



V Bruseli 12. septembra 2022
(OR. en)

12302/22

LIMITE

JUR 579
TELECOM 364
COSI 217
JAI 1155
ENFOPOL 451

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

STANOVISKO PRÁVNEHO SERVISU¹

Od:	Právny servis
Predmet:	Návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie – Správnosť určenia článkov 114 a 16 ZFEÚ ako právnych základov vo vzťahu k ustanoveniam uplatniteľným na presadzovanie práva a justičné orgány

I. ÚVOD

1. V navrhovanom nariadení sa stanovujú harmonizované pravidlá uvádzania systémov umelej inteligencie na trh a do prevádzky v Únii (ďalej len „navrhované nariadenie“)².

¹ Tento dokument obsahuje právne poradenstvo, ktoré je chránené podľa článku 4 ods. 2 nariadenia Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie a ktoré Rada Európskej únie nezverejnila. V prípade neoprávneného uverejnenia si Rada vyhradzuje možnosť použiť všetky dostupné právne prostriedky.

² 8115/21.

2. Na zasadnutí pracovnej skupiny pre telekomunikácie a informačnú spoločnosť 7. apríla 2022 sa právny servis Rady vyjadril k otázke správnosti určenia dvojakeho právneho základu (články 16 a 114 ZFEÚ) pre navrhované nariadenie o systémoch umelej inteligencie. Vysvetlenia potvrdili, že články 16 a 114 ZFEÚ sú správnymi právnymi základmi návrhu a že odkaz na článok 87 ods. 2 ZFEÚ namiesto článku 114 ZFEÚ nie je vhodný. Na žiadosť pracovnej skupiny sa v tomto stanovisku písomne uvádza a ďalej rozvíja príspevok zástupcu právneho servisu Rady na tomto zasadnutí.
3. Systémy umelej inteligencie sú vymedzené v článku 3 ods. 1 navrhovaného nariadenia. Vo všeobecnosti zodpovedajú určitým typom softvéru. Navrhované nariadenie sa vzťahuje na poskytovateľov, ktorí uvádzajú systémy umelej inteligencie na trh, ako aj na poskytovateľov, ktorí uvádzajú systémy umelej inteligencie do prevádzky. Okrem toho sa navrhované nariadenie vzťahuje aj na používateľov. Poskytovateľom môže byť fyzická alebo právnická osoba, orgán verejnej moci alebo verejný subjekt, ktorý vyvíja systém umelej inteligencie alebo ktorý má systém umelej inteligencie vyvinutý s cieľom uviesť ho na trh alebo do prevádzky pod vlastným menom alebo ochrannou známkou. Používateľom môže byť akákoľvek fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo akýkoľvek iný subjekt, ktorý používa systém umelej inteligencie v rámci svojej právomoci.

4. Podľa vymedzenia pojmov v článku 3 by sa orgány presadzovania práva a justičné orgány mohli považovať za poskytovateľov a/alebo používateľov systému umelej inteligencie. Systémy umelej inteligencie, ktorých zamýšľaným účelom vymedzeným poskytovateľom je presadzovanie práva alebo výkon spravodlivosti, sú podľa prílohy III klasifikované ako vysokorizikové. Ako také podliehajú základným požiadavkám (riadenie rizík, testovanie, správa údajov, technická dokumentácia, transparentnosť, ľudský dohľad, presnosť, spoľahlivosť a kybernetická bezpečnosť) a povinnostiam (ako sú systémy riadenia kvality, technická dokumentácia, posudzovanie zhody, nápravné opatrenia, povinnosť informovať, povinnosti dovozcov a distribútorov), ako aj normám a posudzovaniu zhody. Tieto harmonizované pravidlá vychádzajú z pravidiel, ktoré sa uplatňujú na bezpečnosť výrobkov v smernici 2006/42/ES (strojové zariadenia)³ a nariadení 2017/745 (zdravotnícke pomôcky)⁴.
5. Pokiaľ ide o systémy umelej inteligencie, ktoré zahŕňajú používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, patria do kategórie zakázaných systémov umelej inteligencie. Tento zákaz používania systémov umelej inteligencie však podlieha výnimkám. Členské štáty môžu, ale nemusia povoliť používanie takýchto systémov. Ak sú povolené, podliehajú podrobným obmedzeniam a zárukám, aby sa ich používanie obmedzilo na to, čo je nevyhnutne potrebné, a aby sa chránilo základné právo na ochranu osobných údajov. Tieto obmedzenia a záruky sú v navrhovanom nariadení ustanovené na základe článku 16 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“) a musia byť doplnené vnútroštátnym právom. Článok 5 ods. 1 písm. d), článok 5 ods. 2, 3 a 4 navrhovaného nariadenia predstavujú *lex specialis* k smernici 2016/680 (smernica o ochrane údajov v oblasti presadzovania práva), ktorá bola prijatá na základe článku 16 ods. 2 ZFEÚ.

³ Smernica Európskeho parlamentu a Rady 2006/42/ES zo 17. mája 2006 o strojových zariadeniach a o zmene a doplnení smernice 95/16/ES (Ú. v. EÚ L 157, 9.6.2006, s. 24 – 86).

⁴ Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach, zmene smernice 2001/83/ES, nariadenia (ES) č. 178/2002 a nariadenia (ES) č. 1223/2009 a o zrušení smerníc Rady 90/385/EHS a 93/42/EHS (Ú. v. EÚ L 117, 5.5.2017, s. 1 – 175).

V súlade s článkom 5 ods. 1 písm. d) sa ciele týchto systémov obmedzujú na:

- i) cielené pátranie po konkrétnych potenciálnych obetiach trestných činov vrátane nezvestných detí;
- ii) predchádzanie konkrétnemu, závažnému a bezprostrednému ohrozeniu života alebo fyzickej bezpečnosti fyzických osôb alebo teroristickému útoku;
- iii) odhaľovanie, lokalizácia, identifikácia alebo stíhanie páchatel'a trestného činu uvedeného v článku 2 ods. 2 rozhodnutia o európskom zatykači⁵, za ktorý možno podľa právnych predpisov dotknutého členského štátu v tomto členskom štáte uložiť trest odňatia slobody alebo ochranné opatrenie s hornou hranicou trestnej sadzby najmenej tri roky, alebo osoby podozrivej zo spáchania takéhoto trestného činu.

Podľa článku 5 ods. 3 musí používanie takýchto technológií orgánmi presadzovania práva podliehať predchádzajúcemu povoleniu súdneho alebo správneho orgánu. V riadne odôvodnenej naliehavej situácii sa však použitie systému môže začať bez povolenia a o povolenie možno požiadať až počas používania alebo po ňom.

Podľa článku 5 ods. 4 sa členský štát môže rozhodnúť povoliť používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva a vymedziť potrebné podrobné pravidlá týkajúce sa podávania žiadostí o predchádzajúce povolenia, ich vydávania a výkonu, ako aj súvisiacich trestných činov.

6. Právnym základom navrhovaného nariadenia sú články 16 ZFEÚ (ochrana osobných údajov) a 114 ZFEÚ (fungovanie vnútorného trhu). Vzniká preto otázka správnosti určenia týchto právnych základov vo vzťahu k harmonizovaným pravidlám uplatniteľným na systémy umelej inteligencie poskytované alebo používané orgánmi presadzovania práva a justičnými orgánmi.

⁵ Rámcové rozhodnutie Rady 2002/584/SVV z 13. júna 2002 o európskom zatykači a postupoch odovzdávania osôb medzi členskými štátmi (Ú. v. ES L 190, 18.7.2002, s. 1).

7. Toto stanovisko sa najprv zameriava na správnosť určenia článku 114 ZFEÚ ako právneho základu v osobitnom kontexte orgánov presadzovania práva, ktoré sú uvedené vo viacerých ustanoveniach navrhovaného nariadenia, t. j. pokiaľ ide o systémy diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch a vysokorizikové systémy umelej inteligencie uvedené v bode 6 prílohy III. Preto sa zaoberá otázkou, či by namiesto článku 114 ZFEÚ (oddiel II) nebolo správnejšie určiť ako právny základ úpravy poskytovania a používania systémov umelej inteligencie orgánmi presadzovania práva článok 87 ods. 2 ZFEÚ (policačná spolupráca). Analogicky možno záver tejto poznámky uplatniť na justičné orgány uvedené v prílohe III, pokiaľ ide o vysokorizikové systémy umelej inteligencie.
8. Táto poznámka sa zaoberá aj správnosťou určenia článku 16 ZFEÚ ako dodatočného právneho základu a uplatňovaním protokolov č. 21 a 22 v súvislosti s používaním systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch orgánmi presadzovania práva (oddiel III).

II. SPRÁVNOSŤ URČENIA ČLÁNKU 114 ZFEÚ AKO PRÁVNEHO ZÁKLADU

9. Podľa ustálenej judikatúry právny základ aktu Únie nezávisí od presvedčenia inštitúcie, pokiaľ ide o sledovaný cieľ, ale musí sa určiť podľa objektívnych kritérií – medzi ktoré patrí najmä cieľ a obsah opatrenia – pričom tieto kritériá podliehajú súdnemu preskúmaniu. Ak sa preskúmaním dotknutého aktu preukáže, že sleduje dvojaký cieľ alebo že obsahuje dve zložky, a ak jeden z nich možno označiť za hlavný alebo prevažujúci, zatiaľ čo druhý je len doplňujúci, musí sa tento akt zakladať iba na jedinom právnom základe, a to na tom, ktorý si vyžaduje hlavný alebo prevažujúci cieľ alebo zložka. Iba výnimočne, ak sa stanoví, že akt sleduje súčasne niekoľko cieľov, ktoré sú neoddeliteľne prepojené tak, že ani jeden z nich nie je vo vzťahu k inému sekundárny a nepriamy, dotknutý akt môže byť založený na rôznych zodpovedajúcich právnych základoch, ak si tieto právne základy nevyžadujú postupy, ktoré sú navzájom nezlučiteľné. Treba tiež poznamenať, že z článku 114 ods. 1 prvej vety ZFEÚ je zrejmé, že ustanovenia článku sa uplatňujú, „*pokiaľ zmluvy neustanovujú inak*“. Preto je použitie článku 114 ZFEÚ opodstatnené len vtedy, ak ako právny základ na prijatie predmetného opatrenia nemožno použiť žiadne konkrétnejšie ustanovenie⁶. Ak zmluva obsahuje konkrétnejšie ustanovenie, ktoré by mohlo tvoriť právny základ predmetného opatrenia, opatrenie sa musí zakladať na takom ustanovení⁷.

⁶ Stanovisko právneho servisu Rady zo 17. mája 2016, 9007/16, bod 6.

⁷ Rozsudok z 29. apríla 2004, Komisia/Rada, C-338/01, EU:C:2004:253, bod 60.

A. CIEĽ NAVRHOVANÉHO NARIADENIA

10. Navrhovaným nariadením sa harmonizuje uvádzanie na trh, uvádzanie do prevádzky a používanie určitého typu softvéru (systémy umelej inteligencie). Skutočnosť, že orgány verejnej moci a súkromní prevádzkovatelia môžu byť poskytovateľmi alebo používateľmi takýchto systémov umelej inteligencie, nie je sama osebe nezlučiteľná s článkom 114 ZFEÚ ako právnym základom⁸.
11. Okrem toho skutočnosť, že orgány presadzovania práva alebo osoby konajúce v ich mene môžu patriť medzi poskytovateľov alebo používateľov takýchto systémov umelej inteligencie, nestačí na odôvodnenie uplatnenia článku 87 ZFEÚ ako právneho základu. Cieľ a obsah navrhovaného nariadenia sa musia analyzovať s cieľom určiť, či je to potrebné.
12. Cieľom navrhovaného nariadenia je vo všeobecnosti, a to aj pokiaľ ide o systémy diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch a vysokorizikové systémy umelej inteligencie, zabezpečiť jednotnú a vysokú úroveň ochrany v celej Únii a zároveň zabrániť tomu, aby rozdiely bránili voľnému pohybu systémov umelej inteligencie a súvisiacich výrobkov a služieb v rámci vnútorného trhu. Ustanovujú sa v ňom jednotné povinnosti pre prevádzkovateľov a zaručuje jednotnú ochranu naliehavých dôvodov verejného záujmu a práv osôb na celom vnútornom trhu (odôvodnenie 2). V návrhu nariadenia sa konkrétnejšie ustanovujú pravidlá upravujúce uvádzanie určitých systémov umelej inteligencie na trh a do prevádzky, čím sa zabezpečí hladké fungovanie vnútorného trhu a umožní sa, aby tieto systémy využívali zásadu voľného pohybu tovaru a služieb (odôvodnenie 5). Celkovo je cieľom návrhu vytvoriť dôveryhodnú umelú inteligenciu už v štádiu návrhu, ktorá by sa uplatňovala všeobecne, s úplným súborom pravidiel pre vývoj, uvádzanie na trh a používanie výrobkov, služieb a systémov založených na umelej inteligencii. Vzhľadom na to, že umelá inteligencia sa už dostala do veľkého počtu služieb a výrobkov a bude v tom pokračovať aj v budúcnosti, návrh nasleduje logiku vnútorného trhu tým, že ustanovuje „rámec bezpečnosti výrobkov“ zriadený na základe sady štyroch kategórií rizík. Stanovujú sa v ňom požiadavky na vstup na trh a certifikáciu systémov umelej inteligencie s vysokým rizikom prostredníctvom povinného postupu označovania značkou CE.

⁸ Pozri stanovisko právneho servisu Rady (ST 11395/14, body 39 až 41) a precedensy, ako je smernica (EÚ) 2016/2102, smernice 2014/24/EÚ, 2014/25/EÚ a 2014/23/EÚ.

13. Žiadny z uvedených cieľov navrhovaného nariadenia sa netýka zabezpečenia cieľov verejnej bezpečnosti. Aj keď sa ciele verejnej bezpečnosti majú plniť nepriamo prostredníctvom harmonizačného procesu uvádzania systémov umelej inteligencie na trh/do prevádzky/ich používania orgánmi presadzovania práva, Súdny dvor⁹ pri výklade článku 87 ods. 2 ZFEÚ s ohľadom na článok 67 ZFEÚ uviedol, že na to, aby bol akt Únie vzhľadom na svoj účel a obsah založený na článku 87 ods. 2 ZFEÚ, musí byť priamo spojený s cieľmi ustanovenými v článku 67 ZFEÚ (t. j. v tomto prípade s predchádzaním trestnej činnosti a policajnou spoluprácou). V kontexte navrhovaného nariadenia je to vylúčené, keďže jedinými harmonizovanými pravidlami používania takýchto systémov orgánmi presadzovania práva sú buď: 1) pravidlá týkajúce sa bezpečnosti výrobkov, ktoré sa uplatňujú jednotne na všetkých poskytovateľov a používateľov v súvislosti s uvádzaním na trh/uvádzaním do prevádzky alebo používaním systémov umelej inteligencie, alebo 2) pravidlá ochrany osobných údajov, pre ktorú bol pridaný ako právny základ článok 16 ZFEÚ (pozri časť III).
14. V inej veci¹⁰, hoci cieľ zmeny smernice o strelných zbraniach spočíval v zabezpečení vyššej úrovne verejnej bezpečnosti vo vzťahu k teroristickej hrozbe a iným formám trestnej činnosti, Súdny dvor rozhodol, že harmonizácia aspektov týkajúcich sa bezpečnosti tovaru je jedným zo základných prvkov riadneho fungovania vnútorného trhu, pričom rozdielne pravidlá v tejto oblasti môžu vytvárať prekážky obchodu¹¹.

⁹ Rozsudok zo 6. mája 2014, Európska komisia/Európsky parlament a Rada Európskej únie, C43/12, ECLI:EU:C:2014:298.

¹⁰ Rozsudok z 3. decembra 2019, Česká republika/Európsky parlament, C- 482/17, EU:C:2019:1035.

¹¹ Tamtiež, bod 57: „Na rozdiel od tvrdenia Poľskej republiky je pritom charakteristikou strelných zbraní ich nebezpečnosť nielen pre užívateľov, ale aj pre širokú verejnosť, ako to už Súdny dvor uviedol v bode 54 rozsudku z 23. januára 2018, Buhagiar a i. (C- 267/16, EU:C:2018:26), a preto sa úvahy týkajúce sa verejnej bezpečnosti, ako to pripomína piate odôvodnenie smernice 91/477, zdajú byť nevyhnutné v rámci právnej úpravy týkajúcej sa nadobúdania a držby tohto tovaru.“ Pozri aj rozsudok z 23. januára 2018, Albert Buhagiar a i./Minister for Justice, C-267/16, EU:C:2018:26, bod 54: „V tejto súvislosti treba uviesť, že vzhľadom na riziko pre bezpečnosť osôb, ktoré predstavujú strelné zbrane, ich voľný pohyb sa môže dosiahnuť len prostredníctvom prísneho rámca podmienok ich prepravy medzi členskými štátmi, do ktorého patrí zásada predchádzajúceho oprávnenia vydaného členskými štátmi, ktorých sa preprava takého tovaru týka“.

15. Ciele navrhovaného nariadenia vrátane článku 5 ods. 1 písm. d), ods. 2, 3 a 4 o používaní systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva a ustanovenia týkajúce sa vysokorizikových systémov umelej inteligencie uvedených v bode 6 prílohy III nie sú priamo spojené s cieľom verejnej bezpečnosti. Návrh naopak reaguje na hlavné obavy týkajúce sa vplyvu systémov umelej inteligencie na zdravie, bezpečnosť a základné práva. Príslušné ustanovenia sú preto priamo spojené s cieľom zabezpečiť rovnaké podmienky pri uvádzaní systémov umelej inteligencie na trh/do prevádzky alebo používania systémov umelej inteligencie na vnútornom trhu a zároveň chrániť zdravie, bezpečnosť a základné práva používateľov.
16. Vzhľadom na uvedené skutočnosti je hlavným cieľom navrhovaného nariadenia zlepšiť fungovanie vnútorného trhu v zmysle článku 114 ZFEÚ a ciele uvedené v článku 67 ZFEÚ sú s týmto hlavným cieľom spojené len nepriamo a náhodne.

B. OBSAH NAVRHOVANÉHO NARIADENIA

17. Navrhované nariadenie v podstate obsahuje pravidlá týkajúce sa toho, čo je potrebné na uvedenie konkrétneho výrobku (softvéru umelej inteligencie) na trh (alebo na jeho uvedenie do prevádzky) tak, aby sa zaistila jeho bezpečnosť a dodržiavanie základných práv. Stanovuje sa v ňom úplný súbor pravidiel pre vývoj, uvádzanie na trh a používanie výrobkov, služieb a systémov založených na umelej inteligencii. Navrhovaným nariadením sa orgánom presadzovania práva neukladá povinnosť používať systém umelej inteligencie, ktorý bol uvedený na trh zákonne, ani sa ním priamo nereguluje, ako by orgány presadzovania práva mali takýto systém umelej inteligencie používať. Namiesto toho návrh jasne vymedzuje situácie, v ktorých sa zamýšľané použitie považuje za vysokorizikové len preto, že systém umelej inteligencie budú používať orgány presadzovania práva alebo justičné orgány.

18. Mimochodom, článok 29 navrhovaného nariadenia obsahuje pravidlá týkajúce sa podmienok používania vysokorizikových systémov umelej inteligencie, ale toto ustanovenie nie je špecifické pre jednotlivé odvetvia, má obmedzený rozsah pôsobnosti (najmä pokiaľ ide o návod na použitie výrobku) a je neoddeliteľne spojené s povinnosťami, ktoré sa navrhovaným nariadením ukladajú vývojárom systémov umelej inteligencie. Členským štátom sa zároveň poskytuje určitý priestor na stanovenie ďalších pravidiel používania takýchto vysokorizikových systémov umelej inteligencie. Pokiaľ ide o systémy diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch používaných na účely presadzovania práva (článok 5), navrhované nariadenie čiastočne upravuje používanie takýchto systémov z hľadiska ochrany údajov na základe článku 16 ZFEÚ (pozri časť III nižšie).
19. Okrem toho len členské štáty sa môžu rozhodnúť, že stanovia možnosť úplne alebo čiastočne povoliť používanie takýchto systémov diaľkovej biometrickej identifikácie v reálnom čase. Konkrétne podmienky takéhoto používania sa ešte musia stanoviť vo vnútroštátnom práve, ale musia byť v súlade so všeobecnými kritériami a zárukami stanovenými v nariadení: predchádzajúce súdne alebo správne povolenie, žiadosť o predchádzajúce povolenie, jeho vydanie a výkon, ako aj uvedenie trestných činov, v súvislosti s ktorými sa takéto systémy môžu používať.

20. Systémy umelej inteligencie sú osobitným typom softvéru. Harmonizované pravidlá, ktoré sa vzťahujú na uvádzanie na trh alebo do prevádzky/používanie systémov umelej inteligencie, sú teda podobné ako harmonizované pravidlá bezpečnosti výrobkov. Uplatňujú sa jednotným spôsobom bez rozlišovania medzi verejnými a súkromnými používateľmi. Podľa príslušných odôvodnení navrhovaného nariadenia by sa preto mala zabezpečiť konzistentná a vysoká úroveň ochrany v celej Únii. Zároveň by sa malo zabrániť rozdielom, ktoré bránia voľnému pohybu systémov umelej inteligencie a súvisiacich výrobkov a služieb na vnútornom trhu. To by sa dosiahlo ustanovením jednotných povinností pre prevádzkovateľov a zaručením jednotnej ochrany naliehavých dôvodov verejného záujmu a práv osôb na celom vnútornom trhu na základe článku 114 ZFEÚ¹².
21. Navrhované nariadenie obsahuje niekoľko odkazov na presadzovanie práva, riadenie kontroly hraníc a výkon spravodlivosti v prílohe III o vysokorizikových systémoch umelej inteligencie (body 6, 7 a 8). Zahŕňajú podrobný a vyčerpávajúci výpočet zodpovedajúci článku 6 ods. 2 popri iných vysokorizikových systémoch vo vzťahu k rizikám súvisiacim s bezpečnosťou výrobkov uvedeným v článku 6 ods. 1. Podľa článku 6 ods. 1 sa niektoré systémy umelej inteligencie zo svojej podstaty považujú za vysokorizikové z dôvodu ich očakávanej závažnosti a vysokého rizika pre základné práva, zdravie a bezpečnosť. Ďalšie systémy, ktoré sa považujú za vysokorizikové a sú uvedené v prílohe III, zahŕňajú vzdelávanie, riadenie kritickej infraštruktúry, zamestnanosť, biometrickú identifikáciu a kategorizáciu, ako aj prístup k základným verejným a súkromným službám.

¹² Na podporu rozvoja, využívania a zavádzania umelej inteligencie na vnútornom trhu je preto potrebný právny rámec Únie, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorý zároveň spĺňa vysokú úroveň ochrany verejných záujmov, ako sú zdravie a bezpečnosť, a ochrany základných práv, ako sú uznané a chránené právom Únie. Na dosiahnutie tohto cieľa by sa mali stanoviť pravidlá upravujúce uvádzanie určitých systémov umelej inteligencie na trh a do prevádzky, čím sa zabezpečí hladké fungovanie vnútorného trhu a umožní sa, aby tieto systémy využívali zásadu voľného pohybu tovaru a služieb (pozri odôvodnenia 2 a 5 návrhu).

22. V takýchto pravidlách týkajúcich sa vysokorizikových systémov umelej inteligencie sa však nestanovuje, či by tieto systémy mali alebo nemali používať orgány presadzovania práva a justičné orgány (alebo orgány v iných identifikovaných oblastiach). Navrhované nariadenie bude mať len nepriamy vplyv na skutočný vývoj systémov umelej inteligencie, ktoré môžu používať orgány presadzovania práva, a na systémy umelej inteligencie, ktoré sa používajú v súčasnosti a budú používať v budúcnosti. Pravidlá sa teda vzťahujú na systémy umelej inteligencie, ktorých „*zamýšľaný účel*“ je použitie takýmito orgánmi (pozri napr. článok 3 ods. 12, článok 8 ods. 2 a prílohu III). Dôsledkom zaradenia určitého systému umelej inteligencie do zoznamu ako vysokorizikového je uplatňovanie osobitného súboru pravidiel riadenia rizík, správy údajov a technických špecifikácií. Používatelia takýchto vysokorizikových systémov umelej inteligencie musia dodržiavať návod na použitie, uchovávať logy a vykonávať posúdenia vplyvu na ochranu údajov.
23. Okrem toho povinnosti používateľov iné ako tie, ktoré sa týkajú návodu na použitie, sa môžu stanoviť v práve Únie alebo vo vnútroštátnom práve a to bez toho, aby bolo dotknuté rozhodovanie používateľa pri organizovaní jeho vlastných zdrojov a činností na účely vykonávania opatrení ľudského dohľadu uvedených poskytovateľom (článok 29 ods. 2 navrhovaného nariadenia). Tieto pravidlá poskytujú ďalšie záruky ochrany základných práv pre vysokorizikové systémy umelej inteligencie.

24. Vzhľadom na uvedené skutočnosti by sa malo zdôrazniť, že navrhované nariadenie neobsahuje pravidlá, ktorých cieľom by bolo umožniť alebo zabrániť tomu, aby orgány presadzovania práva používali vysokorizikový systém umelej inteligencie uvedený na trh. Na základe navrhovaných pravidiel sa na systém umelej inteligencie vyvinutý alebo používaný orgánmi presadzovania práva v dôsledku jeho zamýšľaného účelu bude uplatňovať osobitné označenie (vysokorizikový). Takýto účel by sa upravoval vnútroštátnym právom a do určitej miery by o ňom rozhodovali samotné orgány presadzovania práva. V navrhovanom nariadení sa skutočne stanovujú minimálne podmienky používania v článku 29 (obmedzené na návod na použitie) pre vysokorizikové systémy umelej inteligencie vrátane tých, ktoré sú uvedené v bodoch 6, 7 a 8 prílohy III, ktoré sa doplnia vnútroštátnym právom. Preto by sa v súlade s judikatúrou Súdneho dvora malo rozlišovať na jednej strane medzi zamýšľaným cieľom navrhovaného nariadenia, ktorým nie je regulovať používanie systémov umelej inteligencie orgánmi presadzovania práva, a na druhej strane účinkami, ktoré môže nepriamo vyvolať¹³ a ktoré sú irelevantné na účely analýzy správnosti určenia právneho základu.
25. Medzi vysokorizikovými systémami umelej inteligencie neprevládajú body 6, 7 a 8 (o presadzovaní práva, migrácii a výkone spravodlivosti). Podľa navrhovaného nariadenia nie je vysokorizikový systém umelej inteligencie v skutočnosti nevyhnutne uvedený v prílohe III. Väčšina rizikových systémov je v skutočnosti uvedená všeobecne v článku 6 ods. 1 písm. a) a b) navrhovaného nariadenia (v súvislosti s bezpečnosťou výrobkov). Ďalšie vysokorizikové systémy umelej inteligencie sú uvedené v prílohe III, ktorá obsahuje body 1 (biometrická identifikácia), 2 (kritická infraštruktúra), 3 (vzdelávanie a odborná príprava) a 4 (zamestnanosť, riadenie pracovníkov a prístup k samostatnej zárobkovej činnosti), ktoré súvisia s inými oblasťami ako spravodlivosť a vnútorné veci („SVV“). Všetci používatelia takýchto vysokorizikových systémov umelej inteligencie podliehajú jednotnému režimu zavedenému nie vzhľadom na ich osobitné postavenie (napríklad či ide o hospodársky subjekt alebo orgán verejnej moci), ale z hľadiska ochrany zdravia, bezpečnosti a základných práv.

¹³ Pozri rozsudok Súdneho dvora z 21. júna 2018, Poľská republika/Európsky parlament, Rada Európskej únie, C-5/16, EU:C:2018:483, body 63 až 68, a rozsudok Súdneho dvora z 22. júna 2022, Leistritz AG/LH, C-534/20, EU:C:2022:495, bod 28.

26. Navrhované nariadenie teda obsahuje harmonizované pravidlá uvádzania na trh, uvádzania do prevádzky a používania systémov umelej inteligencie bez ohľadu na to, či ich používajú súkromní prevádzkovatelia alebo orgány verejnej moci vrátane prípadných¹⁴ orgánov presadzovania práva a justičných orgánov.
27. Okrem používania systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, na ktoré sa vzťahujú osobitné pravidlá spracúvania osobných údajov (pozri časť III nižšie), navrhované nariadenie neobsahuje harmonizované pravidlá používania vysokorizikových systémov umelej inteligencie. Ako bolo vysvetlené v bodoch 18 a 19 vyššie, odkaz na používanie vysokorizikových systémov umelej inteligencie sa v podstate týka návodu na použitie výrobku (článok 29) a súvisí s povinnosťami uloženými vývojom. Ako sa uvádza v bode 22, rozhodnutie o tom, či orgány presadzovania práva alebo justičné orgány môžu používať vysokorizikový systém umelej inteligencie, ktorý je zákonne uvedený na trh podľa navrhovaného nariadenia, prináleží vnútroštátnym orgánom v súlade s vnútroštátnym právom.
28. Článok 87 ods. 2 ZFEÚ, najmä jeho písmeno a), preto nie je správne určeným právnym základom navrhovaného nariadenia. Pravidlá uvedené v návrhu nepodporujú ani nebránia zberu, uchovávaniu, spracúvaniu, analýze a výmene relevantných informácií. Jednoducho, keď takéto činnosti vykonávajú orgány presadzovania práva, bude potrebné dodržiavať niekoľko nešpecifických harmonizovaných podmienok na ochranu práv používateľov. Uvedené ciele navrhovaného nariadenia nezahŕňajú ani vývoj spoločných vyšetrovacích techník. Navrhované požiadavky týkajúce sa používania vysokorizikových systémov umelej inteligencie nie sú špecifické pre oblasť SVV a netýkajú sa policajnej spolupráce *stricto sensu*, ako sa vymedzuje v ZFEÚ.

¹⁴ Pozri stanovisko Súdneho dvora k Istanbulskému dohovoru, A-1/19, EÚ:C:2021:198, najmä body 298 a 301.

29. Pokiaľ ide o ustanovenia článku 5 ods. 4 navrhovaného nariadenia, členský štát sa môže vždy rozhodnúť povoliť používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva. Ak sa tak rozhodne, členský štát je povinný stanoviť potrebné podrobné pravidlá pre žiadosť o predchádzajúce povolenie, jeho vydanie a výkon, ako aj súvisiace trestné činy na vyšetrovanie alebo sťahovanie ktorých sa použitie povoľuje¹⁵. Na základe výsledku rokovaní v Rade by tieto navrhované pravidlá nemali za následok udelenie nových právomocí príslušným vnútroštátnym orgánom. Namiesto toho je obmedzené využívanie existujúcich alebo možných budúcich mechanizmov s cieľom zabezpečiť ochranu práva na súkromie a osobné údaje.
30. Vzhľadom na uvedené skutočnosti je článok 114 ZFEÚ jediným správnym právnym základom pre harmonizované pravidlá týkajúce sa vysokorizikových systémov umelej inteligencie vrátane tých, ktoré používajú orgány presadzovania práva a justičné orgány, a akýkoľvek právny základ v oblasti SVV v tretej časti hlavy V ZFEÚ, ako je článok 87 ZFEÚ, nie je, pokiaľ ide o uvedené harmonizované pravidlá, odôvodnený ani správny.

¹⁵ Treba poznamenať, že článok 5 ods. 4 návrhu má určité vlastnosti podobné článku 15 ods. 1 smernice 2002/58/ES o súkromí a elektronických komunikáciách. Stanovuje sa v ňom najmä možnosť, aby sa členské štáty odchyľili od určitých zákazov stanovených v práve Únie. Vzhľadom na ustálenú judikatúru vnútroštátne ustanovenia určené na odchylenie sa od tohto zákazu budú nevyhnutne patriť do pôsobnosti práva Únie, ktoré zase povedie k uplatneniu Charty vo vzťahu k nim.

III. SPRÁVNOSŤ URČENIA ČLÁNKU 16 ZFEÚ AKO DODATOČNÉHO PRÁVNEHO ZÁKLADU

31. Navrhované nariadenie zahŕňa ako právny základ článok 16 ZFEÚ, pokiaľ ide o spracúvanie osobných údajov v oblasti presadzovania práva, jeho odôvodnenia 25 a 26 obsahujú odkaz na článok 6a protokolu č. 21 a článok 2a protokolu č. 22 o spracúvaní osobných údajov v oblasti predchádzania trestnej činnosti. Podľa názoru Komisie má článok 16 ZFEÚ slúžiť výlučne ako právny základ pre ustanovenia, ktorými sa v porovnaní so smernicou 2016/680 (ďalej len „smernica o presadzovaní práva“) zavádzajú obmedzenia spracúvania biometrických osobných údajov doplnkovým spôsobom. Článok 5 ods. 1 písm. d) je formulovaný ako zásadný zákaz, na ktorý sa vzťahuje súbor troch výnimiek. Konkrétne, používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva je zakázané, pokiaľ to nie je nevyhnutne potrebné na a) cielené pátranie po konkrétnych potenciálnych obetiach trestných činov, b) predchádzanie bezprostrednému teroristickému útoku alebo ohrozeniu života alebo fyzickej bezpečnosti fyzických osôb, c) lokalizáciu alebo identifikáciu alebo stíhanie páchateľa trestného činu alebo osoby podozrivej zo spáchania takéhoto trestného činu (s odkazom na európsky zatykač). K tomuto konkrétnemu používaniu systémov umelej inteligencie orgánmi presadzovania práva sú pripojené ďalšie požiadavky uvedené v článku 5 ods. 2, 3 a 4, najmä posúdenie nevyhnutnosti a primeranosti, predchádzajúce povolenie (s výnimkou núdzových situácií) a rozhodnutie členských štátov, či v takýchto situáciách povolia alebo nepovolia konkrétne používanie nástrojov umelej inteligencie na vnútroštátnej úrovni.
32. Článok 5 je podrobným ustanovením upravujúcim konkrétne používanie nástrojov umelej inteligencie, ktorého cieľom je nielen doplniť existujúci legislatívny rámec Únie (smernica o presadzovaní práva, tiež založená na článku 16 ZFEÚ), ale vyžaduje si aj vnútroštátny vykonávací rámec.

33. Napriek jeho formulácii ako zákazu možno osobitné pravidlo v článku 5 v podstate opísať tak, že stanovuje prísne a výnimočné vymedzenie všeobecného monitorovania jednotlivcov v otvorených priestoroch v reálnom čase pomocou nástrojov umelej inteligencie na účely ich identifikácie. Tento zákaz tiež presahuje rámec jednoduchého používania kamier na zaznamenávanie a vzťahuje sa na používanie nástrojov umelej inteligencie na automatické rozpoznávanie čŕt ľudí vo verejne prístupných priestoroch (črty, ako sú tváre, ale aj chôdza, odtlačky prstov, DNA, hlas, zvuk klávesov a iné biometrické alebo behaviorálne signály). Z toho vyplýva aj súbežné zachytávanie a identifikácia osôb prostredníctvom analytického porovnávania/kontrolovania údajov. Okrem toho treba toto pravidlo posúdiť aj vzhľadom na skutočnosť, že je možné povoliť aj identifikáciu vykonávanú súkromnými používateľmi na verejných priestranstvách v reálnom čase (napr. v prípade podujatí, ako sú futbalové zápasy).
34. Ďalšie vysvetlenia, ktoré poskytla Komisia, naznačujú, že v súčasnosti túto konkrétnu otázku neupravuje s cieľom umožniť orgánom presadzovania práva používať nástroje umelej inteligencie pri rozpoznávaní jednotlivcov v reálnom čase na verejných priestranstvách žiadny členský štát, prípadne len veľmi málo členských štátov. Z praktického hľadiska, hoci nebol predložený žiadny konkrétny dôkaz o tom, že existujúce postupy a nástroje sa budú musieť zmeniť, sa zdá jasné, že budúce techniky vyšetrovania, forenzné metódy a pravidlá zhromažďovania dôkazov budú musieť zahŕňať tento prístup založený na zákaze/výnimkách.
35. Pokiaľ ide o právny základ, zdá sa, že ustanovenia obmedzujúce spracúvanie biometrických osobných údajov doplnkovým spôsobom (v porovnaní so smernicou o presadzovaní práva) sledujú cieľ ochrany osobných údajov stanovením primeraných záruk. Takýto cieľ je neoddeliteľne spojený s cieľom ustanovení patriacich do pôsobnosti článku 114 ZFEÚ bez toho, aby bol jeden cieľ vo vzťahu k druhému druhoradý a nepriamy. Cieľom navrhovaného nariadenia je ustanoviť všeobecný rámec pre systémy umelej inteligencie na základe prístupu založeného na riziku. V tejto súvislosti môže horizontálna regulácia systémov umelej inteligencie zahŕňať prísne záruky uplatniteľné na tento konkrétny systém umelej inteligencie na rozpoznávanie v reálnom čase. Takýto konkrétny systém umelej inteligencie obsahujúci primerané záruky ochrany osobných údajov je preto neoddeliteľne spojený s celkovým cieľom zlepšiť fungovanie vnútorného trhu a nie je vo vzťahu k nemu sekundárny ani nepriamy. Navrhované nariadenie by sa preto malo riadiť dvojitém základom v súlade s príslušnou judikatúrou (pozri bod 9 vyššie).

36. Zostáva však otázka, ktorý právny základ by sa mal použiť na reguláciu spracúvania osobných údajov na účely používania systémov uvedených v článku 5 ods. 1 písm. c) až článku 5 ods. 4 navrhovaného nariadenia. Článok 87 ods. 2 písm. a) ZFEÚ predstavuje právny základ pre opatrenia orgánov presadzovania práva v súvislosti s predchádzaním trestným činom, ich odhaľovaním a vyšetrovaním, ktoré sa týkajú zhromažďovania, uchovávanía, spracúvania, analýzy a výmeny relevantných informácií.
37. Ako však vysvetlil generálny advokát v stanovisku PNR Kanada (A1/15), článok 16 ZFEÚ na jednej strane a článok 87 ods. 2 písm. a) a článok 82 ods. 1 písm. d) ZFEÚ na druhej strane si nemôžu zachovať vzťahy hierarchického typu „*lex generalis – lex specialis*“¹⁶. Článok 16 ods. 2 ZFEÚ je jediným ustanovením, ktoré sa uplatňuje na pravidlá týkajúce sa ochrany fyzických osôb pri spracúvaní osobných údajov orgánmi presadzovania práva členských štátov pri vykonávaní činností zameraných na predchádzanie trestnej činnosti. Samotná skutočnosť, že článok 5 odkazuje na zoznam závažných trestných činov v rámcovom rozhodnutí o európskom zatykači, nemení tento záver: tento odkaz neznamena, že sa toto rámcové rozhodnutie uplatňuje ako také¹⁷. Zoznam závažných trestných činov je len legislatívnou technikou na to, aby nebolo potrebné vytvoriť samostatnú prílohu.
38. Skutočnosťou zostáva, že pravidlo v článku 5 nie je ustanovené ako prostriedok na ďalšie vymedzenie podmienok uplatňovania uvedených opatrení súvisiacich so SVV, ale s cieľom zabezpečiť, aby v budúcnosti akékoľvek používanie biometrickej identifikácie systémami umelej inteligencie v reálnom čase primerane reagovalo na obavy týkajúce sa základných práv a predovšetkým na potrebu zabezpečiť, aby sa biometrické údaje zbierali a spracúvali pri rešpektovaní práva na súkromie a rešpektovaní osobných údajov.

V tejto súvislosti sa nariadenie nezameriava na ustanovenie nového povinného postupu osobitne pre oblasť SVV, ale skôr sa opiera o vyskúšané a overené procesné prostriedky na zabezpečenie dodržiavania základných práv.

¹⁶ Pozri stanovisko generálneho advokáta P. Mengozziho z 8. septembra 2016, *Návrh dohody medzi Kanadou a Európskou úniou*, stanovisko 1/15, EU:C:2016:656 body 112 až 120.

¹⁷ Pokiaľ ide o vykonávanie tohto zoznamu závažných trestných činov členskými štátmi, pozri rozsudok Súdneho dvora z 21. júna 2022, *Liga ľudských práv/Rada ministrov*, C-817/19, EU:C:2022:65, body 150 až 152.

39. Ak je článok 16 ZFEÚ správnym dodatočným právnym základom, vyvoláva to otázky týkajúce sa uplatňovania článku 6a protokolu č. 21 a článku 2a protokolu č. 22. Ako sa vysvetľuje v odôvodneniach 25 a 26 návrhu, znamená to, že ak orgány presadzovania práva v Írsku alebo Dánsku používajú systémy diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na predchádzanie trestnej činnosti a ak Írsko alebo Dánsko nie sú viazané zodpovedajúcimi pravidlami policajnej spolupráce alebo justičnej spolupráce v trestných veciach, tieto dva členské štáty nebudú viazané článkom 5 ods. 1 písm. d) ani článkom 5 ods. 2 a 3 navrhovaného nariadenia. To neznamená, že článok 5 ods. 1 písm. d) a článok 5 ods. 2 a 3 obsahujú pravidlá policajnej spolupráce, ako sú pravidlá výmeny informácií medzi orgánmi presadzovania práva. Znamená to jednoducho, že článok 5 ods. 1 písm. d) a článok 5 ods. 2 a 3 navrhovaného nariadenia, podobne ako smernica 2016/680 (smernica o presadzovaní práva), ktorá je *lex generalis* prijatým na základe článku 16 ZFEÚ, upravujú spracúvanie biometrických osobných údajov v osobitnom kontexte systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na predchádzanie trestnej činnosti – nič viac. Návrh Komisie sa v tomto ohľade riadi prístupom, ktorý v súvislosti so smernicou o presadzovaní práva zvolil zákonodarca Únie, a ako taký potvrdzuje, že použitie článku 87 ods. 2 ZFEÚ v tejto súvislosti nie je preto odôvodnené.
40. Doplnenie článku 16 ZFEÚ k článku 114 ZFEÚ je v tomto prípade odôvodnené skutočnosťou, že článok 5 ods. 1 písm. d) a článok 5 ods. 2 a 3 sú jediné prípady upravujúce používanie systému umelej inteligencie, ktorý bol povolený a ktorý zasahuje do práva na ochranu osobných údajov, čiže ide o *lex specialis* vo vzťahu k všeobecnému rámcu ochrany údajov. Takéto pravidlá ochrany údajov vychádzajúce z *lex specialis*, ktoré majú vplyv na používanie týchto citlivých systémov umelej inteligencie, nemožno vo vzťahu k právnemu základu týkajúcemu sa vnútorného trhu považovať za sekundárne alebo nepriame. Preto je doplnenie článku 16 ZFEÚ ako právneho základu v navrhovanom nariadení dostatočne odôvodnené a použitie článku 87 ods. 2 písm. a) ZFEÚ nie je správne.

IV. ZÁVER

41. Vzhľadom na uvedené skutočnosti zastáva právny servis Rady názor, že:

- a) použitie článkov 16 a 114 ZFEÚ ako právneho základu navrhovaného nariadenia je odôvodnené a správne;
 - b) použitie článku 87 ods. 2 ZFEÚ alebo akéhokoľvek iného právneho základu v oblasti SVV nie je odôvodnené ani správne vo vzťahu k harmonizovaným pravidlám uplatniteľným na systémy umelej inteligencie, ktoré môžu poskytovať alebo používať orgány presadzovania práva alebo justičné orgány.
-