správa dat, technická dokumentace, transparentnost, lidský dohled, přesnost, spolehlivost a kybernetická bezpečnost) a povinnostem (jako jsou systémy řízení kvality, technická dokumentace, posuzování shody, nápravná opatření, informační povinnost, povinnosti dovozců a distributorů), jakož i normám a posuzování shody. Tato harmonizovaná pravidla vycházejí z pravidel, která se vztahují na bezpečnost výrobků ve směrnici 2006/42/ES (stroje)³ a nařízení 2017/745 (zdravotnické prostředky)⁴.
5. Systémy UI zahrnující používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva spadají do kategorie zakázaných systémů UI. Tento zákaz používání systémů UI však podléhá výjimkám. Používání těchto systémů totiž může, ale nemusí být povoleno členskými státy. Pokud jsou povoleny, vztahují se na ně podrobná omezení a záruky, aby bylo omezeno jejich použití na to, co je nezbytně nutné, a aby bylo chráněno základní právo na ochranu osobních údajů. Uvedená omezení a záruky jsou stanoveny v navrhovaném nařízení na základě článku 16 SFEU a musí být doplněny vnitrostátními právními předpisy. Ustanovení čl. 5 odst. 1 písm. d) a čl. 5 odst. 2, 3 a 4 navrhovaného nařízení představují *lex specialis* ke směrnici 2016/680 (směrnice o ochraně údajů při prosazování práva), která byla přijata na základě čl. 16 odst. 2 SFEU.

³ Směrnice Evropského parlamentu a Rady 2006/42/ES ze dne 17. května 2006 o strojních zařízeních a o změně směrnice 95/16/ES, Úř. věst. L 157, 9.6.2006, s. 24.

⁴ Nařízení Evropského parlamentu a Rady (EU) 2017/745 ze dne 5. dubna 2017 o zdravotnických prostředcích, změně směrnice 2001/83/ES, nařízení (ES) č. 178/2002 a nařízení (ES) č. 1223/2009 a o zrušení směrnic Rady 90/385/EHS a 93/42/EHS, Úř. věst. L 117, 5.5.2017, s. 1.

V souladu s čl. 5 odst. 1 písm. d) jsou cíle těchto systémů omezeny na:

- i) cílené vyhledávání určitých potenciálních obětí trestných činů, včetně pohřešovaných dětí;
- ii) prevenci konkrétního, závažného a bezprostředního ohrožení života nebo fyzické bezpečnosti fyzických osob nebo teroristického útoku;
- iii) odhalování, lokalizaci, identifikaci nebo stíhání pachatelů nebo osob podezřelých z trestného činu uvedeného v čl. 2 odst. 2 rozhodnutí o evropském zatýkacím rozkazu⁵, pokud lze tento trestný čin v dotčeném členském státě potrestat trestem odnětí svobody nebo ochranným opatřením spojeným s odnětím osobní svobody s horní hranicí sazby v délce nejméně tři roky, jak je stanoveno v právních předpisech tohoto členského státu.

Podle čl. 5 odst. 3 musí použití těchto technologií donucovacími orgány podléhat předchozímu povolení ze strany justičního nebo správního orgánu. V řádně odůvodněné naléhavé situaci však může být používání systému zahájeno bez povolení a o povolení lze požádat až v průběhu používání nebo po něm.

Podle čl. 5 odst. 4 může členský stát rozhodnout o povolení používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva a vymezit nezbytná podrobná pravidla pro žádost, vydávání a výkon předchozího povolení, jakož i trestné činy, na které se povolení vztahuje.

6. Právním základem navrhovaného nařízení jsou články 16 SFEU (ochrana osobních údajů) a 114 SFEU (fungování vnitřního trhu). Vystává proto otázka vhodnosti těchto právních základů ve vztahu k harmonizovaným pravidlům vztahujícím se na systémy UI poskytované nebo používané donucovacími a justičními orgány.

⁵ Rámcové rozhodnutí Rady 2002/584/SVV ze dne 13. června 2002 o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy, Úř. věst. L 190, 18.7.2002, s. 1.

7. Toto stanovisko se zaměřuje nejprve na vhodnost článku 114 SFEU jakožto právního základu ve zvláštním kontextu donucovacích orgánů, které jsou zmíněny v několika ustanoveních navrhovaného nařízení, tj. pokud jde o systémy biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech a vysoce rizikové systémy UI uvedené v bodě 6 přílohy III. Zabývá se proto otázkou, zda by nebyl vhodnějším právním základem pro poskytování a používání systémů UI donucovacími orgány namísto článku 114 SFEU (oddíl II) čl. 87 odst. 2 SFEU (policejní spolupráce). Závěr této poznámky lze obdobně použít na justiční orgány uvedené v příloze III ohledně vysoce rizikových systémů UI.
8. Tato poznámka se rovněž zabývá vhodností dodatečného právního základu, kterým je článek 16 SFEU, a uplatněním protokolů č. 21 a 22 v souvislosti s používáním systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech donucovacími orgány (oddíl III).

II. VHODNOST ČLÁNKU 114 SFEU JAKO PRÁVNÍHO ZÁKLADU

9. Podle ustálené judikatury nezávisí právní základ aktu Unie na přesvědčení orgánu ohledně sledovaného cíle, nýbrž musí být stanoven v souladu s objektivními kritérii, která mohou být předmětem soudního přezkumu, a to zejména včetně cíle a obsahu opatření. Pokud přezkum opatření ukáže, že sleduje dvojí účel nebo že má dvě složky a jeden z těchto účelů nebo jednu z těchto složek je možné označit za hlavní nebo převažující, zatímco druhý účel nebo složka je pouze vedlejší, musí být toto opatření založeno na jediném právním základu, a sice na tom, který je vyžadován hlavním nebo převažujícím účelem nebo složkou. Pouze výjimečně, prokáže-li se, že akt sleduje současně několik cílů, které jsou neoddělitelně spjaté, aniž by jeden byl vůči druhému vedlejší a nepřímý, může být takový akt založen na různých odpovídajících právních základech, pokud tyto právní základy nepředepisují postupy, které jsou vzájemně neslučitelné. Je třeba rovněž poznamenat, že čl. 114 odst. 1 první věta SFEU jasně stanoví, že ustanovení článku se použijí, „[n]ení-li ve Smlouvách stanoveno jinak“. Použití článku 114 je tedy odůvodněno pouze tehdy, nemůže-li konkrétnější ustanovení představovat právní základ pro přijetí daného opatření⁶. Pokud Smlouva obsahuje konkrétnější ustanovení, které by mohlo být právním základem dotčeného opatření, mělo by se toto opatření zakládat na daném ustanovení⁷.

⁶ Stanovisko právní služby Rady ze dne 17. května 2016, 9007/16, bod 6.

⁷ Rozsudek ze dne 29. dubna 2004 ve věci C-338/01, *Komise v. Rada*, EU:C:2004:253, bod 60.

A. CÍL NAVRHOVANÉHO NAŘÍZENÍ

10. Navrhované nařízení harmonizuje uvádění na trh, uvádění do provozu a používání konkrétního typu softwaru (systémů UI). Skutečnost, že poskytovatelé nebo uživatelé těchto systémů UI mohou být orgány veřejné moci a soukromí provozovatelé, není sama o sobě neslučitelná s právním základem v podobě článku 114 SFEU⁸.
11. Dále skutečnost, že mezi poskytovatele nebo uživatele těchto systémů UI mohou patřit donucovací orgány nebo osoby jednající jejich jménem, nepostačuje k odůvodnění použití článku 87 SFEU jako právního základu. Aby bylo možné určit, zda je použití uvedeného článku nezbytné, je třeba analyzovat cíl a obsah navrhovaného nařízení.
12. Obecně je cílem navrhovaného nařízení, a to i pokud jde o systémy biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech a vysoce rizikové systémy UI, zajistit jednotnou a vysokou úroveň ochrany v celé Unii a zároveň zabránit rozdílům, které jsou překážkou volnému pohybu systémů UI a souvisejících produktů a služeb na vnitřním trhu. Stanoví jednotné povinnosti pro provozovatele a zaručuje jednotnou ochranu naléhavých důvodů obecného zájmu a práv osob na celém vnitřním trhu (2. bod odůvodnění). Konkrétně stanoví navrhované nařízení pravidla regulující uvádění určitých systémů UI na trh a do provozu, čímž zajišťuje bezproblémové fungování vnitřního trhu a umožňuje, aby tyto systémy měly prospěch ze zásady volného pohybu zboží a služeb (5. bod odůvodnění). Celkově se návrh nařízení snaží zavést důvěryhodnou umělou inteligenci již od fáze jejího návrhu, která by byla použitelná ve všech oblastech a obsahovala úplný soubor pravidel pro vývoj, uvádění na trh a používání produktů, služeb a systémů založených na UI. Vzhledem k tomu, že umělá inteligence si již našla cestu do velkého počtu služeb a produktů a bude tomu tak i v budoucnu, vychází návrh z logiky vnitřního trhu tím, že stanoví „rámec pro bezpečnost produktů“, který je založen na souboru čtyř kategorií rizik. Ukládá požadavky na vstup na trh a certifikaci vysoce rizikových systémů UI prostřednictvím povinného postupu označování CE.

⁸ Viz stanovisko právní služby Rady (ST 11395/14, body 39 až 41) a precedenty, jako je směrnice (EU) 2016/2102, směrnice 2014/24/EU, 2014/25/EU a 2014/23/EU.

13. Žádný z uvedených cílů navrhovaného nařízení se netýká zajištění cílů veřejné bezpečnosti. I když má být cílů veřejné bezpečnosti dosaženo nepřímo prostřednictvím procesu harmonizace uvádění na trh/uvádění do provozu/používání systémů UI donucovacími orgány, Soudní dvůr⁹ při výkladu čl. 87 odst. 2 SFEU ve světle článku 67 SFEU uvedl, že k tomu, aby byl akt Unie s ohledem na svůj účel a obsah založen na čl. 87 odst. 2 SFEU, musí mít přímý vztah s cíli stanovenými v článku 67 SFEU (tj. v tomto případě předcházením trestné činnosti a policejní spoluprací). To je v souvislosti s navrhovaným nařízením vyloučeno, neboť jedinými harmonizovanými pravidly pro používání těchto systémů donucovacími orgány jsou buď 1) pravidla bezpečnosti produktů, která se jednotně uplatňují na všechny poskytovatele a uživatele ve vztahu k uvádění na trh/uvádění do provozu nebo používání systémů UI, nebo 2) pravidla pro ochranu osobních údajů, pro něž byl doplněn jako právní základ článek 16 SFEU (viz část III níže).
14. V jiné věci¹⁰, i když cílem změny směrnice o palných zbraních bylo zajištění vyšší úrovně veřejné bezpečnosti v souvislosti s hrozbami terorismu a jiné trestné činnosti, Soudní dvůr rozhodl, že harmonizace aspektů týkajících se bezpečnosti zboží je jedním ze zásadních faktorů pro zajištění řádného fungování vnitřního trhu, neboť odlišné právní úpravy v této oblasti mohou vytvářet překážky obchodu¹¹.

⁹ Rozsudek ze dne 6. května 2014, *Evropská komise v. Evropský parlament a Rada Evropské unie*, C-43/12, EU:C:2014:298.

¹⁰ Rozsudek ze dne 3. prosince 2019, *Česká republika v. Evropský parlament*, C-482/17, EU:C:2019:1035.

¹¹ Tamtéž, bod 57: „Na rozdíl od tvrzení Polské republiky je přitom charakteristikou palných zbraní jejich nebezpečnost nejen pro uživatele, ale také pro širokou veřejnost, jak již Soudní dvůr uvedl v bodě 54 rozsudku ze dne 23. ledna 2018, *Buhagiar a další*, C- 267/16, EU:C:2018:26, a proto se úvahy spojené s veřejnou bezpečností jeví – jak je připomenuto v pátém bodě odůvodnění směrnice 91/477 – při regulaci nabývání a držení tohoto zboží nezbytné“. Viz rovněž rozsudek ze dne 23. ledna 2018, *Albert Buhagiar a další v. Minister for Justice*, C-267/16, EU:C:2018:26, bod 54: „V tomto ohledu je třeba poznamenat, že s ohledem na riziko pro bezpečnost osob, které představují palné zbraně, mohlo být jejich volného pohybu dosaženo pouze prostřednictvím striktního vymezení podmínek pro jejich přepravu mezi členskými státy, mezi něž patří zásada předchozího povolení vydaného členskými státy, jichž se týká přeprava takového zboží“.

15. Cíle navrhovaného nařízení včetně ustanovení čl. 5 odst. 1 písm. d), čl. 5 odst. 2, 3 a 4 o používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva a ustanovení týkajících se vysoce rizikových systémů UI uvedených v bodě 6 přílohy III nemají přímý vztah k cíli veřejné bezpečnosti. Návrh naopak reaguje na hlavní obavy týkající se toho, jaký mají systémy UI dopad na zdraví, bezpečnost a základní práva. Příslušná ustanovení mají proto přímý vztah k cíli, kterým je zajistit rovné podmínky při uvádění na trh/uvádění do provozu nebo používání systémů UI na vnitřním trhu a zároveň chránit zdraví, bezpečnost a základní práva uživatelů.
16. S ohledem na výše uvedené je hlavním cílem navrhovaného nařízení zlepšit fungování vnitřního trhu ve smyslu článku 114 SFEU a cíle uvedené v článku 67 SFEU jsou s tímto hlavním cílem spojeny pouze nepřímo a podružně.

B. OBSAH NAVRHOVANÉHO NAŘÍZENÍ

17. Navrhované nařízení především obsahuje pravidla týkající se toho, co je nezbytné k uvedení konkrétního produktu (software UI) na trh (nebo jeho uvedení do provozu), aby bylo zajištěno, že je bezpečný a respektuje základní práva. Stanoví úplný soubor pravidel pro vývoj, uvádění na trh a používání produktů, služeb a systémů založených na umělé inteligenci. Navrhované nařízení donucovacím orgánům neukládá povinnost používat určitý systém UI, který je v souladu s právními předpisy uveden na trh, ani přímo neupravuje, jak by měly donucovací orgány takový systém UI používat. Namísto toho jasně vymezuje situace, kdy je zamýšlené použití považováno za vysoce rizikové pouze z toho důvodu, že určitý systém UI budou používat donucovací nebo justiční orgány.

18. Článek 29 navrhovaného nařízení mimochodem obsahuje pravidla týkající se podmínek pro používání vysoce rizikových systémů UI, avšak takové ustanovení není specifické pro dané odvětví, má omezenou oblast působnosti (zejména se týká návodu k použití výrobku) a je neoddělitelně spjata s povinnostmi, které jsou v rámci navrhovaného nařízení uloženy vývojářům systémů UI. Poskytuje rovněž členským státům určitou volnost pro stanovení dalších pravidel pro používání těchto vysoce rizikových systémů UI. Pokud jde o systémy biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech používané pro účely prosazování práva (článek 5), navrhované nařízení částečně upravuje používání těchto systémů z hlediska ochrany údajů na základě článku 16 SFEU (viz část III níže).
19. Kromě toho pouze členské státy mohou rozhodnout, že umožní zcela nebo částečně povolit používání takových systémů biometrické identifikace na dálku „v reálném čase“. Zvláštní podmínky pro takové použití je třeba stanovit ve vnitrostátním právu, avšak musí dodržovat obecná kritéria a záruky stanovené v nařízení: předchozí justiční nebo správní povolení, žádost, vydání a výkon předchozího povolení, jakož i uvedení trestných činů, ve vztahu k nimž lze tyto systémy použít.

20. Systémy UI jsou zvláštním druhem softwaru. Harmonizovaná pravidla vztahující se na uvádění těchto systémů na trh nebo do provozu či na jejich používání jsou tedy podobná harmonizovaným pravidlům pro bezpečnost výrobků. Uplatňují se jednotně, aniž by rozlišovala mezi veřejnými a soukromými uživateli. Podle relevantních bodů odůvodnění navrhovaného nařízení by proto měla být v celé Unii zajištěna jednotná a vysoká úroveň ochrany. Zároveň je třeba zabránit rozdílům, které by bránily volnému pohybu systémů UI a souvisejících produktů a služeb v rámci vnitřního trhu. Toho by bylo dosaženo stanovením jednotných povinností pro provozovatele a zaručením jednotné ochrany naléhavých důvodů obecného zájmu a práv osob na celém vnitřním trhu na základě článku 114 SFEU¹².
21. Navrhované nařízení obsahuje v příloze III o vysoce rizikových systémech UI (body 6, 7 a 8) několik odkazů na prosazování práva, řízení ochrany hranic a výkon spravedlnosti. Tyto odkazy zahrnují podrobný a vyčerpávající výčet odpovídající čl. 6 odst. 2, který obsahuje systémy, jež jsou kromě dalších vysoce rizikových systémů v souvislosti s bezpečnostními riziky výrobků uvedenými v čl. 6 odst. 1 rovněž považovány za vysoce rizikové. Podle čl. 6 odst. 1 mají být některé systémy UI ze své podstaty považovány za vysoce rizikové, a to z důvodu jejich očekávané závažnosti a vysokých rizik z hlediska základních práv, zdraví a bezpečnosti. Mezi další systémy považované za vysoce rizikové, které jsou uvedeny v příloze III, patří systémy v oblasti vzdělávání, řízení kritické infrastruktury, zaměstnanosti, biometrické identifikace a kategorizace, jakož i přístupu k základním veřejným a soukromým službám.

¹² Je proto nezbytné zavést právní rámec Unie, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci, s cílem podpořit vývoj, využívání a zavádění umělé inteligence na vnitřním trhu, který by zároveň splňoval vysokou úroveň ochrany veřejných zájmů, jako je například zdraví, bezpečnost a ochrana základních práv, které jsou uznány a chráněny právem Unie. K dosažení tohoto cíle by měla být stanovena pravidla, která budou regulovat uvádění určitých systémů UI na trh a do provozu, a tím zajišťovat bezproblémové fungování vnitřního trhu a umožňovat, aby tyto systémy měly prospěch ze zásady volného pohybu zboží a služeb (viz 2. a 5. bod odůvodnění návrhu).

22. V těchto pravidlech pro vysoce rizikové systémy UI se však nestanoví, zda by donucovací a justiční orgány (nebo orgány v ostatních určených oblastech) měly uvedené systémy používat, či nikoli. Navrhované nařízení bude mít na faktický vývoj systémů UI, které mohou donucovací orgány používat, a na systémy UI používané v současné době i v budoucnu dopady pouze nepřímo. V pravidlech se tedy odkazuje na systémy UI, které jsou „*určené k použití*“ těmito orgány (viz např. čl. 3 bod 12, čl. 8 odst. 2 a příloha III). Důsledkem zařazení určitého systému UI na seznam vysoce rizikových systémů je uplatňování zvláštního souboru pravidel pro řízení rizik, správu dat a technické specifikace. Uživatelé těchto vysoce rizikových systémů UI musí dodržovat návod k použití, vést příslušné protokoly a provádět posouzení vlivu na ochranu osobních údajů.
23. Kromě toho mohou být v unijních nebo vnitrostátních právních předpisech stanoveny jiné povinnosti uživatelů než ty, které se týkají návodu k použití, aniž je dotčena volnost uživatelů při organizaci vlastních zdrojů a činností za účelem provádění opatření v oblasti lidského dohledu uvedených poskytovatelem (čl. 29 odst. 2 navrhovaného nařízení). V těchto pravidlech se stanoví další záruky základních práv týkající se vysoce rizikových systémů UI.

24. S ohledem na výše uvedené skutečnost je třeba zdůraznit, že navrhované nařízení neobsahuje pravidla, jejichž cílem je umožnit, aby byl vysoce rizikový systém UI uvedený na trh používán donucovacími orgány, nebo tomu zabránit. V důsledku navrhovaných pravidel se zvláštní označení (vysoce rizikový) pro systém UI vyvinutý nebo používaný donucovacími orgány použije na základě jeho zamýšleného způsobu použití. Toto použití by se řídilo vnitrostátním právem a do určité míry by o něm rozhodovaly donucovací orgány samotné. Navrhované nařízení totiž stanoví minimální podmínky použití v článku 29 (omezené na návod k použití) pro vysoce rizikové systémy UI, včetně systémů uvedených v bodech 6, 7 a 8 přílohy III, které budou doplněny vnitrostátními právními předpisy. Proto by se v souladu s judikaturou Soudního dvora mělo rozlišovat mezi zamýšleným cílem navrhovaného nařízení, kterým je neupravovat používání systémů UI donucovacími orgány, na straně jedné a účinky, které může toto nařízení mít nepřímo¹³, na straně druhé, přičemž tyto nepřímé účinky jsou pro účely analýzy vhodnosti právního základu irelevantní.
25. Systémy uvedené v bodech 6, 7 a 8 (v oblasti prosazování práva, migrace a výkonu spravedlnosti) mezi vysoce rizikovými systémy UI nepřevažují. Podle navrhovaného nařízení totiž systém UI, který je uveden v příloze III, nemusí být nutně systémem vysoce rizikovým. Většinu vysoce rizikových systémů totiž ve skutečnosti představují systémy, které jsou uvedeny obecně v čl. 6 odst. 1 písm. a) a b) navrhovaného nařízení (v souvislosti s bezpečností výrobků). Další vysoce rizikové systémy UI jsou uvedeny v příloze III, jež zahrnuje body 1 (biometrická identifikace), 2 (kritická infrastruktura), 3 (vzdělávání a odborná příprava) a 4 (zaměstnanost, správa pracovníků a přístup k samostatné výdělečné činnosti), které se týkají jiných oblastí než oblasti spravedlnosti a vnitřních věcí („SVV“). Na všechny uživatele těchto vysoce rizikových systémů UI se vztahuje jednotný režim zavedený nikoli s ohledem na jejich specifický status (například zda se jedná o hospodářský subjekt nebo orgán veřejné správy), ale z hlediska ochrany zdraví, bezpečnosti a základních práv.

¹³ Viz rozsudek Soudního dvora ze dne 21. června 2018, *Polská republika v. Evropský parlament, Rada Evropské unie*, C-5/16, EU:C:2018:483, body 63 až 68, a rozsudek Soudního dvora ze dne 22. června 2022, *Leistritz AG v. LH*, C-534/20, EU:C:2022:495, bod 28.

26. Navrhované nařízení tedy obsahuje harmonizovaná pravidla pro uvádění systémů UI na trh a do provozu a pro jejich používání bez ohledu na to, zda jsou používány soukromými subjekty nebo orgány veřejné správy, a tudíž¹⁴ i donucovacími a justičními orgány.
27. Kromě používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva, které podléhá zvláštním pravidlům pro zpracování osobních údajů (viz část III níže), neobsahuje navrhované nařízení žádná harmonizovaná pravidla pro používání vysoce rizikových systémů UI. Jak bylo vysvětleno v bodech 18 a 19 výše, odkaz na používání vysoce rizikových systémů UI se v zásadě týká návodu k použití výrobku (článek 29) a souvisí s povinnostmi uloženými vývojářům. Jak je uvedeno v bodě 22, rozhodnutí o tom, zda donucovací nebo justiční orgány mohou používat vysoce rizikový systém UI, který je v souladu s právními předpisy uveden na trh podle navrhovaného nařízení, přísluší vnitrostátním orgánům a je třeba jej učinit v souladu vnitrostátními právními předpisy.
28. Článek 87 odst. 2 SFEU, zejména jeho písmeno a), proto není vhodným právním základem pro navrhované nařízení. Pravidla obsažená v návrhu nepodporují shromažďování, uchovávání, zpracovávání, analýzu a výměnu příslušných informací ani těmto činnostem nebrání. Jednoduše řečeno, pokud jsou tyto činnosti vykonávány donucovacími orgány, bude třeba v zájmu ochrany práv uživatelů dodržovat řadu nespecifických, harmonizovaných podmínek. Uvedené cíle navrhovaného nařízení obdobně nezahrnují vypracování společných vyšetřovacích technik. Navrhované požadavky týkající se používání vysoce rizikových systémů UI nejsou specifické pro oblast SVV a netýkají se policejní spolupráce *stricto sensu*, jak je definována ve SFEU.

¹⁴ Viz posudek Soudního dvora týkající se *Istanbulské úmluvy*, A-1/19, EU:C:2021:198, zejména body 298 a 301.

29. Pokud jde o ustanovení čl. 5 odst. 4 navrhovaného nařízení, může členský stát přesto rozhodnout, že používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva povolí. Pokud tak učiní, má členský stát povinnost stanovit nezbytná podrobná pravidla upravující žádosti o předchozí povolení a jejich vydávání a výkon, jakož i trestné činy, ve vztahu k nimž je pro účely jejich vyšetřování nebo stíhání používání uvedených systémů povoleno¹⁵. Na základě výsledku jednání v Radě by tato navrhovaná pravidla nevedla k tomu, že by byly příslušným vnitrostátním orgánům uděleny nové pravomoci. Namísto toho je použití stávajících nebo případných budoucích mechanismů omezeno s cílem zajistit ochranu práva na soukromí a osobních údajů.
30. S ohledem na výše uvedené skutečnosti je jediným vhodným právním základem pro harmonizovaná pravidla týkající se vysoce rizikových systémů UI, včetně těch, které jsou používány donucovacími a justičními orgány, článek 114 SFEU a jakýkoli právní základ z oblasti SVV uvedený v části třetí hlavě V SFEU, jako je článek 87 SFEU, není ve vztahu k těmto harmonizovaným pravidlům odůvodněný ani vhodný.

¹⁵ Je třeba poznamenat, že čl. 5 odst. 4 návrhu se vyznačuje určitými rysy, které jsou podobné čl. 15 odst. 1 směrnice 2002/58 o elektronickém obchodu. Zejména stanoví možnost, aby se členské státy od některých zákazů stanovených v právu Unie odchýlily. S ohledem na ustálenou judikaturu budou vnitrostátní ustanovení, jejichž účelem je odchýlit se od uvedených zákazů, nutně spadat do působnosti práva Unie, což následně povede k tomu, že se na ně bude vztahovat Listina základních práv Evropské unie.

III. VHODNOST ČLÁNKU 16 SFEU JAKOŽTO DODATEČNÉHO PRÁVNÍHO ZÁKLADU

31. Navrhované nařízení zahrnuje jako jeden z právních základů článek 16 SFEU týkající se zpracování osobních údajů v oblasti prosazování práva. Jeho 25. a 26. bod odůvodnění obsahují odkaz na článek 6a protokolu č. 21 a článek 2a protokolu č. 22 týkající se zpracování osobních údajů v oblasti předcházení trestné činnosti. Článek 16 SFEU má podle názoru Komise sloužit výlučně jako právní základ pro ustanovení, jimiž se komplementárním způsobem ve vztahu ke směrnici 2016/680 (dále jen „směrnice o prosazování práva“) zavádějí omezení ohledně zpracování biometrických osobních údajů. Článek 5 odst. 1 písm. c) je formulován v zásadě jako zákaz, na který se vztahuje soubor tří výjimek. Konkrétně je používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva zakázáno, pokud není nezbytně nutné a) provádět cílené vyhledávání potenciálních obětí trestných činů, b) zabránit hrozícímu teroristickému útoku nebo útoku na fyzickou integritu / život osoby, c) lokalizovat, identifikovat nebo stíhat pachatele závažného trestného činu nebo osobu, která je z jeho spáchání podezřelá (s odkazem na evropský zatýkací rozkaz). Další požadavky uvedené v čl. 5 odst. 2, 3 a 4 se vztahují k tomuto konkrétnímu použití systémů UI donucovacími orgány, zejména posouzení nezbytnosti a přiměřenosti, předchozí povolení (s výjimkou mimořádných situací) a rozhodnutí členských států, zda v takových situacích konkrétní použití nástrojů UI na vnitrostátní úrovni povolí, či nikoli.
32. Článek 5 je podrobným ustanovením upravujícím konkrétní použití nástrojů UI, které má nejen doplnit stávající legislativní rámec Unie (směrnice o prosazování práva, která je sama o sobě založena na článku 16 SFEU), ale rovněž vyžaduje příslušný vnitrostátní prováděcí rámec.

33. Navzdory tomu, že specifické pravidlo je v článku 5 formulováno jako zákaz, lze je v podstatě popsat tak, že stanoví přísné a výjimečné vymezení všeobecného monitorování jednotlivců v otevřených prostorech „v reálném čase“ za účelem jejich identifikace. Uvedený zákaz jde rovněž nad rámec pouhého používání kamer pro pořizování záznamů a vztahuje se na používání nástrojů UI pro automatizované rozpoznávání lidských rysů na veřejně přístupných místech (rysy, jako jsou tváře, ale také způsob chůze, otisky prstů, DNA, hlas, úhozy na klávesnici a další biometrické nebo behaviorální signály). Zahrnuje rovněž souběžné zachycování údajů o osobách a jejich identifikaci pomocí analytického srovnání/kontroly údajů. Kromě toho musí být uvedené pravidlo posouzeno rovněž s ohledem na skutečnost, že může být povolena rovněž identifikace „v reálném čase“ prováděná soukromými uživateli na veřejných místech (u takových akcí, jako jsou fotbalové zápasy).
34. Zdá se, že z dalších vysvětlení poskytnutých Komisí vyplývá, že s cílem umožnit donucovacím orgánům používat nástroje UI při odhalování jednotlivců „v reálném čase“ na veřejných místech neupravuje tuto konkrétní otázku v současné době žádný členský stát nebo ji upravuje možná jen velmi malý počet členských států. Z praktického hlediska se však zdá, že ačkoli nebyly uvedeny žádné konkrétní důkazy prokazující, že bude nutno stávající postupy a nástroje změnit, je zřejmé, že tento přístup spočívající ve stanovení zákazu a souvisejících výjimek bude zapotřebí začlenit do budoucích vyšetřovacích technik, forenzních metod a pravidel pro shromažďování důkazů.
35. Pokud jde o právní základ, zdá se, že ustanovení, která komplementárním způsobem (ve srovnání se směrnicí o prosazování práva) zavádějí omezení pro zpracování biometrických osobních údajů, sledují cíl ochrany osobních údajů stanovením vhodných záruk. Takový cíl je neoddělitelně spjat s cílem ustanovení spadajících do oblasti působnosti článku 114 SFEU, aniž by jeden z nich byl ve vztahu k tomu druhému vedlejší a nepřímý. Cílem navrhovaného nařízení je stanovit obecný rámec pro systémy UI na základě přístupu založeného na posouzení rizik. V této souvislosti může horizontální regulace systémů UI zahrnovat přesně vymezené záruky vztahující se na tento konkrétní systém UI pro účely odhalování trestných činů „v reálném čase“. Takový konkrétní systém UI zahrnující vhodné záruky ochrany osobních údajů je proto neoddělitelně spjat s celkovým cílem zlepšit fungování vnitřního trhu a není ve vztahu k tomuto druhému cíli vedlejší ani nepřímý. Navrhované nařízení by se proto mělo v souladu s relevantní judikaturou (viz bod 9 výše) řídit dvojím základem.

36. Zůstává však otázkou, jaký právní základ by měl být použit pro regulaci zpracovávání osobních údajů pro účely používání systémů uvedených v čl. 5 odst. 1 písm. c) až čl. 5 odst. 4 navrhovaného nařízení. Článek 87 odst. 2 písm. a) SFEU totiž představuje právní základ pro opatření donucovacích orgánů týkající se prevence, odhalování a vyšetřování trestných činů, pokud jde o shromažďování, uchovávání, zpracovávání, analýzu a výměnu příslušných informací.
37. Jak vysvětlil generální advokát ve stanovisku týkajícím se Dohody o jmenné evidenci cestujících s Kanadou (A1/15), článek 16 SFEU na jedné straně a čl. 87 odst. 2 písm. a) a čl. 82 odst. 1 písm. d) SFEU na straně druhé však nemohou navzájem vykazovat vztahy hierarchické povahy „*lex generalis – lex specialis*“¹⁶. Ustanovení čl. 16 odst. 2 SFEU je jediným ustanovením, které se vztahuje na pravidla týkající se ochrany fyzických osob v souvislosti se zpracováním osobních údajů donucovacími orgány členských států při výkonu činností za účelem předcházení trestné činnosti. Pouhá skutečnost, že článek 5 odkazuje na seznam závažných trestných činů v rámcovém rozhodnutí o evropském zatýkacím rozkazu, na tomto hodnocení nic nemění: uvedený odkaz neznamena, že se použije dané rámcové rozhodnutí jako takové¹⁷. Jedná se pouze o legislativní techniku spočívající v uvedení seznamu závažných trestných činů, aniž by bylo nutné vytvářet samostatnou přílohu.
38. Skutečností zůstává, že pravidlo uvedené v článku 5 není stanoveno jako prostředek sloužící k dalšímu vymezení podmínek uplatňování daných opatření v oblasti SVV, ale s cílem zajistit, aby se do budoucna při jakémkoli použití biometrické identifikace „v reálném čase“ pomocí systémů UI odpovídajícím způsobem reagovalo na problematické otázky týkající se základních práv a především na potřebu zajistit, aby byly biometrické údaje shromažďovány a zpracovávány při současném respektování práva na soukromí a na ochranu osobních údajů.

V tomto ohledu nemá nařízení za cíl stanovit nový, povinný postup specifický pro oblast SVV, ale spíše využívá osvědčené a vyzkoušené procesní prostředky k zajištění dodržování základních práv.

¹⁶ Viz stanovisko generálního advokáta P. Mengozziho ze dne 8. září 2016, *Návrh dohody mezi Kanadou a Evropskou unií*, posudek 1/15, EU:C:2016:656, body 112 až 120.

¹⁷ Pokud jde o zavedení tohoto seznamu závažných trestných činů členskými státy, viz rozsudek Soudního dvora ze dne 21. června 2022, *Human Rights League v. Rada ministrů*, C-817/19, EU:C:2022:65, body 150 až 152.

39. Je-li článek 16 SFEU vhodným dodatečným právním základem, vyvstávají tím otázky ohledně použití článků 6a a 2a protokolů č. 21 a 22. Jak je vysvětleno ve 25. a 26. bodě odůvodnění návrhu, znamená to, že pokud donucovací orgány v Irsku nebo Dánsku používají systémy biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely předcházení trestné činnosti a pokud Irsko nebo Dánsko nejsou vázány odpovídajícími pravidly policejní spolupráce nebo justiční spolupráce v trestních věcech, nebudou tyto dva členské státy vázány čl. 5 odst. 1 písm. d) a čl. 5 odst. 2 a 3 navrhovaného nařízení. To neznamená, že čl. 5 odst. 1 písm. d) a čl. 5 odst. 2 a 3 obsahují pravidla týkající se policejní spolupráce, jako jsou například pravidla pro sdílení informací mezi donucovacími orgány. Znamená to pouze, že čl. 5 odst. 1 písm. d) a čl. 5 odst. 2 a 3 navrhovaného nařízení podobně jako směrnice 2016/680 (směrnice o prosazování práva), která je *lex generalis* přijatým na základě článku 16 SFEU, upravují zpracování biometrických osobních údajů v konkrétním kontextu systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely předcházení trestné činnosti, a nic více. Návrh Komise v tomto ohledu vychází z přístupu, který normotvůrce Unie zvolil i pro směrnici o prosazování práva, a jako takový potvrzuje, že použití čl. 87 odst. 2 SFEU v této souvislosti proto není odůvodněné.
40. Doplnění článku 16 SFEU k článku 114 SFEU je v tomto případě odůvodněno skutečností, že čl. 5 odst. 1 písm. d) a čl. 5 odst. 2 a 3 jsou jedinými případy upravujícími používání systému UI, který byl povolen a který zasahuje do práva na ochranu osobních údajů, takže jde o *lex specialis* ve vztahu k obecnému rámci pro ochranu údajů. Taková pravidla pro ochranu údajů vycházející z *lex specialis*, která mají dopad na používání uvedených citlivých systémů UI, nelze ve vztahu k právnímu základu týkajícímu se vnitřního trhu považovat za vedlejší nebo nepřímá. Doplnění článku 16 SFEU jakožto právního základu je proto v navrhovaném nařízení dostatečně odůvodněno a použití čl. 87 odst. 2 písm. a) SFEU není vhodné.

IV. ZÁVĚR

41. S ohledem na výše uvedené skutečnosti se právní služba Rady domnívá, že:

- a) použití článků 16 a 114 SFEU jako právních základů navrhovaného nařízení je odůvodněné a vhodné;
 - b) použití čl. 87 odst. 2 SFEU nebo jakéhokoliv jiného právního základu z oblasti SVV ve vztahu k harmonizovaným pravidlům vztahujícím se na systémy UI, které mohou být poskytovány nebo používány donucovacími nebo justičními orgány, není odůvodněné ani vhodné.
-