



**Spoločné stanovisko
EDPB – EDPS 5/2021
k návrhu nariadenia
Európskeho parlamentu a
Rady, ktorým sa stanovujú
harmonizované pravidlá v
oblasti umelej inteligencie
(akt o umelej inteligencii)**

18. jún 2021

Zhrnutie

Európska komisia 21. apríla 2021 predložila návrh nariadenia Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (ďalej len „návrh“). Európsky výbor pre ochranu údajov (EDPB) a Európsky dozorný úradník pre ochranu údajov (EDPS) vítajú záujem zákonodarcu o riešenie využívania umelej inteligencie v rámci Európskej únie (EÚ) a zdôrazňujú, že tento návrh má značne významný **vplyv na ochranu údajov**.

EDPB a EDPS poznamenávajú, že **právnym základom** návrhu je predovšetkým článok 114 Zmluvy o fungovaní Európskej únie (ZFEÚ). Návrh okrem toho vychádza aj z článku 16 ZFEÚ, keďže obsahuje osobitné pravidlá ochrany jednotlivcov v súvislosti so spracúvaním osobných údajov, najmä obmedzenia používania systémov umelej inteligencie na diaľkovú biometrickú identifikáciu v reálnom čase vo verejných priestoroch na účely presadzovania práva. EDPB a EDPS pripomínajú, že v súlade s judikatúrou Súdneho dvora Európskej únie (SDEÚ) článok 16 ZFEÚ predstavuje vhodný právny základ v prípadoch, keď je ochrana osobných údajov jedným zo základných cieľov alebo zložiek pravidiel prijatých zákonodarcom EÚ. Uplatňovanie článku 16 ZFEÚ zahŕňa aj **potrebu zabezpečiť nezávislý dohľad nad dodržiavaním** požiadaviek týkajúcich sa spracúvania osobných údajov, ako sa vyžaduje aj v článku 8 Charty základných práv EÚ.

Pokiaľ ide o **rozsah pôsobnosti návrhu**, EDPB a EDPS jednoznačne vítajú skutočnosť, že sa vzťahuje aj na poskytovanie a používanie systémov umelej inteligencie inštitúciami, orgánmi alebo agentúrami EÚ. **Vylúčenie medzinárodnej spolupráce v oblasti presadzovania práva z rozsahu pôsobnosti návrhu** však vyvoláva vážne obavy EDPB a EDPS, keďže takýmto vylúčením vzniká značné riziko obchádzania (napr. tretie krajiny alebo medzinárodné organizácie prevádzkujúce vysokorizikové aplikácie, na ktoré sa spoliehajú orgány verejnej moci v EÚ).

EDPB a EDPS vítajú **prístup založený na riziku**, ktorý je základom návrhu. Tento prístup by sa však mal objasniť a pojem „riziko pre základné práva“ by sa mal zosúladiť so všeobecným nariadením o ochrane údajov a nariadením (EÚ) 2018/1725 (ďalej len „nariadenie o ochrane údajov inštitúciami EÚ“), keďže sa tu uplatňujú aspekty súvisiace s ochranou osobných údajov.

EDPB a EDPS súhlasia s návrhom v tom, že klasifikácia **systému umelej inteligencie ako vysokorizikového nevyhnutne neznamená, že je sám osebe zákonný** a používateľ ho môže využívať ako taký. Prevádzkovateľ bude pravdepodobne **musieť dodržiavať ďalšie požiadavky vyplývajúce z právnych predpisov EÚ o ochrane údajov**. Dodržiavanie právnych povinností vyplývajúcich z právnych predpisov Únie (vrátane v oblasti ochrany osobných údajov) by navyše malo byť podmienkou možnosti vstupu na európsky trh ako výrobok s označením CE. EDPB a EDPS sa preto domnievajú, že **požiadavka na zabezpečenie súladu so všeobecným nariadením o ochrane údajov a nariadením o ochrane údajov inštitúciami EÚ by sa mala zahrnúť do kapitoly 2 hlavy III**. EDPB a EDPS taktiež považujú za potrebné prispôbiť postup posudzovania zhody návrhu tak, aby tretie strany v prípade vysokorizikových systémov umelej inteligencie vždy vykonávali posudzovanie zhody *ex-ante*.

Vzhľadom na vysoké riziko diskriminácie sa v návrhu zakazuje „sociálne hodnotenie“ [social scoring], keď sa vykonáva „počas určitého obdobia“ alebo „orgánmi verejnej moci alebo v ich mene“. Súkromné spoločnosti, napríklad sociálne médiá a poskytovatelia cloudových služieb, však takisto môžu spracúvať obrovské množstvo osobných údajov a vykonávať sociálne hodnotenie. **V budúcom nariadení o umelej inteligencii by sa preto mal zakázať akýkoľvek druh sociálneho hodnotenia**.

Diaľková biometrická identifikácia jednotlivcov vo verejných priestoroch predstavuje vysoké riziko zásahu do súkromného života jednotlivcov, čo výrazne ovplyvňuje očakávania obyvateľstva, že bude vo verejných priestoroch anonymné. Z týchto dôvodov EDPB a EDPS **vyzývajú na všeobecný zákaz akéhokoľvek**

používania umelej inteligencie na automatické rozpoznávanie ľudských črt – ako sú tvár či chôdza, odtlačky prstov, DNA, hlas, spôsob písania na klávesnici a iné biometrické alebo behaviorálne signály – vo verejných priestoroch v akomkoľvek kontexte. Rovnako sa odporúča **zákaz systémov umelej inteligencie, ktoré na základe biometrických údajov kategorizujú jednotlivcov do skupín** podľa etnického pôvodu, pohlavia, či politickej alebo sexuálnej orientácie alebo iných dôvodov diskriminácie podľa článku 21 Charty. EDPB a EDPS sa okrem toho domnievajú, že používanie umelej inteligencie na **odvodenie emócií fyzickej osoby je absolútne nežiaduce a malo by sa zakázať**.

EDPB a EDPS vítajú **určenie EDPS ako príslušného orgánu** [the competent authority] **a orgánu dohľadu nad trhom** [the market surveillance authority] **pre dohľad nad inštitúciami, agentúrami a orgánmi Únie**. Význam a úlohy EDPS by sa však mali podrobnejšie objasniť, predovšetkým pokiaľ ide o jeho úlohu orgánu dohľadu nad trhom. Okrem toho by sa v budúcom nariadení o umelej inteligencii mala jasne stanoviť **nezávislosť dozorných orgánov** pri plnení svojich úloh v oblasti dohľadu a presadzovania.

Určením orgánov pre ochranu osobných údajov ako vnútroštátnych dozorných orgánov by sa preto zabezpečil harmonizovanejší regulačný prístup, prispelo by sa k jednotnému výkladu ustanovení týkajúcich sa spracúvania údajov a predišlo by sa rozporom pri ich presadzovaní v členských štátoch. EDPB a EDPS sa preto domnievajú, že **orgány pre ochranu osobných údajov by sa podľa článku 59 návrhu mali určiť ako vnútroštátne dozorné orgány**.

V návrhu sa Komisii zveruje rozhodujúca úloha v „Európskej rade pre umelú inteligenciu“ (EAIB). Takáto úloha je v rozpore s potrebou nezávislosti európskeho orgánu pre umelú inteligenciu od akéhokoľvek politického vplyvu. V budúcom nariadení by sa v záujme nezávislosti mala **EAIB poskytnúť väčšia autonómia** a zaistiť, aby mohla konať z vlastnej iniciatívy.

Vzhľadom na rozšírenie systémov umelej inteligencie na jednotnom trhu a pravdepodobnosť cezhraničných prípadov je mimoriadne potrebné harmonizované presadzovanie a riadne rozdelenie právomocí medzi vnútroštátnymi dozornými orgánmi. EDPB a EDPS navrhujú, aby sa pre každý systém umelej inteligencie stanovil **mechanizmus zaručujúci jednotné kontaktné miesto pre jednotlivcov ako aj pre spoločnosti, ktorých sa právne predpisy týkajú**.

Pokiaľ ide o **experimentálne prostredia**, EDPB a EDPS **odporúčajú objasniť ich rozsah a ciele**. V návrhu by sa tiež malo jasne uviesť, že právny základ takýchto experimentálnych prostredí by mal byť v súlade s požiadavkami stanovenými v existujúcom rámci na ochranu údajov.

Certifikačnému systému uvedenému v návrhu **chýba jednoznačný vzťah k právnym predpisom EÚ o ochrane údajov**, ako aj k iným právnym predpisom EÚ a členských štátov, ktoré sa vzťahujú na každú „oblasť“ vysokorizikového systému umelej inteligencie, a nezohľadňuje **zásady minimalizácie údajov a špecificky navrhutej ochrany údajov** ako jeden z aspektov, ktoré je potrebné zohľadniť **pred získaním označenia CE**. EDPB a EDPS preto odporúčajú zmeniť návrh tak, aby sa objasnil vzťah medzi certifikátmi vydanými podľa uvedeného nariadenia a certifikátmi, pečatami a značkami na ochranu údajov. A napokon, orgány pre ochranu osobných údajov by sa mali podieľať na príprave a stanovovaní harmonizovaných noriem a spoločných špecifikácií.

Pokiaľ ide o **kódexy správania**, EDPB a EDPS považujú za **potrebné objasniť**, či sa ochrana osobných údajov má považovať za jednu z „dodatočných požiadaviek“, ktoré môžu kódexy správania upravovať, a zabezpečiť, aby „technické špecifikácie a riešenia“ neboli v rozpore s pravidlami a zásadami existujúceho rámca EÚ na ochranu údajov.

OBSAH

1	ÚVOD.....	5
2	ANALÝZA KLÚČOVÝCH ZÁSAD NÁVRHU	7
2.1	Rozsah pôsobnosti návrhu a vzťah k existujúcemu právnemu rámcu	7
2.2	Prístup založený na riziku	8
2.3	Zakázané používanie umelej inteligencie	10
2.4	Vysokorizikové systémy umelej inteligencie.....	13
2.4.1	Potreba posudzovania zhody <i>ex-ante</i> externými tretími stranami	13
2.4.2	Rozsah pôsobnosti nariadenia sa musí vzťahovať aj na systémy umelej inteligencie, ktoré sa už používajú	13
2.5	Správa a riadenie a Európska rada pre umelú inteligenciu	14
2.5.1	Správa a riadenie.....	14
2.5.2	Európska rada pre umelú inteligenciu.....	16
3	INTERAKCIA S právnym rámcem pre ochranu osobných údajov	17
3.1	Vzťah návrhu k existujúcim právnym predpisom EÚ o ochrane údajov	17
3.2	Experimentálne prostredie a ďalšie spracúvanie (články 53 a 54 návrhu).....	18
3.3	Transparentnosť.....	20
3.4	Spracúvanie osobitných kategórií údajov a údajov týkajúce sa trestných činov	20
3.5	Mechanizmy na zabezpečenie súladu	21
3.5.1	Certifikácia.....	21
3.5.2	Kódexy správania.....	22
4	ZÁVER.....	23

Európsky výbor pre ochranu údajov a Európsky dozorný úradník pre ochranu údajov

so zreteľom na článok 42 ods. 2 nariadenia (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES¹,

so zreteľom na Dohodu o EHP, a najmä na jej prílohu XI a protokol 37, v znení rozhodnutia Spoločného výboru EHP č. 154/2018 zo 6. júla 2018²,

so zreteľom na žiadosť o spoločné stanovisko Európskeho dozorného úradníka pre ochranu údajov a Európskeho výboru pre ochranu údajov z 22. apríla 2021 k návrhu nariadenia, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (akt o umelej inteligencii),

PRIJALI TOTO SPOLOČNÉ STANOVISKO

1 ÚVOD

1. Nástup systémov umelej inteligencie je veľmi dôležitým krokom vo vývoji technológií a v spôsobe, akým s nimi ľudia zaobchádzajú. Umelá inteligencia predstavuje súbor kľúčových technológií, ktoré zásadne zmenia náš každodenný život, či už zo spoločenského alebo hospodárskeho hľadiska. V najbližších rokoch sa očakávajú zásadné rozhodnutia v oblasti umelej inteligencie, ktorá nám pomáha prekonávať niektoré z najväčších výziev, ktorým dnes v mnohých oblastiach čelíme, či už od zdravia po mobilitu, alebo od verejnej správy po vzdelávanie.
2. Tento sľubovaný pokrok však nie je bez rizika. Riziká sú skutočne veľmi relevantné vzhľadom na to, že účinky systémov umelej inteligencie na jednotlivca aj na spoločnosť sú do veľkej miery neznáme. Vytváranie obsahu, predvídanie alebo prijímanie rozhodnutí automatizovaným spôsobom pri využití techník strojového učenia alebo pravidiel logického a pravdepodobnostného odvodzovania, ako to robia systémy umelej inteligencie sa líši od spôsobu, akým by tieto činnosti vykonávali ľudia na základe kreatívneho alebo teoretického uvažovania, s plnou zodpovednosťou za dôsledky.
3. Umelá inteligencia rozšíri množstvo predpovedí, ktoré bude možné vykonať v mnohých oblastiach, počnúc merateľnými koreláciami medzi údajmi, ktoré sú neviditeľné pre ľudské oči, ale viditeľné pre stroje, čím sa zjednoduší náš život a vyrieši veľký počet problémov, zároveň však naruší našu schopnosť vysvetliť príčiny výsledkov v tom zmysle, že pojmy transparentnosti, ľudskej kontroly, zodpovednosti za výsledky a príslušné záväzky budú vážne spochybnené.

¹ Ú. v. EÚ L 295, 21.11.2018, s. 39 – 98.

² Odkazy na „členské štáty“ uvedené v tomto dokumente by sa mali chápať ako odkazy na „členské štáty EHP“.

4. Údaje (osobné a iné ako osobné) v rámci umelej inteligencie sú v mnohých prípadoch kľúčovým predpokladom pre autonómne rozhodnutia, ktoré nevyhnutne ovplyvnia životy jednotlivcov na rôznych úrovniach. EDPB a EDPS preto už v tejto fáze rozhodne tvrdia, že návrh nariadenia, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (akt o umelej inteligencii) (ďalej len „návrh“)³, má **významný vplyv na ochranu údajov**.
5. Prenechanie rozhodovania strojom na základe údajov bude predstavovať riziko pre práva a slobody jednotlivcov, ovplyvní ich súkromný život a môže poškodiť skupiny alebo dokonca spoločnosti ako celok. EDPB a EDPS zdôrazňujú, že práva na súkromný život a na ochranu osobných údajov, ktorým odporuje predpoklad autonómie strojového rozhodovania, ktorý je základom koncepcie umelej inteligencie, sú pilierom hodnôt EÚ uznaných vo Všeobecnej deklarácii ľudských práv (článok 12), Európskom dohovore o ľudských právach (článok 8) a Charte základných práv EÚ (ďalej len „Charta“) (články 7 a 8). Veľmi ambicióznym, no nevyhnutným cieľom je zosúladienie perspektívy rastu, ktorý ponúkajú aplikácie umelej inteligencie, s ústredným postavením a prvoradosťou človeka vo vzťahu k strojom.
6. EDPB a EDPS vítajú zapojenie všetkých zainteresovaných strán hodnotového reťazca umelej inteligencie do regulácie a zahrnutie osobitných požiadaviek na poskytovateľov riešení, keďže títo zohrávajú významnú úlohu pri produktoch, ktoré využívajú ich systémy. Povinnosti jednotlivých strán – používateľa, poskytovateľa, dovozcu alebo distribútora systému umelej inteligencie – však musia byť jasne vymedzené a pridelené. Najmä pri spracúvaní osobných údajov by sa mala venovať osobitná pozornosť súladu týchto úloh a zodpovedností s koncepciou prevádzkovateľa a sprostredkovateľa podľa rámca na ochranu údajov, keďže tieto dve normy nie sú zosúladiené.
7. V návrhu sa priznáva dôležitosť pojmu ľudského dohľadu (článok 14), čo EDPB a EDPS vítajú. Ako už bolo uvedené, vzhľadom na silný potenciálny vplyv určitých systémov umelej inteligencie na jednotlivcov alebo skupiny jednotlivcov by sa skutočné ústredné postavenie človeka malo prejavovať vo forme vysokokvalifikovaného ľudského dohľadu a zákonného spracúvania, pokiaľ sú takéto systémy založené na spracúvaní osobných údajov alebo spracúvajú osobné údaje pri plnení svojich úloh, aby sa tak zabezpečilo, že bude dodržané právo nebyť predmetom rozhodnutia založeného výlučne na automatizovanom spracúvaní.
8. Vzhľadom na to, že mnohé aplikácie umelej inteligencie intenzívne využívajú údaje, návrh by mal taktiež podporovať prijatie prístupu špecificky navrhutej a štandardnej ochrany údajov na všetkých úrovniach, a podporovať účinné vykonávanie zásad ochrany údajov (ako sa predpokladá v článku 25 všeobecného nariadenia o ochrane údajov a článku 27 nariadenia o ochrane údajov inštitúciami EÚ) prostredníctvom moderných [state-of-the-art] technológií.
9. EDPB a EDPS napokon zdôrazňujú, že toto spoločné stanovisko sa poskytuje len ako predbežná analýza návrhu, a nie je ním dotknuté žiadne ďalšie posúdenie a stanovisko k účinkom návrhu a jeho zlučiteľnosti s právnymi predpismi EÚ o ochrane údajov.

³ COM(2021) 206 final.

2 ANALÝZA KLÚČOVÝCH ZÁSAD NÁVRHU

2.1 Rozsah pôsobnosti návrhu a vzťah k existujúcemu právnemu rámcu

10. Podľa dôvodovej správy je **právnym základom** návrhu predovšetkým článok 114 ZFEÚ, v ktorom sa stanovuje prijatie opatrení na zabezpečenie vytvorenia a fungovania vnútorného trhu⁴. Návrh sa okrem toho zakladá na článku 16 ZFEÚ, *keďže obsahuje osobitné pravidlá ochrany jednotlivcov v súvislosti so spracúvaním osobných údajov*, najmä obmedzenia používania systémov umelej inteligencie na diaľkovú biometrickú identifikáciu v reálnom čase vo verejných priestoroch na účely presadzovania práva⁵.
11. EDPB a EDPS pripomínajú, že v súlade s judikatúrou SDEÚ článok 16 ZFEÚ predstavuje vhodný právny základ v prípadoch, keď je ochrana osobných údajov jedným zo základných cieľov alebo zložiek pravidiel prijatých zákonodarcom EÚ⁶. Uplatňovanie článku 16 ZFEÚ zahŕňa aj potrebu zabezpečiť nezávislý dohľad nad dodržiavaním požiadaviek týkajúcich sa spracúvania osobných údajov, ako sa vyžaduje aj v článku 8 Charty.
12. EDPS a EDPB pripomínajú, že už existuje komplexný rámec na ochranu údajov prijatý na základe článku 16 ZFEÚ, ktorý pozostáva zo všeobecného nariadenia o ochrane údajov⁷, nariadenia o ochrane údajov pre inštitúcie, úrady, orgány a agentúry Európskej únie (nariadenie o ochrane údajov inštitúciami EÚ)⁸ a smernice o presadzovaní práva⁹. Podľa návrhu možno za obmedzenia vychádzajúce z článku 16 ZFEÚ, ktoré by mali rovnaký právny základ ako všeobecné nariadenie o ochrane údajov, nariadenie o ochrane údajov inštitúciami EÚ alebo smernica o presadzovaní práva, považovať len za dodatočné obmedzenia uvedené v návrhu, ktoré sa týkajú spracúvania biometrických údajov. Má to významný vplyv na vzťah medzi návrhom a všeobecným nariadením o ochrane údajov, nariadením o ochrane údajov inštitúciami EÚ a smernicou o presadzovaní práva vo všeobecnosti, ako sa uvádza ďalej.
13. Pokiaľ ide o **rozsah pôsobnosti návrhu**, EDPS a EDPB jednoznačne vítajú skutočnosť, že návrh sa vzťahuje aj na používanie systémov umelej inteligencie inštitúciami, orgánmi alebo agentúrami EÚ. Vzhľadom na to, že používanie systémov umelej inteligencie týmito subjektmi môže mať významný vplyv aj na základné práva jednotlivcov, podobne ako v členských štátoch EÚ, je nevyhnutné, aby sa nový regulačný rámec pre umelú inteligenciu uplatňoval na členské štáty EÚ, ako aj na inštitúcie, úrady, orgány a agentúry EÚ s cieľom zabezpečiť jednotný

⁴ Dôvodová správa, s. 5.

⁵ Dôvodová správa, s. 6. Pozri aj odôvodnenie 2 návrhu.

⁶ Stanovisko z 26. júla 2017, PNR Kanada, Stanovisko 1/15, ECLI:EU:C:2017:592, bod 96.

⁷ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1 – 88).

⁸ Nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1725 z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES (Ú. v. EÚ L 295, 21.11.2018, s. 39 – 98).

⁹ Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV (Ú. v. EÚ L 119, 4.5.2016, s. 89 – 131).

prístup v rámci celej Únie. Keďže inštitúcie, úrady, orgány a agentúry EÚ môžu pôsobiť ako poskytovatelia aj používatelia systémov umelej inteligencie, EDPS a EDPB považujú za úplne vhodné zahrnúť tieto subjekty do rozsahu pôsobnosti návrhu na základe článku 114 ZFEÚ.

14. EDPB a EDPS však majú vážne obavy, pokiaľ ide o vylúčenie medzinárodnej spolupráce v oblasti presadzovania práva z rozsahu pôsobnosti stanoveného v článku 2 ods. 4 návrhu. Takýmto vylúčením vzniká značné riziko obchádzania (napr. tretie krajiny alebo medzinárodné organizácie prevádzkujúce vysokorizikové aplikácie, na ktoré sa spoliehajú orgány verejnej moci v EÚ).
15. Vývoj a používanie systémov umelej inteligencie bude v mnohých prípadoch zahŕňať spracúvanie osobných údajov. Mimoriadne dôležité je zabezpečiť jasnosť vzťahu tohto návrhu k existujúcim právnym predpisom EÚ o ochrane údajov. Návrhom nie sú dotknuté všeobecné nariadenie o ochrane údajov, nariadenie o ochrane údajov inštitúciami EÚ a smernica o presadzovaní práva, návrh ich iba dopĺňa. Hoci sa v odôvodneniach návrhu objasňuje, že používanie systémov umelej inteligencie by malo byť stále v súlade s právnymi predpismi o ochrane údajov, **EDPB a EDPS dôrazne odporúčajú v článku 1 objasniť, že právne predpisy Únie na ochranu osobných údajov**, najmä všeobecné nariadenie o ochrane údajov, nariadenie o ochrane údajov inštitúciami EÚ, smernica o súkromí a elektronických komunikáciách¹⁰ a smernica o presadzovaní práva sa uplatňujú na každé spracúvanie osobných údajov, ktoré patrí do rozsahu pôsobnosti tohto návrhu. V príslušnom odôvodnení by sa rovnako malo objasniť, že cieľom návrhu nie je ovplyvniť uplatňovanie existujúcich právnych predpisov EÚ, ktoré upravujú spracúvanie osobných údajov vrátane úloh a právomocí nezávislých dozorných orgánov oprávnených monitorovať dodržiavanie týchto nástrojov.

2.2 Prístup založený na riziku

16. EDPB a EDPS vítajú **prístup založený na riziku**, ktorý je základom návrhu. Návrh sa má vzťahovať na všetky systémy umelej inteligencie vrátane tých, ktoré nezahŕňajú spracúvanie osobných údajov, ale stále môžu mať vplyv na záujmy alebo základné práva a slobody.
17. EDPB a EDPS konštatujú, že v niektorých ustanoveniach návrhu sú vynechané riziká pre skupiny jednotlivcov alebo spoločnosť ako celok (napr. kolektívne účinky s osobitným významom, ako napríklad diskriminácia skupín alebo vyjadrovanie politických názorov vo verejných priestoroch). EDPB a EDPS odporúčajú, aby sa podobne posúdili a zmiernili aj riziká pre skupiny/spoločnosť, ktoré predstavujú systémy umelej inteligencie.
18. EDPB a EDPS zastávajú názor, že by sa mal objasniť v návrhu uvádzaný prístup založený na riziku a pojem „riziko pre základné práva“ by sa mal **zosúladiť so všeobecným nariadením o ochrane údajov**, pokiaľ sa uplatňujú aspekty súvisiace s ochranou osobných údajov. Bez ohľadu na to, či ide o koncových používateľov, len o dotknuté osoby alebo iné osoby, ktorých sa týka systém umelej inteligencie, skutočnosť, že v texte nie je uvedený žiadny odkaz na jednotlivca ovplyvneného systémom umelej inteligencie, pôsobí ako hluché miesto návrhu.

¹⁰ Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávaní osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), zmenená smernicou 2006/24/ES a smernicou 2009/136/ES.

Povinnosti uložené aktérom vo vzťahu k dotknutým osobám by skutočne mali konkrétnejšie vyplývať z ochrany jednotlivca a jeho práv. EDPB a EDPS preto naliehavo vyzývajú zákonodarcov, aby sa v návrhu výslovne zaoberali **právami a prostriedkami nápravy, ktoré majú k dispozícii jednotlivci**, ktorý sú ovplyvňovaní systémami umelej inteligencie.

19. EDPB a EDPS berú na vedomie voľbu poskytujúcu vyčerpávajúci zoznam **vysokorizikových systémov umelej inteligencie**. Táto voľba môže viesť k čiernobielemu prístupu, s nedostatočnými presvedčivými schopnosťami pre vysokorizikové situácie, čo by narušilo celkový prístup založený na riziku, ktorý je základom návrhu. V tomto zozname vysokorizikových systémov umelej inteligencie, ktorý je podrobne opísaný v prílohách II a III k návrhu, taktiež chýbajú niektoré typy prípadov použitia, ktoré so sebou prinášajú významné riziká, ako napríklad používanie umelej inteligencie na stanovenie poistného alebo na posudzovanie liečebných postupov alebo na účely výskumu v oblasti zdravia. EDPB a EDPS tiež zdôrazňujú, že tieto prílohy sa budú musieť pravidelne aktualizovať, aby sa zabezpečilo, že ich rozsah pôsobnosti bude primeraný.
20. V návrhu sa od **poskytovateľov** systému umelej inteligencie vyžaduje, aby vykonali posúdenie rizika, vo väčšine prípadov však prevádzkovateľmi (údajov) budú **používatelia** a nie poskytovatelia systémov umelej inteligencie (napr. používateľ systému rozpoznávania tváre je „prevádzkovateľom“, a preto nie je viazaný požiadavkami na poskytovateľov vysokorizikovej umelej inteligencie podľa návrhu).
21. Okrem toho poskytovateľ **nebude vždy môcť posúdiť všetky použitia** systému umelej inteligencie. Počiatočné posúdenie rizika bude mať teda všeobecnejší charakter ako posúdenie, ktoré vykonáva používateľ systému umelej inteligencie. Hoci z počiatočného posúdenia rizika, ktoré vykoná poskytovateľ, nevyplynie, že systém umelej inteligencie je podľa návrhu „vysokorizikový“, nemalo by to vylučovať **následné (podrobnejšie) posúdenie** [posúdenie vplyvu na ochranu údajov podľa článku 35 všeobecného nariadenia o ochrane údajov, článku 39 nariadenia o ochrane údajov inštitúciami EÚ alebo podľa článku 27 smernice o presadzovaní práva], **ktoré by mal vykonať používateľ systému** vzhľadom na kontext používania a konkrétne prípady použitia. Výklad toho, či určitý druh spracúvania môže viesť k vysokému riziku podľa všeobecného nariadenia o ochrane údajov, nariadenia o ochrane údajov inštitúciami EÚ a smernice o presadzovaní práva sa má vykonať nezávisle od návrhu. Klasifikácia systému umelej inteligencie ako systému, ktorý vzhľadom na jeho vplyv na základné práva predstavuje „vysoké riziko“¹¹, **však vedie k predpokladu „vysokého rizika“ podľa všeobecného nariadenia o ochrane údajov, nariadenia o ochrane údajov inštitúciami EÚ a smernice o presadzovaní práva v rozsahu, v akom sa spracúvajú osobné údaje.**

¹¹ Agentúra Európskej únie pre základné práva (FRA) sa už zaoberala potrebou vykonávať posúdenia vplyvu na základné práva pri používaní umelej inteligencie alebo súvisiacich technológií. Agentúra FRA vo svojej správe z roku 2020 s názvom [Getting the future right – Artificial intelligence and fundamental rights](#) (Správne smerovanie do budúcnosti: Umelá inteligencia a základné práva) identifikovala problémové miesta pri používaní umelej inteligencie, napríklad pri prediktívnom vykonávaní policajných funkcií, lekárskeho diagnostiky, sociálnych služieb a cielennej reklame a zdôraznila, že súkromné a verejné organizácie by mali vykonávať posúdenia toho, ako umelá inteligencia môže poškodzovať základné práva, aby znížovali negatívny vplyv na jednotlivcov.

22. **EDPB a EDPS súhlasia s návrhom v tom, že klasifikácia systému umelej inteligencie ako vysokorizikového nevyhnutne neznamená, že je sám osebe zákonný a používateľ ho môže využívať ako taký. Prevádzkovateľ bude možno musieť dodržať ďalšie požiadavky vyplývajúce z právnych predpisov EÚ o ochrane údajov.** Okrem toho odôvodnenie, z ktorého vychádza článok 5 návrhu, podľa ktorého na rozdiel od zakázaných systémov môžu vysokorizikové systémy v zásade byť prípustné, sa v návrhu musí vyriešiť a vyvrátiť, najmä preto, že navrhované označenie CE neznamená, že príslušné spracúvanie osobných údajov je zákonné.
23. Dodržiavanie právnych povinností vyplývajúcich z právnych predpisov Únie (vrátane v oblasti ochrany osobných údajov) by však malo byť podmienkou možnosti vstupu na európsky trh ako výrobok s označením CE. Na tento účel EDPB a EDPS **odporúčajú, aby sa do hlavy III kapitoly 2 návrhu zahrnula požiadavka na zabezpečenie súladu so všeobecným nariadením o ochrane údajov a nariadením o ochrane údajov inštitúciami EÚ.** Tieto požiadavky budú pred označením CE predmetom auditu (audit tretej strany) v súlade so zásadou zodpovednosti. V kontexte tohto posúdenia treťou stranou bude osobitne relevantné počiatočné posúdenie vplyvu, ktoré vykonáva poskytovateľ.
24. Vzhľadom na to, že vývoj systémov umelej inteligencie vedie k zložitým situáciám, by sa malo poukázať na to, že technické charakteristiky systémov umelej inteligencie (napr. typ prístupu umelej inteligencie) môžu viesť k väčším rizikám. V každom posúdení rizika systému umelej inteligencie by sa preto mali zohľadniť **technické charakteristiky spolu s konkrétnymi prípadmi jeho použitia a kontextom**, v ktorom systém funguje.
25. Vzhľadom na uvedené skutočnosti EDPB a EDPS odporúčajú, aby sa v návrhu upresnilo, že **poskytovateľ** vykoná počiatočné posúdenie rizika predmetného systému umelej inteligencie **vzhľadom na prípady použitia** (ktoré sa spresnia v návrhu – doplnením napríklad ods. 1 písm. a) prílohy III, kde sa neuvádzajú prípady použitia biometrických systémov umelej inteligencie) a že **používateľ** systému umelej inteligencie, vo svojej funkcii prevádzkovateľa systému umelej inteligencie podľa právnych predpisov EÚ o ochrane údajov prípadne vykoná posúdenie vplyvu na ochranu údajov, ako sa podrobne uvádza v článku 35 nariadenia o ochrane údajov, článku 39 nariadenia o ochrane údajov inštitúciami EÚ a článku 27 smernice o presadzovaní práva, a to so zreteľom nielen na technické charakteristiky a **prípady použitia**, ale aj na **konkrétny kontext**, v ktorom umelá inteligencia bude fungovať.
26. Okrem toho by sa mali objasniť niektoré pojmy uvedené v prílohe III k návrhu, napr. pojem „základné súkromné služby“ alebo malý poskytovateľ, ktorý využíva umelú inteligenciu na posúdenie úverovej bonity na vlastnú potrebu.

2.3 Zakázané používanie umelej inteligencie

27. EDPB a EDPS sa domnievajú, že **rušivé formy umelej inteligencie** — najmä tie s vplyvom na ľudskú dôstojnosť – sa majú považovať za zakázané systémy umelej inteligencie podľa článku 5 návrhu namiesto toho, aby boli jednoducho klasifikované ako „vysokorizikové“ v prílohe III k návrhu, ako sú napríklad systémy uvedené v bode 6. Týka sa to najmä porovnávania údajov, ktoré sa vo veľkom rozsahu dotýka aj osôb, pri ktorých neexistoval

žiadny alebo len minimálny dôvod na policajné pozorovanie alebo spracúvanie, čo porušuje zásadu obmedzenia účelu podľa právnych predpisov o ochrane údajov. Využívanie umelej inteligencie v oblasti policajnej práce a presadzovania práva si vyžaduje presné, predvídateľné a primerané pravidlá špecifické pre danú oblasť, ktoré musia zohľadňovať záujmy dotknutých osôb a vplyv na fungovanie demokratickej spoločnosti.

28. V článku 5 návrhu hrozí riziko, že sa „hodnoty“ a zákaz systémov umelej inteligencie budú v protiklade s týmito hodnotami posudzovať len formálne. Kritériá uvedené v článku 5 na identifikáciu zakázaných systémov umelej inteligencie **obmedzujú rozsah zákazu** do takej miery, že by sa v praxi mohol ukázať ako bezvýznamný [napr. „spôsobí alebo by mohol spôsobiť [...] fyzickú alebo psychickú ujmu“ v článku 5 ods. 1 písm. a) a b); obmedzenie na orgány verejnej moci v článku 5 ods. 1 písm. c); nejasné znenie v bodoch i) a ii) písm. c); obmedzenie na diaľkovú biometrickú identifikáciu v reálnom čase bez jasného vymedzenia atď.].
29. Najmä využívanie umelej inteligencie na „sociálne hodnotenie“, ako sa uvádza v článku 5 ods. 1 písm. c) návrhu, môže viesť k diskriminácii a je v rozpore so základnými hodnotami EÚ. V návrhu sa zakazujú tieto postupy len keď sa vykonávajú „počas určitého obdobia“ alebo „orgánmi verejnej moci alebo v ich mene“. Súkromné spoločnosti, najmä sociálne médiá a poskytovatelia cloudových služieb, však takisto môžu spracúvať obrovské množstvo osobných údajov a vykonávať sociálne hodnotenie. **V budúcom návrhu by sa preto mal zakázať akýkoľvek druh sociálneho hodnotenia.** Je potrebné poznamenať, že v kontexte presadzovania práva už článok 4 smernice o presadzovaní práva značne obmedzuje – ak prakticky nezakazuje – takýto druh činností.
30. **Diaľková biometrická identifikácia** jednotlivcov vo verejných priestoroch predstavuje vysoké riziko zásahu do súkromného života jednotlivcov. EDPB a EDPS sa preto **domnievajú, že je potrebný prísnejší prístup.** Používanie systémov umelej inteligencie môže viesť k vážnym problémom v oblasti primeranosti, keďže môže zahŕňať plošné spracúvanie údajov neprimeraného počtu dotknutých osôb na účely identifikácie len niekoľkých jednotlivcov (napr. cestujúci na letiskách a železničných staniaciach). **Jednoduchosť** povahy diaľkových biometrických identifikačných systémov takisto prináša problémy s transparentnosťou a otázky súvisiace s právnym základom spracúvania podľa právnych predpisov EÚ [smernica o presadzovaní práva, všeobecné nariadenie o ochrane údajov, nariadenie o ochrane údajov inštitúciami EÚ a iné uplatniteľné právne predpisy]. Problém týkajúci sa spôsobu, ako náležite informovať jednotlivcov o tomto spracúvaní, je stále nevyriešený, rovnako ako problém účinného a včasného výkonu práv jednotlivcov. To isté platí pre **nezvratný a závažný vplyv na** (primerané) **očakávanie obyvateľstva, že bude vo verejných priestoroch anonymné**, čo má priamy negatívny vplyv na uplatňovanie slobody prejavu, zhromažďovania, združovania, ako aj na slobodu pohybu.
31. V článku 5 ods. 1 písm. d) návrhu sa uvádza rozsiahly **zoznam výnimočných prípadov**, v ktorých je na účely presadzovania práva povolená diaľková biometrická identifikácia v reálnom čase vo verejných priestoroch. EDPB a EDPS sa domnievajú, že **tento prístup je chybný** vo viacerých aspektoch: Po prvé, nie je jasné, čo by sa malo chápať ako „výrazné oneskorenie“ a z akého dôvodu by sa malo považovať za poľahčujúci faktor vzhľadom na to,

že systém hromadnej identifikácie dokáže identifikovať tisíce jednotlivcov za pár hodín. Okrem toho rušivý charakter spracúvania nezávisí vždy od toho, či sa identifikácia vykonáva v reálnom čase alebo nie. Následná diaľková biometrická identifikácia v kontexte politického protestu bude mať pravdepodobne výrazný odstrašujúci účinok na uplatňovanie základných práv a slobôd, ako je sloboda zhromažďovania a združovania, a všeobecnejšie na základné zásady demokracie. Po druhé, rušivý charakter spracúvania nezávisí nevyhnutne od jeho účelu. Používanie tohto systému na iné účely, ako je napríklad súkromná bezpečnosť, predstavuje rovnaké ohrozenie základných práv na rešpektovanie súkromného a rodinného života a ochranu osobných údajov. Napokon, aj pri predpokladaných obmedzeniach bude potenciálny počet podozrivých alebo páchatel'ov trestných činov takmer vždy „dostatočne vysoký“ na odôvodnenie nepretržitého používania systémov umelej inteligencie na odhaľovanie podozrivých osôb, a to aj napriek ďalším podmienkam uvedeným v článku 5 ods. 2 až 4 návrhu. V odôvodnení návrhu sa podľa všetkého neuvádza, že pri monitorovaní otvorených priestranstiev musia byť povinnosti vyplývajúce z právnych predpisov EÚ o ochrane údajov splnené nielen pre podozrivé osoby, ale aj pre všetky osoby, ktoré sú v skutočnosti monitorované.

32. Zo všetkých týchto dôvodov EDPB a EDPS vyzývajú **na všeobecný zákaz akéhokoľvek používania umelej inteligencie na automatické rozpoznávanie ľudských črt – ako sú tvár či chôdza, odtlačky prstov, DNA, hlas, spôsob písania na klávesnici a iné biometrické alebo behaviorálne signály – vo verejných priestoroch v akomkoľvek kontexte**. Súčasným prístupom návrhu je identifikovať všetky systémy umelej inteligencie, ktoré by mali byť zakázané, a zostaviť ich zoznam. V záujme zaistenia súladu by sa preto podľa článku 5 návrhu mali **rozsiahle systémy umelej inteligencie na diaľkovú identifikáciu v online priestoroch zakázať**. Pri zohľadnení smernice o presadzovaní práva, nariadenia o ochrane údajov inštitúciami EÚ a všeobecného nariadenia o ochrane údajov EDPS a EDPB nedokážu identifikovať, ako by tento druh postupu mohol spĺňať požiadavky nevyhnutnosti a primeranosti, a v konečnom dôsledku to vyplýva z toho, čo SDEÚ a ESLP považujú za prijateľné zásahy do základných práv.
33. EDPB a EDPS okrem toho odporúčajú, aby sa orgánom verejnej moci aj súkromným subjektom **zakázali systémy umelej inteligencie, ktoré kategorizujú jednotlivcov na základe biometrických údajov (napríklad rozpoznávanie tváre) do skupín podľa etnického pôvodu, pohlavia, ako aj politickej alebo sexuálnej orientácie alebo iných dôvodov diskriminácie zakázaných podľa článku 21 Charty, alebo systémy umelej inteligencie, ktorých vedecká platnosť nie je preukázaná alebo ktoré sú v priamom rozpore so základnými hodnotami EÚ [napr. polygraf, príloha III bod 6. písm. b) a bod 7 písm. a)]. Príslušne by sa preto podľa článku 5 mala zakázať „biometrická kategorizácia“.**
34. **Ľudskú dôstojnosť ovplyvňuje aj skutočnosť, že počítač určuje alebo klasifikuje budúce správanie človeka nezávislé od jeho slobodnej vôle**. Systémy umelej inteligencie, ktoré majú používať orgány presadzovania práva na individuálne posúdenie rizika fyzických osôb s cieľom posúdiť riziko, ktoré fyzická osoba predstavuje z hľadiska (opakovaného) páchania trestnej činnosti, pozri prílohu III bod 6. písm. a), alebo na predvídanie výskytu alebo opakovaného výskytu skutočného alebo potenciálneho trestného činu na základe profilovania

fyzických osôb alebo na posúdenie osobnostných a povahových rysov alebo trestnej činnosti v minulosti, pozri prílohu III bod 6. písm. e), používané v súlade so zamýšľaným účelom povedú k zásadnému potlačeniu rozhodovania policajných a súdnych orgánov, a k zaobchádzaniu s dotknutou osobou ako s objektom. Takéto systémy umelej inteligencie, ktoré sa dotýkajú podstaty práva na ľudskú dôstojnosť, by mali byť zakázané podľa článku 5.

35. EDPB a EDPS sa okrem toho domnievajú, že používanie umelej inteligencie na **odvodzovanie emócií fyzickej osoby je absolútne nežiaduce a malo by sa zakázať**, s výnimkou určitých presne vymedzených prípadov použitia, konkrétne na zdravotné alebo výskumné účely (napr. pacienti, pri ktorých je dôležité rozpoznávanie emócií), vždy so zavedením primeraných záruk a samozrejme, pri uplatňovaní všetkých ostatných podmienok a obmedzení ochrany údajov vrátane obmedzenia účelu.

2.4 Vysokorizikové systémy umelej inteligencie

2.4.1 Potreba posudzovania zhody *ex-ante* externými tretími stranami

36. EDPB a EDPS vítajú, že systémy umelej inteligencie, ktoré predstavujú vysoké riziko, musia byť pred uvedením na trh alebo iným uvedením do prevádzky v EÚ predmetom predošlého posúdenia zhody. Tento regulačný model je v zásade vítaný, pretože ponúka dobrú rovnováhu medzi otvorenosťou voči inovácii a vysokou úrovňou proaktívnej ochrany základných práv. Využívanie v konkrétnych prostrediach, ako sú rozhodovacie procesy verejných inštitúcií alebo kritická infraštruktúra si vyžaduje stanovenie spôsobov, ako preskúmať úplný zdrojový kód.
37. EDPB a EDPS sa však zasadujú za prispôbenie postupu posudzovania zhody podľa článku 43 návrhu tak, aby sa **v prípade vysokorizikovej umelej inteligencie vo všeobecnosti vykonávalo posudzovanie zhody *ex-ante* tret'ou stranou**. Hoci posudzovanie zhody tret'ou stranou pri spracúvaní osobných údajov s vysokým rizikom nie je požiadavkou podľa všeobecného nariadenia o ochrane údajov ani nariadenia o ochrane údajov inštitúciami EÚ, riziká, ktoré predstavujú systémy umelej inteligencie, je stále ešte potrebné v plnej miere pochopiť. Všeobecným zahrnutím povinnosti posudzovania zhody tret'ou stranou by sa preto ďalej posilnila právna istota a dôvera vo všetky vysokorizikové systémy umelej inteligencie.

2.4.2 Rozsah pôsobnosti nariadenia sa musí vzťahovať aj na systémy umelej inteligencie, ktoré sa už používajú

38. Podľa článku 43 ods. 4 návrhu by sa pri vysokorizikových systémoch umelej inteligencie mal vykonať nový postup posudzovania zhody vždy, keď dôjde k významnej zmene. Je vhodné zabezpečiť, aby systémy umelej inteligencie spĺňali požiadavky nariadenia o umelej inteligencii počas celého svojho životného cyklu. Systémy umelej inteligencie, ktoré boli uvedené na trh alebo uvedené do prevádzky pred uplatňovaním navrhovaného nariadenia (alebo 12 mesiacov po začatí jeho uplatňovania v prípade rozsiahlych informačných systémov uvedených v prílohe IX), sú vylúčené z rozsahu jeho pôsobnosti, pokiaľ nedôjde k „významným zmenám“ koncepcie alebo zamýšľaného účelu týchto systémov (článok 83).

39. Kritérium „významných zmien“ je však nejasné. V odôvodnení 66 návrhu sa stanovuje nižšia úroveň kritéria pre opätovné posúdenie zhody „vždy, keď nastane zmena, ktorá môže ovplyvniť súlad“. Podobné kritérium by bolo vhodné pre článok 83, aspoň pri vysokorizikových systémoch umelej inteligencie. Okrem toho je v záujme odstránenia akýchkoľvek nedostatkov v ochrane potrebné, aby už zavedené systémy umelej inteligencie a systémy, ktoré sú v prevádzke – po určitej fáze vykonávania – taktiež spĺňali všetky požiadavky nariadenia o umelej inteligencii.
40. Bezpečnosť systémov umelej inteligencie ovplyvňujú aj početné možnosti spracúvania osobných údajov a vonkajšie riziká. V článku 83, ktorý je zameraný na „významné zmeny koncepcie alebo zamýšľaný účel“ nie je zahrnutý odkaz na zmeny vonkajších rizík. Do článku 83 návrhu by sa preto mal zahrnúť odkaz na zmeny scenára hrozby vyplývajúce z vonkajších rizík, napr. kybernetických útokov, nepriateľských útokov a odôvodnených sťažností spotrebiteľov.
41. Okrem toho, keďže začatie uplatňovania sa predpokladá 24 mesiacov po nadobudnutí účinnosti budúceho nariadenia, EDPS a EDPB nepovažujú za vhodné vyňať systémy umelej inteligencie, ktoré už boli uvedené na trh, na ešte dlhšie obdobie. Hoci sa v návrhu takisto stanovuje, že požiadavky nariadenia sa zohľadnia pri posudzovaní každého rozsiahleho informačného systému, ako sa stanovuje v právnych aktoch uvedených v prílohe IX, EDPB a EDPS sa domnievajú, že požiadavky týkajúce sa uvedenia systémov umelej inteligencie do prevádzky by mali byť uplatniteľné od dátumu začatia uplatňovania budúceho nariadenia.

2.5 Správa a riadenie a Európska rada pre umelú inteligenciu

2.5.1 Správa a riadenie

42. EDPB a EDPS vítajú určenie EDPS ako príslušného orgánu a orgánu dohľadu nad trhom pre dohľad nad inštitúciami, agentúrami a orgánmi Únie, pokiaľ spadajú do rozsahu pôsobnosti tohto návrhu. EDPS je pripravený plniť svoju novú úlohu regulačného orgánu pre umelú inteligenciu vo verejnej správe EÚ. Význam a úlohy EDPS však nie sú dostatočne podrobne opísané a mali by sa v návrhu ďalej objasniť, predovšetkým pokiaľ ide o jeho úlohu orgánu dohľadu nad trhom.
43. EDPB a EDPS berú na vedomie rozdelenie finančných zdrojov, ktoré sa v návrhu stanovuje pre EAIB a EDPS, ktorý koná ako notifikujúci orgán. Plnenie nových úloh, ktoré boli stanovené pre EDPS, alebo aj výkon funkcie notifikovanej osoby by si však vyžadovali výrazne vyššie finančné a ľudské zdroje.
44. Po prvé, pretože v znení článku 63 ods. 6 sa uvádza, že EDPS koná „ako orgán pre dohľad nad trhom“ pre inštitúcie, agentúry a orgány Únie, ktoré patria do rozsahu pôsobnosti návrhu, čím sa nevyjasňuje, či sa EDPS má považovať za plne realizovaný „orgán dohľadu nad trhom“, ako sa stanovuje v nariadení (EÚ) 2019/1020. Vznikajú tu otázky o praktických povinnostiach a právomociach EDPS. Po druhé a za predpokladu, že prvá otázka bude zodpovedaná kladne, nie je jasné, ako môže úloha EDPS, ako sa stanovuje v nariadení o ochrane údajov inštitúciami EÚ, zahŕňať úlohu stanovenú v článku 11 nariadenia (EÚ) 2019/1020, ktorá zahŕňa „účinný dohľad nad trhom s výrobkami sprístupnenými online“ alebo „fyzické a laboratórne kontroly

na základe primeraných vzoriek“. Existuje riziko, že prevzatie nového súboru úloh bez ďalšieho objasnenia v návrhu by mohlo ohroziť plnenie jeho povinností dozorného úradníka pre ochranu údajov.

45. EDPB a EDPS však zdôrazňujú, že niektoré ustanovenia návrhu, v ktorých sa vymedzujú úlohy a právomoci rôznych príslušných orgánov podľa nariadenia o umelej inteligencii, ich vzťahy, ich povaha a záruka ich nezávislosti, sa v tejto fáze zdajú byť nejasné. Kým v nariadení 2019/1020 sa uvádza, že orgán dohľadu nad trhom musí byť nezávislý, v návrhu nariadenia sa nevyžaduje, aby dozorné orgány boli nezávislé, a dokonca sa od nich vyžaduje, aby Komisii podávali správy o určitých úlohách, ktoré vykonávajú orgány dohľadu nad trhom, ktorými môžu byť rôzne inštitúcie. Keďže v návrhu sa tiež uvádza, že orgány pre ochranu osobných údajov budú orgánmi dohľadu nad trhom pre systémy umelej inteligencie používané na účely presadzovania práva (článok 63 ods. 5), znamená to aj to, že budú podliehať povinnosti podávať správy Komisii (článok 63 ods. 2), pravdepodobne prostredníctvom ich vnútroštátneho dozorného orgánu, čo sa zdá byť nezlučiteľné s ich nezávislosťou.
46. EDPB a EDPS sa preto domnievajú, že tieto ustanovenia je potrebné objasniť, aby boli v súlade s nariadením 2019/1020, nariadením o ochrane údajov inštitúciami EÚ a všeobecným nariadením o ochrane údajov, pričom v návrhu by sa malo jasne stanoviť, že dozorné orgány podľa nariadenia o umelej inteligencii musia byť pri plnení svojich úloh úplne nezávislé, keďže ide o hlavnú záruku riadneho dohľadu nad budúcim nariadením a jeho presadzovania.
47. EDPB a EDPS by taktiež chceli pripomenúť, že orgány pre ochranu údajov v prípade systémov umelej inteligencie zahŕňajúcich osobné údaje už presadzujú všeobecné nariadenie o ochrane údajov, nariadenie o ochrane údajov inštitúciami EÚ a smernicu o presadzovaní práva, aby zabezpečili ochranu základných práv a predovšetkým práva na ochranu údajov. Orgány pre ochranu osobných údajov už preto do určitej miery, ako sa to vyžaduje v návrhu pri vnútroštátnych dozorných orgánoch, rozumejú technológiám umelej inteligencie, údajom a ich spracúvaniu, základným právam, a majú aj odborné znalosti pokiaľ ide o posudzovanie rizík pre základné práva, ktoré predstavujú nové technológie. V prípade systémov umelej inteligencie založených na spracúvaní osobných údajov alebo ktoré spracúvajú osobné údaje, sú navyše ustanovenia návrhu priamo prepojené s právnym rámcom na ochranu údajov, čo bude platiť pre väčšinu systémov umelej inteligencie v rozsahu pôsobnosti nariadenia. Preto budú právomoci dozorných orgánov podľa návrhu a orgánmi pre ochranu osobných údajov navzájom poprepájané.
48. Určením orgánov pre ochranu osobných údajov ako vnútroštátnych dozorných orgánov by sa preto zabezpečil harmonizovanejší regulačný prístup a prispelo by sa k jednotnému výkladu ustanovení týkajúcich sa spracúvania údajov a predišlo by sa rozporom pri ich presadzovaní v členských štátoch. Prínosom pre všetky zainteresované strany hodnotového reťazca umelej inteligencie by bolo aj jednotné kontaktné miesto pre všetky spracovateľské operácie osobných údajov, ktoré patria do rozsahu pôsobnosti návrhu, a obmedzenie interakcií medzi dvoma rôznymi regulačnými orgánmi pre spracúvanie, ktorých sa návrh a všeobecné nariadenie o ochrane údajov týkajú. EDPB a EDPS sa preto domnievajú, že **orgány pre ochranu osobných údajov by sa podľa článku 59 návrhu mali určiť ako vnútroštátne dozorné orgány.**

49. V každom prípade, keďže návrh obsahuje osobitné pravidlá ochrany jednotlivcov pri spracúvaní osobných údajov prijaté na základe článku 16 ZFEÚ, dodržiavanie týchto pravidiel, najmä obmedzenie používania systémov umelej inteligencie na diaľkovú biometrickú identifikáciu v reálnom čase vo verejných priestoroch na účely presadzovania práva, **musí podliehať kontrole nezávislých orgánov**.
50. Návrh však neobsahuje žiadne výslovné ustanovenie, ktorým by sa právomoc zabezpečovať dodržiavanie týchto pravidiel zverila pod kontrolu nezávislých orgánov. Jediný odkaz na príslušné dozorné orgány pre ochranu údajov podľa všeobecného nariadenia o ochrane údajov alebo smernice o presadzovaní práva je uvedený v článku 63 ods. 5 návrhu, ale len ako odkaz na orgány dohľadu nad trhom a alternatívne s niektorými ďalšími orgánmi. EDPB a EDPS sa domnievajú, že týmto spôsobom nie je zabezpečený súlad s požiadavkou nezávislej kontroly stanovenou v článku 16 ods. 2 ZFEÚ a článku 8 Charty.

2.5.2 Európska rada pre umelú inteligenciu

51. Návrhom sa zriaďuje „Európska rada pre umelú inteligenciu“ (EAIB). EDPB a EDPS uznávajú potrebu jednotného a harmonizovaného uplatňovania navrhovaného rámca, ako aj zapojenia nezávislých expertov do prípravy politiky EÚ v oblasti umelej inteligencie. V návrhu sa zároveň predpokladá, že Komisia bude mať rozhodujúcu úlohu. Bola by totiž nielen súčasťou EAIB, ale jej aj predsedala a mala by právo veta pri prijímaní rokovacieho poriadku EAIB. Je to v rozpore s potrebou nezávislosti európskeho orgánu pre umelú inteligenciu od akéhokoľvek politického vplyvu. EDPB a EDPS sa preto domnievajú, že budúce nariadenie o umelej inteligencii by malo **poskytnúť EIAB viac autonómie**, aby mohla skutočne zabezpečovať jednotné uplatňovanie nariadenia na celom jednotnom trhu.
52. EDPB a EDPS tiež poznamenávajú, že EAIB sa neudeľuje žiadna právomoc týkajúca sa presadzovania navrhovaného nariadenia. Vzhľadom na rozširovanie systémov umelej inteligencie na jednotnom trhu a pravdepodobnosť cezhraničných prípadov je však mimoriadne potrebné harmonizované presadzovanie a riadne rozdelenie právomocí medzi vnútroštátnymi dozornými orgánmi. EDPB a EDPS preto odporúčajú, aby sa v budúcom nariadení o umelej inteligencii stanovili mechanizmy spolupráce medzi vnútroštátnymi dozornými orgánmi. EDPB a EDPS navrhujú zaviesť mechanizmus zaručujúci jednotné kontaktné miesto pre jednotlivcov ako aj pre spoločnosti, ktorých sa právne predpisy týkajú, pre každý systém umelej inteligencie, a v prípade organizácií, ktorých činnosť pokrýva viac ako polovicu členských štátov EÚ, EAIB môže určiť vnútroštátny orgán, ktorý bude zodpovedný za presadzovanie nariadenia o umelej inteligencii pri tomto systéme umelej inteligencie.
53. Okrem toho, vzhľadom na nezávislý povahu orgánov, ktoré majú tvoriť EIAB, bude táto rada oprávnená konať z vlastnej iniciatívy a nielen poskytovať Komisii poradenstvo a pomoc. EDPB a EDPS preto zdôrazňujú potrebu rozšírenia úlohy pridelenej rade, ktorá navyše nezodpovedá úlohám uvedeným v návrhu.
54. Na splnenie týchto cieľov **má EAIB mať dostatočné a primerané právomoci** a jej právne postavenie by sa malo objasniť. Predovšetkým sa zdá, že na to, aby vecná pôsobnosť budúceho nariadenia zostala relevantná, je potrebné do jeho prípravy zapojiť orgány zodpovedné za jeho

uplatňovanie. EDPB a EDPS preto odporúčajú, aby bola EAIB splnomocnená navrhovať Komisii zmeny prílohy I, v ktorej sa vymedzujú techniky a prístupy umelej inteligencie, a prílohy III, v ktorej sa uvádzajú vysokorizikové systémy umelej inteligencie uvedené v článku 6 ods. 2. Komisia by sa tiež mala poradiť s EAIB pred každou zmenou týchto príloh.

55. V článku 57 ods. 4 návrhu sa predpokladá výmena informácií radou a inými orgánmi, úradmi, agentúrami a poradnými skupinami Únie. Vzhľadom na svoju predchádzajúcu prácu v oblasti umelej inteligencie a odborné znalosti v oblasti ľudských práv EDPB a EDPS odporúčajú, aby sa Agentúra pre základné práva považovala za jedného z pozorovateľov rady.

3 INTERAKCIA S PRÁVNÝM RÁMCOM PRE OCHRANU OSOBNÝCH ÚDAJOV

3.1 Vzťah návrhu k existujúcim právnym predpisom EÚ o ochrane údajov

56. Jasne vymedzený vzťah medzi návrhom a existujúcimi právnymi predpismi o ochrane údajov je základným predpokladom na zabezpečenie a zachovanie dodržiavania a uplatňovania acquis Únie v oblasti ochrany osobných údajov. Takéto právne predpisy EÚ, najmä všeobecné nariadenie o ochrane údajov, nariadenie o ochrane údajov inštitúciami EÚ a smernica o presadzovaní práva, sa musia považovať za predpoklad, z ktorého môžu vychádzať ďalšie legislatívne návrhy bez toho, aby boli dotknuté existujúce ustanovenia alebo bez zasahovania do nich, a to aj pokiaľ ide o právomoc dozorných orgánov a správu a riadenie.
57. Podľa EDPB a EDPS je preto dôležité, aby sa v návrhu jasne zabránilo akémukoľvek nesúladu a možnému konfliktu so všeobecným nariadením o ochrane údajov, nariadením o ochrane údajov inštitúciami EÚ a smernicou o presadzovaní práva. Je to potrebné nielen v záujme právnej istoty, ale aj na zabránenie tomu, aby návrh priamo alebo nepriamo ohrozil základné právo na ochranu osobných údajov, ako je stanovené v článku 16 ZFEÚ a článku 8 Charty.
58. Stroje, ktoré sa dokážu samostatne učiť, môžu chrániť osobné údaje jednotlivcov len vtedy, ak je to zakotvené už v ich koncepcii. Podstatná je aj okamžitá možnosť uplatniť práva jednotlivcov podľa článku 22 (Automatizované individuálne rozhodovanie vrátane profilovania) všeobecného nariadenia o ochrane údajov alebo článku 23 nariadenia o ochrane údajov inštitúciami EÚ bez ohľadu na účely spracúvania. V tejto súvislosti musia byť v systémoch umelej inteligencie od samého začiatku zahrnuté ďalšie práva dotknutých osôb týkajúce sa práva na vymazanie, práva na opravu podľa právnych predpisov o ochrane údajov, a to bez ohľadu na zvolený prístup umelej inteligencie alebo technickú architektúru.
59. Používanie osobných údajov na učenie systémov umelej inteligencie môže v jadre systému umelej inteligencie viesť k vzniku zaujatých rozhodovacích modelov [biased decision-making patterns]. Preto by sa mali vyžadovať rôzne záruky, a najmä kvalifikovaný ľudský dohľad nad takýmito procesmi, aby sa zabezpečilo dodržiavanie a zaručenie práv dotknutých osôb, ako aj aby sa zabránilo akýmukoľvek negatívnym vplyvom na jednotlivcov. Príslušné orgány by tiež mali mať možnosť navrhovať usmernenia k posudzovaniu zaujatosti v systémoch umelej inteligencie a pomáhať pri výkone ľudského dohľadu.

60. Dotknuté osoby by mali byť vždy informované o tom, keď sa ich údaje používajú na tréovanie umelej inteligencie a/alebo na predpovedanie pomocou umelej inteligencie, o právnom základe takéhoto spracúvania, všeobecnom vysvetlení logiky (postupu) a rozsahu pôsobnosti systému umelej inteligencie. V tejto súvislosti by sa v týchto prípadoch malo vždy zaručiť právo jednotlivcov na obmedzenie spracúvania údajov (článok 18 všeobecného nariadenia o ochrane údajov a článok 20 nariadenia o ochrane údajov inštitúciami EÚ), ako aj na vymazanie údajov (článok 16 všeobecného nariadenia o ochrane údajov a článok 19 nariadenia o ochrane údajov inštitúciami EÚ). Prevádzkovateľ by okrem toho mal mať výslovnú povinnosť informovať dotknutú osobu o príslušných lehotách na vznesenie námietok, obmedzenie, vymazanie údajov atď. Systém umelej inteligencie musí byť schopný splniť všetky požiadavky na ochranu údajov formou primeraných technických a organizačných opatrení. Právo na vysvetlenie by malo zabezpečiť dodatočnú transparentnosť.

3.2 Experimentálne prostredie a ďalšie spracúvanie (články 53 a 54 návrhu)

61. V rámci existujúcich právnych a morálnych hraníc je dôležité podporovať európske inovácie prostredníctvom nástrojov ako je experimentálne prostredie. Experimentálne prostredie umožňuje poskytnúť záruky potrebné na vybudovanie dôvery a možnosti spoľahnúť sa na systémy umelej inteligencie. V zložitých prostrediach môže byť pre odborníkov v oblasti umelej inteligencie ťažké náležite zvážiť všetky záujmy. Najmä v prípade malých a stredných podnikov s obmedzenými zdrojmi môže využívanie experimentálneho prostredia viesť k rýchlejšiemu získaniu informácií, a tým podporiť inovácie.
62. V článku 53 ods. 3 návrhu sa uvádza, že experimentálne prostredie nemá vplyv na právomoci v oblasti dohľadu a nápravy. V prípade, že takéto objasnenie je nápomocné, je potrebné vypracovať aj pokyny alebo usmernenia k tomu, ako dosiahnuť správnu rovnováhu medzi postavením dozorného orgánu na jednej strane a poskytovaním podrobných usmernení prostredníctvom experimentálnych prostredí na strane druhej.
63. V článku 53 ods. 6 sa opisuje, že spôsoby a podmienky fungovania experimentálnych prostredí sa stanovujú vo vykonávacích aktoch. Je dôležité vypracovať osobitné usmernenia s cieľom zabezpečiť konzistentnosť a podporu pri zriaďovaní a prevádzke experimentálnych prostredí. Záväzný vykonávací akt by však mohli obmedziť schopnosť každého členského štátu prispôbiť experimentálne prostredie svojim potrebám a miestnym postupom. EDPB a EDPS preto odporúčajú, aby usmernenia pre experimentálne prostredia namiesto toho poskytovala EAIB.
64. Zámerom článku 54 návrhu je poskytnúť právny základ pre ďalšie spracúvanie osobných údajov na účely vývoja určitých systémov umelej inteligencie vo verejnom záujme v experimentálnom regulačnom prostredí pre umelú inteligenciu. Vzťah medzi článkom 54 ods. 1 návrhu a článkom 54 ods. 2 a odôvodnením 41 návrhu, a teda aj existujúcimi právnymi predpismi EÚ o ochrane údajov, zostáva nejasný. Vo všeobecnom nariadení o ochrane údajov a nariadení o ochrane údajov inštitúciami EÚ však už je stanovený základ pre „ďalšie spracúvanie“. Najmä v prípadoch, keď je umožnenie ďalšieho spracúvania vo verejnom záujme nemusí nájsť rovnováhu medzi záujmami prevádzkovateľa a záujmami dotknutej osoby

brániť inovácii. V článku 54 návrhu sa v súčasnosti neriešia dve dôležité otázky: i) za akých okolností, na základe akých (dodatočných) kritérií sa záujmy dotknutých osôb vážia, a ii) či sa tieto systémy umelej inteligencie budú používať len v experimentálnom prostredí. EDPB a EDPS vítajú požiadavku na právne predpisy Únie alebo členského štátu pri spracúvaní osobných údajov získaných podľa smernice o presadzovaní práva v experimentálnom prostredí, ale odporúčajú podrobnejšiu špecifikáciu v súlade so všeobecným nariadením o ochrane údajov a s nariadením o ochrane údajov inštitúciami EÚ, a najmä objasnenie, že právny základ takýchto experimentálnych prostredí by mal byť v súlade s požiadavkami stanovenými v článku 23 ods. 2 všeobecného nariadenia o ochrane údajov a v článku 25 nariadenia o ochrane údajov inštitúciami EÚ, a spresnenie, že každé použitie experimentálneho prostredia musí byť dôkladne vyhodnotené. Platí to aj pre úplný zoznam podmienok z článku 54 ods. 1 písm. b) až j).

65. Z niektorých ďalších úvah týkajúcich sa opätovného použitia údajov v článku 54 návrhu vyplýva, že prevádzkovanie experimentálneho prostredia je náročné na zdroje, a preto je realistické predpokladať, že možnosť zúčastniť sa by mal len malý počet podnikov. Účasť v experimentálnom prostredí by mohla predstavovať konkurenčnú výhodu. Umožnenie opakovaného použitia údajov by si vyžadovalo starostlivé zváženie toho, ako vybrať účastníkov, aby sa zabezpečilo, že budú patriť do rozsahu pôsobnosti a aby sa predišlo nespravodlivému zaobchádzaniu. EDPB a EDPS sa obávajú, že umožnenie opakovaného použitia údajov v rámci experimentálneho prostredia je odchýlením sa od prístupu založeného na zodpovednosti vo všeobecnom nariadení o ochrane údajov, pri ktorom zodpovednosť nesie prevádzkovateľ a nie príslušný orgán.
66. Okrem toho sa EDPB a EDPS domnievajú, že vzhľadom na ciele experimentálnych prostredí, ktorými sú vývoj, testovanie a validácia systémov umelej inteligencie, nemôžu experimentálne prostredia patriť do rozsahu pôsobnosti smernice o presadzovaní práva. Hoci sa opakované použitie údajov na vedecký výskum predpokladá v smernici o presadzovaní práva, údaje spracúvané na tento sekundárny účel budú podliehať všeobecnému nariadeniu o ochrane údajov alebo nariadeniu o ochrane údajov inštitúciami EÚ a nebudú už podliehať smernici o presadzovaní práva.
67. Nie je jasné, čo bude experimentálne regulačné prostredie zahŕňať. Vzniká otázka, či navrhované experimentálne regulačné prostredie zahŕňa infraštruktúru IT v každom členskom štáte s dodatočnými právnymi dôvodmi na ďalšie spracúvanie, alebo či iba organizuje prístup k odborným znalostiam a usmerneniam v oblasti regulácie. EDPB a EDPS naliehavo vyzývajú zákonodarcu, aby v návrhu objasnil túto koncepciu a aby v návrhu jasne uviedol, že z experimentálneho regulačného prostredia nevyplýva povinnosť príslušných orgánov poskytovať technickú infraštruktúru. V každom prípade sa musia príslušným orgánom poskytnúť finančné a ľudské zdroje v súlade s takýmto objasnením.
68. EDPB a EDPS by napokon chceli zdôrazniť rozvoj cezhraničných systémov umelej inteligencie, ktoré budú k dispozícii pre európsky jednotný digitálny trh ako celok. V prípade takýchto systémov umelej inteligencie by experimentálne regulačné prostredie ako nástroj inovácie nemalo byť prekážkou cezhraničného rozvoja. EDPB a EDPS preto odporúčajú

koordinovaný cezhraničný prístup, ktorý je stále dostatočne dostupný na vnútroštátnej úrovni pre všetky MSP a ktorý ponúka spoločný rámec v celej Európe bez toho, aby bol príliš reštriktívny. Musí sa dosiahnuť rovnováha medzi európskou koordináciou a vnútroštátnymi postupmi, aby sa zabránilo protichodnému vykonávaniu budúceho nariadenia o umelej inteligencii, ktoré by bránilo inováciám v celej EÚ.

3.3 Transparentnosť

69. EDPB a EDPS vítajú, že vysokorizikové systémy umelej inteligencie sa zaregistrujú vo verejnej databáze (podľa článkov 51 a 60 návrhu). Táto databáza by sa mala využiť ako možnosť poskytovať informácie širokej verejnosti o rozsahu využívania systému umelej inteligencie a známych chybách a incidentoch, ktoré by mohli ohroziť jeho fungovanie, a o nápravných opatreniach prijatých poskytovateľmi na ich riešenie a nápravu.
70. Základnou demokratickou zásadou je uplatňovanie systému brzd a protiváh. Skutočnosť, že povinnosť transparentnosti sa nevzťahuje na systémy umelej inteligencie používané na odhaľovanie, prevenciu, vyšetrovanie alebo stíhanie trestných činov, je preto príliš širokou výnimkou. Je potrebné rozlišovať medzi systémami umelej inteligencie, ktoré sa používajú na odhaľovanie alebo prevenciu, a systémami umelej inteligencie, ktorých cieľom je vyšetrovanie alebo pomoc pri stíhaní trestných činov. Záruky v prípade prevencie a odhaľovania musia byť prísnejšie z dôvodu prezumpcie neviny. EDPB a EDPS okrem toho vyjadrujú poľutovanie nad tým, že v návrhu nie sú uvedené varovné upozornenia, čo je možné vykladať ako pozitívny signál pre používanie aj neoverených, vysokorizikových systémov alebo aplikácií umelej inteligencie.
71. V prípadoch, keď je z dôvodu utajenia voči verejnosti možné zabezpečiť len minimálnu alebo žiadnu transparentnosť, a to aj v dobre fungujúcej demokracii, mali by sa zaviesť záruky a tieto systémy umelej inteligencie by mali byť zaregistrované na príslušnom dozornom orgáne a mali by voči nemu byť transparentné.
72. Zabezpečenie transparentnosti systémov umelej inteligencie je veľmi náročným cieľom. Plne kvantitatívny prístup mnohých systémov umelej inteligencie k rozhodovaniu, ktorý je svojou podstatou odlišný od ľudského prístupu a ktorý väčšinou vychádza z kauzálneho a teoretického odôvodnenia, môže byť v rozpore s potrebou vopred získať zrozumiteľné vysvetlenie výsledkov činnosti strojov. V nariadení by sa mali podporovať nové, proaktívnejšie a včasné spôsoby informovania používateľov systémov umelej inteligencie o stave (rozhodovania), v ktorom sa systém nachádza, čím sa zabezpečí včasné varovanie pred možnými škodlivými dôsledkami, aby tak osoby, ktorých práva a slobody môžu byť autonómnymi rozhodnutiami stroja porušené, mohli reagovať alebo rozhodnutie napraviť.

3.4 Spracúvanie osobitných kategórií údajov a údajov týkajúce sa trestných činov

73. Spracúvanie osobitných kategórií údajov v oblasti presadzovania práva sa riadi ustanoveniami rámca EÚ na ochranu údajov vrátane smernice o presadzovaní práva, ako aj jeho vnútroštátnym vykonávaním. V návrhu sa tvrdí, že neposkytuje všeobecný právny základ pre spracúvanie osobných údajov vrátane osobitných kategórií osobných údajov, pozri odôvodnenie 41. V článku 10 ods. 5 návrhu sa zároveň uvádza, že „poskytovatelia takýchto systémov môžu spracúvať

osobitné kategórie osobných údajov“. Okrem toho sa v tom istom ustanovení vyžadujú dodatočné záruky, pričom sa uvádzajú aj príklady. Návrh teda podľa všetkého zasahuje do uplatňovania všeobecného nariadenia o ochrane údajov, smernice o presadzovaní práva a nariadenia o ochrane údajov inštitúciami EÚ. Hoci EDPB a EDPS vítajú pokus o zabezpečenie primeraných záruk, je potrebný ucelenejší regulačný prístup, keďže súčasné ustanovenia podľa všetkého nie sú dostatočne jasné na vytvorenie právneho základu pre spracúvanie osobitných kategórií údajov, a je potrebné ich doplniť dodatočnými ochrannými opatreniami, ktoré je ešte potrebné posúdiť. Okrem toho, keď sa osobné údaje zozbierajú v rámci spracúvania v rozsahu pôsobnosti smernice o presadzovaní práva, je potrebné zohľadniť možné dodatočné záruky a obmedzenia vyplývajúce z vnútroštátnych transpozícií smernice o presadzovaní práva.

3.5 Mechanizmy na zabezpečenie súladu

3.5.1 Certifikácia

74. Jedným z hlavných pilierov návrhu je certifikácia. Certifikačný systém uvedený v návrhu vychádza zo štruktúry subjektov (notifikujúce orgány/notifikované osoby/Komisia) a z mechanizmu posudzovania zhody/certifikácie, ktorý zahŕňa povinné požiadavky, ktoré sa vzťahujú na vysokorizikové systémy umelej inteligencie, a je založený na európskych harmonizovaných normách podľa nariadenia (EÚ) č. 1025/2012 a spoločných špecifikáciách, ktoré stanoví Komisia. Tento mechanizmus sa líši od certifikačného systému zameraného na zabezpečenie súladu s pravidlami a zásadami ochrany údajov opísaného v článkoch 42 a 43 všeobecného nariadenia o ochrane údajov. Nie je však jasný vzťah certifikátov vydaných notifikovanými osobami v súlade s návrhom a certifikácie, pečatami a značkami ochrany údajov stanovenými vo všeobecnom nariadení o ochrane údajov, na rozdiel od toho, čo je stanovené pre iné typy certifikácie [pozri článok 42 ods. 2, pokiaľ ide o certifikácie vydané podľa nariadenia (EÚ) 2019/881].
75. Ak vysokorizikové systémy umelej inteligencie sú založené na spracúvaní osobných údajov alebo osobné údaje spracúvajú s cieľom splniť svoju úlohu, tieto nezrovnalosti môžu spôsobovať právnu neistotu pre všetky dotknuté orgány, pretože môžu viesť k situáciám, v ktorých by systémy umelej inteligencie certifikované podľa návrhu a označené označením CE po uvedení na trh alebo uvedení do prevádzky mohli byť použité spôsobom, ktorý nie je v súlade s pravidlami a zásadami ochrany údajov.
76. V návrhu chýba jasný vzťah k právnym predpisom o ochrane údajov, ako aj k iným právnym predpisom EÚ a členských štátov, ktoré sa vzťahujú na každú „oblasť“ vysokorizikového systému umelej inteligencie uvedenú v prílohe III. Návrh by mal predovšetkým pri aspektoch, ktoré treba zohľadniť pred získaním označenia CE, zahŕňať zásady minimalizácie údajov a špecificky navrhnutej ochrany údajov, vzhľadom na možnú vysokú úroveň zasahovania vysokorizikových systémov umelej inteligencie do základných práv na súkromie a ochranu osobných údajov a na potrebu zabezpečiť vysokú úroveň dôvery v systém umelej inteligencie. EDPB a EDPS preto odporúčajú zmeniť návrh tak, aby sa objasnil vzťah medzi certifikátmi vydanými podľa uvedeného nariadenia a certifikátmi, pečatami a značkami na ochranu údajov.

V neposlednom rade, orgány pre ochranu osobných údajov by sa mali podieľať na príprave a stanovovaní harmonizovaných noriem a spoločných špecifikácií.

77. V súvislosti s článkom 43 návrhu, ktorý sa týka posudzovania zhody, je výnimka z postupu posudzovania zhody stanovená v článku 47 podľa všetkého veľmi široká, pričom zahŕňa príliš veľký počet výnimočných situácií, ako sú napríklad výnimočné dôvody verejnej bezpečnosti alebo ochrana života a zdravia osôb, ochrana životného prostredia a ochrana kľúčových priemyselných a infraštruktúrnych aktív. Navrhujeme zákonodarcov, aby tieto výnimky zúžili.

3.5.2 Kódexy správania

78. Podľa článku 69 návrhu Komisia a členské štáty nabádajú k vypracovaniu kódexov správania určených na podporu toho, aby poskytovatelia systémov umelej inteligencie, ktoré nepredstavujú vysoké riziko, dobrovoľne uplatňovali požiadavky vzťahujúce sa na vysokorizikové systémy umelej inteligencie, ako aj dodatočné požiadavky. V súlade s odôvodnením 78 všeobecného nariadenia o ochrane údajov EDPS a EDPS odporúčajú identifikovať a vymedziť synergie medzi týmito nástrojmi a kódexmi správania stanovenými vo všeobecnom nariadení o ochrane údajov, ktoré podporujú dodržiavanie požiadaviek na ochranu údajov. V tejto súvislosti je dôležité objasniť, či sa ochrana osobných údajov má považovať za jednu z „dodatočných požiadaviek“, ktoré môžu byť predmetom kódexov správania podľa článku 69 ods. 2. Okrem toho je dôležité zabezpečiť, aby „technické špecifikácie a riešenia“, ktoré sú predmetom kódexov správania podľa článku 69 ods. 1 a ktoré sú určené na podporu súladu s požiadavkami návrhu nariadenia o umelej inteligencii, neboli v rozpore s pravidlami a zásadami všeobecného nariadenia o ochrane údajov a nariadenia o ochrane údajov inštitúciami EÚ. Dodržiavanie týchto nástrojov zo strany poskytovateľov systémov umelej inteligencie, ktoré nepredstavujú vysoké riziko – pokiaľ sú takéto systémy založené na spracúvaní osobných údajov alebo spracúvajú osobné údaje na účely plnenia ich úloh – by tým predstavovalo pridanú hodnotu, keďže by sa zabezpečilo, že prevádzkovatelia a sprostredkovatelia budú môcť plniť svoje povinnosti v oblasti ochrany údajov súvisiace s používaním týchto systémov.
79. Právny rámec pre dôveryhodnú umelú inteligenciu by zároveň bol doplnený zahrnutím kódexov správania s cieľom posilniť dôveru v používanie tejto technológie bezpečným spôsobom a v súlade s právom vrátane dodržiavania základných práv. Koncepcia týchto nástrojov by sa však mala posilniť mechanizmami zameranými na overenie toho, či takéto kódexy poskytujú účinné „technické špecifikácie a riešenia“ a stanovujú „jasné ciele a kľúčové ukazovatele výkonnosti na meranie dosahovania týchto cieľov“, ktoré by tvorili neoddeliteľnú súčasť príslušných kódexov. Okrem toho chýbajúci odkaz na (povinné) mechanizmy monitorovania kódexov správania určené na overenie toho, či poskytovatelia systémov umelej inteligencie, ktoré nepredstavujú vysoké riziko dodržiavajú ich ustanovenia, ako aj možnosť, aby jednotliví poskytovatelia vypracovali (a sami vykonávali) uvedené kódexy (pozri oddiel 5.2.7 dôvodovej správy) môžu ešte viac oslabiť účinnosť a vykonateľnosť týchto nástrojov.
80. EDPB a EDPS napokon žiadajú o objasnenie druhov iniciatív, ktoré môže Komisia podľa odôvodnenia 81 návrhu vypracovať „na uľahčenie odstraňovania technických prekážok, ktoré bránia cezhraničnej výmene údajov na účely rozvoja umelej inteligencie“.

4 ZÁVER

81. Hoci EDPB a EDPS vítajú návrh Komisie a domnievajú sa, že takéto nariadenie je potrebné na zaručenie základných práv občanov a obyvateľov EÚ, domnievajú sa, že návrh treba prispôbiť vo viacerých bodoch, aby sa zabezpečila jeho uplatniteľnosť a efektívnosť.
82. Vzhľadom na zložitosť návrhu, ako aj otázok, ktoré sa ním majú riešiť, je ešte potrebné vykonať veľa práce, kým sa v návrhu nebude stanovovať dobre fungujúci právny rámec, ktorým sa účinne doplní všeobecné nariadenie o ochrane základných práv a súčasne podporí inovácia. EDPB a EDPS budú naďalej k dispozícii, aby mohli na tejto ceste ponúknuť svoju podporu.

V Bruseli 18. júna 2021

Za Európsky výbor pre ochranu údajov

predsedníčka

Andrea JELINEK

Za Európskeho dozorného úradníka pre ochranu údajov

dozorný úradník

Wojciech Rafał WIEWIÓROWSKI