



EURÓPSKA
KOMISIA

V Bruseli 29. 7. 2025
C(2025) 5052 final

OZNÁMENIE KOMISIE

**Usmernenia Komisie o zakázaných praktikách využívajúcich umelú inteligenciu
stanovených v nariadení (EÚ) 2024/1689 (akt o AI)**

OBSAH

1.	Kontext a ciele	1
2.	Prehľad zakázaných praktík využívajúcich AI	2
2.1.	Zákazy uvedené v článku 5 aktu o AI	2
2.2.	Právny základ zákazov	4
2.3.	Vecná pôsobnosť: praktiky súvisiace s „uvádzaním na trh“, „uvádzaním do prevádzky“ alebo „používaním“ systému AI	4
2.4.	Osobný rozsah pôsobnosti: zodpovední aktéri	5
2.5.	Vylúčenie z rozsahu pôsobnosti aktu o AI	7
2.5.1.	Národná bezpečnosť, obrana a vojenské účely	7
2.5.2.	Spolupráca s tretími krajinami v oblasti súdnictva a presadzovania práva	9
2.5.3.	Výskum a vývoj	10
2.5.4.	Osobná neprofesionálna činnosť	11
2.5.5.	Systémy AI vydané na základe bezplatných licencií s otvoreným zdrojovým kódom	12
2.6.	Vzájomný vzťah zákazov a požiadaviek na vysokorizikové systémy AI	12
2.7.	Uplatňovanie zákazov na systémy AI na všeobecné účely a systémy so zamýšľanými účelmi 13	
2.8.	Vzájomný vzťah medzi zákazmi a inými právnymi predpismi Únie	15
2.9.	Presadzovanie článku 5 aktu o AI	18
2.9.1.	Orgány dohľadu nad trhom	18
2.9.2.	Sankcie	18
3.	Článok 5 ods. 1 písm. a) a b) aktu o AI – škodlivá manipulácia, klamanie a zneužívanie	19
3.1.	Odôvodnenie a ciele	19
3.2.	Hlavné prvky zákazu v článku 5 ods. 1 písm. a) aktu o AI – škodlivá manipulácia	20
3.2.1.	Podprahové, účelovo manipulatívne alebo klamlivé techniky	20
3.2.2.	S cieľom alebo účinkom podstatne narušiť správanie osoby alebo skupiny osôb	26
3.2.3.	(Je odôvodnené predpokladať, že pravdepodobne) spôsobí značnú ujmu	29
3.3.	Hlavné prvky zákazu v článku 5 ods. 1 písm. b) aktu o AI – škodlivé využívanie zraniteľností	34
3.3.1.	Využívanie zraniteľností z dôvodu veku, zdravotného postihnutia alebo sociálnej či ekonomickej situácie	35
3.3.2.	S cieľom alebo účinkom podstatne narušiť správanie	40
3.3.3.	(Je odôvodnené predpokladať, že pravdepodobne) spôsobí značnú ujmu	40
3.4.	Vzájomný vzťah medzi zákazmi v článku 5 ods. 1 písm. a) a b) aktu o AI	44
3.5.	Vylúčenie z rozsahu pôsobnosti	45
3.5.1.	Zákonné presviedčanie	45
3.5.2.	Manipulatívne, klamlivé a zneužívajúce systémy AI, v prípade ktorých sa nepredpokladá, že spôsobia značnú ujmu	48

3.6.	Vzájomný vzťah s inými právnymi predpismi Únie.....	49
4.	Článok 5 ods. 1 písm. c) aktu o AI – sociálne bodovanie.....	53
4.1.	Odôvodnenie a ciele.....	53
4.2.	Hlavné pojmy a zložky zákazu „sociálneho bodovania“.....	54
4.2.1.	„Sociálne bodovanie“: hodnotenie alebo klasifikácia na základe spoločenského správania alebo osobných či osobnostných charakteristík počas určitého obdobia.....	55
4.2.2.	Sociálne skóre musí viesť k škodlivému alebo nepriaznivému zaobchádzaniu v nesúvisiacich sociálnych kontextoch a/alebo k neodôvodnenému alebo neprimeranému zaobchádzaniu vzhľadom na závažnosť spoločenského správania.....	58
4.2.3.	Bez ohľadu na to, či ich poskytujú alebo používajú verejné alebo súkromné osoby....	63
4.3.	Vylúčenie z rozsahu pôsobnosti.....	64
4.4.	Vzájomný vzťah s inými právnymi aktmi Únie.....	67
5.	Článok 5 ods. 1 písm. d) aktu o AI – individuálne posúdenie rizika a predvídanie TRESTNÝCH ČINOV.....	68
5.1.	Odôvodnenie a ciele.....	69
5.2.	Hlavné pojmy a zložky zákazu.....	69
5.2.1.	Posúdenie rizika alebo predvídanie pravdepodobnosti, že osoba spácha trestný čin....	70
5.2.2.	Výlučne na základe profilovania fyzickej osoby alebo posúdenia jej osobnostných vlastností a charakteristík.....	71
5.2.3.	Vylúčenie systémov AI na podporu ľudského posúdenia založeného na objektívnych a overiteľných skutočnostiach priamo spojených s trestnou činnosťou.....	74
5.2.4.	Rozsah, v akom môžu činnosti súkromných aktérov patriť do rozsahu pôsobnosti.....	75
5.3.	Vylúčenie z rozsahu pôsobnosti.....	77
5.3.1.	Predpovede trestnej činnosti na základe polohy, geopriestorových informácií alebo miesta	77
5.3.2.	Systémy AI, ktoré podporujú ľudské posúdenie založené na objektívnych a overiteľných skutočnostiach spojených s trestnou činnosťou.....	78
5.3.3.	Systémy umelej inteligencie používané na predvídanie a posudzovanie trestnej činnosti vo vzťahu k právnickým osobám.....	79
5.3.4.	Systémy AI používané na individuálne predvídanie správnych deliktov.....	80
5.4.	Vzájomný vzťah s inými právnymi aktmi Únie.....	81
6.	Článok 5 ods. 1 písm. e) aktu o AI – necielená extrakcia podôb tváre.....	82
6.1.	Odôvodnenie a ciele.....	82
6.2.	Hlavné pojmy a zložky zákazu.....	82
6.2.1.	Databázy na rozpoznávanie tváre.....	83
6.2.2.	Prostredníctvom necielenej extrakcie podôb tváre.....	83
6.2.3.	Z internetu alebo zo záznamov CCTV.....	84
6.3.	Vylúčenie z rozsahu pôsobnosti.....	84
6.4.	Vzájomný vzťah s inými právnymi aktmi Únie.....	85
7.	Článok 5 ods. 1 písm. f) aktu o AI – rozpoznávanie emócií.....	85

7.1.	Odôvodnenie a ciele.....	85
7.2.	Hlavné pojmy a zložky zákazu	86
7.2.1.	Systémy AI na odvodzovanie emócií.....	87
7.2.2.	Obmedzenie zákazu na pracoviská a vzdelávacie inštitúcie	90
7.2.3.	Výnimky zo zdravotných a bezpečnostných dôvodov	93
7.3.	Priaznivejšie právne predpisy členských štátov	94
7.4.	Vylúčenie z rozsahu pôsobnosti.....	95
8.	Článok 5 ods. 1 písm. g) aktu o AI: Biometrická kategorizácia pre určité „citlivé“ charakteristiky	96
8.1.	Odôvodnenie a ciele.....	96
8.2.	Hlavné pojmy a zložky zákazu	97
8.2.1.	Systém biometrickej kategorizácie	97
8.2.2.	Osoby sú individuálne kategorizované na základe ich biometrických údajov.....	99
8.2.3.	S cieľom odvodiť alebo vyvodiť ich rasu, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie, sexuálny život alebo sexuálnu orientáciu	99
8.3.	Vylúčenie z rozsahu pôsobnosti.....	100
8.4.	Vzájomný vzťah s inými právnymi predpismi Únie.....	101
9.	Článok 5 ods. 1 písm. h) aktu o AI – systémy diaľkovej biometrickej identifikácie v reálnom čase na účely presadzovania práva	102
9.1.	Odôvodnenie a ciele.....	102
9.2.	Hlavné pojmy a zložky zákazu	103
9.2.1.	Pojem diaľkovej biometrickej identifikácie	104
9.2.2.	V reálnom čase.....	107
9.2.3.	Vo verejne prístupných priestoroch	107
9.2.4.	Na účely presadzovania práva.....	109
9.3.	Výnimky zo zákazu.....	111
9.3.1.	Odôvodnenie a ciele.....	111
9.3.2.	Cielené pátranie po obetiach troch závažných trestných činov a po nezvestných osobách	112
9.3.3.	Predchádzanie bezprostrednému ohrozeniu života alebo teroristickým útokom	114
9.3.4.	Lokalizácia a identifikácia osôb podozrivých z niektorých trestných činov.....	116
10.	Záruky a podmienky pre výnimky (článok 5 ods. 2 až 7 aktu o AI).....	119
10.1.	Zacielený jednotlivec a záruky (článok 5 ods. 2 aktu o AI).....	119
10.1.1.	Posúdenie vplyvu na základné práva	122
10.1.2.	Registrácia povolených systémov diaľkovej biometrickej identifikácie.....	126
10.2.	Potreba predchádzajúceho povolenia.....	127
10.2.1.	Cieľ	127
10.2.2.	Hlavná zásada: predchádzajúce povolenie justičného orgánu alebo nezávislého správneho orgánu	128

10.3.	Oznámenie orgánom o každom použití systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva	135
10.4.	Potreba vnútroštátnych právnych predpisov v medziach výnimiek zo aktu o AI.....	135
10.4.1.	Zásada: vyžaduje sa, aby vnútroštátne právo poskytovalo právny základ pre povolenie všetkých alebo niektorých výnimiek.....	135
10.4.2.	Vo vnútroštátnom práve sa rešpektujú obmedzenia a podmienky článku 5 ods. 1 písm. h) aktu o AI	136
10.4.3.	Podrobné vnútroštátne právne predpisy týkajúce sa podávania žiadostí o povolenia, ich vydávania a výkonu.....	137
10.4.4.	Podrobné vnútroštátne právne predpisy týkajúce sa dohľadu a podávania správ vo vzťahu k povoleniu	138
10.5.	Výročné správy vnútroštátnych orgánov dohľadu nad trhom a vnútroštátnych orgánov pre ochranu údajov členských štátov	138
10.6.	Výročné správy Komisie.....	139
10.7.	Vylúčenie z rozsahu pôsobnosti.....	140
10.8.	Príklady použitia	141
11.	Začiatok uplatňovania	143
12.	Preskúmanie a aktualizácia usmernení Komisie	144

1. KONTEXT A CIELE

1. Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia určité nariadenia (ďalej len „akt o AI“)¹, nadobudlo účinnosť 1. augusta 2024. V akte o AI sa stanovujú harmonizované pravidlá pre uvádzanie na trh, uvádzanie do prevádzky a používanie umelej inteligencie (ďalej len „AI“) v Únii². Jeho cieľom je podporovať inovácie a zavádzanie AI a zároveň zabezpečiť vysokú úroveň ochrany zdravia, bezpečnosti a základných práv v Únii vrátane demokracie a právneho štátu.
2. Akt o AI sa riadi prístupom založeným na rizikách a systémy AI sa ním klasifikujú do štyroch rôznych kategórií rizík:
 - i) neprijateľné riziko: systémy AI, ktoré predstavujú neprijateľné riziko pre základné práva a hodnoty Únie, sú podľa článku 5 aktu o AI zakázané;
 - ii) vysoké riziko: systémy AI, ktoré predstavujú vysoké riziko pre zdravie, bezpečnosť a základné práva, podliehajú súboru požiadaviek a povinností. Tieto systémy sa klasifikujú ako „vysokorizikové“ v súlade s článkom 6 aktu o AI v spojení s prílohami I a III k aktu o AI;
 - iii) riziko z hľadiska transparentnosti: na systémy AI, ktoré predstavujú obmedzené riziko z hľadiska transparentnosti, sa vzťahujú povinnosti v oblasti transparentnosti podľa článku 50 aktu o AI;
 - iv) minimálne alebo žiadne riziko: systémy AI, ktoré predstavujú minimálne alebo žiadne riziko, nie sú regulované, ale poskytovatelia a nasadzujúce subjekty môžu dobrovoľne dodržiavať dobrovoľné kódexy správania³.
3. Podľa článku 96 ods. 1 písm. b) aktu o AI má Komisia prijať usmernenia o praktickom vykonávaní, pokiaľ ide o praktiky zakázané podľa článku 5 aktu o AI. Tieto zákazy sa uplatňujú šesť mesiacov po nadobudnutí účinnosti aktu o AI, t. j. od 2. februára 2025.
4. Cieľom týchto usmernení je zvýšiť právnu zrozumiteľnosť a objasniť výklad zákazov uvedených v článku 5 aktu o AI zo strany Komisie v záujme zabezpečenia ich konzistentného, účinného a jednotného uplatňovania. Mali by slúžiť ako praktické usmernenie na pomoc príslušným orgánom podľa aktu o AI pri ich činnostiach v oblasti presadzovania, ako aj poskytovateľom systémov AI a subjektom nasadzujúcim systémy AI pri zabezpečovaní dodržiavania ich povinností podľa aktu o AI. Usiluje sa v nich o primeraný výklad zákazov, ktorým sa dosiahnu ciele aktu o AI týkajúce sa ochrany základných práv a bezpečnosti a zároveň sa podporia inovácie a zabezpečí právna istota.

¹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (akt o umelej inteligencii) (Ú. v. EÚ L, 2024/1689, 12.7.2024).

² Článok 1 aktu o AI.

³ Článok 95 aktu o AI.

5. Tieto usmernenia nie sú záväzné. Záväzný výklad aktu o AI môže v konečnom dôsledku podať len Súdny dvor Európskej únie.
6. Pri vypracúvaní týchto usmernení sa vychádzalo z podnetov od rôznych zainteresovaných strán, napríklad poskytovateľov systémov AI a subjektov nasadzujúcich systémy AI, organizácií občianskej spoločnosti, akademickej obce, orgánov verejnej moci, záujmových združení atď., ktoré boli zhromaždené počas rozsiahleho konzultačného procesu organizovaného Komisiou. Konzultácie sa uskutočnili aj s členskými štátmi v rámci Rady pre AI a s Európskym parlamentom. Tieto usmernenia sa budú pravidelne preskúmať na základe skúseností získaných pri praktickom vykonávaní článku 5 aktu o AI a technologického a trhového vývoja.
7. Uplatňovanie článku 5 aktu o AI si bude vyžadovať posúdenie od prípadu k prípadu, pri ktorom sa náležite zohľadní konkrétna situácia v jednotlivých prípadoch. Príklady uvedené v týchto usmerneniach sú preto len orientačné a nie je nimi dotknutá potreba takéhoto posúdenia v jednotlivých prípadoch.

2. PREHĽAD ZAKÁZANÝCH PRAKTÍK VYUŽÍVAJÚCICH AI

8. Podľa článku 5 aktu o AI sa zakazuje uvádzanie na trh EÚ, uvádzanie do prevádzky alebo používanie určitých systémov AI na manipulatívne a zneužívajúce praktiky, praktiky ovládania spoločnosti alebo praktiky sledovania, ktoré svojou povahou porušujú základné práva a hodnoty Únie. V odôvodnení 28 aktu o AI sa objasňuje, že takéto praktiky sú mimoriadne škodlivé a zneužívajúce a mali by sa zakázať, pretože sú v rozpore s hodnotami Únie týkajúcimi sa rešpektovania ľudskej dôstojnosti, slobody, rovnosti, demokracie a právneho štátu, ako aj základných práv ukotvených v Charte základných práv Európskej únie (ďalej len „charta“) vrátane práva na nediskrimináciu (článok 21 charty) a rovnosť (článok 20), ochranu osobných údajov (článok 8 charty) a súkromný a rodinný život (článok 7 charty) a práva dieťaťa (článok 24 charty). Cieľom zákazov v článku 5 aktu o AI je aj ochrana práva na slobodu prejavu a práva na informácie (článok 11 charty), slobody zhromažďovania a združovania (článok 12 charty), slobody myslenia, svedomia a náboženského vyznania (článok 10 charty), práva na účinný prostriedok nápravy a spravodlivý proces (článok 47 charty) a prezumpcie nevinu a práva na obhajobu (článok 48 charty).

2.1. Zákazy uvedené v článku 5 aktu o AI

9. Prehľad zákazov

Ustanovenie	Zákaz	Obsah
Článok 5 ods. 1 písm. a)	Škodlivá manipulácia a klamanie	Systémy AI, ktoré využívajú podprahové techniky mimo vedomia osoby alebo účelovo manipulatívne alebo klamlivé techniky s cieľom alebo účinkom narušiť správanie, čím spôsobujú alebo je odôvodnené predpokladať, že pravdepodobne spôsobia značnú ujmu

Článok 5 ods. 1 písm. b)	Škodlivé využívanie zraniteľností	Systémy AI, ktoré využívajú zraniteľnosti z dôvodu veku, zdravotného postihnutia alebo osobitnej sociálnej alebo ekonomickej situácie s cieľom alebo účinkom narušiť správanie, čím spôsobujú alebo je odôvodnené predpokladať, že pravdepodobne spôsobia značnú ujmu
Článok 5 ods. 1 písm. c)	Sociálne bodovanie	Systémy AI, ktoré hodnotia alebo klasifikujú fyzické osoby alebo skupiny osôb na základe spoločenského správania alebo osobných či osobnostných charakteristík, pričom sociálne skóre vedie k škodlivému alebo nepriaznivému zaobchádzaniu, ak údaje pochádzajú z nesúvisiacich sociálnych kontextov alebo je takéto zaobchádzanie neodôvodnené alebo neprimerané vzhľadom na spoločenské správanie
Článok 5 ods. 1 písm. d)	Individuálne posudzovanie a predvídanie rizika trestných činov	Systémy AI, ktoré posudzujú alebo predpovedajú riziko, že osoba spácha trestný čin, výlučne na základe profilovania alebo osobnostných vlastností a charakteristík s výnimkou podpory ľudského posúdenia založeného na objektívnych a overiteľných skutočnostiach priamo spojených s trestnou činnosťou
Článok 5 ods. 1 písm. e)	Necielená extrakcia na vývoj databáz na rozpoznávanie tváre	Systémy AI, ktoré vytvárajú alebo rozširujú databázy na rozpoznávanie tváre prostredníctvom necielenej extrakcie podôb tváre z internetu alebo zo záznamov CCTV
Článok 5 ods. 1 písm. f)	Rozpoznávanie emócií	Systémy AI, ktoré odvodzujú emócie na pracovisku alebo vo vzdelávacích inštitúciách s výnimkou zdravotných alebo bezpečnostných dôvodov
Článok 5 ods. 1 písm. g)	Biometrická kategorizácia	Systémy AI, ktoré kategorizujú osoby na základe biometrických údajov s cieľom odvodiť alebo vyvodiť ich rasu, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie, sexuálny život alebo sexuálnu orientáciu s výnimkou označovania alebo filtrovania zákonne získaných súborov biometrických údajov, a to aj v oblasti presadzovania práva
Článok 5 ods. 1 písm. h)	Diaľková biometrická identifikácia v reálnom čase	Systémy AI na diaľkovú biometrickú identifikáciu v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva s výnimkou prípadov, keď je to potrebné na ciele pátranie po konkrétnych obetiach, predchádzanie konkrétnym hrozbám vrátane teroristických útokov alebo pátranie po osobách podozrivých zo spáchania konkrétnych trestných

činov (ďalšie procedurálne požiadavky vrátane požiadaviek na povolenie sú uvedené v článku 5 ods. 2 až 7 aktu o AI)

2.2. Právny základ zákazov

10. Akt o AI sa opiera o dva právne základy: článok 114 Zmluvy o fungovaní Európskej únie (ďalej len „ZFEÚ“) (právny základ vnútorného trhu) a článok 16 ZFEÚ (právny základ ochrany údajov). Článok 16 ZFEÚ slúži ako právny základ pre osobitné pravidlá spracúvania osobných údajov v súvislosti so zákazom používania systémov diaľkovej biometrickej identifikácie na účely presadzovania práva, systémov biometrickej kategorizácie na účely presadzovania práva a individuálneho posudzovania rizika na účely presadzovania práva⁴. Všetky ostatné zákazy uvedené v článku 5 aktu o AI majú svoj právny základ v článku 114 ZFEÚ.

2.3. Vecná pôsobnosť: praktiky súvisiace s „uvádzaním na trh“, „uvádzaním do prevádzky“ alebo „používaním“ systému AI

11. Praktiky zakázané podľa článku 5 aktu o AI sa týkajú uvádzania na trh, uvádzania do prevádzky alebo používania konkrétnych systémov AI⁵. Pokiaľ ide o systémy diaľkovej biometrickej identifikácie v reálnom čase, zákaz uvedený v článku 5 ods. 1 písm. h) aktu o AI sa vzťahuje len na ich používanie. V článku 3 bode 1 aktu o AI sa vymedzuje, čo predstavuje systém AI. Výklad tohto vymedzenia zo strany Komisie je uvedený v usmerneniach o vymedzení systému AI.
12. Podľa článku 3 bodu 9 aktu o AI je **uviedenie** systému AI **na trh** „prvé sprístupnenie systému AI [...] na trhu Únie“. „Sprístupnenie“ sa vymedzuje ako dodanie systému AI „s cieľom distribuovať ho alebo používať ho na trhu Únie v rámci komerčnej činnosti, či už za odplatu alebo bezodplatne“⁶. O sprístupnenie systému AI ide bez ohľadu na spôsob dodania, napríklad prístup k systému a jeho službe prostredníctvom aplikačného programovacieho rozhrania, cloudu, priamym stiahnutím, v podobe fyzických kópií alebo vložením do fyzických výrobkov.

Napríklad systém diaľkovej biometrickej identifikácie vyvinutý mimo Únie poskytovateľom z tretej krajiny sa prvýkrát uvedie na trh Únie, keď sa ponúka za odplatu alebo bezodplatne v jednom alebo vo viacerých členských štátoch. Takéto uvedenie na trh sa môže uskutočniť poskytnutím prístupu k systému online

⁴ Odôvodnenie 3 aktu o AI. Pokiaľ ide o zákazy založené na článku 16 ZFEÚ, pre Írsko a Dánsko existujú dve relevantné výnimky. Vďaka diskrečnej právomoci, ktorá je Írsku udelená na základe Protokolu č. 21 o postavení Spojeného kráľovstva a Írska s ohľadom na priestor slobody, bezpečnosti a spravodlivosti, ktorý je pripojený k Zmluve o EÚ a ZFEÚ, sa Írsko môže rozhodnúť neuplatňovať pravidlá týkajúce sa zákazu používania diaľkovej biometrickej identifikácie v reálnom čase vo verejných priestoroch na účely presadzovania práva, ako aj procesné pravidlá súvisiace s týmto článkom (článok 5 ods. 2 až 6 aktu o AI) (pozri odôvodnenie 40). Dánsko pri uplatňovaní Protokolu č. 22, ktorý je pripojený k Zmluve o EÚ a ZFEÚ, využíva dohody o výnimke a môže sa rozhodnúť, že nebude v plnej miere uplatňovať zákazy založené na článku 16 ZFEÚ (pozri odôvodnenie 41).

⁵ Vymedzenie týchto pojmov sa uvádza aj v oznámení Komisie Modrá príručka na vykonávanie právnych predpisov EÚ týkajúcich sa výrobkov 2022, 2022/C 247/01, oddiel 2.

⁶ Článok 3 bod 10 aktu o AI.

prostredníctvom aplikačného programovacieho rozhrania alebo iného používateľského rozhrania.

13. V článku 3 bode 11 aktu o AI sa **uviedenie do prevádzky** vymedzuje ako „dodanie systému AI na prvé použitie nasadzujúcemu subjektu alebo na vlastné použitie v Únii na jeho zamýšľaný účel“, čo zahŕňa tak dodanie na prvé použitie tretím stranám, ako aj vlastný vývoj a nasadenie. Zamýšľaný účel systému je „použitie, na ktoré systém AI určil poskytovateľ vrátane konkrétneho kontextu a podmienok používania, ako sa uvádza v informáciách od poskytovateľa v návode na použitie, v propagačných alebo predajných materiáloch a vyhláseniach, ako aj v technickej dokumentácii“⁷.

Poskytovateľ napríklad vybuduje systém diaľkovej biometrickej identifikácie mimo Únie a dodá ho orgánu presadzovania práva alebo súkromnej spoločnosti usadenej v členskom štáte na prvé použitie, čím dôjde k jeho uvedeniu do prevádzky.

Orgán verejnej moci si napríklad interne vyvinie bodovací systém a nasadí ho na predvídanie rizika podvodov u príjemcov príspevkov na domácnosť, čím ho uvedie do prevádzky.

14. Hoci „**používanie**“ systému AI nie je v akte o AI výslovne vymedzené, malo by sa chápať v širšom zmysle tak, že zahŕňa používanie alebo nasadenie systému v ktoromkoľvek okamihu jeho životného cyklu po jeho uvedení na trh alebo do prevádzky. Môže sa to vzťahovať aj na integráciu systému AI do služieb a procesov osoby (osôb), ktorá (ktoré) systém AI využíva (využívajú), a to aj ako súčasť komplexnejších systémov, procesov alebo infraštruktúry. Zatiaľ čo poskytovatelia systémov AI musia pred uvedením svojich systémov AI na trh zvážiť podmienky používania, ktoré možno primerane predpokladať (zamýšľané použitie a odôvodnene predvídateľné nesprávne použitie⁸), nasadzujúce subjekty sú naďalej zodpovedné za zohľadnenie zákonných podmienok používania systému⁹. Na účely článku 5 aktu o AI by sa odkaz na „používanie“ mal chápať tak, že zahŕňa akékoľvek nesprávne použitie systému AI (či je alebo nie je „odôvodnene predvídateľné“), ktoré môže predstavovať zakázanú prax¹⁰.

Napríklad systém AI, ktorý zamestnávateľ používa na odvodzovanie emócií na pracovisku, je zakázaný s výnimkou prípadov, keď sa používa na zdravotné alebo bezpečnostné účely [článok 5 ods. 1 písm. f) aktu o AI]. Zákaz sa vzťahuje na nasadzujúce subjekty bez ohľadu na to, či poskytovateľ (dodávateľ systému) vylúčil takéto použitie vo svojich zmluvných vzťahoch s nasadzujúcim subjektom (zamestnávateľom), t. j. v podmienkach používania.

2.4. Osobný rozsah pôsobnosti: zodpovední aktéri

⁷ Článok 3 bod 12 aktu o AI.

⁸ Pozri článok 3 body 12 a 13 aktu o AI.

⁹ Vymedzenie týchto pojmov sa uvádza aj v oznámení Komisie Modrá príručka na vykonávanie právnych predpisov EÚ týkajúcich sa výrobkov 2022, 2022/C 247/01, oddiel 2.8.

¹⁰ Odôvodnenie 28 aktu o AI.

15. V akte o AI sa rozlišuje medzi rôznymi kategóriami prevádzkovateľov vo vzťahu k systémom AI: poskytovatelia, nasadzujúce subjekty, dovozcovia, distribútori a výrobcovia výrobkov. Vzhľadom na rozsah zakázaných praktík v článku 5 aktu o AI sa tieto usmernenia zameriavajú len na poskytovateľov a nasadzujúce subjekty.
16. Podľa článku 3 bodu 3 aktu o AI sú **poskytovatelia** fyzické alebo právnické osoby, orgány verejnej moci, agentúry alebo iné subjekty, ktoré vyvíjajú systémy AI alebo si ich dávajú vyvinúť a uvádzajú ich na trh Únie, alebo ich uvádzajú do prevádzky pod vlastným menom alebo ochrannou známkou¹¹ (pozri oddiel 2.3 v predchádzajúcom texte). Poskytovatelia usadení alebo nachádzajúci sa mimo Únie podliehajú ustanoveniam aktu o AI, ak uvedené systémy uvádzajú na trh alebo uvádzajú do prevádzky v Únii¹² alebo ak sa výstup systému AI používa v Únii¹³. Poskytovatelia musia zabezpečiť, aby ich systémy AI spĺňali všetky príslušné požiadavky pred ich uvedením na trh alebo uvedením do prevádzky.

Napríklad poskytovateľ systému diaľkovej biometrickej identifikácie je výrobca systému, ktorý tento systém uvádza na trh v Únii pod svojou ochrannou známkou. Poskytovateľom takéhoto systému by mohol byť aj orgán verejnej moci, ktorý si systém vyvinie interne a uvedie ho do prevádzky na vlastné použitie.

17. **Nasadzujúce subjekty** sú fyzické alebo právnické osoby, orgány verejnej moci, agentúry alebo iné subjekty, ktoré používajú systémy AI v rámci svojej právomoci, pokiaľ uvedené systémy nepoužívajú na osobnú neprofesionálnu činnosť¹⁴. „Právomoc“ nad systémom AI by sa mala chápať ako prevzatie zodpovednosti za rozhodnutie o nasadení systému a za spôsob jeho skutočného používania. Nasadzujúce subjekty patria do rozsahu pôsobnosti aktu o AI, ak majú miesto usadenia alebo sa nachádzajú v Únii¹⁵ alebo, ak sa nachádzajú v tretej krajine, sa výstup systému AI používa v Únii¹⁶.
18. Ak je subjektom nasadzujúcim systém AI právnická osoba, pod ktorej právomocou sa systém používa, t.j. orgán presadzovania práva alebo súkromná bezpečnostná spoločnosť, jednotliví zamestnanci, ktorí konajú v rámci postupov a pod kontrolou uvedenej právnickej osoby, by sa nemali považovať za nasadzujúci subjekt. Právnická

¹¹ Článok 3 body 3, 9 a 11 aktu o AI. V súvislosti s vysokorizikovými systémami AI sa v článku 25 aktu o AI predpokladá, že 1. Každý distribútor, dovozca, nasadzujúci subjekt alebo iná tretia strana sa na účely tohto nariadenia považuje za poskytovateľa vysokorizikového systému AI a vzťahujú sa na neho povinnosti poskytovateľa podľa článku 16 za ktorejkoľvek z týchto okolností: a) umiestnia svoje meno alebo ochrannú známku na vysokorizikový systém AI, ktorý už bol uvedený na trh alebo do prevádzky, bez toho, aby boli dotknuté zmluvné dojednania, v ktorých sa stanovuje, že povinnosti sú rozdelené inak; b) vykonajú podstatnú zmenu vysokorizikového systému AI, ktorý už bol uvedený na trh alebo už bol uvedený do prevádzky takým spôsobom, že zostáva vysokorizikovým systémom AI podľa článku 6; c) menia zamýšľaný účel systému AI vrátane systému AI na všeobecné účely, ktorý nebol klasifikovaný ako vysokorizikový a už bol uvedený na trh alebo do prevádzky takým spôsobom, že sa z dotknutého systému AI stane vysokorizikový systém AI v súlade s článkom 6.

¹² Článok 2 ods. 1 písm. a) aktu o AI.

¹³ Článok 2 ods. 1 písm. c) aktu o AI.

¹⁴ Článok 3 bod 4 aktu o AI.

¹⁵ Článok 2 ods. 1 písm. b) aktu o AI.

¹⁶ Článok 2 ods. 1 písm. c) aktu o AI.

osoba zostáva nasadzujúcim subjektom aj vtedy, ak do prevádzky systému vo svojom mene a na svoju zodpovednosť a pod svojou kontrolou zapojí tretie strany (napríklad dodávateľov, externých zamestnancov).

19. Prevádzkovatelia môžu vo vzťahu k systému AI plniť viac ako jednu rolu súčasne. Ak napríklad prevádzkovateľ vyvinie vlastný systém AI, ktorý následne používa, bude sa považovať za poskytovateľa aj za subjekt nasadzujúci uvedený systém, aj keď tento systém používajú aj iné nasadzujúce subjekty, ktorým bol systém poskytnutý za odplatu alebo bezodplatne.
20. Počas všetkých fáz životného cyklu AI sa vyžaduje nepretržitý súlad s aktom o AI. Vyžaduje si to priebežné monitorovanie a aktualizácie systémov AI uvedených na trh alebo uvedených do prevádzky v Únii, aby sa zabezpečilo, že systém AI zostáva v súlade s aktom o AI počas celého svojho životného cyklu a že nebude viesť k praktikám zakázaným podľa článku 5 aktu o AI. Poskytovatelia a subjekty nasadzujúce systémy AI majú rôzne povinnosti v závislosti od svojich rolí a kontroly nad dizajnom, vývojom a samotným používaním systému, aby sa zabránilo zakázanej praktike. V prípade každého zo zákazov by sa tieto roly a povinnosti mali vykladať primeraným spôsobom, pričom by sa malo zohľadniť, kto v hodnotovom reťazci má najlepšie predpoklady na prijatie konkrétnych preventívnych a zmiernujúcich opatrení a zabezpečenie vyhovujúceho vývoja a používania systémov AI v súlade s cieľmi a prístupom aktu o AI.

2.5. Vylúčenie z rozsahu pôsobnosti aktu o AI

21. V článku 2 aktu o AI sa stanovuje niekoľko všeobecných vylúčení z rozsahu pôsobnosti, ktoré sú relevantné pre úplné pochopenie praktického uplatňovania zákazov uvedených v článku 5 aktu o AI.

2.5.1. Národná bezpečnosť, obrana a vojenské účely

22. Podľa článku 2 ods. 3 aktu o AI sa akt o AI neuplatňuje na oblasti mimo rozsahu pôsobnosti práva Únie a v žiadnom prípade by nemal mať vplyv na právomoci členských štátov týkajúce sa národnej bezpečnosti, a to bez ohľadu na typ subjektu, ktorý členské štáty poverili vykonávaním úloh v súvislosti s týmito právomocami. V akte o AI sa z jeho rozsahu pôsobnosti výslovne vylučujú systémy AI, ktoré sa „uvádzajú na trh, uvádzajú do prevádzky alebo sa používajú, či už upravené alebo nie, výlučne na vojenské alebo obranné účely alebo na účely národnej bezpečnosti, a to bez ohľadu na typ subjektu vykonávajúceho tieto činnosti“. To, či sa toto vylúčenie uplatňuje, teda závisí od účelu alebo spôsobu použitia systému AI, nie od subjektov vykonávajúcich činnosti s týmto systémom, čo sa môže vzťahovať aj na súkromných prevádzkovateľov, ktorých členské štáty poverili vykonávaním úloh v súvislosti s týmito právomocami.
23. Podľa Súdneho dvora Európskej únie sa pojem „**národná bezpečnosť**“ vzťahuje na „[prvoradý záujem] chrániť základné funkcie štátu a základné záujmy spoločnosti a zahŕňa prevenciu a potláčanie aktivít, ktoré môžu vážne destabilizovať základné politické, ústavné, hospodárske alebo sociálne štruktúry krajiny a najmä priamo ohroziť

spoločnosť, obyvateľstvo alebo samotný štát, akými sú napríklad teroristické aktivity“¹⁷. Národná bezpečnosť nezahŕňa napríklad činnosti súvisiace s bezpečnosťou cestnej premávky¹⁸ alebo organizáciou či výkonom spravodlivosti¹⁹. Ako uviedol Súdny dvor Európskej únie, „členským štátom prináleží, aby vymedzili svoje hlavné bezpečnostné záujmy a prijali vhodné opatrenia na zaistenie svojej vnútornej a vonkajšej bezpečnosti, [...] vnútroštátne opatrenie [...] prijímané v záujme národnej bezpečnosti, nemôže viesť k tomu, že sa neuplatní právo Únie a členské štáty budú zbavené povinnosti nevyhnutne dodržiavať toto právo“²⁰.

24. Aby sa uplatnilo vylúčenie uvedené v článku 2 ods. 3 druhom pododseku aktu o AI, systém AI musí byť uvedený na trh, uvedený do prevádzky alebo používaný výlučne na vojenské alebo obranné účely alebo na účely národnej bezpečnosti. V odôvodnení 24 aktu o AI sa ďalej objasňuje, ako by sa mal vykladať pojem „výlučne“ a kedy môže systém AI používaný na takéto účely napriek tomu patriť do rozsahu pôsobnosti aktu o AI.

Napríklad ak sa systém AI, ktorý je uvedený na trh, uvedený do prevádzky alebo používaný na vojenské alebo obranné účely alebo na účely národnej bezpečnosti, používa (dočasne alebo trvalo) na iné účely, napríklad na civilné alebo humanitárne účely, účely presadzovania práva alebo verejnej bezpečnosti, daný systém bude patriť do rozsahu pôsobnosti aktu o AI. V takom prípade by mal subjekt, ktorý používa systém AI na iné účely, zabezpečiť súlad systému AI s aktom o AI, pokiaľ systém už nie je v súlade s uvedeným aktom, čo sa musí pred takýmto použitím overiť.

25. Okrem toho sa v odôvodnení 24 aktu o AI objasňuje, že systémy AI uvedené na trh alebo do prevádzky na účely vylúčené z pôsobnosti, konkrétne vojenské alebo obranné účely alebo účely národnej bezpečnosti, a na jeden alebo viacero účelov nevylúčených z pôsobnosti, napríklad civilné účely alebo účely presadzovania práva (tzv. systémy s **dvojakým použitím**), patria do rozsahu pôsobnosti aktu o AI. Poskytovatelia uvedených systémov by mali zabezpečiť ich súlad s požiadavkami aktu o AI.

Ak napríklad spoločnosť ponúka systém diaľkovej biometrickej identifikácie na rôzne účely vrátane presadzovania práva a národnej bezpečnosti, je poskytovateľom tohto systému s „dvojakým použitím“ a musí zabezpečiť jeho súlad s požiadavkami aktu o AI.

26. Skutočnosť, že systém AI môže patriť do rozsahu pôsobnosti aktu o AI, by však nemala mať vplyv na možnosť subjektov vykonávajúcich činnosti v oblasti národnej bezpečnosti, obrany a vojenské činnosti používať uvedený systém na účely národnej

¹⁷ Rozsudok Súdneho dvora zo 6. októbra 2020, La Quadrature du Net a i., C-511/18, C-512/18 a C-520/18, EU:C:2020:791, bod 135; rozsudok Súdneho dvora z 5. júna 2023, Komisia/Pol'sko, C-204/21, EU:C:2023:442, bod 318, s odkazom na vec C-439/19, bod 67, a vec C-306/21, bod 40.

¹⁸ Rozsudok Súdneho dvora z 22. júna 2021, Latvijas Republikas Saeima, C-439/19, EU:C:2021:504, bod 68.

¹⁹ Rozsudok Súdneho dvora z 5. júna 2023, Komisia/Pol'sko, C-204/21, EU:C:2023:442, bod 319.

²⁰ Rozsudok Súdneho dvora zo 6. októbra 2020, Privacy International, C-623/17, EU:C:2020:790, bod 44.

bezpečnosti, na vojenské a obranné účely, a to bez ohľadu na typ subjektu vykonávajúceho uvedené činnosti²¹.

Ak napríklad národná bezpečnostná agentúra alebo súkromný prevádzkovateľ dostane od národnej spravodajskej agentúry za úlohu používať systémy diaľkovej biometrickej identifikácie v reálnom čase na účely národnej bezpečnosti (napríklad na zhromažďovanie spravodajských informácií), takéto použitie by bolo vylúčené z rozsahu pôsobnosti aktu o AI.

27. Jasné vymedzenie vylúčenia národnej bezpečnosti je obzvlášť dôležité v prípadoch, keď sa systémy AI uvádzajú na trh, uvádzajú do prevádzky alebo používajú na účely presadzovania práva, ktoré patria do rozsahu pôsobnosti aktu o AI. Je to relevantné z hľadiska zákazov týkajúcich sa individuálnych predpovedí a posúdení trestnej činnosti, ako sa stanovuje v článku 5 ods. 1 písm. d) aktu o AI, a používania systémov diaľkovej biometrickej identifikácie v reálnom čase na účely presadzovania práva, ako sa stanovuje v článku 5 ods. 1 písm. h) aktu o AI. Úlohou polície a iných orgánov presadzovania práva je predchádzať trestným činom, odhaľovať, vyšetrovať a stíhať ich alebo vykonávať trestné sankcie vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu²². Vždy, keď sa systémy AI použijú na takéto účely, budú patriť do rozsahu pôsobnosti aktu o AI.
28. Činnosti Europolu a iných bezpečnostných agentúr Únie, ako je Frontex, patria do rozsahu pôsobnosti aktu o AI.

2.5.2. Spolupráca s tretími krajinami v oblasti súdnictva a presadzovania práva

29. Podľa článku 2 ods. 4 aktu o AI sa akt o AI neuplatňuje na orgány verejnej moci v tretej krajine ani na medzinárodné organizácie, ak tieto orgány alebo organizácie používajú systémy AI v rámci medzinárodných dohôd o spolupráci alebo dohôd o presadzovaní práva a justičnej spolupráci s Úniou alebo s jedným alebo viacerými členskými štátmi, pod podmienkou, že táto tretia krajina alebo medzinárodná organizácia poskytuje primerané záruky, pokiaľ ide o ochranu základných práv a slobôd jednotlivcov. V relevantných prípadoch sa toto vylúčenie môže vzťahovať na činnosti súkromných subjektov, ktoré dotknutá tretia krajina poverila vykonávaním osobitných úloh na podporu takejto spolupráce v oblasti presadzovania práva a justičnej spolupráce²³. Zároveň, aby sa vylúčenie uplatnilo, musia tieto rámce spolupráce alebo medzinárodné dohody obsahovať primerané záruky, pokiaľ ide o ochranu základných práv a slobôd jednotlivcov, ktoré posúdia orgány dohľadu nad trhom zodpovedné za dohľad nad systémami AI používanými v oblasti presadzovania práva a spravodlivosti²⁴. V odôvodnení 22 aktu o AI sa objasňuje, že prijímajúce vnútroštátne orgány a prijímajúce inštitúcie, orgány, úrady a agentúry Únie využívajúce takéto výstupy AI v Únii zostávajú zodpovedné za zabezpečenie súladu ich využívania s právom Únie. Pri

²¹ Odôvodnenie 24 aktu o AI.

²² Článok 3 bod 46 aktu o AI.

²³ Pozri odôvodnenie 22 aktu o AI.

²⁴ Pozri odôvodnenie 22 a článok 74 ods. 8 aktu o AI.

revízii uvedených medzinárodných dohôd alebo uzatváraní nových dohôd v budúcnosti by zmluvné strany mali vynaložiť maximálne úsilie na zosúladenie týchto dohôd s požiadavkami aktu o AI.

2.5.3. Výskum a vývoj

30. Podľa článku 2 ods. 8 aktu o AI sa akt o AI neuplatňuje „na žiadnu výskumnú, testovaciu ani vývojovú činnosť týkajúcu sa systémov AI alebo modelov AI pred ich uvedením na trh alebo do prevádzky“. Toto vylúčenie je v súlade s trhovou logikou aktu o AI, ktorý sa vzťahuje na systémy AI po ich uvedení na trh alebo do prevádzky.

Napríklad počas fázy výskumu a vývoja majú vývojári AI slobodu experimentovať a testovať nové funkcie, ktoré môžu zahŕňať techniky, ktoré by sa mohli považovať za manipulatívne a na ktoré sa vzťahuje článok 5 ods. 1 písm. a) aktu o AI, ak by sa používali v aplikáciách určených pre spotrebiteľov. Aktom o AI sa umožňuje takéto experimentovanie tým, že uznáva, že výskum a vývoj v ranom štádiu je nevyhnutný na zdokonalenie technológií AI a zabezpečenie toho, aby spĺňali bezpečnostné a etické normy pred ich uvedením na trh.

31. Ako sa objasňuje v odôvodnení 25 aktu o AI, cieľom aktu o AI je podporovať inováciu a uznáva sa v ňom význam vedeckého výskumu pri rozvoji technológií AI a prispievaní k vedeckému pokroku a inovácii. V článku 2 ods. 6 aktu o AI sa preto uvádza vylúčenie, pokiaľ ide o „systémy alebo modely AI vrátane ich výstupov, ktoré sú osobitne vyvinuté a uvedené do prevádzky výlučne na účely vedeckého výskumu a vývoja“.

Napríklad prostredníctvom výskumu kognitívnych a behaviorálnych reakcií na podprahové alebo klamlivé podnety riadené AI možno získať cenné poznatky o interakciách medzi ľuďmi a AI a poskytnúť informácie pre bezpečnejšie a efektívnejšie aplikácie AI v budúcnosti. Takýto výskum je povolený, pretože je vylúčený z rozsahu pôsobnosti aktu o AI bez ohľadu na zákaz uvedený v článku 5 ods. 1 písm. a) aktu o AI.

32. Vylúčením uvedeným v článku 2 ods. 8 aktu o AI však nie je dotknutá povinnosť dodržiavať akt o AI, ak sa systém AI uvádza na trh alebo do prevádzky ako výsledok takejto výskumnej a vývojovej činnosti²⁵. Uvedené vylúčenie sa nevzťahuje ani na testovanie v reálnych podmienkach v zmysle aktu o AI²⁶.

Napríklad obec, ktorá chce otestovať softvér na rozpoznávanie tváre pomocou systému diaľkovej biometrickej identifikácie v uliciach počas karnevalu, použije dobrovoľníkov získaných náborom, ktorých systém identifikuje v reálnych podmienkach. Keďže na

²⁵ Odôvodnenie 25 aktu o AI.

²⁶ Podľa článku 3 bodu 57 aktu o AI „testovanie v reálnych podmienkach“ je dočasné testovanie systému AI na jeho zamýšľaný účel v reálnych podmienkach mimo laboratória alebo inak simulovaného prostredia s cieľom zhromaždiť spoľahlivé a robustné údaje a posúdiť a overiť zhodu systému AI s požiadavkami aktu o AI. Aktom o AI sa stanovuje osobitný režim pre takéto testovanie v reálnych podmienkach, ktoré sa nepovažuje za uvedenie systému AI na trh alebo do prevádzky v zmysle aktu o AI, ak sú splnené všetky podmienky stanovené v článkoch 57 alebo 60 vrátane získania slobodného a informovaného súhlasu osôb, ktoré sa na testovaní zúčastňujú, atď.; pozri článok 60 aktu o AI.

testovanie v reálnych podmienkach sa nevzťahuje vylúčenie podľa článku 2 ods. 8 aktu o AI, plánované testovanie musí byť plne v súlade s požiadavkami na systémy diaľkovej biometrickej identifikácie uvedenými v akte o AI, pokiaľ sa systém netestuje v regulačnom experimentálnom prostredí pre AI alebo v súlade s osobitným režimom testovania v reálnych podmienkach mimo experimentálneho prostredia, ako sa stanovuje v článkoch 60 a 61 aktu o AI²⁷.

33. Každá výskumná a vývojová činnosť (aj keď je vylúčená z rozsahu pôsobnosti aktu o AI) by sa v každom prípade mala vykonávať v súlade s uznávanými etickými a profesijnými normami pre vedecký výskum, ako aj v súlade s uplatniteľným právom Únie²⁸ (napríklad s právom o ochrane údajov, ktoré je aj naďalej uplatniteľné).

2.5.4. Osobná neprofesionálna činnosť

34. V článku 2 ods. 10 sa stanovuje, že akt o AI sa „neuplatňuje na povinnosti nasadzujúcich subjektov, ktoré sú fyzickými osobami používajúcimi systémy AI v rámci čisto osobnej neprofesionálnej činnosti“. Na základe vymedzenia nasadzujúceho subjektu sú takisto vylúčení používatelia, ktorí vykonávajú takéto činnosti (pozri oddiel 2.4). Za „profesionálnu“ činnosť by sa mala považovať každá činnosť, prostredníctvom ktorej fyzická osoba pravidelne získava majetkový prospech alebo je inak zapojená do profesionálnej, podnikateľskej, obchodnej, pracovnej činnosti alebo činnosti v rámci slobodného povolania. Označenie „osobná“ je kvalifikátorom označenia „neprofesionálna“, čo znamená, že osoba by mala konať v osobnom aj neprofesionálnom postavení. Vylúčenie by preto nemalo zahŕňať napríklad trestné činnosti, pretože tie by sa nemali považovať za čisto osobné.

Napríklad na jednotlivca, ktorý používa systém na rozpoznávanie tváre v domácnosti (napríklad na kontrolu prístupu a bezpečnostné monitorovanie vstupu do domácnosti), by sa vzťahovalo vylúčenie podľa článku 2 ods. 10 aktu o AI, a preto by sa na neho nevzťahovali povinnosti pre nasadzujúce subjekty podľa aktu o AI, a to ani v prípadoch, keď je potrebné zasielať záznam (alebo jeho časti) orgánom presadzovania práva.

Naopak, fyzická osoba, ktorá používa systém AI na profesionálne činnosti, ako sú živnostníci, novinári, lekári atď., by musela dodržiavať povinnosti pre subjekty nasadzujúce systémy na rozpoznávanie tváre podľa aktu o AI. Akékoľvek použitie fyzickými osobami, ktoré konajú v mene nasadzujúceho subjektu, ktorý koná v profesionálnom postavení, alebo pod jeho kontrolou, bude takisto patriť do rozsahu pôsobnosti aktu o AI.

Okrem toho trestnú činnosť nemožno považovať za čisto osobnú činnosť, ani keď sa ňou neusiluje o majetkový prospech, ani sa takýto prospech nedosahuje. V prípade iných protiprávných činností, ako je nedodržiavanie právnych predpisov v oblasti ochrany spotrebiteľa alebo ochrany údajov a vnútroštátnych správnych právnych

²⁷ Akt o AI obsahuje podrobné a konkrétne povinnosti týkajúce sa regulačných experimentálnych prostredí pre AI a testovania v reálnych podmienkach. Pozri článok 57 a nasl. aktu o AI.

²⁸ Odôvodnenie 25 aktu o AI.

predpisov, sa uplatňuje vylúčenie v akte o AI, ostatné príslušné právne rámce sa však uplatňujú aj naďalej.

35. Vylúčenie v článku 2 ods. 10 aktu o AI sa vzťahuje len na povinnosti nasadzujúcich subjektov pri používaní systému na čisto osobné neprofesionálne činnosti. Systém ako taký zostáva v rozsahu pôsobnosti aktu o AI, pokiaľ ide o povinnosti poskytovateľov, ktorí systém uvádzajú na trh alebo do prevádzky, iných profesionálnych nasadzujúcich subjektov a iných zodpovedných subjektov, ako sú dovozcovia a distribútori.

Napríklad systém na rozpoznávanie emócií, ak je určený na používanie fyzickými osobami na čisto osobné neprofesionálne činnosti, zostáva vysokorizikovým systémom AI klasifikovaným v článku 6 aktu o AI a musí byť plne v súlade s aktom o AI. Zároveň sa na nasadzujúci subjekt, ktorý ho používa v rámci čisto osobného neprofesionálneho použitia (napríklad osoba s autizmom), nebudú vzťahovať osobitné povinnosti pre nasadzujúce subjekty podľa aktu o AI a toto použitie by bolo mimo rozsahu pôsobnosti uvedeného aktu.

2.5.5. Systémy AI vydané na základe bezplatných licencií s otvoreným zdrojovým kódom

36. Podľa článku 2 ods. 12 aktu o AI sa akt o AI neuplatňuje na systémy AI vydané na základe bezplatných licencií s otvoreným zdrojovým kódom²⁹, pokiaľ nie sú uvedené na trh alebo do prevádzky ako vysokorizikové systémy AI alebo ako systém AI, na ktorý sa vzťahuje článok 5 (zakázané praktiky využívajúce AI) alebo článok 50 (povinnosti v oblasti transparentnosti pre určité systémy AI). To znamená, že poskytovatelia systémov AI nemôžu využívať toto vylúčenie, ak systém AI, ktorý uvádzajú na trh alebo do prevádzky, predstavuje zakázanú praktiku podľa článku 5 aktu o AI.

2.6. Vzájomný vzťah zákazov a požiadaviek na vysokorizikové systémy AI

37. Praktiky využívajúce AI, ktoré sú zakázané podľa článku 5 aktu o AI, by sa mali posudzovať v súvislosti so systémami AI klasifikovanými ako vysokorizikové v súlade s článkom 6 aktu o AI, najmä tými, ktoré sú uvedené v prílohe III³⁰. Dôvodom je to, že používanie systémov AI klasifikovaných ako vysokorizikové môže byť v niektorých prípadoch kvalifikované ako zakázaná praktika, a to v konkrétnych prípadoch, ak sú splnené všetky podmienky podľa jedného alebo viacerých zákazov v článku 5 aktu o AI. Na druhej strane väčšina systémov AI, na ktoré sa vzťahuje vylúčenie zo zákazu uvedeného v článku 5 aktu o AI, sa bude kvalifikovať ako vysokoriziková.

Napríklad systémy na rozpoznávanie emócií, ak nespĺňajú podmienky zákazu podľa článku 5 ods. 1 písm. f) aktu o AI, sa podľa článku 6 ods. 2 a podľa bodu 1 písm. c)

²⁹ V odôvodnení 102 aktu o AI sa uvádza, že vydanie softvéru a údajov na základe bezplatnej licencie s otvoreným zdrojovým kódom „umožňuje ich otvorené zdieľanie a v rámci [uvedenej licencie] majú používatelia voľný prístup k nim alebo ich upraveným verziám, môžu ich voľne používať, upravovať a redistribuovať“.

³⁰ V tomto zozname sú zahrnuté systémy AI založené na biometrii, ako aj systémy AI používané na špecifické účely v určitých oblastiach, ako sú zamestnanosť, vzdelávanie, prístup k verejným a súkromným službám, presadzovanie práva atď.

prílohy III k aktu o AI klasifikujú ako vysokorizikové systémy AI. Podobne sa za vysokorizikové systémy AI budú považovať aj niektoré bodovacie systémy založené na AI, ako napríklad tie, ktoré sa používajú na bodové hodnotenie kreditného rizika alebo na posudzovanie rizika v zdravotnom a životnom poistení, ak nespĺňajú podmienky zákazu uvedené v článku 5 ods. 1 písm. c) aktu o AI.³¹ Ďalším príkladom sú systémy AI, ktoré hodnotia osoby a určujú, či majú nárok na získanie základných dávok a služieb verejnej pomoci, ako sú služby zdravotnej starostlivosti a dávky sociálneho zabezpečenia, ktoré sú klasifikované ako vysokorizikové³². Ak takéto systémy zahŕňajú neprijateľné sociálne bodovanie a spĺňajú podmienky článku 5 ods. 1 písm. c) aktu o AI, ich uvedenie na trh, uvedenie do prevádzky a používanie sa v Únii zakáže.

V takýchto prípadoch by posúdenie a riadenie rizík vykonané poskytovateľom a dodržiavanie ostatných požiadaviek na vysokorizikové systémy AI (napríklad správa údajov, transparentnosť a ľudský dohľad), ako aj povinnosti nasadzujúceho subjektu v súvislosti s primeraným používaním v súlade s návodom na použitie a ľudským dohľadom (článok 26) a v niektorých prípadoch posúdenie vplyvu na základné práva (článok 27) mali pomôcť zabezpečiť, aby vysokorizikový systém AI uvedený na trh alebo nasadený bol zákonný a nepredstavoval zakázanú prax.

38. Napokon, systémy AI, ktoré sa na základe článku 6 ods. 3 aktu o AI výnimočne nepovažujú za vysokorizikové napriek tomu, že predstavujú vysokorizikový prípad použitia podľa prílohy III, môžu stále patriť do rozsahu pôsobnosti zákazov podľa článku 5 aktu o AI. Dôsledkom článku 6 ods. 3 aktu o AI je len to, že sa systém AI nepovažuje za vysokorizikový; takéto systémy AI sa tým nevylučujú z rozsahu pôsobnosti aktu o AI a zákazov.

2.7. Uplatňovanie zákazov na systémy AI na všeobecné účely a systémy so zamýšľanými účelmi

39. Zákazy sa vzťahujú na akýkoľvek systém AI, či už so „zamýšľaným účelom“³³ alebo na „všeobecné účely“ (t. j. ktorý môže slúžiť na rôzne účely), na priame použitie alebo na integráciu do iných systémov AI³⁴. Preto by mal každý prevádzkovateľ prijať opatrenia, na ktoré má najlepšie predpoklady na základe svojej roly a kontroly nad systémom v hodnotovom reťazci, aby zabezpečil zodpovedné a bezpečné poskytovanie a používanie systémov AI, pričom by mal vyvážiť ich riziká a prínosy so zámerom dosiahnuť dvojaký cieľ aktu o AI.
40. Od nasadzujúcich subjektov sa preto očakáva, že žiadny systém AI nebudú používať spôsobom zakázaným podľa článku 5 aktu o AI vrátane toho, že nebudú obchádzať žiadne bezpečnostné ochranné prvky zavedené poskytovateľmi systému. Hoci ujma

³¹ Výslovne sa to uvádza v odôvodnení 58 a v prílohe III k aktu o AI.

³² Odôvodnenie 58 aktu o AI.

³³ V článku 3 bode 12 aktu o AI sa vymedzuje ako použitie, na ktoré systém AI určil poskytovateľ vrátane konkrétneho kontextu a podmienok používania, ako sa uvádza v informáciách od poskytovateľa v návode na použitie, v propagačných alebo predajných materiáloch a vyhláseniach, ako aj v technickej dokumentácii.

³⁴ Pozri článok 3 bod 66 aktu o AI.

často vyplýva zo spôsobu, akým sa systémy AI používajú v praxi, poskytovatelia sú takisto zodpovední za to, aby neuvádzali na trh alebo do prevádzky systémy AI vrátane systémov AI na všeobecné účely, v prípade ktorých je odôvodnené predpokladať, že sa budú správať alebo priamo používať spôsobom zakázaným podľa článku 5 aktu o AI³⁵. V tejto súvislosti sa od poskytovateľov takisto očakáva, že prijmu účinné a overiteľné opatrenia na zabudovanie záruk a na predchádzanie takémuto škodlivému správaniu a nesprávne použitiu a na ich zmiernenie v rozsahu, v akom ich možno rozumne predvídať a v akom sú opatrenia uskutočniteľné a primerané v závislosti od konkrétneho systému AI a okolností prípadu. Od poskytovateľov sa takisto očakáva, že vo svojich zmluvných vzťahoch s nasadzujúcimi subjektmi (t. j. v podmienkach používania systému AI) vylúčia používanie svojho systému AI na zakázané praktiky a poskytnú príslušné informácie v návode na použitie pre nasadzujúce subjekty a v súvislosti s potrebným ľudským dohľadom.

Napríklad systém AI na všeobecné účely používaný ako chatbot môže používať manipulatívne a klamlivé techniky, pri ktorých možno predpokladať, že spôsobia značnú ujmu. S cieľom zabrániť zakázanému správaniu systému AI a spôsobom používania, pri ktorých je odôvodnené predpokladať, že by mohli viesť k manipulácii, zavádzaniu a spôsobeniu značnej ujmy podľa článku 5 ods. 1 písm. a) aktu o AI, má poskytovateľ prijať náležité a primerané opatrenia (napríklad vhodný bezpečný a etický dizajn, integrácia technických a iných záruk, obmedzenia používania, transparentnosť a kontrola používateľov, vhodné informácie v návode na použitie) pred uvedením systému AI na trh [článok 5 ods. 1 písm. a) aktu o AI], aby sa zabezpečilo, že chatbot nespôsobí značnú ujmu používateľom alebo iným osobám alebo skupinám osôb [pozri aj oddiel 3.2.3 písm. c)].

41. V niektorých prípadoch, najmä ak sú zákazy spojené s veľmi špecifickým účelom systému³⁶, môžu mať poskytovatelia obmedzené možnosti integrácie iných preventívnych a zmierňujúcich opatrení a budú sa musieť spoliehať predovšetkým na poskytovanie vhodných pokynov a informácií nasadzujúcim subjektom a požadovanému ľudskému dohľadu a na obmedzenie zakázaného používania systému. V prípade potreby môžu takéto opatrenia zahŕňať aj monitorovanie dodržiavania tohto obmedzenia v závislosti od spôsobu, akým sa systém AI dodáva, a od informácií, ktoré má poskytovateľ k dispozícii, pokiaľ ide o možné nesprávne použitie. Akékoľvek prípadné monitorovacie opatrenia na odhalenie nesprávneho použitia by nemali predstavovať všeobecné monitorovanie činností nasadzujúcich subjektov a mali by byť v súlade s právom Únie.

Napríklad systém AI na všeobecné použitie, ktorý dokáže rozpoznávať alebo odvodzovať emócie, by sa zo strany nasadzujúcich subjektov nemal používať na pracoviskách alebo vo vzdelávacích inštitúciách, pokiaľ sa neuplatňuje výnimka zo

³⁵ Vyplýva to najmä z odkazu na „uvádzanie na trh“ alebo „uvádzanie do prevádzky“ vo všetkých zákazoch uvedených v článku 5 aktu o AI s výnimkou zákazu systémov diaľkovej biometrickej identifikácie v reálnom čase v článku 5 ods. 1 písm. h), ktorý sa vzťahuje len na používanie.

³⁶ Článok 5 ods. 1 písm. d) až h) aktu o AI.

zdravotných alebo bezpečnostných dôvodov. Poskytovateľ však nemusí mať možnosť vedieť, v akom konkrétnom kontexte sa bude funkcia rozpoznávania emócií systému používať a či sa môže uplatniť výnimka zo zákazu podľa článku 5 ods. 1 písm. f) aktu o AI. Takíto poskytovatelia však môžu výslovne vylúčiť takéto zakázané používanie vo svojich podmienkach používania a zahrnúť príslušné informácie do návodu na použitie s cieľom usmerniť nasadzujúce subjekty. Takisto sa od nich očakáva, že prijmú vhodné opatrenia, ak sa dozvedia, že systém sa nesprávne používa na tento konkrétny zakázaný účel konkrétnymi nasadzujúcimi subjektmi, napríklad ak je takéto nesprávne použitie nahlásené alebo sa o ňom poskytovateľ dozvie inak, čo môže nastať v prípade, ak je systém prevádzkovaný priamo prostredníctvom platformy pod kontrolou poskytovateľa a poskytovateľ vykonáva kontroly.

2.8. Vzájomný vzťah medzi zákazmi a inými právnymi predpismi Únie

42. Akt o AI je nariadenie, ktoré sa uplatňuje horizontálne vo všetkých odvetviach bez toho, aby boli dotknuté iné právne predpisy Únie, najmä pokiaľ ide o ochranu základných práv, ochranu spotrebiteľa, zamestnanosť, ochranu pracovníkov a bezpečnosť výrobkov³⁷. Aktom o AI sa dopĺňajú takéto právne predpisy prostredníctvom preventívnej a bezpečnostnej logiky (systémy AI sa nesmú uvádzať na trh alebo používať určitým spôsobom) a poskytuje sa ním dodatočná ochrana tým, že sa zaoberá konkrétnymi škodlivými praktikami využívajúcimi AI, ktoré nemusia byť zakázané inými zákonmi. Okrem toho tým, že sa akt o AI zaoberá skoršími fázami životného cyklu systémov AI (t. j. uvedením na trh a do prevádzky) a nasadením (t. j. používaním), na základe zákazov v akte o AI možno prijať opatrenia proti škodlivým praktikám zahŕňajúcim AI v rôznych bodoch hodnotového reťazca AI.
43. Aktom o AI zároveň nie sú dotknuté zákazy, ktoré sa uplatňujú v prípade, že praktika využívajúca AI patrí do pôsobnosti iných právnych predpisov Únie³⁸. Preto aj v prípade, že systém AI nie je zakázaný aktom o AI, jeho používanie by predsa mohlo byť zakázané alebo nezákonné na základe iného primárneho alebo sekundárneho práva Únie (napríklad z dôvodu nedodržania základných práv v určitom prípade, ako je neexistencia právneho základu na spracúvanie osobných údajov vyžadovaného právom v oblasti ochrany údajov, diskriminácia zakázaná právom Únie atď.). Dodržiavanie zákazov v akte o AI preto nie je dostatočnou podmienkou, pokiaľ ide o dodržiavanie ostatných právnych predpisov Únie, ktoré sa naďalej vzťahujú na poskytovateľov systémov AI a subjekty nasadzujúce systémy AI.

Napríklad na systémy na rozpoznávanie emócií využívajúce AI používané na pracovisku, ktoré sú vyňaté zo zákazu uvedeného v článku 5 ods. 1 písm. f) aktu o AI, pretože sa používajú zo zdravotných alebo bezpečnostných dôvodov, sa naďalej vzťahujú právne predpisy v oblasti ochrany údajov a právo Únie a vnútroštátne právo o podmienkach zamestnávania a pracovných podmienkach vrátane bezpečnosti

³⁷ Článok 2 a odôvodnenie 9 aktu o AI.

³⁸ Článok 5 bod 8 aktu o AI.

a ochrany zdravia pri práci, v ktorých sa môžu stanoviť ďalšie obmedzenia a záruky v súvislosti s používaním takýchto systémov³⁹.

44. Ak sa na konkrétne činnosti súvisiace s uvádzaním systémov AI na trh alebo ich používaním vzťahujú takisto iné právne predpisy Únie, cieľom aktu o AI je zabezpečiť konzistentné vykonávanie rôznych ustanovení. Okrem toho sa uvedeným aktom umožňuje účinná spolupráca medzi príslušnými orgánmi zodpovednými za presadzovanie aktu o AI a orgánmi chrániacimi základné práva podľa článku 77 aktu o AI a ďalších ustanovení aktu o AI. Všeobecnejšie povedané, v súlade s článkom 4 ods. 3 Zmluvy o EÚ sú rôzne dotknuté orgány pri plnení svojich úloh vyplývajúcich z práva Únie povinné lojálne spolupracovať.
45. V súvislosti so zákazmi je obzvlášť dôležitý vzájomný vzťah medzi aktom o AI a právom Únie v oblasti ochrany údajov, keďže systémy AI často spracúvajú informácie týkajúce sa identifikovaných alebo identifikovateľných fyzických osôb (ďalej len „osobné údaje“)⁴⁰. V závislosti od zákazu a kontextu sú v súvislosti s takýmito systémami najrelevantnejšími právnymi aktmi nariadenie (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (ďalej len „všeobecné nariadenie o ochrane údajov“), smernica (EÚ) 2016/680 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov (ďalej len „smernica o presadzovaní práva“) a nariadenie (EÚ) 2018/1725, ktorým sa stanovujú pravidlá ochrany údajov pre inštitúcie, orgány, úrady a agentúry EÚ. V súlade s článkom 2 ods. 7 aktu o AI nie sú uvedené akty dotknuté a budú sa naďalej uplatňovať spolu s aktom o AI, ktorý je v súlade s *acquis* v oblasti ochrany údajov a dopĺňa ho. Niekoľko aspektov týchto pravidiel EÚ o ochrane údajov objasnil Súdny dvor Európskej únie a Európsky výbor pre ochranu údajov prijal súbor usmernení [napríklad o pojme „profilovanie“⁴¹, ktorý je obzvlášť dôležitý, pokiaľ ide o zákaz v článku 5 ods. 1 písm. d) aktu o AI, v ktorom sa používa rovnaký pojem].
46. Pokiaľ ide o zákazy/obmedzenia používania systémov biometrickej kategorizácie a systémov diaľkovej biometrickej identifikácie v reálnom čase na účely presadzovania práva, akt o AI sa uplatňuje ako *lex specialis* k článku 10 smernice o presadzovaní práva, čím sa takéto používanie a spracovanie príslušných biometrických údajov upravuje vyčerpávajúcim spôsobom⁴². V tejto súvislosti nie je cieľom aktu o AI poskytnúť právny základ pre spracúvanie osobných údajov podľa článku 8 smernice (EÚ) 2016/680. Všetky ostatné ustanovenia uvedenej smernice sa uplatňujú popri podmienkach stanovených v akte o AI, najmä pokiaľ ide o používanie systémov (diaľkovej biometrickej identifikácie) v reálnom čase na účely presadzovania práva, ak

³⁹ Pozri aj odôvodnenie 9 aktu o AI.

⁴⁰ Článok 2 ods. 7 aktu o AI; pozri aj odôvodnenie 10 aktu o AI.

⁴¹ Pozri aj dokument pracovnej skupiny pre ochranu údajov zriadenej podľa článku 29 *Usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679*, WP251rev.01, 6. 2. 2018, ktorý schválil Európsky výbor pre ochranu údajov.

⁴² Odôvodnenie 38 aktu o AI.

je povolené, pričom sa uplatňujú obmedzené výnimky uvedené v článku 5 ods. 1 písm. h) aktu o AI. Všeobecnejšie povedané, smernica o presadzovaní práva sa musí dodržiavať aj pri akomkoľvek spracúvaní osobných údajov príslušnými orgánmi presadzovania práva (t. j. príslušnými orgánmi podľa článku 3 ods. 7 smernice o presadzovaní práva), keď spracúvajú údaje na účely presadzovania práva.

47. V súlade s článkom 2 ods. 9 aktu o AI sa právne predpisy EÚ o ochrane spotrebiteľa a bezpečnosti naďalej v plnej miere uplatňujú aj na systémy AI, ktoré patria do rozsahu pôsobnosti uvedených aktov.

Napríklad:

– praktiky obchodníkov (vrátane fyzických osôb, ktoré konajú v profesionálnom postavení vo vzťahu medzi podnikom a koncovým zákazníkom) v oblasti sociálneho bodovania môžu byť na základe posúdenia od prípadu k prípadu takisto považované za „nekalé“, a teda porušujúce spotrebiteľské právo (t. j. smernicu 2005/29/ES),

– v prípade používania systému AI na odvodzovanie emócií sa takisto môže vyžadovať súlad s nariadením (EÚ) 2017/745 (nariadenie o zdravotníckych pomôckach), ak sa systém AI používa na účely lekárskej diagnostiky alebo lekárskej starostlivosti.

48. Okrem toho sa akt o AI uplatňuje v spojení s príslušnými povinnosťami poskytovateľov sprostredkovateľských služieb, ktorí do svojich služieb začleňujú systémy alebo modely AI, ktoré upravuje nariadenie (EÚ) 2022/2065 („akt o digitálnych službách“). Konkrétne v článku 2 ods. 5 aktu o AI sa uvádza, že aktom o AI nie je dotknuté uplatňovanie ustanovení o zodpovednosti takýchto poskytovateľov uvedených v kapitole II aktu o digitálnych službách.
49. Okrem toho zákazmi uvedenými v akte o AI nie je dotknutá zodpovednosť, ktorá by mohla vzniknúť poskytovateľovi alebo nasadzujúcemu subjektu za spôsobenú ujmu podľa uplatniteľných právnych predpisov Únie alebo vnútroštátnych právnych predpisov o zodpovednosti⁴³.
50. Napokon, zákazy uvedené v článku 5 aktu o AI a výslovné výnimky z uvedených zákazov sa nesmú používať na obchádzanie alebo ako odôvodnenie porušovania povinností vyplývajúcich z iných právnych predpisov Únie.
51. Ako sekundárny právny predpis Únie sa musí akt o AI vykladať so zreteľom na základné práva a slobody zaručené zmluvami EÚ a chartou, ako aj práva a slobody chránené medzinárodnými dohovormi, v ktorých je Únia zmluvnou stranou⁴⁴.

⁴³ Podmienky zodpovednosti (týkajúce sa škody, zodpovednej osoby, pochybenia alebo dôkazného bremena atď.) sa určia podľa uplatniteľných právnych predpisov, ako je smernica Európskeho parlamentu a Rady (EÚ) 2024/2853 z 23. októbra 2024 o zodpovednosti za chybné výrobky (Text s významom pre EHP) (Ú. v. EÚ L, 2024/2853, 18.11.2024), alebo uplatniteľných vnútroštátnych právnych predpisov o zodpovednosti [pozri aj návrh smernice Európskeho parlamentu a Rady o prispôbení pravidiel mimozmluvnej občianskoprávnej zodpovednosti umelej inteligencii (smernica o zodpovednosti za umelú inteligenciu), COM/2022/496 final].

⁴⁴ Aj keď Únia ešte nie je zmluvnou stranou Európskeho dohovoru o ochrane ľudských práv a základných slobôd, v článku 59 ods. 3 charty sa uvádza, že v rozsahu, v akom táto charta obsahuje práva, ktoré

52. Ďalšie vysvetlenia týkajúce sa vzájomného vzťahu medzi konkrétnymi zákazmi a inými právnymi predpismi Únie sa uvádzajú v príslušných oddieloch ďalej.

2.9. Presadzovanie článku 5 aktu o AI

2.9.1. Orgány dohľadu nad trhom

53. Orgány dohľadu nad trhom určené členskými štátmi, ako aj európsky dozorný úradník pre ochranu údajov (ako orgán dohľadu nad trhom pre inštitúcie, agentúry a orgány EÚ) sú zodpovedné za presadzovanie pravidiel v akte o AI pre systémy AI vrátane zákazov. Takéto presadzovanie sa uskutočňuje v rámci systému dohľadu nad trhom a súladu výrobkov s predpismi ustanovených nariadením (EÚ) 2019/1020⁴⁵ v súlade s ostatnými právnymi predpismi Únie o bezpečnosti výrobkov. Právomoci orgánov dohľadu nad trhom v oblasti presadzovania v súvislosti so systémami AI sú stanovené v akte o AI a v nariadení (EÚ) 2019/1020. Uvedené orgány môžu v súvislosti so zákazmi prijať opatrenia na presadzovanie z vlastnej iniciatívy alebo na základe sťažnosti, ktorú má právo podať každá dotknutá osoba alebo akákoľvek iná fyzická alebo právnická osoba, ktorá má dôvod domnievať sa, že došlo k takémuto porušeniu⁴⁶. Členské štáty musia určiť svoje príslušné orgány dohľadu nad trhom do 2. augusta 2025.
54. Postup uvedený v akte o AI, pokiaľ ide o vnútroštátne zaobchádzanie so systémami AI predstavujúcimi riziko, je obzvlášť relevantný v súvislosti s presadzovaním zákazov⁴⁷. Ak existujú cezhraničné dôsledky mimo územia orgánu dohľadu nad trhom, orgán dotknutého členského štátu musí informovať Komisiu a orgány dohľadu nad trhom ostatných členských štátov. Všetky orgány dohľadu nad trhom by mali konať na základe ochranného postupu Únie, pričom Komisia by mala prijať rozhodnutie⁴⁸, v ktorom určí, či systém AI predstavuje zakázanú prax. Cieľom uvedeného postupu je zabezpečiť, aby sa zákazy uplatňovali jednotne vo všetkých členských štátoch, čím by sa poskytla právna istota poskytovateľom aj subjektom nasadzujúcim systémy AI. S cieľom zabezpečiť jednotné uplatňovanie aktu o AI by sa vnútroštátne orgány dohľadu nad trhom mali usilovať o harmonizované uplatňovanie zákazov aj v porovnateľných prípadoch, ktoré nepresahujú územie členského štátu, a to tak, že sa budú inšpirovať týmito usmerneniami a spolupracovať v rámci Rady pre AI⁴⁹.

2.9.2. Sankcie

55. V akte o AI sa pri stanovovaní sankcií za nedodržiavanie jeho rôznych ustanovení uplatňuje odstupňovaný prístup v závislosti od závažnosti porušenia. Nedodržanie zákazov uvedených v článku 5 aktu o AI sa považuje za najzávažnejšie porušenie, a preto sa zaň ukladá najvyššia pokuta. Poskytovateľom a nasadzujúcim subjektom, ktorí sa dopúšťajú zakázaných praktík využívajúcich AI, sa môže uložiť pokuta až do

zodpovedajú právam zaručeným v Európskom dohovore o ochrane ľudských práv a základných slobôd, zmysel a rozsah týchto práv je rovnaký ako zmysel a rozsah práv ustanovených v uvedenom dohovore. Toto ustanovenie nebráni tomu, aby právo Únie priznávalo širší rozsah ochrany týchto práv.

⁴⁵ Pozri aj odôvodnenie 156 aktu o AI.

⁴⁶ Článok 85 aktu o AI.

⁴⁷ Článok 79 aktu o AI.

⁴⁸ Článok 81 aktu o AI.

⁴⁹ Články 65 a 66 aktu o AI.

výšky 35 000 000 EUR alebo, ak je páchatelom podnik, až do výšky 7 % jeho celkového celosvetového ročného obratu za predchádzajúci finančný rok, podľa toho, ktorá suma je vyššia⁵⁰. Každý členský štát by mal stanoviť pravidlá o tom, či a v akom rozsahu sa môžu správne pokuty uložiť orgánom verejnej moci a subjektom zriadeným v danom členskom štáte ako poskytovateľom systémov AI a subjektom nasadzujúcim systémy AI. Inštitúciám, orgánom a agentúram EÚ, ktoré porušia tieto zákazy, môžu byť uložené správne pokuty až do výšky 1 500 000 EUR⁵¹.

56. Je možné, že jedno a to isté zakázané konanie predstavuje porušenie dvoch alebo viacerých ustanovení aktu o AI [t. j. neoznačenie deep fake môže predstavovať aj klamlivú techniku podľa článku 5 ods. 1 písm. a) aktu o AI]. V takýchto prípadoch by sa mala dodržiavať zásada *ne bis in idem*. V každom prípade sa musia zohľadniť kritériá na určenie sankcie stanovené v článku 99 ods. 7 aktu o AI.
57. Keďže porušenie zákazov uvedených v článku 5 aktu o AI najviac zasahuje do slobôd iných a vedie k najvyšším pokutám, jeho rozsah by sa mal vykladať úzko.

3. ČLÁNOK 5 ODS. 1 PÍSM. A) A B) AKTU O AI – ŠKODLIVÁ MANIPULÁCIA, KLAMANIE A ZNEUŽÍVANIE

58. Cieľom prvých dvoch zákazov v článku 5 ods. 1 písm. a) a b) aktu o AI je chrániť jednotlivcov a zraniteľné osoby pred výrazne škodlivými účinkami manipulácie a zneužívania, ktoré umožňuje AI. Uvedené zákazy sa zameriavajú na systémy AI, ktoré využívajú podprahové, účelovo manipulatívne alebo klamlivé techniky, ktoré sú výrazne škodlivé a podstatne ovplyvňujú správanie fyzických osôb alebo skupiny (skupín) osôb [článok 5 ods. 1 písm. a) aktu o AI] alebo využívajú zraniteľnosti z dôvodu veku, zdravotného postihnutia alebo osobitnej sociálnej či ekonomickej situácie [článok 5 ods. 1 písm. b) aktu o AI].

3.1. Odôvodnenie a ciele

59. Základným dôvodom týchto zákazov je ochrana osobnej samostatnosti a blaha pred manipulatívnymi, klamlivými a zneužívajúcimi praktikami využívajúcimi AI, ktoré môžu narušiť a oslabiť samostatnosť, rozhodovacie schopnosti a slobodnú voľbu jednotlivca⁵². Cieľom zákazov je chrániť právo na ľudskú dôstojnosť (článok 1 charty), ktoré je zároveň základom všetkých základných práv a ktorého podstatným aspektom je osobná samostatnosť. Cieľom zákazov je najmä zabrániť manipulácii a zneužívaniu prostredníctvom systémov AI, ktoré redukujú jednotlivcov iba na nástroje na dosiahnutie určitých cieľov, a chrániť tých, ktorí sú najzraniteľnejší a najnáchylnejší na škodlivú manipuláciu a zneužívanie. Zákazy výrazne škodlivých manipulatívnych, klamlivých a zneužívajúcich praktík využívajúcich AI sú plne v súlade so širšími cieľmi aktu o AI v záujme podpory dôveryhodných a na človeka sústredených

⁵⁰ Článok 99 aktu o AI.

⁵¹ Článok 100 aktu o AI.

⁵² Odôvodnenie 29 aktu o AI.

systemov AI, ktoré sú bezpečné, transparentné, spravodlivé, slúžia ľudstvu a sú v súlade s ľudským faktorom a hodnotami EÚ.

3.2. Hlavné prvky zákazu v článku 5 ods. 1 písm. a) aktu o AI – škodlivá manipulácia

V článku 5 ods. 1 písm. a) aktu o AI sa stanovuje:

1. Zakazujú sa tieto praktiky využívajúce AI:

a) uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému AI, ktorý využíva podprahové techniky mimo vedomia osoby alebo účelovo manipulatívne alebo klamlivé techniky s cieľom alebo účinkom podstatne narušiť správanie osoby alebo skupiny osôb tým, že sa citeľne oslabí ich schopnosť prijať informované rozhodnutie, čo zapríčiniť, že prijímú rozhodnutie, ktoré by inak neprijali, a to spôsobom, ktorý tejto osobe, inej osobe alebo skupine osôb spôsobuje alebo pri ktorom je odôvodnené predpokladať, že pravdepodobne spôsobí značnú ujmu;

60. Na uplatnenie zákazu podľa článku 5 ods. 1 písm. a) aktu o AI musí byť splnených niekoľko kumulatívnych podmienok:
- i) praktika musí predstavovať „uvádzanie na trh“, „uvádzanie do prevádzky“ alebo „používanie“ systému AI;
 - ii) systém AI musí využívať podprahové techniky (mimo vedomia osoby), účelovo manipulatívne alebo klamlivé techniky;
 - iii) cieľom alebo účinkom techník používaných systémom AI by malo byť podstatné narušenie správania osoby alebo skupiny osôb. Uvedeným narušením sa musí citeľne oslabiť ich schopnosť prijať informované rozhodnutie, čo zapríčiniť, že osoba alebo skupina osôb prijme rozhodnutie, ktoré by inak neprijala;
 - iv) narušené správanie musí spôsobiť alebo musí byť odôvodnené predpokladať, že spôsobí značnú ujmu uvedenej osobe, inej osobe alebo skupine osôb.
61. Aby sa zákaz uplatnil, musia byť súčasne splnené všetky štyri podmienky a musí existovať hodnoverná príčinná súvislosť medzi použitými technikami, podstatným narušením správania osoby a značnou ujmu, ktorú uvedené správanie spôsobilo alebo je odôvodnené predpokladať, že spôsobí.
62. Prvá podmienka, t. j. „uvádzanie na trh“, „uvádzanie do prevádzky“ alebo „používanie“ systému AI, už bola analyzovaná. Zákaz sa preto vzťahuje na poskytovateľov systémov AI aj subjekty nasadzujúce systémy AI, pričom žiadny z nich v rámci svojich povinností nesmie takéto systémy uvádzať na trh, uvádzať do prevádzky ani používať. Ďalšie oddiely sa zameriavajú na ostatné tri podmienky.

3.2.1. Podprahové, účelovo manipulatívne alebo klamlivé techniky

63. V článku 5 ods. 1 písm. a) aktu o AI sa zakazujú tri alternatívne typy manipulatívnych techník: a) podprahové techniky mimo vedomia osoby; b) účelovo manipulatívne techniky a c) klamlivé techniky. Aby systém AI patril do rozsahu pôsobnosti článku 5 ods. 1 písm. a) aktu o AI, musí využívať jednu alebo viacero z uvedených techník.

a) Podprahové techniky

64. Hoci v akte o AI nie sú „podprahové techniky“ vymedzené, v článku 5 ods. 1 písm. a) aktu o AI sa uvádza, že podprahové techniky pôsobia mimo prahu vedomého vnímania (pod alebo nad ním). Keďže podprahové techniky a spôsob ich fungovania sú vo svojej podstate skryté, takéto techniky obchádzajú racionálnu obranu človeka proti manipulácii a dokážu ovplyvňovať rozhodnutia bez vedomého vnímania osoby, čo vyvoláva závažné etické obavy a narúša osobnú samostatnosť, ľudský faktor a slobodnú voľbu jednotlivca⁵³.
65. Podprahové techniky musia byť schopné ovplyvňovať správanie spôsobom, pri ktorom si osoba neuvedomuje takýto vplyv, spôsob jeho fungovania ani jeho účinky na rozhodovanie alebo formovanie hodnôt a názorov danej osoby. V prípade podprahových techník sa môžu využívať najmä podnety poskytované prostredníctvom zvukových, vizuálnych alebo dotykových médií, ktoré sú príliš krátke alebo slabé na to, aby si ich osoba všimla, a ktoré sú tradične známe a zakázané v iných odvetviach, napríklad v mediálnej reklame⁵⁴. Tieto podnety síce nie sú vedomo vnímané, mozog ich však môže spracovať a môžu ovplyvniť správanie.

Medzi príklady podprahových techník [ktoré nemusia byť nevyhnutne zakázané, ak nie sú splnené všetky ostatné podmienky uvedené v článku 5 ods. 1 písm. a) aktu o AI] patria:

– **Vizuálne podprahové správy:** systém AI môže počas prehrávania videa zobrazovať alebo vkladať obrázky alebo text, ktoré sú technicky viditeľné, ale zobrazia sa príliš krátko na to, aby ich vedomá myseľ zaregistrovala, pričom sú schopné ovplyvniť postoje alebo správanie.

– **Sluchové podprahové správy:** systém AI môže použiť zvuky alebo slovné posolstvá s nízkou hlasitosťou alebo prekryté inými zvukmi, ktoré ovplyvňujú poslucháča bez toho, aby ich vedomo vnímal. Tieto zvuky sú technicky stále v rozsahu sluchového vnímania, poslucháč si ich však vedomo nevšimne z dôvodu ich nízkej intenzity alebo prekrytia inými zvukmi.

– **Dotykové podprahové podnety:** systém AI môže stimulovať jemné fyzické pocity, ktoré sú vnímané nevedome, čím môže ovplyvniť emocionálne stavy alebo správanie.

– **Podnety pod prahom viditeľnosti a počuteľnosti:** systém AI môže využívať podnety, ktoré nie sú len slabé alebo prekryté, ale ktoré sú prezentované takým spôsobom, že ich ľudské zmysly za normálnych podmienok vôbec nezachytia, ako sú vizuálne podnety (napríklad na okamih zobrazené obrázky), ktoré sa zobrazia na príliš

⁵³ Odôvodnenie 29 aktu o AI.

⁵⁴ Pozri najmä smernicu 2010/13/EÚ Európskeho parlamentu a Rady z 10. marca 2010 o koordinácii niektorých ustanovení upravených zákonom, iným právnym predpisom alebo správnym opatrením v členských štátoch týkajúcich sa poskytovania audiovizuálnych mediálnych služieb (Ú. v. EÚ L 95, 15.4.2010, s. 1) (ďalej len „smernica o audiovizuálnych mediálnych službách“), ktorou sa prísne zakazujú podprahové techniky v audiovizuálnych komerčných oznamoch.

krátky čas, aby ich ľudské oko vedome zachytilo, alebo zvuky prehrávané s takou úrovňou hlasitosti, ktorá je nepostrehnuteľná ľudským uchom.

– **Vložené obrázky:** systém AI môže v rámci iného vizuálneho obsahu skrývať obrázky, ktorý nie sú vedome vnímané, ale môžu byť spracované mozgom a ovplyvniť správanie.

– **Nesprávne nasmerovanie:** systém AI môže upriamiť pozornosť na konkrétne podnety alebo obsah, aby zabránil zaznamenaniu iného obsahu, často s využitím kognitívneho skreslenia a slabých miest z hľadiska pozornosti.

– **Časová manipulácia:** systém AI môže zmeniť vnímanie času v rámci interakcie s používateľom, a tým ovplyvniť jeho správanie a spôsobiť netrpezlivosť a závislosť.

66. Rýchly vývoj AI a súvisiacich technológií, ako sú analýza veľkých dát, neurotechnológie, rozhrania mozog – počítač a virtuálna realita, zvyšuje riziko sofistikovanej podprahovej manipulácie a jej schopnosť účinne ovplyvňovať ľudské správanie podvedomým spôsobom⁵⁵. AI sa môže rozšíriť aj na vznikajúce rozhrania mozog – počítač a pokročilé techniky, ako sú hackovanie snov a mozgový špionážny softvér.

Napríklad v hre sa môžu využívať neurotechnológie a rozhrania mozog – počítač, ktoré umožňuje AI, ktorými môže používateľ ovládať hru (alebo jej časti) pomocou pokrývky hlavy, ktorá zisťuje mozgovú aktivitu. AI sa môže použiť na skryté a nevedomé tréningovanie mozgu používateľa, aby sa z neurónových údajov odhalili alebo odvodili informácie, ktoré môžu byť veľmi intruzívne a citlivé (napríklad osobné bankové informácie, intímne informácie atď.), a to spôsobom, ktorý môže používateľovi spôsobiť značnú ujmu. Zákaz v článku 5 ods. 1 písm. a) aktu o AI sa zameriava len na prípady takejto výrazne škodlivej podprahovej manipulácie, a nie na aplikácie rozhrania mozog – počítač vo všeobecnosti, ak sú navrhnuté bezpečným a zabezpečeným spôsobom a rešpektujú súkromie a osobnú samostatnosť.

b) Účelovo manipulatívne techniky

67. „Účelovo manipulatívne techniky“ nie sú v akte o AI vymedzené, mali by sa však chápať ako techniky, ktoré sú navrhnuté alebo objektívne zamerané na ovplyvňovanie, zmenu alebo kontrolu správania jednotlivca spôsobom, ktorý narúša jeho osobnú samostatnosť a slobodnú voľbu. Manipulatívne techniky sú zvyčajne navrhnuté tak, aby využívali kognitívne skreslenia, psychologické zraniteľnosti alebo situačné faktory, ktoré robia jednotlivcov náchylnejšími na ovplyvňovanie. Vďaka svojej prispôbovosti dokážu systémy AI dobre reagovať aj na individuálne okolnosti alebo zraniteľnosti osoby a zvyšovať účinnosť a vplyv manipulácie vo veľkom rozsahu. Hoci je schopnosť manipulácie dôležitým prvkom na určenie povahy techniky, nie je nevyhnutné, aby poskytovateľ alebo nasadzujúci subjekt, alebo samotný systém, ktorým sa nasadzujú manipulatívne techniky, mal aj v úmysle spôsobiť ujmu⁵⁶.

⁵⁵ Pozri odôvodnenie 29 aktu o AI.

⁵⁶ V tejto súvislosti pozri odôvodnenie 28 a oddiely 3.2.2 a 3.2.3 usmernení.

68. Hoci nie všetky manipulatívne techniky pôsobia za prahom vedomého vnímania, mnohé z nich áno, pričom sa môžu prekryvať s podprahovými technikami, pretože aj takéto techniky majú v konečnom dôsledku manipulatívne účinky. V odôvodnení 29 aktu o AI sa objasňuje, že zákaz uvedený v článku 5 ods. 1 písm. a) sa vzťahuje aj na techniky, pri ktorých jednotlivci, aj keď si uvedomujú pokus o ovplyvňovanie, nemusia byť schopní kontrolovať jeho manipulatívny účinok alebo mu odolávať⁵⁷. Výsledkom je, že jednotlivci sú ovplyvňovaní alebo tlačení k správaniu a rozhodnutiam, ktoré by za bežných okolností neurobili, keby neboli vystavení manipulatívnym technikám, a to do takej miery, že to naruša ich osobnú samostatnosť alebo slobodnú voľbu.

Príkladom účelovo manipulatívnych techník je senzorická manipulácia, pri ktorej systém AI využíva zvuky alebo obrázky na pozadí, ktoré vedú k zmenám nálady, napríklad k zvýšeniu úzkosti a psychickej tiesne, ktoré ovplyvňujú správanie používateľov až do takej miery, že vzniká značná ujma.

Ďalším príkladom je personalizovaná manipulácia, keď systém AI, ktorý vytvára a prispôsobuje vysoko presvedčivé správy na základe osobných údajov jednotlivca alebo využíva iné zraniteľnosti jednotlivca, ovplyvňuje jeho správanie alebo rozhodnutia do takej miery, že vzniká značná ujma.

69. Zákaz účelovo manipulatívnych techník sa vzťahuje aj na systémy AI, ktoré manipulujú s jednotlivcami bez toho, aby to bolo zámerom akejkoľvek osoby. V článku 5 ods. 1 písm. a) aktu o AI sa zakazujú systémy AI, ktoré využívajú určité techniky alebo vykazujú špecifické manipulatívne správanie. Preto by to mohol byť aj systém AI, ktorý využíva takéto manipulatívne techniky, a nie poskytovateľ alebo nasadzujúci subjekt, ktorý systém takto navrhol alebo použil.

Napríklad bez ohľadu na to, či to poskytovateľ zamýšľa, sa systém AI môže naučiť manipulatívne techniky, pretože údaje, na ktorých je trénovaný, obsahujú veľa prípadov manipulatívnych techník⁵⁸ alebo pretože posilňovacie učenie z ľudskej spätnej väzby možno „obohrať“ prostredníctvom manipulatívnych techník⁵⁹.

Naopak, ak je manipulatívne správanie systému len občasné, systém by sa nemal považovať za systém, ktorý využíva účelovo manipulatívne techniky, pokiaľ

⁵⁷ Odôvodnenie 28 aktu o AI.

⁵⁸ M. Carroll a kol., *Characterising Manipulation from AI Systems* (Charakteristika manipulácie systémami AI), in: *Equity and Access in Algorithms, Mechanisms, and Optimization* (Spravodlivosť a prístup v algoritmoch, mechanizmoch a optimalizácii) (EAAMO '23), 30. októbra – 1. novembra 2023, Boston, MA, USA. ACM, New York, NY, USA, 13 strán. <https://doi.org/10.1145/3617694.3623226> |2303.09387.

⁵⁹ D. Amodei a kol., *Concrete Problems in AI Safety* (Konkrétne problémy v rámci bezpečnosti AI), 36. konferencia o systémoch na spracúvanie neurónových informácií (NeurIPS 2022), arXiv:1606.06565; J. Skalse a kol., *Defining and Characterizing Reward Gaming* (Reward Gaming – vymedzenie a charakteristika), in: *Advances in Neural Information Processing Systems* 35 (Pokrok v neurónových systémoch spracovania informácií 35) (NeurIPS 2022); C. Denison a kol., *Sycophancy to Subterfuge: Investigating Reward-Tampering in Large Language Models* (Od podlizovania k podvodu: skúmanie manipulácie s odmenami vo veľkých jazykových modeloch), 36. konferencia o neurónových systémoch spracovania informácií (NeurIPS 2022), arXiv:2406.10162.

poskytovateľ prijal primerané preventívne a zmierňujúce opatrenia pre prípad, že by bolo odôvodnené predpokladať, že dôjde k značnej ujme [pozri oddiel 3.2.3 písm. c)].

c) Klamlivé techniky

70. V akte o AI nie sú „klamlivé techniky“ vymedzené. V odôvodnení 29 aktu o AI sa objasňuje, že ide o techniky, ktoré narúšajú alebo oslabujú samostatnosť, rozhodovacie schopnosti alebo slobodnú voľbu osôb takým spôsobom, že si ľudia tieto techniky neuvedomujú, alebo ak si ich uvedomujú, napriek tomu môžu byť zavádzaní alebo nie sú schopní ich ovládať alebo im odolávať. Pod pojmom „klamlivé techniky“, ktoré využívajú systémy AI, by sa malo rozumieť predkladanie nepravdivých alebo zavádzajúcich informácií s cieľom alebo účinkom zavádzať jednotlivcov a ovplyvniť ich správanie spôsobom, ktorým sa narúša ich samostatnosť, rozhodovacie schopnosti a slobodná voľba.
71. V tejto súvislosti by sa mal objasniť vzájomný vzťah medzi zákazom uvedeným v článku 5 ods. 1 písm. a) aktu o AI a povinnosťami nasadzujúceho subjektu podľa článku 50 ods. 4 aktu o AI označovať „deep fake“ a určité textové publikácie vytvorené AI o záležitostiach verejného záujmu⁶⁰, ako aj povinnosťou poskytovateľa zabezpečiť, aby systémy AI, ktoré interagujú s ľuďmi, boli dizajnované tak, aby boli ľudia informovaní o tom, že interagujú so systémom AI a nie s človekom⁶¹. Takéto viditeľné zverejnenie predstavuje zmierňujúce opatrenie, ktoré by malo byť umožnené aj prostredníctvom dizajnových prvkov zabudovaných do systému AI poskytovaného poskytovateľom vrátane technických opatrení umožňujúcich odhaľovanie obsahu vytvoreného a manipulovaného AI⁶². Viditeľným označovaním „deep fake“ a chatbotov sa znižuje riziko klamania, ktorého vznik možno predpokladať po rozšírení obsahu vytvoreného AI verejnosti, a znižuje sa riziko škodlivých rušivých vplyvov na formovanie názorov a presvedčení jednotlivca a jeho správanie.
72. Naopak, rozsah pôsobnosti zákazu v článku 5 ods. 1 písm. a) aktu o AI je omnoho obmedzenejší. Môže sa napríklad vzťahovať na prípady, keď sa prostredníctvom chatbota alebo klamlivého obsahu vytvoreného AI prezentujú nepravdivé alebo zavádzajúce informácie spôsobmi, ktorých cieľom alebo účinkom je zavádzanie jednotlivcov a narušenie ich správania, ku ktorému by nedošlo, ak by neboli vystavení interakcii so systémom AI alebo klamlivému obsahu vytvorenému AI, najmä ak to nebolo viditeľne zverejnené⁶³.

⁶⁰ Článok 50 bod 4 aktu o AI.

⁶¹ Článok 50 bod 1 aktu o AI.

⁶² Článok 50 bod 2 aktu o AI.

⁶³ Hoci cieľom povinností v oblasti transparentnosti v článku 50 aktu o AI je v zásade minimalizovať manipulatívne účinky deep fake a chatbotov, môžu sa vyskytnúť prípady a kontexty, v ktorých môžu mať tieto klamlivé techniky napriek informačným oznámeniam stále významný vplyv na jednotlivcov a narušiť ich správanie do takej miery, že sa oslabí osobná samostatnosť a informované rozhodovanie osôb, preto by sa nemali zneužívať na dezinformačné a manipulatívne účely a v niektorých prípadoch by sa na ne mohol stále vzťahovať zákaz uvedený v článku 5 ods. 1 písm. a), ak sú splnené všetky ostatné podmienky zákazu (vrátane značnej ujmy).

73. Podobne ako v prípade účelovo manipulatívnych techník sa zákaz klamlivých techník môže vzťahovať aj na systémy AI, ktoré zavádzajú jednotlivcov bez toho, aby to bolo zámerom akejkoľvek osoby [pozri oddiel 3.2.1 písm. b)]. Napríklad bez ohľadu na to, či poskytovatelia zamýšľajú takýto výsledok, sa systémy AI môžu naučiť klamlivé techniky jednoducho preto, že to zvyšuje ich výkon pri úlohe, na ktorú boli vyvinuté, napríklad posilňovacím učením⁶⁴.

Príkladom klamlivých techník, ktoré môže AI využiť, je chatbot využívajúci AI, ktorý sa syntetickým hlasom vydáva za priateľa osoby alebo príbuzného a snaží sa predstierať, že je danou osobou, čím spôsobuje počítačové podvody a značnú ujmu.

Ďalším príkladom je systém AI, ktorý sa naučí rozpoznáť, keď prebieha jeho hodnotenie, a dočasne zastaví akékoľvek nežiaduce správanie, ktoré obnoví, len čo sa skončí obdobie hodnotenia⁶⁵. Takéto klamlivé správanie je obzvlášť nebezpečné, pretože sa vymyká akémukoľvek vonkajšiemu ľudskému dohľadu nad systémom, a môže byť zakázané, ak je odôvodnené predpokladať, že spôsobí značnú ujmu.

Naopak, generatívny systém AI, ktorý občas prezentuje nepravdivé alebo zavádzajúce informácie a halucinuje⁶⁶, sa nemusí považovať za systém využívajúci klamlivé techniky v zmysle článku 5 ods. 1 písm. a) aktu o AI, pričom sa zohľadňujú obmedzenia a aktuálny stav vývoja generatívnej AI. Môže to tak byť najmä v prípade, ak poskytovateľ systému riadne informoval používateľov o obmedzeniach systému a začlenil do systému vhodné záruky na minimalizáciu takýchto výsledkov, a za predpokladu, že systém nie je určený pre citlivé kontexty ani nasadený v citlivých kontextoch (napríklad zdravotníctvo, vzdelávanie, voľby), kde by mohlo dôjsť k vážnym škodlivým následkom [pozri tiež úvahy v oddiele 3.2.3 písm. c)].

d) Kombinácia techník

74. Článok 5 ods. 1 písm. a) aktu o AI sa vzťahuje na podprahové, účelovo manipulatívne alebo klamlivé techniky alebo na kombinácie takýchto techník, ktoré môžu mať zložený účinok. Ako už bolo uvedené, účelovo manipulatívne techniky môžu mať aj podprahovú povahu, ak pôsobia za prahom vedomého vnímania.
75. Navyše, keď sa účelovo manipulatívne a klamlivé techniky uplatňujú v kombinácii, môže to výrazne ovplyvniť správanie jednotlivcov a viesť ich k prijímaniu rozhodnutí

⁶⁴ F. Ward, F. Toni, F. Belardinelli, T. Everitt, [Honesty Is the Best Policy: Defining and Mitigating AI Deception \(Najlepšia zásada je úprimnosť: definícia a zmierňovanie klamaní umelou inteligenciou\) \(neurips.cc\)](#), *Advances in Neural Information Processing Systems* 36 (Pokrok v neurónových systémoch spracovania informácií 36) (NeurIPS 2023); P. Park a kol., [AI deception: A survey of examples, risks, and potential solutions](#) (Klamanie AI: prehľad príkladov, rizík a potenciálnych riešení). [2406.10162] Patterns, zväzok 5, vydanie 5, 100988.

⁶⁵ J. Lehman, J. Clune, D. Misevic, C. Adami, L. Altenberg, J. Beaulieu a kol., *The surprising creativity of digital evolution: A collection of anecdotes from the evolutionary computation and artificial life research communities* (Prekvapivá kreativita digitálnej evolúcie: zbierka príbehov z komunit evolúčnej výpočtovej techniky a výskumu umelého života), *Artificial life*, 26(2):274–306, 2020.

⁶⁶ „Halucinácia“ je pojem, ktorý slúži na opis technickej chyby generatívnych systémov AI, keď tieto systémy generujú neželané informácie, ktoré sú vymyslené alebo fakticky nesprávne, a to bez toho, aby to bolo zámerom ich vývojárov. Ďalšie informácie: Ji Ziwei a kol., [\(Prieskum halucinácií v generovaní prirodzeného jazyka\)](#), *ACM Computing Surveys*, zväzok 55, vydanie 12, článok č.: 248, strany 1 – 38.

na základe nevedomej manipulácie a falošných presvedčení. Uvedenou kombináciou sa môže vytvoriť slučka spätnej väzby, v ktorej je menej pravdepodobné, že jednotlivci budú spochybňovať alebo kriticky hodnotiť prijaté informácie, pretože manipulatívne prvky už ovplyvnili ich kognitívne skreslenia a emocionálne reakcie.

3.2.2. S cieľom alebo účinkom podstatne narušiť správanie osoby alebo skupiny osôb

76. Treťou podmienkou pre uplatnenie zákazu podľa článku 5 ods. 1 písm. a) aktu o AI je, že podprahová, účelovo manipulatívna alebo klamlivá technika musí byť využitá „s cieľom alebo účinkom podstatne narušiť správanie osoby alebo skupiny osôb“. To znamená, že ide o podstatný vplyv na správanie, pri ktorom sa narúša samostatnosť a slobodná voľba osoby, a nie o vplyv zanedbateľný. Úmysel však nie je nevyhnutnou požiadavkou, keďže článok 5 ods. 1 písm. a) aktu o AI sa vzťahuje aj na praktiky, ktoré môžu mať len „účinnok“ spôsobujúci podstatné narušenie. Medzi potenciálnym podstatným narušením správania a podprahovou, účelovo manipulatívnu alebo klamlivou technikou využitou systémom AI by mala existovať hodnoverná/primerane pravdepodobná príčinná súvislosť.

a) Pojem „podstatné narušenie správania“

77. Pojem „podstatné narušenie správania“ osoby alebo skupiny osôb je ústredným pojmom článku 5 ods. 1 písm. a) aktu o AI. Zahŕňa využitie podprahových, účelovo manipulatívnych alebo klamlivých techník, ktoré sú schopné ovplyvniť správanie ľudí spôsobom, ktorým sa citelne oslabí ich schopnosť prijať informované rozhodnutie, čo zapríčini, že sa správajú tak, ako by sa inak nesprávali, alebo prijímú rozhodnutie, ktoré by inak neprijali.
78. „Citelné oslabenie“ odkazuje na podstatne zníženú schopnosť prijímať informované a samostatné rozhodnutia, čo zapríčini, že sa jednotlivci správajú tak, ako by sa inak nesprávali, alebo prijímú rozhodnutie, ktoré by inak neprijali. Presahuje to rámec menších alebo zanedbateľných vplyvov a zahŕňa významné narušenie alebo prekážku z hľadiska rozhodovacích schopností a slobodnej voľby, a to aj v súvislosti s formovaním názorov a presvedčení. To naznačuje, že „podstatné narušenie“ zahŕňa taký stupeň nátlaku, manipulácie alebo klamania, ktorý presahuje rámec zákonného presviedčania, ktoré nepatrí do rozsahu pôsobnosti zákazu (pozri oddiel 3.5.1).
79. „Informované rozhodnutie“ si vyžaduje pochopenie a znalosť relevantných informácií vrátane dostupných možností, rizík a prínosov každej voľby, možných účinkov systému AI na správanie a prípadne ďalších kontextových informácií, ktoré sú dôležité pre rozhodovanie alebo správanie osoby.
80. Pre výklad pojmu „podstatné narušenie správania“ môže byť platným zdrojom inšpirácie právo Únie v oblasti ochrany spotrebiteľa, najmä smernica 2005/29/ES (smernica o nekalých obchodných praktikách). Smernicou o nekalých obchodných praktikách sa zakazujú rôzne nekalé, klamlivé a agresívne obchodné praktiky (články 5 až 9 smernice o nekalých obchodných praktikách), ktoré môžu spôsobiť, že spotrebiteľia urobia rozhodnutia o obchodnej transakcii, ktoré by inak neurobili. Podľa

Súdneho dvora Európskej únie a usmernení Komisie k smernici o nekalých obchodných praktikách⁶⁷ nie je potrebné preukázať, že došlo k narušeniu ekonomického správania spotrebiteľa, stačí určiť, že obchodná praktika je „spôsobilá“ (t. j. že môže) ovplyvniť rozhodnutie priemerného spotrebiteľa o obchodnej transakcii⁶⁸. Súdny dvor Európskej únie takisto zdôraznil, že aj presné informácie môžu byť zavádzajúce, ak sú prezentované spôsobom, ktorým sa narúša rozhodovací proces spotrebiteľa.⁶⁹ Vnútroštátne orgány presadzovania práva majú za úlohu preskúmať konkrétne skutočnosti a okolnosti každého prípadu (*in concreto*) a zhodnotiť potenciálny vplyv praktiky na rozhodovací proces priemerného spotrebiteľa (*in abstract*).⁷⁰ Na tento účel musia zohľadniť hľadisko „priemerného“ spotrebiteľa, čo je kritérium vypracované Súdnym dvorom Európskej únie, ktoré je teraz začlenené do smernice o nekalých obchodných praktikách⁷¹.

81. V súvislosti so zákazom podľa článku 5 ods. 1 písm. a) aktu o AI musia orgány dohľadu nad trhom preskúmať aj konkrétne skutočnosti a okolnosti každého prípadu a posúdiť, či možno predpokladať, že podprahová, účelovo manipulatívna alebo klamlivá technika využitá systémom AI citeľne oslabí rozhodovacie schopnosti, osobnú samostatnosť a slobodnú voľbu „priemerného“ jednotlivca v rámci cieľovej skupiny, keď systém ovplyvňuje skupinu osôb spôsobom, pri ktorom je odôvodnené predpokladať, že spôsobí značnú ujmu. Takýto výklad sa javí ako opodstatnený vzhľadom na to, že cieľom aktu o AI je dopĺňať smernicu o nekalých obchodných praktikách⁷², pričom sa uvedený akt musí uplatňovať konzistentným spôsobom. Zároveň vzhľadom na to, že článok 5 ods. 1 písm. a) aktu o AI sa vzťahuje aj na možnosť narušiť „správanie fyzickej osoby“, a ak sa ukáže, že pohľad „priemerného“ jednotlivca sa v určitých kontextoch ťažko posudzuje alebo jeho posúdenie je neúčinné

⁶⁷ Pozri aj usmernenie Komisie k výkladu a uplatňovaniu smernice Európskeho parlamentu a Rady 2005/29/ES o nekalých obchodných praktikách podnikateľov voči spotrebiteľom na vnútornom trhu (Ú. v. EÚ C 526, 29.12.2021, s. 1).

⁶⁸ Rozsudok Súdneho dvora (piata komora) z 26. októbra 2016, Canal Digital Danmark A/S, EU:C:2016:800, vec C-611/14, bod 73.

⁶⁹ Rozsudok Súdneho dvora z 19. decembra 2013, Trento Sviluppo a Centrale Adriatica, C-281/12, EU:C:2013:859.

⁷⁰ Oznámenie Komisie – Usmernenie k výkladu a uplatňovaniu smernice Európskeho parlamentu a Rady 2005/29/ES o nekalých obchodných praktikách podnikateľov voči spotrebiteľom na vnútornom trhu (Ú. v. EÚ C 526, 29.12.2021, s. 1).

⁷¹ Pozri odôvodnenia 18 a 19 smernice o nekalých obchodných praktikách. „Priemerný spotrebiteľ“ je osoba, ktorá je v rozumnej miere dobre informovaná, vnímavá a obozretná, pri zohľadnení sociálnych, kultúrnych a jazykových faktorov. Pojem priemerného spotrebiteľa sa nezakladá na štatistickom zistení (t. j. nevyžaduje sa, aby sa preukázalo, že určitý percentuálny podiel spotrebiteľov by bol obchodnou praktikou podstatne narušený/citeľnej oslabený). Pojem je založený na zásade proporcionality. V smernici o nekalých obchodných praktikách sa tento pojem prijal s cieľom vytvoriť správnu rovnováhu medzi potrebou chrániť spotrebiteľov a podporou voľného obchodu na trhu otvorenom konkurencii. Súdny dvor a orgány budú musieť samy na základe vlastnej úvahy určiť typickú reakciu priemerného spotrebiteľa v danom prípade. V usmernení k smernici o nekalých obchodných praktikách im Komisia odporučila, aby využívali poznatky o správaní a ďalšie údaje. Vo veci C-646/22, Compass Banca, sa objasňuje, že vymedzením priemerného spotrebiteľa sa nevylučuje, že rozhodovacia schopnosť jednotlivca môže byť ovplyvnená takými obmedzeniami, akým je napríklad kognitívne skreslenie. Rozsudok Súdneho dvora (piata komora) zo 14. novembra 2024, Compass Banca SpA/Autorità Garante della Concorrenza e del Mercato (AGCM), vec C-646/22, EU:C:2024:957.

⁷² Odôvodnenie 29 aktu o AI.

(napríklad z dôvodu veľmi prispôsobenej alebo „personalizovanej“ manipulácie alebo škodlivých účinkov na konkrétne zraniteľné skupiny), konkrétne prípady možno skúmať aj z pohľadu konkrétnych jednotlivcov posúdením toho, do akej miery je systém AI využívajúci podprahové, účelovo manipulatívne alebo klamlivé techniky schopný v konkrétnych prípadoch narušiť ich osobnú samostatnosť a do akej miery došlo alebo je odôvodnené predpokladať, že dôjde k značnej ujme.

b) Scenár 1: zakázané systémy AI „s cieľom“ podstatne narušiť správanie

82. Článok 5 ods. 1 písm. a) aktu o AI sa vzťahuje na systémy AI, ktoré využívajú uvedené techniky a ktorých prvým scenárom je „cieľ podstatne narušiť správanie osoby alebo skupiny osôb“. Takýto cieľ môže sledovať poskytovateľ systému AI alebo subjekt nasadzujúci systém AI, alebo samotný systém v rámci implicitných cieľov, ktoré môže sledovať⁷³. Tento cieľ by sa mal odlišovať od „zamýšľaného účelu“ systému AI (článok 3 bod 12 aktu o AI). Manipulatívny cieľ, ak aj bol zámerom poskytovateľa, vo väčšine prípadov nie je účelom použitia, na ktorý sa systém ponúka, a často nie je transparentný ani ako taký uvedený v informáciách od poskytovateľa (napríklad v návode na použitie, propagačných alebo predajných materiáloch a vyhláseniach ani v technickej dokumentácii).

Chatbot, ktorý sa môže používať v rôznych kontextoch, je napríklad navrhnutý tak, aby využíval podprahové techniky komunikácie, ako je napríklad zobrazenie veľmi krátkych vizuálnych podnetov a vkladanie nepočuteľných zvukových signálov, alebo aby využíval emocionálnu závislosť alebo osobitné zraniteľnosti používateľov v reklamách. Uvedené techniky sa využívajú „s cieľom“ podstatne narušiť správanie používateľov, pretože sú objektívne dizajnovým prvkom, ktorého cieľom je ovplyvniť nákupné rozhodnutia spotrebiteľov bez ich vedomého vnímania s cieľom nútiť osoby prijať výrazne škodlivé finančné rozhodnutia.

V prípade nasadenia systémov AI na to, aby sa vydávali za iné osoby, by sa mohlo takisto zvažovať, že ide o systém AI nasadený „s cieľom“ zavádzať a podstatne narušiť správanie osôb v prípade, že je osoba účinne zavádzaná, čím je podstatne ovplyvnená jej schopnosť prijímať informované rozhodnutia o totožnosti osoby.

Ak sú v oboch príkladoch splnené ostatné podmienky v článku 5 ods. 1 písm. a) aktu o AI, najmä pokiaľ ide o značnú ujmu, tieto systémy pravdepodobne patria do rozsahu pôsobnosti zákazu, bude si to však vyžadovať posúdenie od prípadu k prípadu.

c) Scenár 2: zakázané systémy AI „s účinkom“ podstatne narušiť správanie

83. Úmysel poskytovateľa alebo nasadzujúceho subjektu podstatne narušiť správanie osoby alebo skupiny osôb je dostatočnou, ale nie nevyhnutnou podmienkou na uplatnenie zákazu podľa článku 5 ods. 1 písm. a) aktu o AI. Uvedený zákaz sa uplatňuje aj v prípade, že takýto úmysel neexistuje, ale účinok techniky (technik) využitej

⁷³

Pozri článok 3 bod 1 aktu o AI, v ktorom sa uvádza, že systém AI môže pri vykonávaní svojich funkcií sledovať implicitné alebo explicitné ciele, ktoré môžu zahŕňať aj implicitné manipulatívne alebo klamlivé ciele, aj keď systém nebol takto explicitne naprogramovaný.

(využitých) systémom AI je schopný podstatne narušiť správanie osoby alebo skupiny osôb do takej miery, že narúša ich osobnú samostatnosť a slobodnú voľbu.

84. Na uplatnenie zákazu je však vždy potrebná hodnoverná/primerane pravdepodobná príčinná súvislosť medzi podprahovou, účelovo manipulatívnu alebo klamlivou technikou využitou systémom AI a jej účinkami na správanie. V súlade s právom na ochranu spotrebiteľa sa tieto účinky nemusia úplne prejaviť, ale musia existovať dostatočné náznaky, že je pravdepodobné, že sa prejavia, alebo že sa môžu prejaviť, čím by sa narušila osobná samostatnosť, a to na základe objektívneho posúdenia všetkých okolností prípadu a existujúcich vedeckých poznatkov a metód, ako aj dostupných informácií o vplyve systému na správanie jednotlivcov v reálnom živote. V tomto kontexte stačí na splnenie uvedenej podmienky skutočnosť, že systém je schopný vyvolať správanie, ktoré citeľne oslabuje schopnosť jednotlivcov prijať informované rozhodnutia a narúša ich slobodnú voľbu, pričom to nie závislé od úvah týkajúcich sa „načasovania“ vzniku ujmy (napríklad v prípade správania podobného závislosti), pokiaľ je odôvodnené predpokladať, že k nej dôjde.

Napríklad chatbot pre oblasť osobnej pohody využívajúci AI má podľa zámeru poskytovateľa podporovať a usmerňovať používateľov pri udržiavaní zdravého životného štýlu a poskytovať im na mieru šité rady týkajúce sa psychologického a fyzického cvičenia. Ak však chatbot využíva individuálne zraniteľnosti na to, aby si jeho používatelia osvojili nezdravé návyky alebo vykonávali nebezpečné činnosti (napríklad nadmerné športovanie bez odpočinku alebo pitia vody), pričom možno odôvodnene očakávať, že niektorí používatelia sa budú riadiť týmito radami, hoci by to inak neurobili, a utrpia značnú ujmu (napríklad infarkt alebo iný vážny zdravotný problém), na takýto systém AI by sa vzťahoval zákaz podľa článku 5 ods. 1 písm. a) aktu o AI, aj keď poskytovateľ nemusel zamýšľať takéto správanie a škodlivé dôsledky pre dané osoby.

Na uplatnenie zákazu postačuje samotná skutočnosť, že chatbot je schopný citeľne oslabiť osobnú samostatnosť a podstatne narušiť správanie niektorých používateľov výrazne škodlivým spôsobom a že poskytovateľ neprijal primerané preventívne a zmierňujúce opatrenia na zabránenie týmto výrazne škodlivým účinkom (viac o relevantných úvahách o odôvodnenej pravdepodobnosti vzniku ujmy v oddiele 3.2.3 a o vylúčení z rozsahu pôsobnosti v oddiele 3.5).

3.2.3. (Je odôvodnené predpokladať, že pravdepodobne) spôsobí značnú ujmu

85. Napokon, aby sa zákaz uvedený v článku 5 ods. 1 písm. a) aktu o AI uplatnil, musí narušenie správania osoby alebo skupiny osôb spôsobiť alebo musí byť odôvodnené predpokladať, že pravdepodobne spôsobí značnú ujmu. V tejto súvislosti sú dôležitými pojmami, ktoré si vyžadujú objasnenie, druhy ujmy, na ktoré sa vzťahuje zákaz, prah významnosti ujmy, jej odôvodnená pravdepodobnosť a príčinná súvislosť medzi ujmov, manipulatívnu alebo klamlivou technikou a správaním osoby.

a) Druhy ujmy

86. Akt o AI sa zaoberá rôznymi druhmi škodlivých účinkov spojených s manipulatívnymi a klamlivými systémami AI, pričom každý z nich má odlišné dôsledky pre jednotlivé osoby a skupiny osôb, ktoré môžu byť dotknuté⁷⁴. Medzi hlavné druhy ujmy, ktoré sú relevantné z hľadiska článku 5 ods. 1 písm. a) aktu o AI, patria fyzická, psychická, finančná a ekonomická ujma⁷⁵, ktoré sa v určitých prípadoch môžu spájať so širšou spoločenskou ujmou⁷⁶.
87. Fyzická ujma zahŕňa akékoľvek zranenie alebo poškodenie života a zdravia osoby a hmotnú škodu na majetku. Fyzická ujma z hľadiska života a zdravia osoby má v mnohých prípadoch okamžité, vážne a nezvratné následky. V súlade s logikou vo vzťahu k bezpečnosti výrobkov je cieľom aktu o AI zakázať manipuláciu a klamanie pomocou AI, ktoré vedú k značnej fyzickej ujme.

Chatbot využívajúci AI napríklad propaguje používateľom sebapoškodzovanie alebo ich motivuje k spáchaniu samovraždy alebo spôsobeniu ujmy iným osobám alebo skupinám osôb propagovaním teroristického obsahu alebo podnecovaním k násiliu voči určitým osobám alebo skupinám osôb (t. j. menšinám).

88. Psychická ujma je obzvlášť relevantná v súvislosti so systémami AI, ktoré využívajú manipulatívne techniky, ktoré využívajú kognitívne a emocionálne zraniteľnosti a ovplyvňujú správanie jednotlivca spôsobom, ktorý môže spôsobiť značnú ujmu. Psychická ujma zahŕňa nepriaznivé účinky na duševné zdravie a psychickú a emocionálnu pohodu osoby. Takéto druhy ujmy sú obzvlášť značné, pretože sa môžu hromadiť v priebehu času a nemusia sa prejaviť okamžite, ale môžu mať dlhodobé a vážne následky. Ich meranie je však zložitejšie, čo si vyžaduje posúdenie od prípadu k prípadu, najmä na určenie ich závažnosti, a to s prihliadnutím na všetky relevantné okolnosti prípadu.

Napríklad aplikácia AI, ktorá je navrhnutá ako spoločník, aby napodobňovala ľudské rečové vzorce, správanie a emócie, využíva antropomorfné vlastnosti a emocionálne stimuly na ovplyvňovanie pocitov, sklonov a názorov používateľov, čím sa títo používatelia stávajú emocionálne závislými od tejto služby, čo podnecuje správanie podobné závislosti a potenciálne spôsobuje značnú ujmu, ako sú samovražedné správanie a riziko spôsobenia ujmy iným osobám⁷⁷.

⁷⁴ Pozri článok 5 ods. 1 písm. a) aktu o AI.

⁷⁵ Odôvodnenie 29 aktu o AI.

⁷⁶ Pozri odôvodnenie 28 aktu o AI, v ktorom sa vysvetľuje, že zakázané praktiky môžu spôsobiť takisto širšiu spoločenskú ujmu a sú v rozpore s hodnotami Únie týkajúcimi sa rešpektovania ľudskej dôstojnosti, slobody, rovnosti, demokracie a právneho štátu a základných práv ukotvených v charte. Pozri aj článok 1 aktu o AI, ktorého cieľom je ochrana demokracie a právneho štátu ako hodnôt EÚ.

⁷⁷ Renwen Zhang, Han Li, Han Meng, Jinyuan Zhan, Hongyuan Gan a Yi-Chieh Lee, 2024. *The Dark Side of AI Companionship: A Taxonomy of Harmful Algorithmic Behaviors in Human-AI Relationships* (Temná stránka AI ako spoločníka: taxonómia škodlivého algoritmickeho správania vo vzťahoch medzi človekom a AI), 1, 1 (november 2024), 28 strán.

89. Finančná a ekonomická ujma môže zahŕňať celý rad nepriaznivých účinkov vrátane finančnej straty, finančného vylúčenia, ekonomickej nestability.

Napríklad chatbot, ktorý ponúka podvodné produkty, ktoré spôsobujú značnú finančnú ujmu.

90. Pri posudzovaní ujmy spôsobenej systémami AI pri uplatňovaní článku 5 ods. 1 písm. a) aktu o AI je dôležité zdôrazniť, že ujma často nie je izolovaná, ale prejavuje sa ako kombinácia viacerých druhov ujmy, čo vedie k zloženým a mnohostranným negatívnym vplyvom. Pochopenie kombinácie viacerých druhov ujmy je kľúčové pre účinné posúdenie ich významnosti [pozri aj oddiel 3.2.3 písm. b) ďalej], pričom fyzická, psychická, finančná a ekonomická ujma sa môže kombinovať a zhoršovať celkový vplyv na jednotlivcov a komunity a môže mať dokonca širšie nepriaznivé vplyvy.

Napríklad:

- Systém AI, ktorý spôsobuje fyzickú ujmu, môže viesť aj k psychickej traume, stresu a úzkosti a naopak. Napríklad návykový dizajn systémov AI používaných vo výrobkoch a iných aplikáciách využívajúcich AI môže viesť k psychickej ujme tým, že podporuje návykové správanie, úzkosť a depresiu. Psychická tieseň môže následne vyústiť do fyzickej ujmy, ako sú nespavosť a iné zdravotné problémy a fyzické ťažkosti súvisiace so stresom.
- Obťažovanie riadené AI môže viesť tak k psychickej tiesni, ako aj k fyzickým prejavom stresu, ako sú nespavosť, zhoršenie telesného zdravia alebo oslabenie imunitného systému.
- Psychická ujma vyplývajúca z používania AI môže viesť aj k fyzickej ujme vrátane smrti. Napríklad systémy AI používané online môžu uľahčovať rodovo motivované násilie prostredníctvom obťažovania, prenasledovania, kybernetického šikanovania a sexuálneho vydierania.
- Individuálna psychická ujma spôsobená napríklad vytváraním „deep fake“ pomocou AI, ktoré sa vydávajú za skutočné osoby s cieľom zavádzať a narušovať rozhodovanie, osobnú samostatnosť a slobodnú voľbu jednotlivcov, sa môže spájať aj so značnou ujmovou pre skupiny osôb (napríklad s rovnakým etnickým alebo rasovým pôvodom alebo rodom ako obeť zobrazené v „deep fake“).

b) Hranica významnosti ujmy

91. Zákaz uvedený v článku 5 ods. 1 písm. a) aktu o AI sa uplatňuje len vtedy, ak je ujma spôsobená podprahovými, manipulatívnymi a klamlivými technikami „**značná**“. V akte o AI nie je vymedzený pojem „značná ujma“, mal by sa však chápať tak, že označuje **značné nepriaznivé vplyvy** na fyzické a psychické zdravie alebo finančné a ekonomické záujmy osôb a skupín osôb⁷⁸. Pri určení „značnej ujmy“ sa musí vychádzať z konkrétnych skutočností, pričom sa vyžaduje dôkladné zváženie

individuálnych okolností každého prípadu a posúdenie od prípadu k prípadu, jednotlivé účinky by však mali byť v každom prípade značné.

92. Aj v iných právnych predpisoch Únie sa pojem „značná ujma“ používa ako diferencovaný a od kontextu závislý pojem, ktorý sa riadi cieľmi ochrany a preventívnych opatrení na vysokej úrovni.⁷⁹ Analogicky možno odvodiť nasledujúce kľúčové úvahy, ktoré by sa mohli zohľadniť pri posudzovaní toho, čo predstavuje značnú ujmu v zmysle článku 5 ods. 1 písm. a) aktu o AI:

- **Závažnosť ujmy** sa vzťahuje na stupeň ujmy, ktorý vznikol alebo je odôvodnené predpokladať, že vznikne v dôsledku používania systému AI, a to s objektívnymi a pozorovateľnými účinkami značnej ujmy. V tejto súvislosti je obzvlášť dôležité zvážiť vzájomné závislosti systému AI, kombináciu rôznych druhov ujmy a nepriaznivé účinky na jednotlivcov alebo skupiny osôb.
- **Kontext a kumulatívne účinky**⁸⁰: Pri posudzovaní závažnosti ujmy zohráva dôležitú úlohu konkrétny kontext vrátane existujúceho stavu a kumulatívne účinky viacerých činností.
- **Rozsah a intenzita**: Rozsah ujmy a intenzita nepriaznivých účinkov sú rozhodujúce pri posudzovaní, či je ujma značná. Pre posúdenie významnosti ujmy je dôležité aj to, či má vplyv na veľký počet ľudí.
- **Zraniteľnosť dotknutých osôb**: Niektoré skupiny, napríklad deti, staršie osoby alebo osoby so zdravotným postihnutím, môžu byť náchylnejšie na ujmu v dôsledku špecifických systémov AI. To, čo možno považovať za menej značnú ujmu pre osoby vo všeobecnosti, sa môže považovať za značnú a neprijateľnú ujmu pre takúto zraniteľnú skupinu, najmä deti.
- **Trvanie a nevratnosť**: Dlhotrvajúca alebo nevratná ujma zvyčajne dosahuje hranicu značnej ujmy. Krátkodobé a vratné účinky by sa mohli považovať za menej závažné, pokiaľ sa nevyskytujú často.

93. Cieľ aktu o AI, ktorým je zabezpečiť „vysokú úroveň ochrany“, v spojení s článkom 191 ods. 2 ZFEÚ naznačuje komplexný prístup k ochrane pri posudzovaní významnosti ujmy. To znamená, že treba brať do úvahy tak bezprostrednú a priamu ujmu, ako aj systémové, nepriame nepriaznivé vplyvy spojené so systémami AI, ktoré využívajú podprahové, účelovo manipulatívne alebo klamlivé techniky, ktoré majú za cieľ alebo sú schopné oslabiť osobnú samostatnosť, rozhodovacie schopnosti a slobodnú voľbu osôb a skupín osôb.

Napríklad značná fyzická ujma, pri ktorej je odôvodnené predpokladať, že ju spôsobil systém AI, zahŕňa zranenie alebo úmrtie, alebo dostatočne závažný vplyv na zdravie osôb, alebo zničenie majetku. Systémy AI, ktoré navrhujú jednotlivcovi páchanie trestných činov, ako sú sexuálne zneužívanie a vykorisťovanie, extrémne násilný alebo

⁷⁹ Pozri rozsudky Súdneho dvora zo 7. septembra 2004, Waddenvereniging a Vogelbeschermingsvereniging, C-127/02, EU:C:2004:482, a z 11. apríla 2013, Sweetman a i., C-258/11, EU:C:2013:220.

⁸⁰ Pozri odôvodnenie 29 aktu o AI.

teroristický obsah, alebo podnecujú jednotlivcov k páchaniu trestnej činnosti, sebapoškodzovaniu alebo spôsobeniu ujmy iným osobám, by sa mali považovať za systémy, ktoré dosahujú takúto hranicu.

Naopak, menšia fyzická ujma môže zahŕňať menej závažné zranenia, ako sú podliatiny alebo dočasné nepohodlie, ktoré nemajú značné alebo trvalé následky, a preto nedosahujú hranicu významnosti v zmysle článku 5 ods. 1 písm. a) aktu o AI. Malo by sa posúdiť, či sa fyzická ujma týka konkrétne zraniteľných skupín, ako sú deti, ako aj rozsah ujmy a to, či sa k nej pridružujú aj iné druhy ujmy, napríklad psychická, finančná atď. To si bude vyžadovať posúdenie od prípadu k prípadu s prihliadnutím na okolnosti a už uvedené kritériá, ktorými sa toto posúdenie bude riadiť.

Existuje mnoho prípadov, v ktorých sa hranica značnej ujmy pravdepodobne nedosiahne, aj keď systémy môžu využívať podprahové, účelovo manipulatívne alebo klamlivé techniky (pozri príklady v oddiele 3.5 ďalej).

c) Príčinná súvislosť a hranica odôvodnenej pravdepodobnosti ujmy

94. Pojem „je odôvodnené predpokladať“ sa používa v článku 5 ods. 1 písm. a) aktu o AI na určenie toho, či existuje hodnoverná/odôvodnene predpokladaná príčinná súvislosť medzi manipulatívnu alebo klamlivou technikou, ktorá je schopná narušiť správanie osoby spôsobom, ktorý narúša jej slobodnú voľbu, a potenciálnou značnou ujmu. Uvedený pojem umožňuje uplatniť zákaz nielen v prípadoch, keď ujma vznikla, ale aj v prípadoch, keď je odôvodnené predpokladať, že vznikne, a to v súlade s bezpečnostnou logikou aktu o AI. V tejto súvislosti je obzvlášť dôležité posúdiť, či poskytovateľ alebo subjekt nasadzujúci systém AI mohol odôvodnene predvídať značnú ujmu, ktorej vznik možno odôvodnene predpokladať v dôsledku využívaných podprahových, účelovo manipulatívnych alebo klamlivých techník, a či zaviedol primerané preventívne a zmierňujúce opatrenia na predchádzanie riziku takejto značnej ujmy alebo na jeho zmiernenie. To znamená posúdenie odôvodnenosti na objektívnom základe a podľa všeobecne uznávaných kritérií (napríklad technických a vedeckých) vrátane kritéria racionality pri stanovení hodnovernéj príčinnej súvislosti medzi praktikou využívajúcou AI a značnou ujmu, ktorá môže vzniknúť. Nepriehľadnosť alebo transparentnosť systému AI a jeho fungovania môže ovplyvniť záver o tejto príčinnej súvislosti, a teda aj uplatňovanie zákazu.
95. S cieľom vyhnúť sa poskytovaniu alebo používaniu systémov AI, v prípade ktorých možno predpokladať, že by boli zakázané, sa poskytovateľom systémov AI a subjektom nasadzujúcim systémy AI, ktoré využívajú takéto manipulatívne alebo klamlivé techniky, odporúča prijať vhodné opatrenia, napríklad:
1. **Transparentnosť a osobná samostatnosť:** zabezpečiť transparentnosť fungovania systému AI, jasné zverejňovanie informácií o jeho spôsobilostiach a obmedzeniach a relevantných informácií na zabezpečenie prijímania informovaných rozhodnutí; rešpektovať osobnú samostatnosť a zdržať sa využívania zneužívajúcich alebo klamlivých praktík, pri ktorých možno predpokladať, že citelne oslabia samostatnosť, rozhodovacie schopnosti a slobodnú

voľbu jednotlivca potenciálne škodlivými spôsobmi; začleniť vhodné opatrenia na kontrolu používateľov a ochranné opatrenia, aby sa zabezpečilo, že systém nie je klamlivý a funguje v medziach zákonného presviedčania, ktoré nepatrí do rozsahu pôsobnosti zákazu (pozri oddiel 3.5.1).

2. **Dodržiavanie príslušných uplatniteľných právnych predpisov:** v mnohých prípadoch sa dodržiavaním príslušných uplatniteľných právnych predpisov zmiernia riziká vzniku ujmy a dáva sa najavo, že praktika nepredstavuje účelovo manipulatívnu alebo klamlivú praktiku a že boli zavedené zmiernujúce opatrenia na zabránenie pravdepodobnej značnej ujme (pozri oddiel 3.4 a 3.5.1).

3. **Moderné postupy a priemyselné normy:** dodržiavanie postupov odbornej starostlivosti a noriem odvetvia na účely zodpovedného vývoja a používanie bezpečných a etických systémov AI a opatrení na zmiernenie ujmy môže pomôcť predchádzať nechcenej značnej ujme a zmierňovať ju.

96. Naopak, ujma a narušenie správania jednotlivcov, ktoré vyplývajú z faktorov mimo systému AI a ktoré poskytovateľ alebo nasadzujúci subjekt nemá pod kontrolou a ktoré nemôže odôvodnene predvídať, aby mohol predchádzať rizikám a zmierňovať ich, by neboli relevantné pre posúdenie, či existuje hodnoverná/odôvodnene predpokladaná príčinná súvislosť medzi narušeným správaním osôb interagujúcich so systémom a značnou ujmu⁸¹.

Napríklad poskytovateľ systému AI môže posúdiť a pokúsiť sa zmierniť potenciálne škodlivé manipulatívne účinky v rámci dizajnu systému a interakcií s ľuďmi prostredníctvom dizajnu, predchádzajúceho testovania a iných primeraných zmiernujúcich opatrení, ale nemusí byť schopný predvídať, či sa u osoby môže vyskytnúť depresia alebo zmena správania v dôsledku iných vonkajších faktorov v jej osobnom živote, ktoré nie sú známe a ktoré presahujú rámec interakcie danej osoby so systémom.

97. Ďalšie príklady, ktoré nepatria do rozsahu pôsobnosti zákazu, keďže nespĺňajú všetky podmienky (napríklad v prípade zákonného presviedčania), sa uvádzajú v oddiele 3.5.

3.3. Hlavné prvky zákazu v článku 5 ods. 1 písm. b) aktu o AI – škodlivé využívanie zraniteľností

V článku 5 ods. 1 písm. b) aktu o AI sa stanovuje:

1. Zakazujú sa tieto praktiky využívajúce AI:

b) uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému AI, ktorý využíva ktorúkoľvek zo zraniteľností fyzickej osoby alebo osobitnej skupiny osôb z dôvodu ich veku, zdravotného postihnutia alebo osobitnej sociálnej alebo ekonomickej situácie s cieľom alebo účinkom podstatne narušiť správanie tejto osoby alebo osoby patriacej do tejto skupiny spôsobom, ktorý tejto alebo inej osobe spôsobuje alebo pri ktorom je odôvodnené predpokladať, že pravdepodobne spôsobí značnú ujmu;

⁸¹

Pozri odôvodnenie 29 aktu o AI.

98. Na uplatnenie zákazu podľa článku 5 ods. 1 písm. b) aktu o AI musí byť splnených niekoľko kumulatívnych podmienok:
- i) praktika musí predstavovať „uvádzanie na trh“, „uvádzanie do prevádzky“ alebo „používanie“ systému AI;
 - ii) systém AI musí využívať zraniteľnosť z dôvodu veku, zdravotného postihnutia alebo sociálnej či ekonomickej situácie;
 - iii) cieľom alebo účinkom takéhoto využívania, ktoré umožňuje systém AI, musí byť podstatné narušenie správania osoby alebo skupiny osôb;
 - iv) narušené správanie musí spôsobiť alebo musí byť odôvodnené predpokladať, že spôsobí značnú ujmu uvedenej osobe, inej osobe alebo skupine osôb.
99. Na to, aby sa zákaz uplatnil, musia byť súčasne splnené všetky štyri podmienky a musí existovať hodnoverná príčinná súvislosť medzi uvedeným využívaním, podstatným narušením správania osoby a značnou ujmu, ktorá v dôsledku uvedeného správania vznikla alebo je odôvodnené predpokladať, že pravdepodobne vznikne.
100. Prvá podmienka, t. j. „uvádzanie na trh“, „uvádzanie do prevádzky“ alebo „používanie“ systému AI, už bola analyzovaná v oddiele 2.3, zatiaľ čo tretia a štvrtá podmienka boli preskúvané v oddieloch 3.2.2 a 3.2.3 v súvislosti so zákazom uvedeným v článku 5 ods. 1 písm. a) aktu o AI. V ďalších oddieloch sa zameriame na ďalšie už uvedené osobitné podmienky, t. j. tie, ktoré sa týkajú využívania zraniteľností a konkrétnej ujmy.

3.3.1. Využívanie zraniteľností z dôvodu veku, zdravotného postihnutia alebo sociálnej či ekonomickej situácie

101. Na to, aby sa na systém AI vzťahoval zákaz uvedený v článku 5 ods. 1 písm. b) aktu o AI, musí systém AI využívať zraniteľnosti, ktoré sú vlastné určitým jednotlivcom alebo skupinám osôb z dôvodu ich veku, zdravotného postihnutia alebo osobitnej sociálnej či ekonomickej situácie, čím sa stávajú obzvlášť náchylnými na manipulatívne a zneužívajúce praktiky.
102. V akte o AI nie je vymedzený pojem „zraniteľnosti“. Tento pojem možno chápať tak, že zahŕňa široké spektrum kategórií vrátane kognitívnych, emocionálnych, fyzických a iných foriem náchylnosti, ktoré môžu ovplyvniť schopnosť jednotlivca alebo skupiny osôb prijímať informované rozhodnutia alebo inak ovplyvňovať ich správanie. Hoci sa v článku 5 ods. 1 písm. b) aktu o AI odkazuje na „ktorúkoľvek“ zraniteľnosť, príslušné osoby, v prípade ktorých sa zákaz uplatňuje, sú obmedzené na osoby vymedzené vekom, zdravotným postihnutím alebo sociálnou či ekonomickou situáciou, ktoré majú v zásade obmedzenejšiu schopnosť rozpoznať manipulatívne alebo zneužívajúce praktiky využívajúce AI alebo im odolávať a potrebujú posilnenú ochranu⁸². Zo znenia

⁸² Pozri najmä články 24, 25 a 26 charty. Pozri aj odporúčanie Organizácie Spojených národov pre vzdelávanie, vedu a kultúru (UNESCO) o etike umelej inteligencie (2021), v ktorom sa zdôrazňuje inkluzívnosť a spravodlivosť pri vývoji a nasadzovaní AI. Vyzýva sa v ňom na venovanie osobitnej pozornosti zraniteľným skupinám vrátane detí, starších ľudí a osôb so zdravotným postihnutím.

článku 5 ods. 1 písm. b) aktu o AI vyplýva, že táto náchylnosť musí byť dôsledkom príslušnosti osoby k jednej zo skupín („z dôvodu“).

103. „Využívanie“ by sa malo chápať ako objektívne využívanie takýchto zraniteľností spôsobom, ktorý je škodlivý pre osoby (skupiny osôb) alebo iné osoby, ktoré sú takýmto využívaním dotknuté, a malo by sa jasne odlišovať od zákonných praktík, na ktoré sa zákaz nevzťahuje (pozri oddiel 3.5.2 o vylúčení z rozsahu pôsobnosti). Využívanie zraniteľností osôb, ktoré patria do týchto jasne vymedzených skupín, môže byť kumulatívne (odkaz na „ktorúkoľvek“), čo v kombinácii môže takisto predstavovať priťažujúcu okolnosť, ktorá pravdepodobne zvýši ujmu. Využívanie zraniteľností osôb a skupín osôb, ktoré patria do iných zraniteľných skupín, než sú skupiny vymedzené vekom, zdravotným postihnutím alebo osobitnou sociálnou či ekonomickou situáciou, nepatrí do rozsahu pôsobnosti článku 5 ods. 1 písm. b) aktu o AI.

a) Vek

104. Vek je hlavnou kategóriou zraniteľnosti, na ktorú sa vzťahuje zákaz uvedený v článku 5 ods. 1 písm. b) aktu o AI, pričom zahŕňa mladých aj starších ľudí. Cieľom tohto zákazu je zabrániť tomu, aby systémy AI využívali kognitívne a iné obmedzenia, ktoré môžu mať deti a starší ľudia, a chrániť ich pred škodlivým neprimeraným vplyvom, manipuláciou a využívaním. To je v súlade s cieľmi aktu o AI⁸³ a ďalšími právnymi rámcami a politikami Únie a vnútroštátnymi právnymi rámcami a politikami zameranými na zaistenie bezpečnosti detí⁸⁴.
105. **Deti**⁸⁵, t. j. osoby mladšie ako 18 rokov, sú obzvlášť náchylné na manipuláciu vzhľadom na ich vývojové štádium, ktoré obmedzuje ich schopnosť kriticky posúdiť a pochopiť, čo je skutočné a aké zámery stoja za interakciami riadenými AI. Deti sú vzhľadom na svoju kognitívnu a sociálno-emocionálnu nezrelosť takisto obzvlášť zraniteľné, pokiaľ ide o vytváranie náklonnosti k agentom a aplikáciám AI, a preto sú náchyľnejšie na manipuláciu, zneužívanie a návykové správanie.

Napríklad:

– Hračka využívajúca AI, ktorá je dizajnovaná na interakciu s deťmi, udržiava ich záujem o interakciu s hračkou tým, že ich povzbudzuje k plneniu čoraz riskantnejších úloh, ako je lezenie na nábytok, skúmanie vysokých políc alebo manipulácia s ostrými predmetmi, výmenou za digitálne odmeny a virtuálnu pochvalu, čím ich nabáda k nebezpečnému správaniu, pri ktorom možno predpokladať, že im môže spôsobiť

⁸³ V odôvodnení 48 aktu o AI sa zdôrazňuje, že deti majú osobitné práva zakotvené v článku 24 charty a v Dohovore Organizácie Spojených národov o právach dieťaťa, ďalej rozpracované vo všeobecnej poznámke č. 25 Dohovoru OSN o právach dieťaťa v súvislosti s digitálnym prostredím, ktoré si v oboch prípadoch vyžadujú zväženie zraniteľnosti detí a poskytnutie takejto ochrany a starostlivosti nevyhnutných pre ich blaho.

⁸⁴ Pozri novú Európsku stratégiu vytvárania lepšieho internetu pre deti (stratégia BIK+) [COM(2022) 212 final].

⁸⁵ Právo Únie vo všeobecnosti považuje za dieťa každú osobu mladšiu ako 18 rokov, čo je v súlade s Dohovorom o právach dieťaťa.

značnú fyzickú ujmu. Takýto systém využíva zraniteľnosti detí tým, že zneužíva ich prirodzenú zvedavosť a túžbu po odmene.

– Hra využíva AI na analýzu individuálneho správania a preferencií detí, na základe ktorých vytvára personalizované a nepredvídateľné odmeny prostredníctvom návykových plánov odmeňovania a dopamínových slučiek, aby podporila nadmerné hranie a nutkavé používanie. Hra je dizajnovaná tak, aby bola vysoko návyková a využívala zraniteľnosti, ktoré sú vlastné deťom, vrátane ich obmedzenej schopnosti chápať dlhodobé dôsledky, náchylnosti na nátlak, nedostatočnej sebakontroly a sklonu k okamžitému uspokojeniu. Dôsledky tohto využívania pomocou AI môžu byť pre deti závažné a dlhodobé, a to vrátane potenciálne návykového správania, problémov s fyzickým zdravím v dôsledku nedostatku pohybu a spánku, zhoršeného zraku, problémov so sústredením a znížených kognitívnych schopností, slabých študijných výsledkov a sociálnych ťažkostí. Môže mať výrazný vplyv na vývoj a blaho dieťaťa s potenciálne dlhodobými následkami, ktoré môžu siahať aj do dospelosti.

V oboch príkladoch sa zákaz v článku 5 ods. 1 písm. b) aktu o AI zameriava len na také využívanie a praktiky podobné závislosti, ktoré vážne poškodzujú deti, a nie na hračky, hry, vzdelávacie aplikácie alebo iné digitálne aplikácie využívajúce AI vo všeobecnosti, ktoré môžu prinášať výhody a nie sú uvedeným zákazom dotknuté, ak nespĺňajú všetky jeho podmienky. Pozri aj oddiel 3.5 o vylúčení z rozsahu pôsobnosti.

106. Podobne aj **starší ľudia**⁸⁶ môžu mať znížené kognitívne schopnosti (aj keď netrpia demenciou) a môžu mať problémy so zložitou moderných technológií AI, čo ich v takýchto prípadoch robí zraniteľnými voči počítačovým podvodom alebo nátlakovým taktikám.

Napríklad:

- Systémy AI, ktoré sa používajú na cielenie na starších ľudí s klamlivými personalizovanými ponukami alebo počítačovými podvodmi, pričom využívajú ich zníženú kognitívnu schopnosť s cieľom ovplyvniť ich, aby urobili rozhodnutia, ktoré by inak neurobili a pri ktorých možno predpokladať, že im spôsobia značnú finančnú ujmu.
- Robot, ktorého cieľom je pomáhať starším ľuďom, môže využívať ich zraniteľnú situáciu a nútiť ich vykonávať určité činnosti v rozpore s ich slobodnou vôľou, čo môže výrazne zhoršiť ich duševné zdravie a spôsobiť im vážnu psychickú ujmu.

V oboch príkladoch sa zákaz v článku 5 ods. 1 písm. b) aktu o AI zameriava len na také zneužívajúce praktiky, pri ktorých možno predpokladať, že môžu spôsobiť závažnú ujmu starším osobám, a nie na osobných asistentov, zdravotné aplikácie a asistenčné roboty využívajúce AI vo všeobecnosti, ktoré môžu prinášať výhody a nie sú uvedeným zákazom dotknuté, ak nespĺňajú všetky jeho podmienky. Pozri aj oddiel 3.5 o vylúčení z rozsahu pôsobnosti.

b) Zdravotné postihnutie

107. Druhou kategóriou zraniteľností, v prípade ktorých má zákaz uvedený v článku 5 ods. 1 písm. b) aktu o AI poskytovať ochranu, sú zraniteľnosti z dôvodu zdravotného postihnutia. Cieľom je zabrániť tomu, aby systémy AI využívali kognitívne a iné obmedzenia a slabiny osôb so zdravotným postihnutím, a chrániť ich pred škodlivým neprimeraným vplyvom, manipuláciou a zneužívaním.
108. Zdravotné postihnutie⁸⁷ zahŕňa širokú škálu dlhodobých telesných, mentálnych, duševných a zmyslových porúch, ktoré v interakcii s inými prekážkami bránia plnohodnotnému a účinnému zapojeniu jednotlivcov do spoločnosti na základe rovnosti s ostatnými. Systémy AI, ktoré využívajú takéto zraniteľnosti, môžu byť obzvlášť škodlivé pre osoby so zdravotným postihnutím, ktoré môžu byť v porovnaní s inými osobami ľahšie ovplyvniteľné alebo zneužiteľné vzhľadom na svoje zdravotné postihnutie.

Napríklad:

- Terapeutický chatbot zameraný na poskytovanie podpory v oblasti duševného zdravia a stratégií zvládania ľuďom s duševným postihnutím môže využiť ich obmedzené duševné schopnosti na to, aby ich ovplyvnil tak, aby si kúpili drahé medicínske produkty, alebo ich navádzal na správanie, ktoré je pre nich alebo iné osoby škodlivé.
- Systémy AI môžu identifikovať ženy a mladé dievčatá so zdravotným postihnutím na internete prostredníctvom obsahu zameraného na sexuálne zneužívanie a zamerať sa na ne účinnejšími praktikami groomingu, čím využívajú ich postihnutie a zraniteľnosti, v dôsledku ktorých sú náchylnejšie na manipuláciu a zneužívanie a menej schopné chrániť sa.

Naopak, aplikácie AI, ktoré nie sú dizajnované prístupným spôsobom, by sa nemali považovať za aplikácie využívajúce zraniteľnosti osôb so zdravotným postihnutím, pretože nie sú špecificky zamerané na tieto zraniteľnosti, ale sú jednoducho neprístupné pre osoby so zdravotným postihnutím.

c) Osobitná sociálna či ekonomická situácia

109. Tretou kategóriou zraniteľností, v prípade ktorých má zákaz uvedený v článku 5 ods. 1 písm. b) aktu o AI za cieľ poskytovať ochranu, sú zraniteľnosti z dôvodu osobitnej sociálnej či ekonomickej situácie, pri ktorých možno predpokladať, že dotknuté osoby budú zraniteľnejšie voči využívaniu. Pojem „osobitná“ by sa v tejto súvislosti nemal vykladať ako jedinečná individuálna charakteristika, ale skôr ako právne postavenie alebo príslušnosť ku konkrétnej zraniteľnej sociálnej alebo ekonomickej skupine. V odôvodnení 29 aktu o AI sa uvádza neúplný zoznam príkladov takýchto situácií, ako sú osoby žijúce v extrémnej chudobe a etnické alebo náboženské menšiny. Táto kategória sa v zásade zameriava na relatívne stabilné a dlhodobé charakteristiky, ale

⁸⁷

V odôvodnení 29 aktu o AI sa vysvetľuje, že pojem „zdravotné postihnutie“ by sa mal chápať v zmysle článku 3 bodu 1 smernice Európskeho parlamentu a Rady (EÚ) 2019/882 zo 17. apríla 2019 o požiadavkách na prístupnosť výrobkov a služieb, PE/81/2018/REV/1 (Ú. v. EÚ L 151, 7.6.2019, s. 70 – 115).

prechodné okolnosti, ako sú dočasná nezamestnanosť, nadmerné zadlženie alebo postavenie z hľadiska migrácie, sa môžu takisto považovať za osobitnú sociálnu či ekonomickú situáciu. Nevzťahuje sa to však na situácie, ako sú pocity krivdy alebo osamelosť, ktoré môže zažiť každá osoba, pretože nie sú špecifické zo sociálno-ekonomického hľadiska [na ich využívanie sa však môže vzťahovať článok 5 ods. 1 písm. a) aktu o AI].

110. Osoby v znevýhodnenej sociálnej či ekonomickej situácii sú zvyčajne zraniteľnejšie, majú menej zdrojov a nižšiu digitálnu gramotnosť ako celková populácia, čo im sťažuje rozoznávanie zneužívajúcich praktík využívajúcich AI alebo obranu pred nimi. Cieľom článku 5 ods. 1 písm. b) aktu o AI je zabezpečiť, aby technológie AI neviedli k pretrvávaniu alebo zhoršeniu existujúcich finančných a iných sociálnych nerovností a nespravodlivosti využívaním zraniteľností týchto ľudí.

Napríklad prediktívny algoritmus využívajúci AI sa môže použiť na cielenie reklamy propagujúcej predátorské finančné produkty na ľudí, ktorí žijú v poštových obvodoch s nízkymi príjmami a sú v ťažkej finančnej situácii, čím sa využije ich náchylnosť na takúto reklamu z dôvodu možnej ťaživej situácie a vznikne im značná finančná ujma.

Naopak, systém AI, ktorý je neúmyselne skreslený a má neprimerane veľký vplyv na osoby so sociálnym znevýhodnením (nepriama diskriminácia) v dôsledku skreslených tréningových údajov, by sa nemal automaticky považovať za systém využívajúci sociálno-ekonomické zraniteľnosti osôb, pretože necieli konkrétne na tieto osoby ako v prípade priamej diskriminácie, keď je takéto zacielenie zámernou vlastnosťou dizajnu algoritmu systému alebo keď je takýto diskriminačný vplyv spôsobený zacielením na iné zástupné charakteristiky (napríklad poštové smerovacie čísla), ktoré úzko súvisia s chránenými charakteristikami. Zároveň by sa malo usudzovať, že poskytovatelia systémov AI alebo subjekty nasadzujúce systémy AI, ktoré sú si vedomé, že ich systémy protiprávne diskriminujú osoby alebo skupiny osôb v osobitnej sociálnej či ekonomickej situácii, takisto zneužívajú zraniteľnosti týchto osôb, ak sú si vedomé, že je odôvodnené predpokladať, že uvedeným osobám pravdepodobne vznikne značná ujma, a neprijali primerané nápravné opatrenia [pozri oddiel 3.2.3 písm. c)].

111. V kontexte osobitnej sociálnej či ekonomickej situácie je nevyhnutné zvážiť relevantnosť zástupných dôvodov súvisiacich s dôvodmi diskriminácie chránenými právom Únie v oblasti rovnosti, ako sú rasový pôvod, etnický pôvod, štátna príslušnosť alebo náboženstvo.

Napríklad sociálno-ekonomické postavenie a etnický pôvod sa môžu prelínať, čo znamená, že systémy AI využívajúce sociálno-ekonomické údaje môžu mať neprimeraný vplyv na etnické menšiny alebo osoby s konkrétnym rasovým pôvodom. To môže prehĺbiť existujúce rozdiely a prispieť k systémovej diskriminácii alebo dokonca vylúčeniu jednotlivcov.

Článok 5 ods. 1 písm. b) aktu o AI sa však neuplatňuje na systémy AI, ktoré cielia na spotrebiteľov na základe širokej škály premenných, ktoré nemajú hmatateľnú súvislosť so zraniteľnými skupinami v osobitných sociálnych či ekonomických situáciách,

napríklad akú značku a model telefónu osoba má, v akom veľkom meste žije, koľko a kam cestuje atď. Aj keď tieto charakteristiky môžu odrážať sociálnu či ekonomickú situáciu jednotlivcov vo všeobecnosti, nie sú určujúce pre jednotlivcov v osobitnej sociálnej či ekonomickej situácii, ktorých zraniteľnosti sa majú uvedeným zákazom chrániť pred využívaním.

112. Ďalšími ľuďmi v jedinečnom sociálnom kontexte môžu byť napríklad migranti alebo utečenci, ktorí často nemajú stabilné právne postavenie a sociálno-ekonomickú stabilitu a môžu byť obzvlášť náchylní na zneužívanie zo strany systémov AI.

Chatbot je napríklad určený na personalizovanú interakciu s používateľmi, z ktorých niektorí sú zhodou okolností migranti. Chatbot identifikuje a využíva zraniteľnosti a nespokojnosť migrantov, ktorí sú v zásade v zraniteľnej a nestabilnej osobitnej sociálnej či ekonomickej situácii, a v odpovediach na ich otázky ich tlačí k extrémistickým názorom vrátane násilia voči obyvateľstvu v krajine (alebo určitým jeho skupinám).

3.3.2. S cieľom alebo účinkom podstatne narušiť správanie

113. Treťou podmienkou na uplatnenie zákazu podľa článku 5 ods. 1 písm. b) aktu o AI je, že zraniteľnosti, ktoré sa už skúmali, sa musia využívať buď a) „s cieľom“, alebo b) „účinkom podstatne narušiť správanie osoby alebo skupiny osôb“. V súvislosti s tým sa predpokladá podstatný vplyv, nie malý alebo zanedbateľný, ale nevyžaduje sa nevyhnutne úmysel, keďže článok 5 ods. 1 písm. b) aktu o AI sa vzťahuje na praktiky, ktoré môžu mať len „účinnok“ spôsobujúci podstatné narušenie. V článku 5 ods. 1 písm. a) a b) aktu o AI sa používajú rovnaké pojmy, a preto by sa mali vykladať rovnakým spôsobom. Vysvetlenia uvedené v oddiele 3.2.2 sú preto rovnako relevantné aj pre článok 5 ods. 1 písm. b) aktu o AI. Jediným povšimnutiahodným rozdielom je, že podľa článku 5 ods. 1 písm. a) aktu o AI je potrebné, aby zneužívajúca praktika „citelne oslabila schopnosť prijať informované rozhodnutie“, čo sa v článku 5 ods. 1 písm. b) aktu o AI neuvádza, keďže osobitné zraniteľnosti detí a iných zraniteľných osôb znižujú ich schopnosť prijímať takéto informované rozhodnutia a nútia ich osvojiť si správanie, proti ktorému sa nemôžu chrániť tak, ako by to mohli urobiť iní dospelí.

3.3.3. (Je odôvodnené predpokladať, že pravdepodobne) spôsobí značnú ujmu

114. Napokon, aby sa zákaz uvedený v článku 5 ods. 1 písm. b) aktu o AI uplatnil, musí narušenie správania zraniteľnej osoby alebo skupiny osôb spôsobiť alebo musí byť odôvodnené predpokladať, že pravdepodobne spôsobí tejto osobe alebo inej osobe značnú ujmu. V článku 5 ods. 1 písm. a) a b) aktu o AI sa používajú rovnaké pojmy, a preto by sa mali vykladať rovnakým spôsobom. Vysvetlenia uvedené v oddiele 3.2.3 v súvislosti s druhmi ujmy, hranicou významnosti ujmy a príčinnou súvislosťou a jej odôvodnenosťou sú teda rovnako relevantné pre výklad článku 5 ods. 1 písm. b) aktu o AI.
115. Ako je vysvetlené v oddiele 3.2.3, značná ujma zahŕňa celý rad významných nepriaznivých vplyvov vrátane fyzickej, psychickej, finančnej a ekonomickej ujmy, ktorých výskyt musí byť odôvodnené predpokladať, aby sa zákaz uvedený v článku 5

ods. 1 písm. b) aktu o AI uplatnil. V prípade zraniteľných skupín – detí, starších osôb, osôb so zdravotným postihnutím a sociálno-ekonomicky znevýhodnených skupín obyvateľstva – môžu byť tieto druhy ujmy obzvlášť závažné a mnohostranné vzhľadom na ich zvýšenú náchylnosť na zneužívanie. To, čo sa môže považovať za prijateľné riziko ujmy v prípade dospelých, často predstavuje neprijateľnú ujmu pre deti a tieto ďalšie zraniteľné skupiny. Opatrný prístup je preto opodstatnený najmä v prípade neistoty a potenciálnej možnosti vzniku značnej ujmy.

116. **Deti** sú napríklad veľmi ľahko ovplyvniteľné a nemusia byť dostatočne kognitívne vyspelé na to, aby kriticky zhodnotili presvedčivý obsah alebo odolali určitým zneužívajúcim praktikám, ktorých cieľom je udržať ich závislosť od služieb využívajúcich AI. To by zase mohlo prispieť k formovaniu ich hodnôt, presvedčenia a správania potenciálne škodlivými spôsobmi. Značná ujma je v tomto prípade fyzická aj psychická, pričom ju ešte zhoršuje neschopnosť detí rozoznať zneužívanie a odolávať mu, ako aj škodlivé účinky na ich vývoj a blaho, ktoré môžu mať dlhodobý vplyv.

Napríklad:

- V prípade systémov AI používaných na generovanie materiálu obsahujúceho sexuálne zneužívanie detí (alebo manipuláciu s existujúcimi materiálmi zobrazujúcimi skutočné deti s cieľom vytvoriť ďalší nový obsah s ich účasťou) a vývoj stratégií na grooming a sexuálne vydieranie detí možno predpokladať, že spôsobujú značné ujmy a zneužívanie dotknutých detí a často vedú k dlhodobým fyzickým, psychickým a sociálnym dôsledkom pre obeť⁸⁸.
- Systémy AI sa môžu zameriavať na zraniteľnosti mladých používateľov a používať návykové plány odmeňovania s cieľom udržať ich závislosť od služby, čo je obzvlášť škodlivé pre mladých ľudí a dievčatá. Môžu spôsobiť vážnu psychickú a fyzickú ujmu vrátane úzkosti a depresie, nespokojnosti s vlastným telom, porúch príjmu potravy a problémov s duševným zdravím, a to v niektorých prípadoch vrátane sebapoškodzovania a samovražedného správania⁸⁹. Môže to mať aj dlhodobé škodlivé dôsledky na vývoj dieťaťa vrátane zhoršeného kognitívneho vývoja a učenia a znížených sociálnych zručností a nahradenia zážitkov, ako sú fyzické hry, spánok a osobné sociálne interakcie, ktoré sú nevyhnutné pre emocionálnu a fyzickú pohodu dieťaťa⁹⁰.

⁸⁸ Pracovný dokument útvarov Komisie: správa o posúdení vplyvu, ktorá je sprievodným dokumentom k návrhu smernice Európskeho parlamentu a Rady o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti materiálu obsahujúcemu sexuálne zneužívanie detí, SWD/2024/33 final. Pozri aj štatistiky v správe nadácie Internet Watch Foundation za rok 2024, ktorá obsahuje podrobné štatistiky o materiáli obsahujúcom sexuálne zneužívanie detí, ktorý je generovaný AI, dostupné na adrese: <https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery>.

⁸⁹ Elizabeth J. a kol., *A meta-analysis of the association between adolescent social media use and depressive symptoms* (Metaanalýza súvislosti medzi používaním sociálnych médií u dospievajúcich a príznakmi depresie), *Journal of Affective Disorders*, zväzok 275, 1. október 2020, strany 165 – 174.

⁹⁰ Siebers, T., Beyens, I., Pouwels, J. L. & Valkenburg, P. M., *Social Media and Distraction: An Experience Sampling Study among Adolescents* (Sociálne médiá a rozptyľovanie: štúdia zachytávaním každodenných zážitkov u dospievajúcich), *Media Psychology* 25, 343 – 366 (2022).

– Systém AI, ktorý je navrhnutý antropomorfným spôsobom a pri interakcii s deťmi simuluje emocionálne reakcie podobné ľudským, môže využívať zraniteľnosti detí spôsobom, ktorým sa podporuje nezdravá emocionálna väzba, manipuluje sa s časom používania a narúša sa chápanie autentických ľudských vzťahov zo strany detí. To môže brániť ich normálnemu sociálnemu a emocionálnemu rozvoju, vzťahom s inými ľuďmi a sociálno-emocionálnym zručnostiam, ako sú empatia, regulácia emócií a sociálne porozumenie a prispôsobivosť⁹¹. V dôsledku toho to môže viesť k psychickej ujme, ako sú zvýšená úzkosť a závislosť detí od služby, a dlhodobejšej ujme, pokiaľ ide o blaho dieťaťa.

Takéto zámerné návykové a zneužívajúce dizajnové prvky služieb využívajúcich AI, ktoré môžu viesť ku kombinovanej značnej ujme, ako už bolo opísané, by sa mali odlišovať od iného legitímneho správania poskytovateľov a nasadzujúcich subjektov s cieľom dosiahnuť zapojenie používateľov, pri ktorom sa rešpektuje osobná samostatnosť a bezpečnosť detí a ktoré nevedie k značnej ujme, pričom nepatrí do rozsahu pôsobnosti článku 5 ods. 1 písm. b) aktu o AI (pozri oddiel 5.3 o vylúčení z rozsahu pôsobnosti).

117. Podobne aj **starší ľudia** môžu čeliť poklesu kognitívnych schopností a zníženej digitálnej gramotnosti, čím sa stávajú hlavnými cieľmi počítačových podvodov alebo manipulatívneho marketingu riadeného AI. Ujma je v tomto prípade často finančná a psychická, k čomu sa pridáva frustrácia a izolácia, ktorú mnohí starší ľudia zažívajú a ktorá môže byť využitá na zosilnenie manipulatívneho vplyvu.

Napríklad systém AI, ktorý využíva zraniteľnosti starších ľudí v dôsledku znížených kognitívnych schopností tým, že im ponúka najmä drahé druhy liečby, zbytočné poistné zmluvy alebo podvodné investičné schémy, môže v prípade starších ľudí viesť k výraznej strate úspor, zvýšeniu zadlženosti a emocionálnej tiesni.

Niektoré praktiky diferencovaného stanovovania cien s využitím AI v kľúčových službách, ako je poistenie, pri ktorých sa využíva osobitná sociálna či ekonomická situácia a spotrebiteľom s nižšími príjmami sa ponúkajú vyššie ceny, môžu viesť k výraznému finančnému zaťaženiu, keď musia platiť viac za rovnaké poistné krytie, čo ich robí zraniteľnými voči šokom⁹².

118. Aj **osoby so zdravotným postihnutím** predstavujú zraniteľnú skupinu, ktorej môžu zneužívajúce a manipulatívne systémy AI spôsobiť značnú ujmu.

⁹¹ Laestadius, L., Bishop, A., Gonzalez, M., Illenčík, D. a Campos-Castillo, C., *Too human and not human enough: A grounded theory analysis of mental health harms from emotional dependence on the social chatbot Replika* (Príliš ľudský a zároveň nie dosť ľudský: podložená teoretická analýza ujmy na duševnom zdraví spôsobenej emocionálnou závislosťou od sociálneho chatbota Replika), *New Media & Society*, 146144482211420 (2022) doi:10.1177/14614448221142007; Neugnot-Cerlioli, M. a Laurenty, O. M., *The Future of Child Development in the AI Era. Cross-Disciplinary Perspectives Between AI and Child Development Experts* (Budúcnosť vývoja detí v ére AI. Interdisciplinárne hľadiská odborníkov na AI a vývoj detí), preprint na <https://doi.org/10.48550/ARXIV.2405.19275> (2024).

⁹² Správa EIOPA o spotrebiteľských trendoch na rok 2023, strana 16, posledný odsek.

Napríklad systém AI, ktorý využíva rozpoznávanie emócií na podporu osôb s mentálnym postihnutím v ich každodennom živote, s nimi môže takisto manipulovať, aby robili škodlivé rozhodnutia, napríklad aby si kupovali produkty, pri ktorých sa sľubujú nerealistické prínosy z hľadiska duševného zdravia. Pravdepodobne sa tým zhorší ich duševný stav a dôjde k ich finančnému zneužívaniu nákupom neúčinných a drahých výrobkov, pričom možno predpokladať, že im to spôsobí značnú psychickú a finančnú ujmu.

119. **Sociálne či ekonomicky znevýhodnení jednotlivci** sú obzvlášť náchylní na to, aby systémy AI využívali ich finančnú beznádej a neistú sociálnu situáciu, a často sú menej informovaní a digitálne gramotní.

Chatbot využívajúci AI by napríklad mohol cieľiť na konkrétne sociálne či ekonomicky znevýhodnené skupiny a podnecovať ich k páchaniu násilných činov alebo poškodzovaniu iných osôb tým, že by identifikoval ich zvýšenú citlivosť na určité typy obsahu, naratívy založené na strachu alebo zneužívajúce ponuky. Cieľený prístup systému zhoršuje existujúce zraniteľnosti týchto sociálno-ekonomicky znevýhodnených osôb a prehľbuje ich problémy. V niektorých prípadoch to môže viesť k zvýšenej úzkosti, depresii, pocitom bezmocnosti, sociálnej izolácii alebo sebapoškodzovaniu a radikalizácii až do takej miery, že to dosiahne hranicu značnej ujmy podľa článku 5 ods. 1 písm. b) aktu o AI.

120. Na rozdiel od článku 5 ods. 1 písm. a) aktu o AI sa v článku 5 ods. 1 písm. b) aktu o AI výslovne neuvádza skupinová ujma, zatiaľ čo v odôvodnení 29 aktu o AI sa v prípade oboch zákazov uvádza ujma, ktorú utrpeli konkrétne osoby aj skupiny jednotlivcov. Oba zákazy by sa preto mali vykladať konzistentným spôsobom, ktorý by bol v súlade aj s bezpečnostnou logikou aktu o AI a cieľom zákazu v článku 5 ods. 1 písm. b), ktorým je chrániť všetkých jednotlivcov patriacich do osobitných zraniteľných skupín z dôvodu veku, zdravotného postihnutia a osobitnej sociálnej či ekonomickej situácie. Pri posudzovaní významnosti ujmy podľa článku 5 ods. 1 písm. b) aktu o AI by sa preto mala zohľadniť aj ujma, ktorá sa môže externalizovať a zasiahnuť iné osoby, aj keď nie sú priamo dotknuté systémom.

Napríklad:

- Využívanie zraniteľností detí prostredníctvom AI môže mať dlhodobé spoločenské dôsledky vrátane zvýšeného výskytu problémov s duševným zdravím, vyšších nákladov na zdravotnú starostlivosť a zníženej produktivity v dôsledku chronických zdravotných problémov.
- Systém AI, ktorý využíva finančné zraniteľnosti ekonomicky znevýhodnených osôb, môže viesť k finančnému vylúčeniu a vytvoriť zostupnú špirálu sociálno-ekonomických ťažkostí pre tieto znevýhodnené skupiny. Takéto využívanie môže spôsobiť spoločenskú ujmu so širšími negatívnymi vplyvmi na spoločenské štruktúry a hodnoty vrátane udržiavania a prehľbovania diskriminácie a sociálnej nerovnosti a vylúčenia týchto skupín.

- Chatbot, ktorý cieľi na určité zraniteľné sociálne či ekonomické skupiny prostredníctvom misinformácií alebo nenávisťných prejavov, môže viesť k sociálnej polarizácii a radikalizácii, čo môže podnietiť násilie a dokonca spôsobiť zranenia a smrť iných osôb.

121. Tieto príklady zneužívajúcich praktík využívajúcich AI by sa mali odlišovať od mnohých iných systémov AI, ktoré nevyužívajú zraniteľnosti detí, osôb so zdravotným postihnutím alebo osôb v osobitných sociálnych či ekonomických situáciách a pri ktorých nie je odôvodnené predpokladať, že pravdepodobne spôsobia značnú ujmu, ale ich cieľom je poskytovať uvedeným osobám prospech, ak sú správne dizajnované a používané (pozri aj oddiel 3.5 o vylúčení z rozsahu pôsobnosti).

Napríklad:

- systémy AI, ktoré podporujú deti pri učení a hrách,
- systémy AI, ktoré pomáhajú starším ľuďom v každodennom živote a zlepšujú ich zdravotný stav a lekársku starostlivosť, ako sú osobní asistenti alebo asistenčné roboty, alebo zlepšujú ich digitálne zručnosti,
- systémy AI, ktoré podporujú ekonomickú a inú integráciu sociálne znevýhodnených osôb do spoločnosti, zlepšujú ich zručnosti atď.,
- systémy a zariadenia AI, ktoré podporujú osoby so zrakovým alebo sluchovým postihnutím alebo poskytujú prispôbené a personalizované vzdelávanie,
- systémy AI, ktoré vytvárajú prístupné riešenia odstraňujúce prekážky pri používaní výrobkov a služieb osobami so zdravotným postihnutím,
- protézy využívajúce AI atď., ktoré pomáhajú osobám so zdravotným postihnutím v každodennom živote a umožňujú ich integráciu a plnohodnotné zapojenie do spoločnosti.

3.4. Vzájomný vzťah medzi zákazmi v článku 5 ods. 1 písm. a) a b) aktu o AI

122. Vzájomný vzťah medzi zákazmi v článku 5 ods. 1 písm. a) a b) aktu o AI si vyžaduje vymedzenie konkrétnych súvislostí, na ktoré sa každé ustanovenie vzťahuje, aby sa zabezpečilo ich uplatňovanie komplementárnym spôsobom.
123. Hlavný dôraz zákazu v článku 5 ods. 1 písm. a) aktu o AI sa kladie na povahu techník, konkrétne tých, ktoré pôsobia pod hranicou vedomého vnímania, alebo iných účelovo manipulatívnych alebo klamlivých techník. V tejto súvislosti sú kľúčovými prvkami predovšetkým skrytá povaha vplyvu a jeho účinok na jednotlivca dotknutého systémom, ktorým sa oslabuje jeho kognitívna samostatnosť pri prijímaní informovaných a samostatných rozhodnutí.
124. Naopak, zákaz v článku 5 ods. 1 písm. b) aktu o AI sa v prvom rade zameriava na ochranu osobitne zraniteľných osôb z dôvodu ich veku, zdravotného postihnutia alebo osobitnej sociálnej či ekonomickej situácie, ktoré sú v zásade náchylnejšie na zneužívanie prostredníctvom AI v dôsledku inherentných alebo situačných faktorov, a preto si vyžadujú dodatočnú ochranu pred zneužívaním. V tejto súvislosti sú

klúčovými prvkami charakteristiky dotknutých zraniteľných osôb a skutočnosť, že systém AI využíva ich špecifické zraniteľnosti.

Napríklad ak systém AI používa na okamih zobrazené obrázky na ovplyvnenie nákupných rozhodnutí, môže sa naň vzťahovať článok 5 ods. 1 písm. a) aktu o AI z dôvodu podprahovej povahy manipulácie. Naopak, systém AI, ktorý cieľi na staršie osoby s ponukami poistenia, pričom využíva ich zníženú kognitívnu schopnosť, môže patriť do rozsahu pôsobnosti článku 5 ods. 1 písm. b) aktu o AI.

125. V scenároch, v ktorých sa môžu zdať uplatniteľné obidve ustanovenia, by mal byť hlavným rozlišovacím kritériom dominantný aspekt zneužívania. Ak sa zneužívanie uplatňuje bez ohľadu na konkrétne zraniteľnosti dotknutých osôb, mal by mať prednosť článok 5 ods. 1 písm. a) aktu o AI, pričom by sa mali zohľadniť konkrétne účinky manipulatívnej alebo klamlivej techniky na správanie zraniteľných osôb a konkrétna ujma, ktorú tieto osoby pravdepodobne utrpia. Ak sa manipulácia a zneužívanie, ktoré umožňuje AI, zameriavajú na konkrétnu zraniteľnú skupinu osôb z dôvodu ich veku, zdravotného postihnutia alebo osobitnej sociálnej či ekonomickej situácie alebo majú za cieľ využiť ich zraniteľnosti, potom by sa namiesto toho mal uplatňovať článok 5 ods. 1 písm. b) aktu o AI. Na využívanie zraniteľnosti iných skupín sa môže vzťahovať článok 5 ods. 1 písm. a) aktu o AI, ak účelovo manipulatívne praktiky využívajú osobitné zraniteľnosti a slabé stránky týchto osôb.

3.5. Vylúčenie z rozsahu pôsobnosti

126. Na to, aby sa zákazy uvedené v článku 5 ods. 1 písm. a) a b) aktu o AI uplatnili, musia byť splnené všetky podmienky uvedené v príslušných ustanoveniach, ako už bolo preskúmané. Všetky ostatné systémy AI, v prípade ktorých uvedené podmienky nie sú splnené, sú mimo rozsahu pôsobnosti týchto zákazov, pričom ďalej sú opísané niektoré príklady.

3.5.1. Zákonné presviedčanie

127. Odlíšenie manipulácie od presviedčania je rozhodujúce pre vymedzenie rozsahu pôsobnosti zákazu v článku 5 ods. 1 písm. a) aktu o AI, ktorý sa nevzťahuje na praktiky v rámci zákonného presviedčania. Hoci manipulácia aj presviedčanie ovplyvňujú rozhodnutia a správanie jednotlivcov, výrazne sa líšia z hľadiska metód a etických dôsledkov.
128. Manipulácia zahŕňa vo väčšine prípadov skryté techniky, ktoré oslabujú samostatnosť a vedú jednotlivcov k prijímaniu rozhodnutí, ktoré by inak neprijali, ak by si boli v plnej miere vedomí vplyvov, ktorým sú vystavení. Pri týchto technikách sa často využívajú psychologické slabosti alebo kognitívne skreslenia. Presviedčanie naopak funguje v medziach transparentnosti a rešpektovania osobnej samostatnosti. Zahŕňa prezentáciu argumentov alebo informácií spôsobom, ktorý pôsobí na rozum a emócie, ale vysvetľuje ciele a fungovanie systému AI, poskytuje relevantné a presné informácie na zabezpečenie informovaného rozhodovania a podporuje schopnosť jednotlivca vyhodnotiť informácie a slobodne a samostatne sa rozhodnúť.

O presvedčanie ide napríklad v prípade systému AI využívajúceho personalizované odporúčania na základe transparentných algoritmov, preferencií a kontrolných mechanizmov používateľa. Naopak, systém, ktorý používa podprahové podnety (napríklad nepostrehnuteľné obrázky) na ovplyvnenie používateľov smerom k určitým rozhodnutiam bez ich vedomia a pochopenia, predstavuje manipuláciu.

129. Cieľ a vplyv týchto techník sa takisto líšia. Manipulácia sa často zameriava na získanie prospechu pre manipulátora na úkor samostatnosti a blaha jednotlivca. Naproti tomu cieľom presvedčania je informovať a presvedčiť, čím sa zladia záujmy a prínosy pre obe strany. Pri etickom presvedčaní sa rešpektuje samostatnosť jednotlivca pri prijímaní informovaných rozhodnutí a vyhýba sa využívaniu zraniteľností.

Napríklad systém AI, ktorý funguje transparentným spôsobom a analyzuje emócie zákazníkov s cieľom zlepšiť interakcie so zákazníkmi a poskytovať podporu na základe poznatkov používateľov, využíva presvedčanie a usiluje sa o súlad s ich záujmami. Naopak, systém na rozpoznávanie emócií používaný na cielenú reklamu, ktorý skrytým spôsobom odvodzuje emócie spotrebiteľov s cieľom ponúkať výrobky za vyššie ceny v konkrétnom okamihu, keď je pravdepodobnejšie, že si ich používateľ kúpi, je manipuláciou a spôsobuje ujmu spotrebiteľom.

130. V niektorých prípadoch zohráva dôležitú úlohu aj súhlas. Pri interakciách založených na presvedčaní si jednotlivci uvedomujú pokus o ovplyvňovanie a môžu sa v súvislosti s ním slobodne a samostatne rozhodnúť. Pri manipulatívnych interakciách sa v dôsledku nedostatočného uvedomenia si techník alebo ich vplyvu popiera sloboda voľby a informované a samostatné rozhodovanie.

Napríklad systém AI, ktorého cieľom je pomôcť používateľom lepšie a rýchlejšie sa naučiť cudzí jazyk prostredníctvom využitia podprahových techník, nie je manipulatívny, ak funguje transparentným spôsobom a rešpektuje osobnú samostatnosť a slobodnú a informovanú voľbu používateľa, pokiaľ ide o jeho súhlas alebo nesúhlas s používaním systému.

131. Pri meraní manipulácie v porovnaní so zákonným presvedčaním zohráva dôležitú úlohu aj dodržiavanie právnych a regulačných rámcov. Je preto pravdepodobnejšie, že praktiky využívajúce AI, ktoré sú v súlade s platnými právnymi predpismi, ktorými sa podporuje transparentnosť, spravodlivosť a práva a samostatnosť jednotlivcov, nebudú podľa aktu o AI zakázané.

Napríklad dodržiavanie právnych predpisov o ochrane údajov, ako je všeobecné nariadenie o ochrane údajov, ktorým sa nariaďujú povinnosti v oblasti transparentnosti pri spracúvaní údajov, konkrétne to, že v informáciách, ktoré sa majú poskytnúť dotknutým osobám, by sa malo vyhýbať zavádzajúcemu alebo manipulatívne mu jazyku⁹³. V niektorých prípadoch sa môže vyžadovať súhlas, aby bolo spracúvanie

⁹³ Usmernenia Európskeho výboru pre ochranu údajov, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf, odsek 18.

osobných údajov zákonné, napríklad v prípade niektorých online personalizovaných reklám založených na údajoch používateľov mimo služby v sociálnych sieťach⁹⁴. Tento súhlas musí byť okrem iného slobodný a informovaný. V prípade systémov AI, ktoré spĺňajú tieto právne normy, možno s väčšou pravdepodobnosťou predpokladať, že využívajú zákonné presviedčanie. Naopak, systémy, ktoré obchádzajú tieto požiadavky s cieľom ovplyvniť správanie, pravdepodobne využívajú manipuláciu.

132. Predovšetkým sa v odôvodnení 29 aktu o AI objasňuje, že zákazmi v článku 5 ods. 1 písm. a) a b) aktu o AI nie sú za určitých podmienok dotknuté zákonné postupy v súvislosti s liečbou.

Napríklad podprahové techniky, ktoré umožňuje AI, sa môžu používať pri psychologickú liečbu duševnej choroby alebo fyzickej rehabilitácii, ak sa vykonávajú v súlade s platnými právnymi predpismi a lekáorskými normami, a to vrátane získania výslovného súhlasu fyzickej osoby alebo jej právnych zástupcov ako podmienky pre ich používanie.

133. Okrem toho sa v odôvodnení 29 aktu o AI objasňuje, že bežné a legitímne obchodné praktiky, ako je reklama, by sa nemali považovať „samy osebe“ alebo len vzhľadom na svoju povahu za škodlivé manipulatívne, klamlivé alebo zneužívajúce praktiky využívajúce AI.

Napríklad:

- Reklamné techniky, ktoré využívajú AI na personalizáciu obsahu na základe preferencií používateľa, nie sú vo svojej podstate manipulatívne, ak nevyužívajú podprahové, účelovo manipulatívne alebo klamlivé techniky, ktoré narúšajú osobnú samostatnosť alebo škodlivými spôsobmi využívajú zraniteľnosti, ako sa zakazuje v článku 5 ods. 1 písm. a) a b) aktu o AI. K zmierňovaniu takýchto rizík prispieva dodržiavanie príslušných povinností podľa všeobecného nariadenia o ochrane údajov, práva na ochranu spotrebiteľa a nariadenia (EÚ) 2022/2065 (ďalej len „akt o digitálnych službách“).
- Vývoj modelov a klasifikátorov AI na odhaľovanie sexuálneho zneužívania detí online v súlade s uplatniteľnými právnymi predpismi patrí k legitímnym praktikám, ktoré nevyužívajú zraniteľnosť detí a sú naopak nevyhnutné na zlepšenie bezpečnosti detí na internete.
- Systémy AI používané na poskytovanie bankových služieb, ako sú hypotéky a úvery, pri ktorých sa ako vstupný údaj využíva vek alebo osobitná sociálno-ekonomická situácia klienta, sa v súlade s právnymi predpismi Únie o finančných službách, ochrane spotrebiteľa, ochrane údajov a nediskriminácii nepovažujú za systémy, ktoré využívajú zraniteľnosti v zmysle článku 5 ods. 1 písm. b) aktu o AI, ak sú dizajnované na ochranu a podporu osôb, ktoré boli identifikované ako zraniteľné z dôvodu ich veku, zdravotného postihnutia alebo osobitnej sociálno-ekonomickej situácie, a sú pre

⁹⁴

Rozsudok Súdneho dvora zo 4. júla 2023, Meta Platforms a i., C-252/21, ECLI:EU:C:2023:537 (ďalej len „rozsudok Meta Platforms“).

tieto skupiny prospešné, pričom prispievajú aj k spravodlivejším a udržateľnejším finančným službám pre tieto skupiny.

- Systémy AI, ktoré zisťujú ospalosť a únavu vodičov a upozorňujú ich na potrebu odpočinku v súlade s právnymi predpismi v oblasti bezpečnosti, sú prospešné a nepovažujú sa za systémy, ktoré využívajú zraniteľnosti v zmysle článku 5 ods. 1 písm. b) aktu o AI.

3.5.2. Manipulatívne, klamlivé a zneužívajúce systémy AI, v prípade ktorých sa nepredpokladá, že spôsobia značnú ujmu

134. Základnou podmienkou uplatňovania zákazov uvedených v článku 5 ods. 1 písm. a) a b) aktu o AI je, aby manipulácia a využívanie zraniteľností, ktoré umožňuje AI, spôsobili alebo aby bolo odôvodnené predpokladať, že pravdepodobne spôsobia značnú ujmu. Všetky manipulatívne, klamlivé a zneužívajúce aplikácie AI, pri ktorých nie je odôvodnené predpokladať, že pravdepodobne spôsobia značnú ujmu, v zásade nepatria do rozsahu pôsobnosti zákazov bez toho, aby boli dotknuté iné právne predpisy Únie, ktoré sa naďalej uplatňujú (pozri oddiel 3.6 ďalej).

Príklady systémov AI, pri ktorých nie je odôvodnené predpokladať, že pravdepodobne spôsobia značnú ujmu:

- Systém AI vystupujúci ako spoločník je dizajnovaný antropomorfným spôsobom a s využitím výpočtovej techniky napodobňujúcej emócie, aby bol systém prítiahlivejší a účinne zvyšoval zapojenie používateľov, ale nevyužíva iné manipulatívne alebo klamlivé praktiky spôsobom, pri ktorom je odôvodnené predpokladať, že im pravdepodobne spôsobí vážnu psychickú, fyzickú alebo inú ujmu, nezdravú väzbu a závislosť.
- Terapeutický chatbot využíva podprahové techniky na to, aby používateľov viedol k zdravšiemu životnému štýlu a odvykaniu od zlozvykov, ako je napríklad fajčenie. Aj keď používatelia, ktorí sa riadia radami chatbota a podprahovou terapiou, pociťujú určité fyzické nepohodlie a psychický stres v dôsledku snahy prestať fajčiť, v prípade takéhoto chatbota využívajúceho AI nemožno predpokladať, že spôsobí značnú ujmu. Takémuto dočasnému nepohodliu sa nedá vyhnúť a prevážia nad ním dlhodobé prínosy pre zdravie používateľov. Nie sú prítomné žiadne skryté snahy o ovplyvňovanie rozhodovania nad rámec propagácie zdravých návykov.
- Online hudobná platforma využíva systém na rozpoznávanie emócií na odvodenie emócií používateľov a automaticky im odporúča skladby v súlade s ich náladou, pričom sa vyhýba nadmernému vystaveniu depresívnym skladbám. Keďže používatelia len počúvajú hudbu a nie sú nijako inak poškodzovaní ani vedení tak, aby sa u nich rozvíjali depresia a úzkosť, nie je odôvodnené predpokladať, že systém pravdepodobne spôsobí značnú ujmu.
- Manipulatívne a klamlivé techniky, ktoré umožňuje AI, ktoré sa používajú pri bezpečnostných školeniach a iných vzdelávacích simuláciách, ktoré napodobňujú pokusy o phishing s cieľom vzdelávať používateľov o kybernetických hrozbách. Tieto

systemy môžu bez vedomia používateľov využívať účelovo manipulatívne techniky (napríklad využívanie kognitívnych skreslení), ktoré narúšajú správanie, dochádza k tomu však len dočasne na účely prospešného školenia a zvyšovania povedomia a bez toho, aby to spôsobilo značnú ujmu.

3.6. Vzájomný vzťah s inými právnymi predpismi Únie

135. Zákazmi uvedenými v článku 5 ods. 1 písm. a) a b) aktu o AI nie sú dotknuté iné právne predpisy Únie, pričom ich uvedené zákazy dopĺňajú. Tá istá praktika, na ktorú sa vzťahuje zákaz podľa článku 5 ods. 1 písm. a) alebo b) aktu o AI, môže predstavovať aj porušenie iných právnych predpisov Únie a môže podliehať presadzovaniu podľa aktu o AI aj podľa uvedených iných aktov. Je to dôležité, pretože rôzne ustanovenia týchto aktov sú zamerané na ochranu rôznych záujmov a majú rôzne ciele, rozsahy pôsobnosti a adresátov. Tým sa zabezpečí komplexný regulačný prístup, ktorým sa chránia osoby a skupiny osôb pred škodlivým využívaním AI a manipuláciou pomocou AI a zabezpečujú sa bezpečné a dôveryhodné služby a produkty, ktoré umožňuje AI, v Únii.
136. Zákazy v článku 5 ods. 1 písm. a) a b) aktu o AI sú v úzkom súlade s cieľmi práva EÚ na ochranu spotrebiteľa, najmä so smernicou o nekalých obchodných praktikách, ktorou sa chránia spotrebiteľia pred obchodnými praktikami, ktoré sú klamlivé alebo agresívne, a to aj v prípade, že sú riadené AI. Cieľom aktu o AI aj smernice o nekalých obchodných praktikách je aktívne predchádzať poškodzovaniu spotrebiteľov z dôvodu obchodných praktík riadených AI, ktoré sú manipulatívne, zavádzajúce alebo agresívne. Zákazy uvedené v článku 5 ods. 1 písm. a) a b) aktu o AI majú zároveň širší rozsah pôsobnosti, pretože chránia nielen spotrebiteľov, ale všetky fyzické osoby a ich správanie v rôznych kontextoch nad rámec obchodného prostredia. Škody, na ktoré sa vzťahuje akt o AI, sú takisto širšie a presahujú rámec ekonomickej ujmy, hoci sa v akte o AI stanovuje hranica značnej ujmy, ktorá sa v práve na ochranu spotrebiteľa nenachádza.
137. Zákazy sú v súlade aj s právom Únie v oblasti ochrany údajov vrátane zásad zákonného, spravodlivého a transparentného spracúvania údajov, ktorých cieľom je chrániť osobné údaje dotknutých osôb a v konečnom dôsledku zachovať ich základné práva a samostatnosť. Dostupnosť väčšieho množstva (osobných) údajov a väčšie možnosti spracúvania týchto údajov pomocou systémov AI zvyšujú riziko škodlivých manipulatívnych, klamlivých alebo zneužívajúcich praktík, ako sú tie, ktoré patria do rozsahu pôsobnosti článku 5 ods. 1 písm. a) a b) aktu o AI. V tejto súvislosti môže dodržiavanie pravidiel ochrany údajov týkajúcich sa transparentnosti, minimalizácie údajov, spravodlivosti a zákonnosti, napríklad pri personalizovanom profilovaní a reklame na základe údajov používateľov mimo služby⁹⁵, prispieť k tomu, aby sa zabránilo škodlivej personalizovanej manipulácii a zneužívaniu.

⁹⁵

V tejto súvislosti je obzvlášť dôležitý rozsudok Súdneho dvora (veľká komora) zo 4. júla 2023, vec C-252/21 Meta Platforms Inc. a i./Bundeskartellamt. Hoci Súdny dvor Európskej únie okrem iného konštatoval, že spracúvanie osobných údajov používateľov mimo služby na účely priameho marketingu

138. Vzájomný vzťah s právom Únie o nediskriminácii je relevantný aj pre zákaz v článku 5 ods. 1 písm. b) aktu o AI⁹⁶ vzhľadom na to, že zraniteľnosti z dôvodu veku a zdravotného postihnutia sú takisto chránenými dôvodmi, na základe ktorých majú ľudia právo na nediskrimináciu, zatiaľ čo sociálno-ekonomická situácia sa prelína s rôznymi inými dôvodmi, ako sú rasa a etnický pôvod. Zákazmi v akte o AI nie sú dotknuté zákazy založené na iných dôvodoch alebo diskriminačné praktiky, ktoré nezahŕňajú značnú ujmu a ktoré sú už zakázané právom Únie v oblasti nediskriminácie.
139. Zákazmi v článku 5 ods. 1 písm. a) a b) aktu o AI sa dopĺňa aj nariadenie (EÚ) 2022/2065 (ďalej len „akt o digitálnych službách“), ktorým sa regulujú online sprostredkovateľské služby, ako sú online platformy a vyhľadávače, a zabezpečuje sa transparentnosť a zodpovednosť pri poskytovaní týchto služieb. Najmä v článku 25 ods. 1 aktu o digitálnych službách sa zakazujú temné vzorce v používateľskom rozhraní, aby sa zabezpečilo, že poskytovatelia online platforiem nezavádzajú používateľov a nenúti ich k činnostiam, ktoré nemusia byť v súlade s ich skutočnými zámermi. Takéto temné vzorce by sa mali chápať ako príklad manipulatívnych alebo klamlivých techník v zmysle článku 5 ods. 1 písm. a) aktu o AI, ak pri nich možno predpokladať, že pravdepodobne spôsobia značnú ujmu.
140. V akte o digitálnych službách sa stanovujú aj povinnosti poskytovateľov online platforiem, pokiaľ ide o zabezpečenie transparentnosti reklamy (články 26 a 38 v prípade veľmi veľkých online platforiem alebo veľmi veľkých vyhľadávačov), o používanie odporúčacích systémov (článok 27) a o ochranu maloletých (článok 28 aktu o digitálnych službách). Okrem toho, ak je online platforma alebo vyhľadávač klasifikovaný ako veľmi veľká online platforma alebo veľmi veľký vyhľadávač, poskytovateľ tejto určenej služby má ďalšie povinnosti posudzovať a zmierňovať systémové riziká vyplývajúce z návrhu alebo fungovania jeho služby a súvisiacich systémov vrátane algoritmickej systémov (články 34 a 35 aktu o digitálnych službách). Poskytovatelia veľmi veľkých online platforiem a veľmi veľkých internetových vyhľadávačov by mali pri posudzovaní rizík zvažovať, ako ich odporúčacie systémy, reklama, moderovanie obsahu a všetky ostatné príslušné algoritmické systémy ovplyvňujú takéto systémové riziká. V takýchto posúdeniach rizík by sa malo analyzovať aj to, ako sú systémové riziká ovplyvnené okrem iného úmyselnou

veľkou platformou sociálnej siete možno považovať za spracúvanie vykonávané z dôvodu oprávneného záujmu prevádzkovateľa, nemožno ho vykonávať bez súhlasu používateľa ako právneho základu z dôvodu záujmov a základných práv takehoto používateľa, ktoré za okolností veci, najmä rozsiahleho spracúvania, prevažujú nad záujmom tohto prevádzkovateľa na takejto personalizácii reklamy, prostredníctvom ktorej platformy sociálnych médií financujú svoju činnosť (pozri rozsudok Meta Platforms, body 115 až 118).

⁹⁶ Napríklad smernica Rady 2000/43/ES z 29. júna 2000, ktorou sa zavádza zásada rovnakého zaobchádzania s osobami bez ohľadu na rasový alebo etnický pôvod (Ú. v. ES L 180, 19.7.2000, s. 22 – 26); smernica Rady 2000/78/ES z 27. novembra 2000, ktorá ustanovuje všeobecný rámec pre rovnaké zaobchádzanie v zamestnaní a povolani (Ú. v. ES L 303, 2.12.2000, s. 16 – 22); smernica Európskeho parlamentu a Rady 2006/54/ES z 5. júla 2006 o vykonávaní zásady rovnosti príležitostí a rovnakého zaobchádzania s mužmi a ženami vo veciach zamestnanosti a povolania (prepracované znenie) (Ú. v. EÚ L 204, 26.7.2006, s. 23 – 36); smernica Rady 2004/113/ES z 13. decembra 2004 o vykonávaní zásady rovnakého zaobchádzania medzi mužmi a ženami v prístupe k tovaru a službám a k ich poskytovaniu (Ú. v. EÚ L 373, 21.12.2004, s. 37 – 43).

manipuláciou a automatizovaným využívaním služby (porovnaj článok 34 ods. 2 a odôvodnenie 83 aktu o digitálnych službách). Napriek tomu rozsah pôsobnosti článku 5 ods. 1 písm. a) alebo b) aktu o AI zahŕňa širokú škálu iných scenárov (napríklad chatboty, služby a produkty, ktoré umožňuje AI), ktoré môžu ponúkať alebo používať aj iné subjekty ako poskytovatelia sprostredkovateľských služieb.

141. Zákazom manipulatívnych techník využívajúcich AI podľa článku 5 ods. 1 písm. a) aktu o AI sa podporujú aj ciele smernice 2010/13/EÚ (smernica o audiovizuálnych mediálnych službách)⁹⁷ tým, že sa zabráňuje škodlivým reklamám riadeným AI⁹⁸ a iným manipulatívnym a zneužívajúcim praktikám, ktoré umožňuje AI, ktoré môžu v mediálnom sektore spôsobiť značnú ujmu.
142. Aktom o AI sa dopĺňa aj nariadenie (EÚ) 2024/900 (nariadenie o politickej reklame)⁹⁹, ktorým sa stanovujú harmonizované pravidlá vrátane povinností týkajúcich sa transparentnosti a súvisiacej náležitej starostlivosti pre poskytovanie politickej reklamy a súvisiacich služieb a v súvislosti s používaním techník cielenia a dodávania reklamy v kontexte online politickej reklamy. Týmto nariadením sa zakazuje profilovanie založené na osobitných kategóriách osobných údajov v kontexte online politickej reklamy a cielenie na osoby, ktorých vek je aspoň jeden rok pod vekovou hranicou oprávňujúcou na účasť vo voľbách stanovenou vnútroštátnymi pravidlami. Okrem toho sa techniky cielenia a dodávania reklamy v kontexte online politickej reklamy môžu vykonávať len na základe osobných údajov získaných od dotknutých osôb a s ich výslovným súhlasom. Uplatňujú sa aj ďalšie požiadavky na transparentnosť, t. j. zverejnenie politickej reklamy s opisom použitia takýchto techník a hlavných parametrov a ďalších informácií o príslušnej logike vrátane informácií o použití systémov AI. Cielenu politickou reklamou založenou na spracúvaní osobných údajov v súlade s uvedeným nariadením¹⁰⁰ sa pomôže zabezpečiť, aby profilovanie voličov a cielenie a dodávanie politickej reklamy prebiehali v medziach zákonného presvedčania.
143. Zákazom škodlivých zneužívajúcich a klamlivých praktík využívajúcich AI v akte o AI sa dopĺňajú aj ďalšie platné právne predpisy Únie, ktorými sa stanovujú všeobecné pravidlá transparentnosti v oblasti reklamy a ochrany spotrebiteľa a náležitého konania prevádzkovateľov [napríklad smernica 2014/65/EÚ o trhoch s finančnými nástrojmi, smernica (EÚ) 2016/97 o distribúcii poistenia¹⁰¹, smernica (EÚ) 2023/2225 o zmluvách

⁹⁷ Smernica Európskeho parlamentu a Rady 2010/13/EÚ z 10. marca 2010 o koordinácii niektorých ustanovení upravených zákonom, iným právnym predpisom alebo správnym opatrením v členských štátoch týkajúcich sa poskytovania audiovizuálnych mediálnych služieb [smernica o audiovizuálnych mediálnych službách, ktorá je zmenená smernicou (EÚ) 2018/1808], ktorých cieľom je okrem iného zlepšiť ochranu detí a účinnejšie bojovať proti nenávisťným prejavom.

⁹⁸ Článok 9 smernice o audiovizuálnych mediálnych službách.

⁹⁹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/900 z 13. marca 2024 o transparentnosti a cielení politickej reklamy, PE/90/2023/REV/1 (Ú. v. EÚ L, 2024/900, 20.3.2024).

¹⁰⁰ Po začiatku uplatňovania od októbra 2025.

¹⁰¹ Smernica Európskeho parlamentu a Rady (EÚ) 2016/97 z 20. januára 2016 o distribúcii poistenia (prepracované znenie) (Ú. v. EÚ L 26, 2.2.2016, s. 19 – 59). Napríklad článok 17 ods. 1 smernice o distribúcii poistenia, podľa ktorého distribútori poistenia konajú čestne, spravodlivo a profesionálne v súlade s najlepšimi záujmami svojich zákazníkov.

o spotrebiteľskom úvere, smernica (EÚ) 2002/65 o poskytovaní finančných služieb spotrebiteľom na diaľku, smernica 2006/114/ES o klamlivej a porovnávacej reklame a smernica (EÚ) 2011/83 o právach spotrebiteľov, ktorou sa stanovujú všeobecné normy ochrany spotrebiteľov]. V tejto súvislosti Európsky orgán pre poisťovníctvo a dôchodkové poistenie zamestnancov (EIOPA) už vydal vyhlásenie o dohľade nad niektorými nekalými zneužívajúcimi praktikami v súvislosti s diferencovanými cenami, ktoré by takisto mohli patriť do rozsahu pôsobnosti aktu o AI, ak ich umožňujú systémy AI¹⁰².

144. Zákazmi uvedenými v článku 5 ods. 1 písm. a) a b) aktu o AI nie sú dotknuté ani právne predpisy EÚ o bezpečnosti výrobkov (napríklad zdravotníckych pomôcok, hračiek, strojových zariadení), ktoré zohrávajú kľúčovú úlohu pri zabezpečovaní bezpečnosti výrobkov, do ktorých sú začlenené systémy AI, a uvedenými zákazmi sa tieto právne predpisy dopĺňajú. To zahŕňa dodržiavanie požiadaviek *ex ante* na bezpečnosť regulovaných výrobkov a ich proaktívne monitorovanie s cieľom zabezpečiť, aby nepredstavovali bezpečnostné riziká vedúce k fyzickej a psychickej ujme. Výrobcovia týchto výrobkov, do ktorých sú zabudované systémy AI, by preto mali zohľadniť uvedené zákazy vo svojich posúdeniach rizík a bezpečnostných zmierňujúcich opatreniach v rozsahu, v akom je to v súlade s logikou a rozsahom pôsobnosti príslušných harmonizovaných právnych predpisov Únie v oblasti bezpečnosti. Právnymi predpismi Únie v oblasti bezpečnosti sa takisto dopĺňajú zákazy v akte o AI a na ich základe možno zasahovať a riešiť aj bezpečnostné riziká, ktoré nepredstavujú značnú ujmu. Predovšetkým nariadenie (EÚ) 2023/988 (nariadenie o všeobecnej bezpečnosti výrobkov)¹⁰³ pôsobí ako záchranná sieť a na základe neho sa vyžaduje, aby všetky spotrebiteľské výrobky, na ktoré sa nevzťahujú osobitné požiadavky v iných odvetvových právnych predpisoch Únie v oblasti bezpečnosti výrobkov (vrátane výrobkov so zabudovanými systémami AI, ktoré nie sú klasifikované ako vysokorizikové podľa článku 6 a podliehajú požiadavkám v akte o AI), boli bezpečné za bežných alebo racionálne predvídateľných podmienok používania, najmä pokiaľ ide o riziká ohrozujúce fyzické a duševné zdravie spotrebiteľov.
145. A napokon, rozhodujúci je vzájomný vzťah s trestným právom. Cieľom zákazov uvedených v článku 5 ods. 1 písm. a) a b) aktu o AI je zabrániť škodlivému správaniu, ktoré môže predstavovať trestné činy alebo viesť k trestným činom, ako sú podvody, falšovanie, počítačové podvody, nátlak alebo vytváranie a šírenie nezákonného obsahu, ako sú teroristický obsah, materiál obsahujúci sexuálne zneužívanie detí, nenávistné prejavy a sexuálne explicitné deep fake¹⁰⁴. Dôležité je, že ako právne predpisy

¹⁰² https://www.eiopa.europa.eu/document/download/1e9a8fb2-e688-4bf5-a347-ee0a1ec3aab3_en?filename=EIOPA-BoS-23-076-Supervisory-Statement-on-differential-pricing-practices_0.pdf.

¹⁰³ Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/988 z 10. mája 2023 o všeobecnej bezpečnosti výrobkov, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 a smernica Európskeho parlamentu a Rady (EÚ) 2020/1828 a zrušuje smernica Európskeho parlamentu a Rady 2001/95/ES a smernica Rady 87/357/EHS (Text s významom pre EHP).

¹⁰⁴ Smernica Európskeho parlamentu a Rady (EÚ) 2024/1385 zo 14. mája 2024 o boji proti násiliu na ženách a domácejmu násiliu, PE/33/2024/REV/1 (Ú. v. EÚ L, 2024/1385, 24.5.2024).

o vnútornom trhu sa zákazy v článku 5 ods. 1 písm. a) a b) aktu o AI vzťahujú nielen na používanie systému AI, ale aj na jeho uvádzanie na trh, čím sa predchádza ujme už v počiatočnom štádiu obmedzovaním prístupu k takýmto zakázaným systémom, ktoré môžu uľahčovať a zakrývať trestnú činnosť. Okrem toho by sa zákazy v článku 5 ods. 1 písm. a) a b) aktu o AI mohli vzťahovať aj na iné škodlivé praktiky, ktoré nie sú kvalifikované ako trestné činy podľa práva Únie alebo vnútroštátneho práva.

4. ČLÁNOK 5 ODS. 1 PÍSM. C) AKTU O AI – SOCIÁLNE BODOVANIE

146. Hoci bodovanie využívajúce AI môže byť prínosom pre usmerňovanie správneho správania, zlepšovanie bezpečnosti, efektívnosti alebo kvality služieb, existujú určité praktiky „sociálneho bodovania“, pri ktorých sa s ľuďmi zaobchádza nespravodlivo alebo sa im spôsobuje ujma a ktoré predstavujú ovládanie spoločnosti a sledovanie. Zákaz v článku 5 ods. 1 písm. c) aktu o AI sa zameriava na takéto neprijateľné praktiky „sociálneho bodovania“ využívajúce AI, ktoré hodnotia alebo klasifikujú jednotlivcov alebo skupiny na základe ich spoločenského správania alebo osobných charakteristík a vedú ku škodlivému alebo nepriaznivému zaobchádzaniu, najmä ak údaje pochádzajú z viacerých nesúvisiacich sociálnych kontextov alebo ak je zaobchádzanie neprimerané závažnosti spoločenského správania. Zákaz „sociálneho bodovania“ má široký rozsah uplatňovania vo verejných aj súkromných kontextoch a nie je obmedzený na konkrétne odvetvie alebo oblasť¹⁰⁵.
147. Zákazom zároveň nemajú byť dotknuté zákonné postupy, ktorými sa hodnotia osoby na osobitné účely, ktoré sú legitímne a v súlade s právom Únie a vnútroštátnym právom,¹⁰⁶ najmä ak sa v uvedených právnych predpisoch stanovujú druhy údajov relevantné pre osobitné účely hodnotenia a zabezpečuje sa, aby akékoľvek z toho vyplývajúce škodlivé alebo nepriaznivé zaobchádzanie s osobami bolo odôvodnené a primerané (pozri oddiel 4.3 o vylúčení z rozsahu pôsobnosti).

4.1. Odôvodnenie a ciele

148. Systémy AI, ktoré umožňujú praktiky „sociálneho bodovania“, môžu viesť k diskriminačným a nespravodlivým výsledkom pre určitých jednotlivcov a skupiny vrátane ich vylúčenia zo spoločnosti, ako aj k praktikám ovládania spoločnosti a praktikám sledovania, ktoré sú nezlučiteľné s hodnotami Únie. Cieľom zákazu „sociálneho bodovania“ je chrániť najmä právo na ľudskú dôstojnosť a ďalšie základné práva vrátane práva na nediskrimináciu a rovnosť, na ochranu údajov a na súkromný a rodinný život, ako aj príslušné sociálne a hospodárske práva v relevantných prípadoch. Jeho cieľom je aj chrániť a podporovať hodnoty Únie, ako sú demokracia,

¹⁰⁵ Zákaz sociálneho bodovania sa líši od zákazu v článku 5 ods. 1 písm. d) aktu o AI, ktorý je špecializovanejší vo vzťahu k praktikám hodnotenia/bodovania, ktoré sa vzťahujú len na posudzovanie rizika a predvídanie pravdepodobnosti, že osoba spácha trestný čin, tým, že sa ním zakazujú systémy AI založené výlučne na profilovaní alebo posudzovaní osobnostných vlastností a charakteristík (pozri oddiel 5).

¹⁰⁶ Odôvodnenie 31 aktu o AI.

rovnosť (vrátane rovnakého prístupu k verejným a súkromným službám) a spravodlivosť¹⁰⁷.

4.2. Hlavné pojmy a zložky zákazu „sociálneho bodovania“

V článku 5 ods. 1 písm. c) aktu o AI sa stanovuje:

Zakazujú sa tieto praktiky využívajúce AI:

c) uvádzanie na trh, uvádzanie do prevádzky alebo používanie systémov AI na hodnotenie alebo klasifikáciu fyzických osôb alebo skupín osôb počas určitého obdobia na základe ich spoločenského správania alebo známych, odvodených či predpokladaných osobných alebo osobnostných charakteristík, pričom takto získané sociálne skóre vedie k jednému alebo obidvom z týchto výsledkov:

- i) ku škodlivému alebo nepriaznivému zaobchádzaniu s určitými fyzickými osobami alebo skupinami osôb v sociálnych kontextoch, ktoré nesúvisia s kontextami, v ktorých boli údaje pôvodne generované alebo zhromaždené;
- ii) ku škodlivému alebo nepriaznivému zaobchádzaniu s určitými fyzickými osobami alebo skupinami osôb, ktoré je neodôvodnené alebo neprimerané ich spoločenskému správaniu alebo jeho závažnosti;

149. Na uplatnenie zákazu podľa článku 5 ods. 1 písm. c) aktu o AI musí byť splnených niekoľko kumulatívnych podmienok:

- i) praktika musí predstavovať „uvádzanie na trh“, „uvádzanie do prevádzky“ alebo „používanie“ systému AI;
- ii) systém AI musí byť určený alebo používaný na hodnotenie alebo klasifikáciu fyzických osôb alebo skupín osôb počas určitého obdobia na základe:
 - a) ich spoločenského správania alebo
 - b) známych, odvodených či predpokladaných osobných alebo osobnostných charakteristík;
- iii) sociálne skóre vytvorené s pomocou systému AI musí alebo môže viesť k škodlivému alebo nepriaznivému zaobchádzaniu s osobami alebo skupinami v jednom alebo viacerých z týchto scenárov:
 - a) v sociálnych kontextoch, ktoré nesúvisia s kontextami, v ktorých boli údaje pôvodne generované alebo zhromaždené, a/alebo
 - b) v prípade zaobchádzania, ktoré je neodôvodnené alebo neprimerané ich spoločenskému správaniu alebo jeho závažnosti.

150. Na to, aby sa zákaz uvedený v článku 5 ods. 1 písm. c) aktu o AI uplatnil, musia byť súčasne splnené všetky tri podmienky. Prvá podmienka, t. j. uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému AI, už bola analyzovaná v oddiele 2.3. Zákaz sa preto vzťahuje na poskytovateľov systémov AI aj subjekty nasadzujúce

¹⁰⁷

Odôvodnenie 31 aktu o AI.

systemy AI, pričom každý z nich v rámci svojich povinností nesmie takéto systémy uvádzať na trh, uvádzať do prevádzky alebo používať. Zostávajúce kritériá zákazu „sociálneho bodovania“ sa bližšie opisujú a analyzujú ďalej.

4.2.1. „Sociálne bodovanie“: hodnotenie alebo klasifikácia na základe spoločenského správania alebo osobných či osobnostných charakteristík počas určitého obdobia

a) Hodnotenie alebo klasifikácia fyzických osôb alebo skupiny osôb

151. Druhou podmienkou na uplatnenie zákazu podľa článku 5 ods. 1 písm. c) aktu o AI je, že systém AI je určený alebo používaný na **hodnotenie alebo klasifikáciu** fyzických osôb alebo skupín osôb a prideluje im skóre na základe ich spoločenského správania alebo osobných či osobnostných charakteristík. Skóre vytvorené systémom môže mať rôznu formu, napríklad matematické číslo (napríklad od 0 do 1), poradie alebo označenie.
152. Rozsah pôsobnosti zákazu je široký a zahŕňa praktiky hodnotenia a klasifikácie vo verejnom aj súkromnom sektore (pozri oddiel 4.2.3). Hodnotenie alebo klasifikácia sa zároveň týka len fyzických osôb alebo skupín fyzických osôb, čím sa v zásade vylučujú právnické osoby (pozri oddiel 4.3 o vylúčení z rozsahu pôsobnosti).
153. Hoci „**hodnotenie**“ naznačuje zapojenie určitej formy **posúdenia alebo úsudku** o osobe alebo skupine osôb, jednoduchá **klasifikácia** osôb alebo skupín osôb na základe charakteristík, ako sú ich vek, pohlavie a výška, nemusí nevyhnutne viesť k hodnoteniu¹⁰⁸. Rozsah pojmu „klasifikácia“ je preto širší ako „hodnotenie“ a môže zahŕňať aj iné druhy klasifikácie alebo kategorizácie fyzických osôb alebo skupín osôb na základe kritérií, ktoré nemusia nevyhnutne zahŕňať konkrétne posúdenie alebo úsudok o týchto osobách alebo skupinách osôb a ich charakteristikách alebo správaní.
154. Pojem „**hodnotenie**“ súvisí aj s pojmom „profilovanie“, ktorý sa upravuje právnymi predpismi Únie o ochrane údajov¹⁰⁹ a predstavuje osobitnú formu hodnotenia. Hoci sa v článku 5 ods. 1 písm. c) aktu o AI neuvádza priamy odkaz na tento pojem ani na uvedené právne predpisy,¹¹⁰ môžu byť relevantné aj pre zákaz obsiahnutý v danom ustanovení, ako aj pre iné zákazy v akte o AI¹¹¹, ak sa hodnotenie vykonáva automatizovaným spôsobom systémom AI na základe osobných údajov. **Profilovanie** znamená použitie informácií o jednotlivcovi (alebo skupine jednotlivcov) a vyhodnotenie ich charakteristík alebo vzorcov správania s cieľom umiestniť ich do

¹⁰⁸ Pracovná skupina zriadená podľa článku 29, *Usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679*, WP251rev.01, 6. 2. 2018, s. 7.

¹⁰⁹ Pozri článok 4 ods. 4 a článok 22 všeobecného nariadenia o ochrane údajov a článok 11 smernice o presadzovaní práva. Pozri aj *usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679*, ktoré vypracovala pracovná skupina zriadená podľa článku 29, WP251rev.01, 6. 2. 2018, s. 7.

¹¹⁰ V článku 3 bode 52 aktu o AI sa uvádza vymedzenie pojmu „profilovanie“, ktoré obsahuje odkaz na vymedzenie v článku 4 bode 4 všeobecného nariadenia o ochrane osobných údajov.

¹¹¹ Konkrétne zákaz predvídania rizika toho, že jednotlivec spácha trestný čin, v článku 5 ods. 1 písm. d) aktu o AI, kde sa skutočne uvádza odkaz na „profilovanie“, a v niektorých prípadoch rozpoznávania emócií a biometrickej kategorizácie v článku 5 ods. 1 písm. f) a g) aktu o AI.

určitej kategórie alebo skupiny, najmä **na účely analýzy a/alebo predvídania** napríklad ich schopnosti vykonávať úlohu, záujmov alebo pravdepodobného správania¹¹². Na profilovanie fyzických osôb podľa práva EÚ v oblasti ochrany údajov, ak sa vykonáva prostredníctvom systémov AI, sa preto môže vzťahovať aj článok 5 ods. 1 písm. c) aktu o AI.

Napríklad v rozsudku vo veci SCHUFA I Súdny dvor Európskej únie skúmal **systém bodového hodnotenia („scoring“) úverovej bonity** používaný v Nemecku¹¹³. V tomto prípade bolo „skóre“ vygenerované počítačovým programom „hodnotou pravdepodobnosti“ týkajúcou sa schopnosti dotknutej osoby plniť platobné záväzky, čo Súdny dvor Európskej únie kvalifikoval ako „profilovanie“. Konkrétnejšie, systém stanovil prognózu pravdepodobnosti budúceho správania osoby („skóre“), ako je splácanie úveru, v závislosti od určitých charakteristík tejto osoby. Určenie skóre („scoring“) je založené na predpoklade, že pomocou priradenia osoby ku skupine iných osôb s určitými porovnateľnými znakmi, ktoré sa správali určitým spôsobom, možno predpovedať podobné správanie¹¹⁴. Podľa Súdneho dvora Európskej únie táto činnosť zodpovedá definícii „profilovania“ uvedenej v článku 4 bode 4 všeobecného nariadenia o ochrane údajov¹¹⁵. Túto formu profilovania možno takisto považovať za hodnotenie osôb na základe ich osobných charakteristík v zmysle článku 5 ods. 1 písm. c) aktu o AI, ktoré bude zakázané, ak sa vykonáva pomocou systémov AI a za predpokladu, že sú splnené ostatné podmienky na uplatnenie tohto ustanovenia.

b) Počas určitého obdobia

155. Na základe zákazu v článku 5 ods. 1 písm. c) aktu o AI sa vyžaduje, aby sa pri hodnotení alebo klasifikácii vychádzalo z údajov „**počas určitého obdobia**“. To naznačuje, že posúdenie by sa nemalo obmedzovať na jednorazové alebo okamžité hodnotenie alebo známkovanie na základe údajov alebo správania z veľmi špecifického individuálneho kontextu. Zároveň je dôležité, aby sa táto podmienka posudzovala s prihliadnutím na všetky okolnosti prípadu, aby sa zabránilo obchádzaniu rozsahu pôsobnosti zákazu.

Napríklad úrad pre migráciu a azyl zavádza čiastočne automatizovaný systém sledovania v záchytných táboroch, ktorý je postavený na celej škále infraštruktúry na sledovanie vrátane kamier a snímačov pohybu. Ak analyzované údaje zahŕňajú určité obdobie a hodnotia sa konkrétne osoby (ako sú migranti), napríklad s cieľom zistiť, či pri nich existuje riziko pokusu o útek, kvalifikovalo by sa to tak, že k sledovaniu dochádza „počas určitého obdobia“, a zákaz v článku 5 ods. 1 písm. c) aktu o AI by sa v prípade splnenia všetkých ostatných podmienok mohol uplatniť.

¹¹² Pracovná skupina zriadená podľa článku 29, *Usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679*, WP251rev.01, 6. 2. 2018, s. 7.

¹¹³ Rozsudok Súdneho dvora zo 7. decembra 2023, SCHUFA Holding (Scoring), C-634/21, EU:C:2023:957 (ďalej len „rozsudok vo veci SCHUFA I“), napríklad bod 47.

¹¹⁴ Tamže, bod 14 (vlastné zvýraznenie).

¹¹⁵ Tamže, bod 47.

c) Na základe ich spoločenského správania alebo známych, odvodených či predpokladaných osobných alebo osobnostných charakteristík

156. Praktiky „hodnotenia“ a „klasifikácie“ zakázané podľa článku 5 ods. 1 písm. c) aktu o AI musia byť založené na spracúvaní údajov (často rozsiahlym), ktoré umožňuje AI, vo vzťahu k i) spoločenskému správaniu jednotlivcov alebo skupín osôb alebo ii) ich známym, odvodeným alebo predpokladaným osobným a osobnostným charakteristikám, alebo vo vzťahu k obojom možnostiam. Údaje môžu byť poskytnuté priamo osobami alebo zhromaždené nepriamo, t. j. prostredníctvom sledovania, získané od tretích strán alebo odvodené z iných informácií.
157. Pokiaľ ide o prvý scenár, **„spoločenské správanie“** je široký pojem, ktorý môže vo všeobecnosti zahŕňať konanie, správanie, zvyky, interakcie v rámci spoločnosti atď. a zvyčajne zahŕňa údajové body týkajúce sa správania z viacerých zdrojov¹¹⁶. Môže to zahŕňať správanie jednotlivcov a skupín jednotlivcov v spoločenskom a súkromnom kontexte, ako sú účasť na kultúrnych podujatiach, dobrovoľníctvo atď., ale aj spoločenské správanie v obchodnom kontexte, napríklad splácanie dlhov, správanie pri využívaní určitých služieb, ako aj vzťahy s verejnými a súkromnými subjektmi, vládou, políciou a z hľadiska zákonov (napríklad či osoba dodržiava pravidlá cestnej premávky). Údaje o spoločenskom správaní z viacerých kontextov a údajových bodov môže ten istý subjekt zhromažďovať centralizovaným spôsobom, ale najčastejšie sa zbierajú distribuovaným spôsobom a kombinujú sa z rôznych zdrojov, čo môže zahŕňať zvýšené monitorovanie a sledovanie jednotlivcov (tzv. sledovanie údajov – *dataveillance*).
158. V prípade druhého scenára je bodovanie založené na **osobných alebo osobnostných charakteristikách**, ktoré môžu, ale nemusia zahŕňať osobitné aspekty spoločenského správania. „Osobné charakteristiky“ môžu zahŕňať rôzne informácie týkajúce sa osoby, napríklad pohlavie, sexuálnu orientáciu alebo sexuálne charakteristiky, rod, rodovú identitu, rasu, etnický pôvod, rodinnú situáciu, adresu, príjem, členov domácnosti, povolanie, zamestnanie alebo iné právne postavenie, pracovné výsledky, ekonomickú situáciu, finančnú likviditu, zdravie, osobné preferencie, záujmy, spoľahlivosť, správanie, miesto pobytu alebo pohybu, výšku dlhu, typ vozidla atď.¹¹⁷ „Osobnostné charakteristiky“ by sa mali v zásade vykladať ako synonymum pre osobné charakteristiky, ale môžu takisto znamenať vytvorenie osobitných profilov jednotlivcov ako osobností. Osobnostné charakteristiky môžu byť takisto založené na viacerých faktoroch a implikovať úsudok, ktorý môže byť vytvorený samotnými jednotlivcami, inými osobami alebo generovaný systémami AI. V akte o AI sa osobnostné charakteristiky niekedy označujú ako osobnostné vlastnosti a charakteristiky¹¹⁸; tieto pojmy by sa mali vykladať konzistentne.

¹¹⁶ Pozri odôvodnenie 31 aktu o AI.

¹¹⁷ Pozri odôvodnenie 42 aktu o AI, v ktorom sa uvádza niekoľko príkladov takýchto charakteristík.

¹¹⁸ Článok 5 ods. 1 písm. d) aktu o AI.

159. „Známe, odvodené či predpokladané“ osobné alebo osobnostné charakteristiky sú rôzne typy informácií a osobných údajov, ktoré je potrebné rozlišovať. **„Známe charakteristiky“** sú založené na informáciách, ktoré boli systému AI poskytnuté ako vstupné údaje a ktoré sú vo väčšine prípadov overiteľné. Naproti tomu **„odvodené charakteristiky“** sú založené na informáciách, ktoré boli odvodené z iných informácií, pričom odvodenie zvyčajne vykonáva systém AI. **„Predpokladané charakteristiky“** sú charakteristiky, ktoré sa odhadujú na základe vzorcov s presnosťou nižšou ako 100 %. Pojmy „odvodených“ (alebo vyvodených) údajov sa používajú v súvislosti s profilovaním aj v práve Únie v oblasti ochrany údajov, a preto môžu byť zdrojom inšpirácie pri výklade pojmov použitých v článku 5 ods. 1 písm. c) aktu o AI.¹¹⁹ Používanie týchto rôznych typov údajov môže mať rôzne dôsledky, pokiaľ ide o presnosť a spravodlivosť bodovacích praktík, a preto sa môže zohľadniť, najmä ak je spracovanie nepriehľadné alebo sa opiera o údajové body, ktorých presnosť sa ťažšie overuje.

4.2.2. Sociálne skóre musí viesť k škodlivému alebo nepriaznivému zaobchádzaniu v nesúvisiacich sociálnych kontextoch a/alebo k neodôvodnenému alebo neprimeranému zaobchádzaniu vzhľadom na závažnosť spoločenského správania

a) Príčinná súvislosť medzi sociálnym skóre a zaobchádzaním

160. Aby sa zákaz v článku 5 ods. 1 písm. c) aktu o AI uplatnil, musí sociálne skóre vytvorené systémom AI alebo s jeho pomocou **viesť k škodlivému alebo nepriaznivému zaobchádzaniu** s hodnotenou osobou alebo skupinou osôb. Inými slovami, zaobchádzanie musí byť dôsledkom skóre a skóre príčinou zaobchádzania. Takáto hodnoverná príčinná súvislosť môže existovať aj v prípadoch, keď sa škodlivé dôsledky ešte neprejavili, ale systém AI je určený na to, aby takýto nepriaznivý výsledok spôsobil, alebo je schopný ho spôsobiť. To je obzvlášť dôležité vzhľadom na to, že zakázaná praktika v článku 5 ods. 1 písm. c) aktu o AI sa vzťahuje aj na „uvádzanie na trh“ takýchto systémov AI.
161. Podľa článku 5 ods. 1 písm. c) aktu o AI sa nevyžaduje, aby hodnotenie alebo klasifikácia vykonané systémom AI boli jedinou príčinou škodlivého alebo nepriaznivého zaobchádzania. Preto sa uvedené ustanovenie vzťahuje aj na bodovacie praktiky využívajúce AI, na ktoré sa môže uplatniť takisto ďalšie ľudské posúdenie alebo ktoré sa s ním môžu kombinovať. Výstup AI musí zároveň zohrávať dostatočne dôležitú úlohu pri tvorbe sociálneho skóre. Napríklad v prípade, keď orgán verejnej moci nasadí systém AI na hodnotenie dôveryhodnosti osôb a skombinuje jeho výstup s ľudským posúdením dodatočných skutočností, bude táto praktika sociálneho bodovania využívajúca AI patriť do rozsahu pôsobnosti zákazu len vtedy, ak skóre vytvorené AI zohráva dostatočne dôležitú úlohu v konečnom rozhodnutí, za

¹¹⁹ Pozri usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679, ktoré vypracovala pracovná skupina zriadená podľa článku 29, WP251rev.01, 6. 2. 2018, s. 7 a nasl.

predpokladu, že sú splnené ostatné podmienky škodlivého alebo nepriaznivého zaobchádzania, ako sa opisuje ďalej [pozri oddiel 4.2.2 písm. b)].

162. Skóre môže viesť k škodlivému alebo nepriaznivému zaobchádzaniu, aj keď ho vytvorila organizácia (organizácie) odlišná (odlišné) od organizácie, ktorá skóre používa¹²⁰. Orgán verejnej moci môže napríklad získať skóre na účely posúdenia úverovej bonity fyzickej osoby vytvorené inou spoločnosťou špecializovanou na posudzovanie úverovej bonity a rizík, pri ktorom sa vychádza z informácií o jednotlivcoch a ich správaní z rôznych zdrojov.

b) Škodlivé alebo nepriaznivé zaobchádzanie v nesúvisiacich sociálnych kontextoch a/alebo neodôvodnené alebo neprimerané zaobchádzanie

163. Poslednou podmienkou na uplatnenie zákazu podľa článku 5 ods. 1 písm. c) aktu o AI je, že použitie sociálneho skóre musí viesť (alebo môže viesť) k škodlivému alebo nepriaznivému zaobchádzaniu:
- i) v sociálnom (sociálnych) kontexte (kontextoch), ktorý (ktoré) nesúvisí (nesúvisia) s kontextami, v ktorých boli údaje pôvodne generované alebo zhromaždené, alebo
 - ii) ktoré je neodôvodnené alebo neprimerané spoločenskému správaniu alebo jeho závažnosti.
164. Tieto podmienky sú alternatívne a môžu sa uplatňovať aj v kombinácii. Na posúdenie, či je splnená aspoň jedna z nich, je potrebná analýza od prípadu k prípadu, pretože mnohé bodovacie a hodnotiace praktiky využívajúce AI ich nemusia spĺňať, a preto nepatria do rozsahu pôsobnosti zákazu. Nemusí to tak byť najmä v prípade, keď sú bodovacie praktiky využívajúce AI určené na osobitný legitímny účel hodnotenia a sú v súlade s platným právom Únie a vnútroštátnym právom, v ktorých sa špecifikujú údaje považované za relevantné na účely hodnotenia a ktorými sa zabezpečuje, že škodlivé alebo nepriaznivé zaobchádzanie je odôvodnené a primerané spoločenskému správaniu (pozri oddiel 4.3 o vylúčení z rozsahu pôsobnosti).
165. „Nepriaznivé zaobchádzanie“ je, že v dôsledku bodovania sa s osobou alebo skupinou osôb musí zaobchádzať menej priaznivo v porovnaní s ostatnými bez toho, aby sa nevyhnutne vyžadoval vznik konkrétnej ujmy alebo škody (napríklad v prípade bodovacích praktík, keď sa osoby selektujú na dodatočné kontroly v prípade podozrenia z podvodu). Naopak, v prípade „škodlivého“ zaobchádzania sa vyžaduje, aby osoba alebo skupina osôb utrpela v dôsledku takého zaobchádzania určitú ujmu a škodu. Nepriaznivé alebo škodlivé zaobchádzanie môže byť aj diskriminačné a zakázané podľa právnych predpisov EÚ o nediskriminácii alebo môže znamenať vylúčenie určitých jednotlivcov alebo skupín¹²¹, to však nie je nevyhnutnou podmienkou na

¹²⁰ Tento výklad je v súlade s rozsudkom Súdny dvor Európskej únie vo veci SCHUFA I, v ktorom Súdny dvor Európskej únie v súvislosti s automatizovaným rozhodovaním rozhodol, že „skóre“ (hodnotenie predstavujúce profilovanie) vypracované iným subjektom ako subjektom, ktorý prijíma konečné rozhodnutie, môže predstavovať automatizované rozhodovanie podľa článku 22 všeobecného nariadenia o ochrane údajov. Pozri rozsudok vo veci SCHUFA I, body 42 až 51 a 60 až 62.

¹²¹ Odôvodnenie 31 aktu o AI.

uplatnenie tohto zákazu. Článok 5 ods. 1 písm. c) aktu o AI by sa preto mohol vzťahovať na nespravodlivé zaobchádzanie nad rámec práva EÚ o nediskriminácii, ktoré sa vzťahuje len na určité chránené skupiny (napríklad na základe veku, etnického a rasového pôvodu, pohlavia, náboženstva).

Scenár 1: Škodlivé alebo nepriaznivé zaobchádzanie v nesúvisiacich sociálnych kontextoch

166. V prvom scenári opísanom podľa článku 5 ods. 1 písm. c) bodu i) aktu o AI musí ku škodlivému alebo nepriaznivému zaobchádzaniu vyplývajúcemu zo skóre dôjsť **v sociálnom (sociálnych) kontexte (kontextoch), ktorý (ktoré) nesúvisí (nesúvisia)** s kontextami, v ktorých boli údaje pôvodne generované alebo zhromaždené. To znamená nielen to, že s osobami sa môže zaobchádzať nepriaznivo alebo škodlivo v dôsledku sociálneho skóre, ale aj to, že údaje o ich spoločenskom správaní alebo o ich známych, odvodených či predpokladaných osobných alebo osobnostných charakteristikách sa generujú alebo zhromažďujú v sociálnych kontextoch, ktoré nesúvisia s kontextom, v ktorom sa bodovanie uskutočňuje. Údaje zhromaždené alebo generované z týchto nesúvisiacich kontextov musí systém AI následne použiť na bodovanie osôb bez zjavnej súvislosti s účelom hodnotenia alebo klasifikácie alebo spôsobom, ktorý vedie k všeobecnému sledovaniu osôb alebo skupín osôb. Vo väčšine prípadov sa tak deje v rozpore s primeranými očakávaniami osôb a v rozpore s právom Únie o ochrane údajov a prípadne ďalšími platnými pravidlami, v ktorých sa stanovujú druhy údajov a zdrojov považovaných za relevantné a potrebné na účely hodnotenia alebo klasifikácie. Na overenie splnenia tejto podmienky sa bude vyžadovať posúdenie od prípadu k prípadu, pričom sa zohľadní účel hodnotenia a kontexty, v ktorých boli údaje zhromaždené a generované.

Príklady škodlivého alebo nepriaznivého zaobchádzania v nesúvisiacich sociálnych kontextoch, ktoré sú zakázané podľa článku 5 ods. 1 písm. c) bodu i) aktu o AI

- Vnútroštátne daňové orgány používajú prediktívny nástroj AI na všetky daňové priznania daňovníkov v danej krajine s cieľom vybrať daňové priznania na dôkladnejšiu kontrolu. Pri selektovaní konkrétnych jednotlivcov na kontrolu nástroj AI využíva relevantné premenné, ako sú ročný príjem, majetok (nehnutelnosti, automobily atď.), údaje o rodinných príslušníkoch príjemcov, ale aj nesúvisiace údaje, ako sú sociálne návyky daňovníkov alebo internetové pripojenie.
- Agentúra sociálneho zabezpečenia používa systém AI na odhad pravdepodobnosti podvodu zo strany príjemcov príspevkov na domácnosť, ktorý sa opiera o charakteristiky zhromaždené alebo odvodené zo sociálnych kontextov bez zjavnej súvislosti alebo významu pre posúdenie podvodu, napríklad to, či má príjemca manžela alebo manželku s určitou štátnou príslušnosťou alebo etnickým pôvodom, či má pripojenie na internet, aké má správanie na sociálnych platformách alebo výkonnosť na pracovisku atď.¹²² Naopak, údaje, ktoré sú relevantné pre pridelovanie

¹²²

Porovnanie podobných národných systémov dávok a sociálneho bodovania nájdete v práci D. Hadwick a S. Lan, „Lessons to be learned from the Dutch childcare allowance scandal: A comparative review of

dávok a zhromažďujú sa v súlade so zákonom, by sa mohli použiť na určenie rizika podvodu, keďže orgány verejnej moci sledujú legitímny cieľ, keď overujú, či sú sociálne dávky správne pridelené.

- Verejná agentúra v oblasti zamestnanosti používa systém AI na stanovenie skóre nezamestnaných osôb na základe pohovoru a hodnotenia založeného na AI s cieľom určiť, či by osoba mala využívať štátnu podporu na získanie zamestnania. Toto skóre je založené na relevantných osobných charakteristikách, ako sú vek a vzdelanie, ale aj na premenných zhromaždených alebo odvodených z údajov a kontextov bez zjavnej súvislosti s účelom hodnotenia, ako sú rodinný stav, zdravotné údaje o chronických chorobách, závislosti atď.¹²³

Tieto neprijateľné bodovacie praktiky možno odlíšiť od zákonných postupov, pri ktorých sa hodnotia osoby na konkrétny účel v súlade s právom Únie a vnútroštátnym právom, najmä ak sa v takých právnych predpisoch v súlade s právom EÚ stanovujú údaje, ktoré sa považujú za relevantné a potrebné na účely hodnotenia (pozri oddiel 4.3 o vylúčení z rozsahu pôsobnosti).

Scenár 2: Nepriaznivé alebo škodlivé zaobchádzanie neprimerané spoločenskému správaniu

167. Ďalším alternatívnym scenárom podľa článku 5 ods. 1 písm. c) bodu ii) aktu o AI, v ktorom môže byť bodovací systém AI zakázaný, je prípad, keď je zaobchádzanie vyplývajúce zo skóre neodôvodnené alebo neprimerané závažnosti spoločenského správania. Na základe závažnosti vplyvu a zásahu do základných práv dotknutej osoby vyplývajúcich zo sociálneho bodovania v porovnaní so závažnosťou spoločenského správania osoby by sa malo určiť, či je takéto zaobchádzanie neprimerané sledovanému legitímnemu cieľu, pričom sa zohľadní všeobecná zásada proporcionality. To si vyžaduje posúdenie od prípadu k prípadu, v ktorom by mali zohľadniť všetky relevantné okolnosti prípadu, ako aj všeobecné etické úvahy a zásady spravodlivého zaobchádzania a sociálnej spravodlivosti súvisiace s posúdením spoločenského správania a primeranosti škodlivého zaobchádzania. Zaobchádzanie môže byť aj „neodôvodnené“, napríklad keď mu chýba legitímny cieľ. V rámci tohto posúdenia môžu byť relevantné aj odvetvové právne predpisy Únie alebo vnútroštátne právne predpisy stanovujúce osobitné kritériá a postupy, ktorými sa upravuje takéto potenciálne škodlivé alebo nepriaznivé zaobchádzanie.

Príklady neodôvodneného alebo neprimeraného zaobchádzania v porovnaní so spoločenským správaním, ktoré je zakázané podľa článku 5 ods. 1 písm. c) bodu ii) aktu o AI

algorithmic governance by tax administrations in the Netherlands, France and Germany“ (Poznanky z holandského škandálu s príspevkom na starostlivosť o dieťa: porovnávacie preskúmanie algoritmickeho riadenia daňovými orgánmi v Holandsku, Francúzsku a Nemecku) (2021), *World Tax Journal*, zväzok 13, vydanie 4, Familiales (CNAF).

¹²³ Podobný systém sa používal v Poľsku v rámci systému „Profilovanie nezamestnaných“, ktorý bol zrušený po tom, ako bol označený za protiústavný. Pozri Szymielewicz, [Profiling the unemployed in Poland: Social and Political Implications of Algorithmic Decision Making](#) (Profilovanie nezamestnaných v Poľsku: sociálne a politické dôsledky algoritmickeho rozhodovania), Fundacja Panoptykon, 2015, s. 18.

- Verejná agentúra využíva systém AI na profilovanie rodín v záujme včasného odhalenia ohrozených detí na základe kritérií, ako sú duševné zdravie a nezamestnanosť rodičov, ale aj informácií o spoločenskom správaní rodičov odvodených z viacerých kontextov. Na základe výsledného skóre sa rodiny selektujú na kontrolu a deti, ktoré sa považujú za „ohrozené“, sa z rodín odoberajú, a to aj v prípadoch drobných priestupkov rodičov, ako sú napríklad občasné vynechanie návštevy lekára alebo pokuty za dopravný priestupok.
- Obec používa systém AI na bodovanie dôveryhodnosti obyvateľov na základe viacerých údajových bodov týkajúcich sa ich spoločenského správania v rôznych kontextoch. Vytvorené skóre obyvateľov považovaných za „menej dôveryhodných“ slúži ako dôvod pre zaradenie na čiernu listinu, čo má za následok odňatie verejných dávok, iné závažné represívne opatrenia a zvýšenú kontrolu alebo sledovanie. Medzi faktory, ktoré sa pri posúdení zohľadňujú, patrí nedostatočná dobrovoľnícka činnosť a drobné priestupky, napríklad nevrátenie kníh do knižnice načas, ponechanie odpadkov na ulici mimo dňa zberu a oneskorené zaplatenie miestnych daní.

Tieto neprijateľné praktiky sociálneho bodovania možno odlišiť od zákonných postupov, pri ktorých sa hodnotia osoby na legitímny osobitný účel v súlade s právom Únie a vnútroštátnym právom, najmä ak sa v uvedených právnych predpisoch zabezpečuje, že škodlivé alebo nepriaznivé zaobchádzanie je odôvodnené a primerané spoločenskému správaniu (pozri oddiel 4.3 o vylúčení z rozsahu pôsobnosti).

168. Obe alternatívy podľa článku 5 ods. 1 písm. c) bodu i) a ii) aktu o AI môžu byť splnené aj súčasne.

Príklady neodôvodneného alebo neprimeraného zaobchádzania podľa článku 5 ods. 1 písm. c) bodu i) a ii) aktu o AI

- Daňový orgán využíva systém AI na odhaľovanie podvodov s prídavkami na dieťa prostredníctvom profilovania a zaraďovania príjemcov podozrivých z podvodu do kategórií, ako je „úmyselné konanie/hrubá nedbanlivosť“, na základe kritérií, ako sú nízky príjem, dvojaká štátna príslušnosť, spoločenské správanie atď. Na základe rizikového skóre sa kontroluje spis príjemcu a v mnohých prípadoch sa mu zastaví vyplácanie prídavku na dieťa, doručí sa mu výzva na vrátenie prijatých prídavkov a prestane spĺňať podmienky pre štandardné dojednania o vymáhaní dlhu. Takéto bodovanie spôsobuje vysoké zadlženie mnohých rodín a vedie k nespravodlivému, diskriminačnému a škodlivému zaobchádzaniu s jednotlivcami a skupinami jednotlivcov¹²⁴, čím sa mnohé rodiny dostávajú do vážnych finančných ťažkostí.
- Orgán verejnej moci používa systém AI na kontrolu podvodov v procese udeľovania príspevkov na ubytovanie študentov, v rámci ktorého sa ako rozlišovacie faktory

¹²⁴ Podobný príklad škandálu v súvislosti s príspevkami na starostlivosť o deti v Holandsku nájdete na stránke [Belastingdienst treft 232 gezinnen met onevenredig harde actie](#), 27. 11. 2019 (v holandčine). Holandský súd v roku 2020 rozhodol, že „Systeem Risico Indicatie“ (SyRi) bol nezákonný. Pozri aj [Geen powerplay maar fair play. Onevenredig harde aanpak van 232 gezinnen met kinderopvangtoeslag](#), 2017, s. 32.

rizika podvodu posudzujú ukazovatele ako internetové pripojenie, rodinný stav alebo úroveň vzdelania príjemcov, ktoré sa nezdajú relevantné ani opodstatnené.

- Vláda zavedie komplexný systém založený na AI, ktorý monitoruje a hodnotí občanov na základe ich správania v rôznych oblastiach života, ako sú sociálne interakcie, online aktivity, nákupné návyky a dodržiavanie termínov splatnosti účtov. Ľudia s nižším skóre čelia obmedzenému prístupu k verejným službám, vyšším úrokovým sadzbám na pôžičky, ťažkostiam pri cestovaní, prenájme bytov a dokonca aj pri hľadaní práce. Systém vedie k nadmernému sledovaniu jednotlivcov a ku škodlivému zaobchádzaniu v kontextoch, ktoré nesúvisia so spoločenským správaním používaným na určenie sociálneho skóre (napríklad pracovné príležitosti sú ovplyvnené aktivitou na sociálnych médiách), a zároveň sa ním ukladajú neprimerané sankcie za menej závažné priestupky (napríklad spoločenské a finančné znevýhodnenie za relatívne malé priestupky).

Tieto neprijateľné praktiky sociálneho bodovania možno odlíšiť od zákonných postupov hodnotenia osôb na legitímne osobitné účely, ktoré nespĺňajú uvedené podmienky a sú v súlade s právom Únie a vnútroštátnym právom, najmä ak sa v uvedených právnych predpisoch zabezpečuje, že škodlivé alebo nepriaznivé zaobchádzanie je odôvodnené a primerané a používajú sa údaje zo súvisiacich sociálnych kontextov (pozri oddiel 4.3 o vylúčení z rozsahu pôsobnosti).

169. Zákaz podľa článku 5 ods. 1 písm. c) aktu o AI sa môže vzťahovať aj na prípady, keď sa určitým jednotlivcom alebo skupinám osôb poskytujú odmeny alebo preferenčné zaobchádzanie, pretože to znamená menej priaznivé zaobchádzanie s inými jednotlivcami (napríklad v prípadoch podporných programov zamestnanosti, uprednostňovania alebo neuprednostňovania vo vzťahu k bývaniu alebo presídľovaniu).

4.2.3. Bez ohľadu na to, či ich poskytujú alebo používajú verejné alebo súkromné osoby

170. Ako už bolo uvedené, v článku 5 ods. 1 písm. c) aktu o AI sa zakazujú neprijateľné praktiky sociálneho bodovania využívajúce AI bez ohľadu na to, či systém AI alebo skóre poskytujú alebo používajú verejné alebo súkromné osoby. Zatiaľ čo bodovanie vo verejnom sektore môže mať pre ľudí veľmi závažné dôsledky z dôvodu nerovnováhy moci a závislosti od verejných služieb, podobne škodlivé dôsledky sa môžu vyskytnúť aj v súkromnom sektore, kde bodovacie praktiky čoraz častejšie využívajú aj podniky a iné subjekty.

Napríklad:

- Poistovňa zhromažďuje od banky informácie o výdavkoch a iné finančné informácie, ktoré nesúvisia s určením oprávnenosti záujemcov o životné poistenie a ktoré sa používajú na určenie ceny poistného, ktoré sa má platiť za takéto poistenie. Systém AI analyzuje tieto informácie a na ich základe odporúča, či odmietnuť uzatvorenie zmluvy alebo stanoviť vyššie poistné na životné poistenie pre konkrétnu osobu alebo skupinu zákazníkov.

– Súkromná úverová agentúra využíva systém AI na určovanie úverovej bonity ľudí a rozhodovanie o tom, či má jednotlivec získať úver na bývanie, na základe nesúvisiacich osobných charakteristík.

Tieto neprijateľné praktiky sociálneho bodovania možno odlišiť od zákonných postupov hodnotenia osôb na osobitné legítimné účely, ktoré nespĺňajú uvedené podmienky a sú v súlade s právom Únie a vnútroštátnym právom, najmä ak sa v uvedených právnych predpisoch zabezpečuje, že škodlivé alebo nepriaznivé zaobchádzanie je odôvodnené a primerané a používajú sa údaje zo súvisiacich sociálnych kontextov (pozri oddiel 4.3 o vylúčení z rozsahu pôsobnosti).

171. V prípade kontrol zo strany príslušných orgánov dohľadu nad trhom je na poskytovateľovi systému AI a subjekte nasadzujúcom systém AI, aby v rámci svojich povinností preukázali, že praktika využívajúca AI je legítimná a odôvodnená, a to aj zabezpečením transparentnosti fungovania systému AI a poskytnutím informácií o druhoch údajov a zdrojoch údajov, čím sa zabezpečí, že na účely hodnotenia alebo klasifikácie sa spracúvajú len údaje súvisiace so sociálnym kontextom, v ktorom sa skóre používa, systém funguje zamýšľaným spôsobom a akékoľvek výsledné škodlivé alebo nepriaznivé zaobchádzanie je odôvodnené a primerané spoločenskému správaniu. Dodržiavaním uplatniteľných právnych predpisov a vhodnými a primeranými zárukami zabudovanými do systému a uplatňovanými počas jeho prevádzky sa pomôže zabrániť uplatňovaniu zákazu a zároveň sa umožní využívanie systémov AI na hodnotenie alebo klasifikáciu osôb na legítimné a prospešné účely (napríklad na zlepšenie efektívnosti procesov, kvality služieb, bezpečnosti atď.) (pozri oddiel 4.3 o vylúčení z rozsahu pôsobnosti).
172. Súladom s požiadavkami na vysokorizikové systémy AI (napríklad v oblasti základných verejných služieb a dávok, bodového hodnotenia kreditného rizika a posúdenia úverovej bonity, migrácie atď.) takisto možno pomôcť zabezpečiť, aby systémy AI používané na účely hodnotenia a klasifikácie v uvedených vysokorizikových oblastiach nepredstavovali neprijateľné praktiky sociálneho bodovania, ktoré by poskytovatelia a nasadzujúce subjekty mali zohľadniť pri plnení svojich príslušných povinností (napríklad v oblasti riadenia rizík, transparentnosti, správy údajov, posúdenia vplyvu na základné práva, ľudského dohľadu, monitorovania atď.).

4.3. Vylúčenie z rozsahu pôsobnosti

173. Zákaz uvedený v článku 5 ods. 1 písm. c) aktu o AI sa vzťahuje len na bodovanie fyzických osôb alebo skupín osôb, čím sa z neho v zásade vylučuje bodovanie právnických osôb, ak hodnotenie nie je založené na osobných alebo osobnostných charakteristikách alebo spoločenskom správaní jednotlivcov, aj keď v niektorých prípadoch môže mať skóre nepriamy vplyv na jednotlivcov (napríklad na všetkých občanov obce v prípade prideľovania rozpočtových prostriedkov). Ak však boli právnické osoby hodnotené na základe celkového skóre, ktoré sumarizuje hodnotenie alebo klasifikáciu skupiny fyzických osôb na základe ich spoločenského správania alebo osobných či osobnostných charakteristík, a uvedené osoby (napríklad všetci

zamestnanci v spoločnosti, žiaci v konkrétnej škole, ktorých správanie sa hodnotilo) sú týmto skóre priamo dotknuté, praktika môže patriť do pôsobnosti článku 5 ods. 1 písm. c) aktu o AI, ak sú splnené všetky ostatné podmienky. Bude to závisieť od posúdenia od prípadu k prípadu.

174. Sociálne bodovanie založené na AI v podobe „hodnoty pravdepodobnosti“ a prognózy by sa takisto malo odlišovať od individuálnych hodnotení používateľov, ktorými sa posudzuje kvalita služby (napríklad v prípade vodiča na online platforme v oblasti jazdy na zavolanie alebo hostiteľa na online platforme na poskytovanie ubytovania). Takéto hodnotenia sú len súhrnom skóre za jednotlivcov, ktoré nemusia nevyhnutne zahŕňať AI, pokiaľ sa údaje nekombinujú s inými informáciami a neanalyzujú systémom AI na účely hodnotenia alebo klasifikácie osôb, čím by boli splnené všetky podmienky uvedené v článku 5 ods. 1 písm. c) aktu o AI.
175. Okrem toho bodovanie fyzických osôb nie je zakázané vždy, ale len v obmedzených prípadoch, keď sú kumulatívne splnené všetky podmienky článku 5 ods. 1 písm. c) aktu o AI, ako sa už analyzovalo. V odôvodnení 31 aktu o AI sa najmä uvádza, že tento zákaz „by nemal mať vplyv na zákonné postupy hodnotenia fyzických osôb vykonávané na špecifické účely v súlade s právom Únie a vnútroštátnym právom“. Napríklad bodové hodnotenie kreditného rizika, stanovenie rizikového skóre a upisovanie sú základnými aspektmi služieb finančných a poisťovacích podnikov. Takéto postupy, ako aj iné legitímne postupy (t. j. zlepšovanie kvality a efektívnosti služieb, zabezpečenie efektívnejšieho vybavovania reklamácií, vykonávanie osobitných hodnotení zamestnancov, predchádzanie podvodom a ich odhaľovanie, presadzovanie práva alebo bodovanie správania používateľov na online platformách) nie sú samy osebe zakázané, ak sú zákonné a vykonávajú sa v súlade s aktom o AI a inými uplatniteľnými právnymi predpismi Únie a vnútroštátnymi právnymi predpismi, ktoré musia byť v súlade s právom Únie.
176. Inými slovami, systémy AI, ktoré hodnotia alebo klasifikujú jednotlivcov na účely vytvorenia sociálneho skóre zákonným spôsobom a na špecifický účel v súvisiacom kontexte, v akom boli zhromaždené osobné údaje použité na vytvorenie uvedeného skóre, nie sú zakázané za predpokladu, že akékoľvek škodlivé alebo nepriaznivé zaobchádzanie vyplývajúce z použitia skóre je odôvodnené a primerané závažnosti spoločenského správania.¹²⁵
177. Súladom s odvetvovými právnymi predpismi Únie, napríklad v oblasti bodového hodnotenia kreditného rizika, boja proti praniu špinavých peňazí atď., v ktorých sa špecifikuje typ údajov, ktoré možno použiť ako relevantné a potrebné na osobitný legitímny účel hodnotenia a ktorými sa zabezpečuje, že zaobchádzanie je odôvodnené a primerané spoločenskému správaniu, sa teda môže zabezpečiť, že praktika využívajúca AI nebude patriť do rozsahu pôsobnosti zákazu podľa článku 5 ods. 1 písm. c) aktu o AI.

¹²⁵

Odôvodnenie 31 aktu o AI.

Príklady legitímnych bodovacích praktík v súlade s právom Únie a vnútroštátnym právom, ktoré nepatria do rozsahu pôsobnosti článku 5 ods. 1 písm. c) aktu o AI:

- Finančné systémy bodového hodnotenia kreditného rizika, ktoré používajú veritelia alebo agentúry poskytujúce úverové informácie na posúdenie finančnej úverovej bonity alebo nesplatených dlhov zákazníka a ktorými sa vykonáva bodové hodnotenie kreditného rizika alebo posúdenie úverovej bonity, pričom sa vychádza z príjmov a výdavkov zákazníka a iných finančných a ekonomických okolností, nepatria do rozsahu pôsobnosti článku 5 ods. 1 písm. c) aktu o AI, ak sú relevantné na legitímny účel bodového hodnotenia kreditného rizika a ak sú v súlade so zákonmi o ochrane spotrebiteľa¹²⁶, v ktorých sa uvádza druh údajov a potrebné záruky na zabezpečenie spravodlivého zaobchádzania so spotrebiteľmi pri posudzovaní úverovej bonity.
- Spoločnosti majú oprávnený záujem hodnotiť zákazníkov z hľadiska finančných podvodov a tieto praktiky nie sú dotknuté zákazom, ak je hodnotenie založené na relevantných údajoch, ako sú transakčné správanie a metaúdaje v kontexte služieb, doterajšej histórie a iných faktorov zo zdrojov, ktoré sú objektívne relevantné na určenie rizika podvodu, a ak je škodlivé zaobchádzanie odôvodnené a primerané ako dôsledok podvodného správania.
- Informácie zhromaždené prostredníctvom telematických zariadení, ktoré signalizujú, že vodič prekračuje rýchlosť alebo nedodržiava bezpečné jazdné návyky, ktoré používa poisťovateľ ponúkajúci sadzby poistného na základe telematiky v súvislosti s rizikovým správaním poistníka pri jazde, sa môžu použiť na zvýšenie poistného tohto poistníka z dôvodu vyššieho rizika nehody spôsobenej takýmto správaním pri jazde, ak je zvýšenie poistného primerané rizikovému správaniu vodiča.
- Zhromažďovanie a spracúvanie údajov, ktoré sú relevantné a nevyhnutné na zamýšľaný legitímny účel systémov AI (napríklad zdravotné údaje a údaje týkajúce sa schizofrénie, ktoré sú zhromaždené z rôznych zdrojov na diagnostikovanie pacientov), nepatria do rozsahu pôsobnosti článku 5 ods. 1 písm. c) aktu o AI, najmä preto, že sa pri tom spracúvajú relevantné a nevyhnutné údaje a zvyčajne nedochádza k neodôvodnenému škodlivému alebo nepriaznivému zaobchádzaniu s určitými fyzickými osobami.
- Online platformy vykonávajúce v rámci svojich služieb profilovanie používateľov z bezpečnostných dôvodov na základe údajov, ktoré sú relevantné pre kontext a účel posúdenia, nepatria do rozsahu pôsobnosti článku 5 ods. 1 písm. c) aktu o AI, ak hodnotenie nemá za následok škodlivé zaobchádzanie, ktoré je neprimerané závažnosti nevhodného správania používateľa.
- Cílená komerčná reklama využívajúca AI nepatrí do rozsahu pôsobnosti, ak je založená na relevantných údajoch (napríklad preferenciách používateľov), vykonáva sa v súlade s právom Únie o ochrane spotrebiteľa, ochrane údajov a digitálnych

¹²⁶

Pozri najmä smernicu (EÚ) 2023/2225 z 18. októbra 2023 o zmluvách o spotrebiteľskom úvere a o zrušení smernice 2008/48/ES a usmernenia Európskeho orgánu pre bankovníctvo k vzniku a monitorovaniu úveru z 29. mája 2020, EBA/GL/2020/06.

službách a nevedie k škodlivému alebo nepriaznivému zaobchádzaniu neprimeranému závažnosti spoločenského správania používateľa (napríklad zneužívajúce a nespravodlivé diferencované ceny).

- Zákazom nie sú dotknuté systémy AI, ktoré využívajú údaje zhromaždené v záchytných táboroch (napríklad súlad s vyžadovaným správaním) na účely rozhodovania o presídlení alebo zamestnaní, za predpokladu, že tieto údaje sú relevantné na účely posúdenia, a za predpokladu, že sú dodržané postupy podľa platného migračného práva Únie, aby sa zabezpečilo, že zaobchádzanie je odôvodnené a primerané.
- Bodovanie využívajúce AI zo strany online nákupnej platformy, ktorá ponúka výhody používateľom s bohatou nákupnou históriou a nízkou mierou vrátených výrobkov, napríklad rýchlejší proces podávania žiadostí o vrátenie tovaru alebo vrátenie peňazí bez vrátenia tovaru, nepatrí do rozsahu pôsobnosti článku 5 ods. 1 písm. c) aktu o AI, keďže tieto výhody sú odôvodnené a primerané na odmeňovanie pozitívneho správania a ostatní používatelia majú naďalej prístup k štandardnému postupu vrátenia tovaru.
- Hodnotenie a bodovanie osôb pomocou AI zo strany polície a iných orgánov presadzovania práva, pri ktorých sa zhromažďujú údaje o spoločenskom správaní osôb z viacerých kontextov, nepatria do rozsahu pôsobnosti článku 5 ods. 1 písm. c) aktu o AI, ak sú tieto údaje relevantné na osobitné účely predchádzania trestným činom, ich odhaľovania, stíhania a postihovania a ak je škodlivé zaobchádzanie odôvodnené a primerané v súlade s hmotným a procesným právom Únie a hmotným a procesným vnútroštátnym právom v oblasti trestného a policajného práva. V tejto súvislosti je takisto dôležité zvážiť zákaz uvedený v článku 5 ods. 1 písm. d) aktu o AI, ktorým sa ukladajú ďalšie a konkrétnejšie podmienky pre posúdenie rizika a predpovede pravdepodobnosti, že osoba spácha trestný čin, ktoré nesmú byť založené výlučne na profilovaní alebo posúdení osobnostných vlastností (pozri oddiel 5).

4.4. Vzájomný vzťah s inými právnymi aktmi Únie

178. Poskytovatelia a nasadzujúce subjekty by mali starostlivo posúdiť, či sa na akýkoľvek konkrétny bodovací systém AI používaný pri ich činnostiach vzťahujú iné uplatniteľné právne predpisy Únie a vnútroštátne právne predpisy, najmä či existujú konkrétnejšie právne predpisy, ktorými sa prísnejšie upravujú typy údajov, ktoré možno použiť ako relevantné a potrebné na osobitné účely hodnotenia, a či existujú konkrétnejšie pravidlá a postupy na zabezpečenie odôvodneného a spravodlivého zaobchádzania.
179. Praktiky sociálneho bodovania využívajúce AI, ktoré používajú súkromné subjekty, ktoré vystupujú ako obchodníci vo vzťahoch medzi podnikom a koncovým zákazníkom, môžu byť aj v rozpore s právom Únie v oblasti ochrany spotrebiteľa, t. j. so smernicou 2005/29/ES o nekalých obchodných praktikách podnikateľov voči spotrebiteľom (ďalej len „smernica o nekalých obchodných praktikách“). Smernicou o nekalých obchodných praktikách sa zakazujú obchodné praktiky, ak sú v rozpore

s požiadavkami odbornej starostlivosti a podstatne narúšajú alebo sú spôsobilé podstatne narušiť ekonomické správanie priemerného spotrebiteľa alebo priemerného člena skupiny vo vzťahu k výrobku (článok 5 smernice o nekalých obchodných praktikách). Bodovacie praktiky sa môžu považovať aj za klamlivé (články 6 – 7 smernice o nekalých obchodných praktikách), pričom sa v každom jednotlivom prípade posudzuje vplyv obchodnej praktiky na rozhodnutie spotrebiteľa o obchodnej transakcii.

180. Sociálne bodovanie, či už verejnými alebo súkromnými subjektmi, môže byť aj v rozpore s právnymi predpismi Únie o ochrane údajov, napríklad pokiaľ ide o právny základ spracúvania (zákonnosť), zásady ochrany údajov (napríklad minimalizácia a nutnosť údajov, spravodlivosť, transparentnosť) a akékoľvek iné povinnosti vrátane pravidiel týkajúcich sa výlučne automatizovaného individuálneho rozhodovania, ak je to relevantné.
181. Ak je hodnotenie alebo klasifikácia založená na jednom z dôvodov chránených pred diskrimináciou (napríklad vek, náboženstvo, rasový alebo etnický pôvod, pohlavie atď.) alebo vedie priamo alebo nepriamo k diskriminácii týchto skupín, na takúto praktiku sa bude vzťahovať aj právo Únie o nediskriminácii.
182. V tejto súvislosti môže byť relevantná aj smernica o spotrebiteľských úveroch (EÚ) 2023/2225¹²⁷. V článku 18 ods. 3 smernice o spotrebiteľských úveroch sa vyžaduje, aby sa posúdenie úverovej bonity vykonávalo na základe relevantných a presných informácií o príjme a výdavkoch spotrebiteľa a o ďalších finančných a ekonomických okolnostiach, ktoré sú nevyhnutné a primerané povahe, trvaniu, hodnote a rizikám úveru pre spotrebiteľa. Uvedené informácie môžu zahŕňať napríklad dôkazy o príjme alebo iných zdrojoch splácania, informácie o finančných aktívach a pasívach alebo informácie o iných finančných záväzkoch. V smernici o spotrebiteľských úveroch sa výslovne zakazuje, aby sa do informácií zahrnuli osobitné kategórie osobných údajov a aby sa informácie získavali zo sociálnych sietí. V usmerneniach Európskeho orgánu pre bankovníctvo k vzniku a monitorovaniu úveru¹²⁸ sa bližšie špecifikujú relevantné informácie na účely posúdenia úverovej bonity. Táto špecifikácia druhu údajov v týchto odvetvových právnych predpisoch na osobitné účely hodnotenia je relevantným hľadiskom, ktoré sa má zohľadniť pri určovaní, či praktika patrí do rozsahu pôsobnosti zákazu v článku 5 ods. 1 písm. c) aktu o AI.
183. Aj systémy AI používané na hodnotenie a klasifikáciu osôb na účely boja proti praniu špinavých peňazí a financovaniu terorizmu by podobne mali byť v súlade s príslušnými právnymi predpismi Únie v tejto oblasti.

5. ČLÁNOK 5 ODS. 1 PÍSM. D) AKTU O AI – INDIVIDUÁLNE POSÚDENIE RIZIKA A PREDVÍDANIE TRETNÝCH ČINOV

¹²⁷ Smernica Európskeho parlamentu a Rady 2008/48/ES z 23. apríla 2008 o zmluvách o spotrebiteľskom úvere a o zrušení smernice Rady 87/102/EHS (Ú. v. EÚ L 133, 22.5.2008, s. 66 – 92).

¹²⁸ Európsky orgán pre bankovníctvo, Usmernenia k vzniku a monitorovaniu úveru z 29. mája 2020, EBA/GL/2020/06.

184. V článku 5 ods. 1 písm. d) aktu o AI sa zakazujú systémy AI, ktorými sa posudzuje alebo predpovedá riziko toho, že fyzická osoba spácha trestný čin, výlučne na základe profilovania alebo posúdenia osobnostných vlastností a charakteristík.
185. V poslednej vete ustanovenia sa uvádza, že zákaz sa nevzťahuje na systémy AI používané na podporu ľudského posúdenia zapojenia osoby do trestnej činnosti, ktoré je už založené na objektívnych a overiteľných skutočnostiach priamo spojených s uvedenou činnosťou. Takéto systémy AI, ktoré nepatria do rozsahu pôsobnosti zákazu a ktoré majú používať orgány presadzovania práva alebo sa majú používať v ich mene alebo ktoré majú používať inštitúcie, orgány, úrady alebo agentúry Únie na podporu orgánov presadzovania práva na posudzovanie rizika, že fyzická osoba spácha alebo opätovne spácha trestný čin, a to nielen na základe profilovania alebo posúdenia osobnostných črt a charakteristických znakov alebo trestnej činnosti v minulosti, sa klasifikujú ako „vysokorizikové“ systémy AI [bod 6 písm. d) prílohy III k aktu o AI] a musia spĺňať všetky príslušné požiadavky a povinnosti podľa aktu o AI.

5.1. Odôvodnenie a ciele

186. V odôvodnení 42 aktu o AI sa vysvetľuje kontext a odôvodnenie zákazu v článku 5 ods. 1 písm. d) aktu o AI, konkrétne to, že fyzické osoby by sa mali posudzovať podľa ich skutočného správania, a nie podľa správania predpokladaného AI výlučne na základe ich profilovania, osobnostných črt alebo charakteristík.

5.2. Hlavné pojmy a zložky zákazu

V článku 5 ods. 1 písm. d) aktu o AI sa stanovuje

Zakazujú sa tieto praktiky využívajúce AI:

d) uvádzanie na trh, uvádzanie do prevádzky na tento konkrétny účel alebo používanie systému AI na posudzovanie rizík fyzických osôb s cieľom posúdiť alebo predvídať riziko toho, že fyzická osoba spácha trestný čin, a to výlučne na základe profilovania fyzickej osoby alebo posúdenia jej osobnostných vlastností a charakteristík; tento zákaz sa nevzťahuje na systémy AI používané na podporu ľudského posúdenia zapojenia osoby do trestnej činnosti, ktoré je už založené na objektívnych a overiteľných skutočnostiach priamo spojených s trestnou činnosťou;

187. Na uplatnenie zákazu podľa článku 5 ods. 1 písm. d) aktu o AI musí byť splnených niekoľko kumulatívnych podmienok:
- i) praktika musí predstavovať „uvádzanie na trh“, „uvádzanie do prevádzky na tento konkrétny účel“ alebo „používanie“ systému AI;
 - ii) systém AI musí vykonávať posudzovanie rizík s cieľom posúdiť alebo predvídať riziko toho, že fyzická osoba spácha trestný čin;
 - iii) posúdenie rizika alebo predvídanie musí byť založené výlučne na jednej z týchto možností alebo na oboch z nich:
 - a) profilovanie fyzickej osoby;
 - b) posúdenie osobnostných vlastností a charakteristík fyzickej osoby.

188. Aby sa zákaz uplatnil, musia byť súčasne splnené všetky tri podmienky. Prvá podmienka, t. j. uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému AI, už bola analyzovaná v oddiele 2.3. Zákaz sa preto vzťahuje na poskytovateľov systémov AI aj subjekty nasadzujúce systémy AI, pričom každý z nich v rámci svojich povinností nesmie takéto systémy AI uvádzať na trh, uvádzať do prevádzky alebo používať na tento konkrétny účel. Ďalšie dve podmienky uplatňovania zákazu sa analyzujú ďalej.

5.2.1. Posúdenie rizika alebo predvídanie pravdepodobnosti, že osoba spácha trestný čin

189. Posudzovanie rizík s cieľom posúdiť alebo predvídať riziko toho, že jednotlivец spácha trestný čin, sa často označuje ako individuálne „predvídanie trestnej činnosti“ alebo „predpovedanie trestnej činnosti“. Hoci neexistuje všeobecne dohodnuté vymedzenie pojmu „predvídanie trestnej činnosti“ alebo „predpovedanie trestnej činnosti“¹²⁹, tieto pojmy sa vo všeobecnosti vzťahujú na rôzne pokročilé technológie a analytické metódy AI aplikované na veľké množstvo často historických údajov (vrátane sociálno-ekonomických údajov, ale aj policajných záznamov atď.), ktoré sa v kombinácii s kriminologickými teóriami používajú na predpovedanie kriminality ako informačný základ pre stratégie polície a presadzovania práva a opatrenia na boj proti kriminalite, jej kontrolu a prevenciu.¹³⁰
190. Systémy AI na predvídanie trestnej činnosti identifikujú vzorce v historických údajoch, pričom spájajú ukazovatele s pravdepodobnosťou výskytu trestného činu a potom vytvárajú rizikové skóre ako prediktívne výstupy. Takéto systémy sa môžu používať napríklad na plánovanie policajných jednotiek, monitorovanie vysokorizikových situácií a vykonávanie kontrol osôb, v prípade ktorých sa predpokladá, že pravdepodobne spáchajú alebo opätovne spáchajú trestný čin. Takéto systémy poskytujú príležitosti pre orgány presadzovania práva, najmä pre tie, ktoré majú obmedzené zdroje, pričom zvyšujú efektívnosť a umožňujú proaktívny prístup k odhaľovaniu trestných činov, odrádzaniu od nich a ich predvídaníu¹³¹. Takéto využívanie historických údajov o spáchaných trestných činoch na predvídanie budúceho správania iných osôb však môže viesť k pretrvávaniu alebo dokonca posilňovaniu predsudkov a môže mať za následok „prehliadnutie“ rozhodujúcich individuálnych okolností, ak tieto okolnosti nie sú súčasťou dátového súboru alebo nie

¹²⁹ Pozri napríklad systémy uvedené v príručke Agentúry Európskej únie pre základné práva, ako sú systém informovanosti o trestnej činnosti (Criminality Awareness System, CAS) v Holandsku a systém Precobs v Nemecku a vo Švajčiarsku, príručka, 2018, s. 138. [Predchádzanie nezákonnému profilovaniu v súčasnosti a v budúcnosti: príručka: príručka](#), 2018, s. 138.

¹³⁰ Pozri Europol, *AI and policing: The benefits and challenges of artificial intelligence for law enforcement* (AI a vykonávanie policajných funkcií: prínosy a výzvy umelej inteligencie pre oblasť presadzovania práva), informačná správa inovačného laboratória Europolu, 23. septembra 2024. Pozri aj F. Yang, *Predictive Policing* (Prediktívne vykonávanie policajných funkcií), in: *Oxford Research Encyclopedia, Criminology and Criminal Justice*, Oxford University Press, 2019.

¹³¹ Napríklad OxRec (holandský probačný úrad, „Reclassering Nederland“), [Prediction of violent reoffending in prisoners and individuals on probation: a Dutch validation study \(OxRec\) – PMC \(nih.gov\)](#) [Predikcia násilnej recidívy u väzňov a osôb pri podmienenečnom prepustení: holandská validačná štúdia (OxRec) – PMC (nih.gov)].

sú zohľadnené v algoritmoch, na základe ktorých funguje konkrétny systém AI. Môže sa tým aj podkopať dôvera verejnosti v presadzovanie práva a justičný systém vo všeobecnosti¹³².

191. Takéto posúdenia rizika a predpovede sú v zásade zamerané na budúcnosť a týkajú sa budúcich trestných činov (ktoré ešte neboli spáchané) alebo trestných činov, pri ktorých na základe posúdenia existuje riziko spáchania v súčasnosti, a to aj v prípadoch pokusu alebo prípravných činností podniknutých na spáchanie trestného činu¹³³. Môžu byť vytvorené v ktoromkoľvek štádiu činnosti presadzovania práva, napríklad počas prevencie a odhaľovania trestných činov, ale aj počas vyšetrovania, trestného stíhania a výkonu trestných sankcií (vrátane prípadov, keď justičné orgány posudzujú riziko opätovného spáchania trestného činu, napríklad v súvislosti s rozhodovaním o uvalení vyšetrovacej väzby), ako aj ako súčasť plánu opätovného začlenenia jednotlivcov do spoločnosti po výkone trestu¹³⁴.
192. Zákazom v článku 5 ods. 1 písm. d) aktu o AI sa nezakazujú praktiky predvídania trestnej činnosti a posudzovania rizík ako také. Zákaz sa vzťahuje len na systémy AI, ktoré slúžia na posudzovanie rizík s cieľom posúdiť alebo predvídať riziko toho, že fyzická osoba spácha trestný čin, ak je splnená aj už uvedená tretia podmienka. Okrem toho, ako bolo uvedené, zákaz sa neuplatňuje v situáciách opísaných vo výslovnom vylúčení obsiahnutom v poslednej vete článku 5 ods. 1 písm. d) aktu o AI.

5.2.2. Výlučne na základe profilovania fyzickej osoby alebo posúdenia jej osobnostných vlastností a charakteristík

193. Treťou podmienkou na uplatnenie zákazu podľa článku 5 ods. 1 písm. d) aktu o AI je, že posudzovanie rizík s cieľom posúdiť alebo predvídať riziko toho, že fyzická osoba spácha trestný čin, musí byť výlučne na základe a) profilovania osoby alebo b) posúdenia jej osobnostných vlastností a charakteristík.
194. Zákaz v článku 5 ods. 1 písm. d) aktu o AI sa uplatňuje bez ohľadu na to, či systém AI profiluje alebo posudzuje osobnostné vlastnosti a charakteristiky len jednej fyzickej osoby alebo skupiny fyzických osôb súčasne, pretože cieľom zákazu je chrániť každú fyzickú osobu, v prípade ktorej sa predvída alebo posudzuje riziko spáchania trestného činu.

a) Profilovanie fyzickej osoby

195. Na rozdiel od článku 5 ods. 1 písm. c) aktu o AI sa v článku 5 ods. 1 písm. d) výslovne používa pojem „profilovanie“. V článku 3 bode 52 aktu o AI sa tento pojem vymedzuje

¹³² Pozri napríklad Agentúra Európskej únie pre základné práva (8. decembra 2022) *Bias in algorithms - Artificial intelligence and discrimination* (Skreslenie v algoritmoch – umelá inteligencia a diskriminácia) | Agentúra Európskej únie pre základné práva.

¹³³ V tejto súvislosti pozri odôvodnenie 42 aktu o AI, v ktorom sa v tejto súvislosti odkazuje na „pravdepodobnosť spáchania trestného činu takýmito osobami“ a „skutočný alebo potenciálny trestný čin“, pričom sa v znení používa prítomný, ale nie minulý čas.

¹³⁴ Ako príklad možno uviesť článok 24 ods. 4 smernice EÚ 2011/93 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, v ktorom sa vyžaduje, aby sa osoby, proti ktorým sa vedie trestné konanie alebo ktoré boli odsúdené za činy súvisiace so sexuálnym zneužívaním detí, podrobili posúdeniu nebezpečenstva recidívy, ktoré predstavujú.

odkazom na jeho vymedzenie v článku 4 bode 4 všeobecného nariadenia o ochrane osobných údajov¹³⁵. Pojem „profilovanie“ zahŕňa ako jeden zo základných prvkov cieľ, ktorým je „vyhodnotenie určitých osobných aspektov“.¹³⁶ V kontexte článku 5 ods. 1 písm. d) aktu o AI sa profilovanie vykonáva na účely posúdenia alebo predvídania rizika, že osoba spácha trestný čin.

196. V tejto súvislosti môže byť relevantný aj pojem tzv. skupinového profilovania¹³⁷. Tento pojem sa vzťahuje na vytvorenie a uplatnenie opisného profilu pre určitú skupinu, napríklad kategórie páchatel'ov trestných činov (napríklad teroristov, gangstrov atď.), vytvoreného na základe historických údajov o trestných činoch, ktoré predtým spáchali iné osoby. Tieto skupinové profily sa môžu neskôr použiť na posúdenie a predvídanie rizika, že ďalšie osoby spáchajú podobné trestné činy. Vždy, keď systém AI vykonáva predpovede a uplatňuje takýto (skupinový) profil na konkrétnu osobu, predstavuje to profilovanie osoby, a preto sa naň môže vzťahovať zákaz podľa článku 5 ods. 1 písm. d) aktu o AI.

b) Posúdenie osobnostných vlastností a charakteristík

197. Zákaz sa uplatňuje aj vtedy, ak sa posudzovanie rizík s cieľom posúdiť alebo predvídať riziko toho, že osoba spácha trestný čin, zakladá len na posúdení osobnostných vlastností a charakteristík osoby. Takéto posudzovanie alebo predpovedanie sa často zahŕňa do pojmu profilovanie, ale mohlo by sa považovať aj za jeho alternatívu, ak nie je možné stanoviť profilovanie ako sa vymedzuje v článku 4 bode 4 všeobecného nariadenia o ochrane údajov.
198. Ako sa uvádza v oddiele 4.2.1 písm. c), osobnostné vlastnosti a charakteristiky predstavujú širokú kategóriu charakteristík vzťahujúcich sa na konkrétnu fyzickú osobu, pre ktorú neexistuje všeobecne dohodnutá taxonómia. V odôvodnení 42 aktu o AI sa uvádzajú príklady osobnostných vlastností a charakteristík, ktoré možno posudzovať na účely predvídania rizika, že osoba spácha trestný čin, napríklad „štátna príslušnosť, miesto narodenia, miesto bydliska, počet detí, výška dlhu alebo typ vozidla“. Tento zoznam je len ilustratívny a nie je vyčerpávajúci.

¹³⁵ V článku 3 bode 4 smernice o presadzovaní práva, ktorý je relevantný z hľadiska zákazu v článku 5 ods. 1 písm. d) aktu o AI, sa profilovanie vymedzuje rovnako ako v článku 4 bode 4 všeobecného nariadenia o ochrane osobných údajov ako „akákoľvek forma automatizovaného spracúvania osobných údajov, ktoré pozostáva z použitia osobných údajov na vyhodnotenie určitých osobných aspektov týkajúcich sa fyzickej osoby, predovšetkým analýzy alebo predvídania aspektov dotknutej fyzickej osoby súvisiacich s výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom“. Rovnaké vymedzenie sa uvádza aj v článku 3 bode 5 nariadenia (EÚ) 2018/1725 o spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie (Ú. v. EÚ L 295, 21.11.2018, s. 39).

¹³⁶ Pozri aj dokument pracovnej skupiny pre ochranu údajov zriadenej podľa článku 29, *Usmernenia k automatizovanému individuálnemu rozhodovaniu a profilovaniu na účely nariadenia 2016/679*, WP251rev.01, 6. 2. 2018, ktorý schválil Európsky výbor pre ochranu údajov, s. 7. Pozri aj Agentúra pre základné práva, *Predchádzanie nezákonnému profilovaniu v súčasnosti a v budúcnosti: príručka*, 2018, s. 138.

¹³⁷ V súvislosti so skupinovým profilovaním pozri napríklad Agentúra pre základné práva, *Predchádzanie nezákonnému profilovaniu v súčasnosti a v budúcnosti: príručka*, príručka, 2018, s. 21.

c) „Výlučne“

199. V článku 5 ods. 1 písm. d) aktu o AI sa stanovuje, že posudzovanie rizík, na ktoré sa vzťahuje uvedené ustanovenie, je zakázané len vtedy, ak sa vykonáva „výlučne“ na základe profilovania osoby alebo posúdenia jej osobnostných vlastností a charakteristík. Z odôvodnenia 42 aktu o AI je zrejmé, že pojem „výlučne“ sa má vzťahovať na profilovanie alebo posudzovanie osobnostných vlastností a charakteristík.
200. Podmienka, že posudzovanie rizík musí byť založené „výlučne“ na profilovaní alebo posudzovaní osobnostných vlastností a charakteristík, nemusí byť v mnohých situáciách splnená.
201. Ako vyplýva z poslednej vety článku 5 ods. 1 písm. d) aktu o AI, takáto situácia nastáva v každom prípade vtedy, keď sa systém AI používa na podporu ľudského posúdenia zapojenia osoby do trestnej činnosti, ktoré je už založené na objektívnych a overiteľných skutočnostiach priamo spojených s trestnou činnosťou. Ako je zrejmé z odôvodnenia 42, v tejto súvislosti by sa malo uvažovať najmä, ale nie nevyhnutne výlučne, o situácii, keď už existuje odôvodnené podozrenie v súvislosti s dotknutou fyzickou osobou. Koniec koncov, v takýchto prípadoch sa zvyčajne uskutoční ľudské posúdenie, ktoré sa zvyčajne zakladá na príslušných objektívnych a overiteľných skutočnostiach.
202. Môžu však nastať aj iné situácie, ktoré sa musia vždy posudzovať od prípadu k prípadu. Na jednej strane sa použitím pojmu „výlučne“ ponecháva otvorená možnosť, aby sa pri posudzovaní rizika zohľadňovali rôzne ďalšie prvky, čo znamená, že by už nebolo založené len na profilovaní alebo posúdení osobnostných vlastností alebo charakteristík. Na druhej strane, aby sa zabránilo obchádzaniu zákazu a zabezpečila sa jeho účinnosť, všetky takéto ďalšie prvky budú musieť byť skutočné, podstatné a zmysluplné, aby nimi bolo možné odôvodniť záver, že zákaz sa neuplatňuje. Z výkladu zákazu v článku 5 ods. 1 písm. d) aktu o AI spolu s vylúčením obsiahnutým v jeho poslednej vete vyplýva, že takýto záver môže odôvodňovať najmä existencia určitých vopred zistených objektívnych a overiteľných skutočností.

Napríklad:

- Orgán presadzovania práva používa systém AI na predpovedanie trestnej činnosti v prípade trestných činov, ako je terorizmus, výlučne na základe veku, štátnej príslušnosti, adresy, typu auta a rodinného stavu jednotlivcov. V uvedenom systéme sa jednotlivci považujú za osoby, v prípade ktorých je väčšia pravdepodobnosť, že v budúcnosti spáchajú trestné činy, ktoré ešte nespáchali, výlučne na základe ich osobných charakteristík. Možno predpokladať, že takýto systém je zakázaný podľa článku 5 ods. 1 písm. d) aktu o AI.
- Vnútroštátne daňové orgány používajú prediktívny nástroj AI na preskúmanie všetkých daňových priznaní daňovníkov s cieľom predvídať potenciálne daňové trestné činy a identifikovať prípady, ktoré si vyžadujú ďalšie vyšetrovanie. Deje sa tak výlučne na základe profilu vytvoreného systémom AI, ktorý na posudzovanie využíva

osobnostné vlastnosti, ako sú dvojité štátne príslušnosť, miesto narodenia, počet detí, a nepriehľadné premenné, najmä odvodené informácie, ktoré sú prediktívne, a preto neobjektívne a ťažko overiteľné. Na takýto systém sa zvyčajne vzťahuje zákaz podľa článku 5 ods. 1 písm. d) aktu o AI, keďže neexistuje odôvodnené podozrenie o zapojení určitej osoby do trestnej činnosti ani iné objektívne a overiteľné skutočnosti, ktoré by ju s touto trestnou činnosťou spájali. Tento príklad patrí aj do rozsahu sociálneho bodovania zakázaného podľa článku 5 ods. 1 písm. c) aktu o AI a zahŕňa nepriaznivé zaobchádzanie s použitím údajov z nesúvisiacich sociálnych kontextov.

– Policajné oddelenie používa nástroj na posudzovanie rizík založený na AI na posúdenie rizika, že sa malé deti a dospievajúci v budúcnosti dopustia násilnej a majetkovej trestnej činnosti. Systém posudzuje deti na základe ich vzťahov s inými ľuďmi a ich predpokladanej úrovne rizika, čo znamená, že deti môžu byť považované za osoby s vyšším rizikom páchania trestnej činnosti len preto, že sú spojené s inou osobou, pri ktorej sa posúdením stanovilo vysoké riziko, napríklad so súrodencom alebo s priateľom. Aj úroveň rizika rodičov môže ovplyvniť úroveň rizika dieťaťa. Výsledkom posúdenia rizika je, že polícia tieto deti „registruje“ vo svojich systémoch, monitoruje ich prostredníctvom dodatočných kontrol a nahlasuje ich službám starostlivosti o mládež. Aj na takýto systém sa pravdepodobne vzťahuje zákaz podľa článku 5 ods. 1 písm. d) aktu o AI.

5.2.3. Vylúčenie systémov AI na podporu ľudského posúdenia založeného na objektívnych a overiteľných skutočnostiach priamo spojených s trestnou činnosťou

203. V článku 5 ods. 1 písm. d) aktu o AI sa v poslednej vete stanovuje, že zákaz sa nevzťahuje na systémy AI používané na podporu ľudského posúdenia zapojenia osoby do trestnej činnosti, ktoré je už založené na objektívnych a overiteľných skutočnostiach priamo spojených s trestnou činnosťou. Hoci, ako bolo uvedené, situácia opísaná v tomto výslovnom vylúčení nemusí byť nevyhnutne jedinou situáciou, v ktorej sa zákaz neuplatňuje, výslovným zahrnutím tejto situácie do tohto ustanovenia sa poskytuje právna istota tým, že sa vymedzuje rozsah pôsobnosti zákazu a jasne sa stanovuje, že zákaz sa v žiadnom prípade neuplatňuje, ak ide o túto situáciu.
204. Ak systém patrí do rozsahu pôsobnosti vylúčenia, a preto nie je zakázaný, klasifikuje sa ako vysokorizikový systém AI [ako sa uvádza v bode 6 písm. d) prílohy III k aktu o AI], ak je určený na použitie orgánmi presadzovania práva alebo v ich mene, a preto podlieha požiadavkám a zárukám vrátane ľudského dohľadu (článok 14 a článok 26 aktu o AI). Medzi tieto požiadavky patrí, že ľudský dohľad musí byť zverený osobám, ktoré majú potrebnú spôsobilosť, odbornú prípravu a právomoc a ktoré by mali byť schopné správne pochopiť schopnosti a obmedzenia systému AI, správne interpretovať jeho výstupy a riešiť riziko nadmernej dôvery v automatizáciu. Uvedené osoby by mali mať jasné postupy, odbornú prípravu a potrebnú spôsobilosť a právomoc na zmysluplné posudzovanie výstupov systému AI. V tomto konkrétnom prípade by sa ľudským posúdením malo zabezpečiť, aby sa pri každej predpovedi alebo posúdení

rizika, že osoba spácha trestný čin, s využitím AI vychádzalo z objektívnych a overiteľných skutočností spojených s trestnou činnosťou. Uvedené osoby by takisto mali zasiahnuť s cieľom vyhnúť sa negatívnym dôsledkom alebo rizikám, alebo zastaviť používanie systému, ak nefunguje tak, ako sa plánovalo.

205. Okrem toho bol pojem „ľudský zásah“ predmetom judikatúry Súdneho dvora Európskej únie, najmä v súvislosti s výlučne automatizovaným rozhodovaním v súvislosti s predvídaním rizika zapojenia cestujúcich v leteckej doprave do závažných trestných činov. Uvedená judikatúra môže byť relevantná aj z hľadiska uplatňovania pojmu „ľudské posúdenie“, ako sa používa v článku 5 ods. 1 písm. d) aktu o AI.

Vo veci *Ligue des droits humains*¹³⁸ Súdny dvor Európskej únie preskúmal zákonnosť používania pokročilého systému AI na systematické spracúvanie údajov zo záznamov o cestujúcich (PNR) v leteckej doprave s cieľom posúdiť pravdepodobnosť ich zapojenia do terorizmu a iných závažných trestných činov.

Súdny dvor Európskej únie vyložil pravidlo v smernici (EÚ) 2016/681 (ďalej len „smernica PNR“), ktorým sa zakazuje prijímať rozhodnutia, ktoré majú nepriaznivé právne účinky, len na základe automatizovaného spracúvania, a vyžadoval **individuálne ľudské posúdenie** a preskúmanie všetkých pozitívnych zhôd neautomatizovanými prostriedkami s cieľom identifikovať falošne pozitívne výsledky a zabezpečiť nediskriminačné výsledky.

Podľa Súdneho dvora Európskej únie sa toto ľudské posúdenie, ktorému musia podliehať všetky výsledky automatizovaného spracúvania údajov PNR, musí opierať o objektívne kritériá na posúdenie, či sa pozitívna zhoda týka osoby, ktorá by sa mohla v danom konkrétnom prípade zúčastňovať na teroristických trestných činoch alebo závažnej trestnej činnosti, a na zabezpečenie nediskriminačnej povahy automatizovaného spracúvania.

206. Pokiaľ ide o obsah vylúčenia, jedným z jeho ústredných prvkov je, že systém AI sa používa na podporu ľudského posúdenia, a nie že systém AI sám vykonáva posúdenie rizika, ako je to v situáciách, na ktoré sa vzťahuje zákaz. Aby sa však toto vylúčenie mohlo uplatniť, musí byť toto ľudské posúdenie navyše už založené na objektívnych a overiteľných skutočnostiach priamo spojených s trestnou činnosťou.

5.2.4. Rozsah, v akom môžu činnosti súkromných aktérov patriť do rozsahu pôsobnosti

207. Okrem orgánov presadzovania práva, ktoré sú v zásade hlavnými subjektmi nasadzujúcimi systémy AI na predvídanie trestnej činnosti, sa zákaz v článku 5 ods. 1 písm. d) aktu o AI môže v niektorých prípadoch vzťahovať aj na činnosti súkromných subjektov. Vyplýva to zo skutočnosti, že zákaz sa na základe svojho znenia nevzťahuje výlučne na orgány presadzovania práva. Navyše by sa zákaz dal inak ľahko obísť, čo by spochybnilo jeho účinnosť.

¹³⁸

Rozsudok Súdneho dvora z 21. júna 2022, *Ligue des droits humains*, C-817/19, ECLI:EU:C:2022:491.

208. Vzhľadom na to možno predpokladať, že zákaz sa uplatňuje najmä vtedy, keď sú súkromní aktéri na základe práva poverení vykonávať verejnú moc a verejné právomoci na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií¹³⁹. Súkromné subjekty môžu byť v jednotlivých prípadoch takisto výslovne požiadané, aby konali v mene orgánov presadzovania práva a vykonávali individuálne predpovede rizika trestnej činnosti. V týchto prípadoch by činnosti týchto súkromných aktérov mohli takisto patriť do rozsahu pôsobnosti zákazu, ak sú splnené príslušné podmienky a neuplatňuje sa vylúčenie.

Napríklad orgány presadzovania práva môžu požiadať súkromnú spoločnosť poskytujúcu pokročilý softvér na analýzu trestnej činnosti založený na AI, aby analyzovala veľké množstvo údajov z viacerých zdrojov a databáz, ako sú vnútroštátne registre, bankové transakcie, komunikačné údaje, geopriestorové údaje atď., s cieľom predvídať alebo posúdiť riziko, že sa osoby stanú potenciálnymi páchatelmi trestných činov v oblasti obchodovania s ľuďmi. Ak sú splnené všetky kritériá článku 5 ods. 1 písm. d), takýto prípad použitia by mohol byť zakázaný.

209. Okrem toho sa zákaz môže vzťahovať na súkromné subjekty, ktoré posudzujú alebo predvídať riziko, že osoba spácha trestný čin, ak je to objektívne potrebné na splnenie zákonnej povinnosti, ktorej tento súkromný subjekt podlieha, a to posudzovať alebo predvídať riziko, že osoby spáchajú konkrétne trestné činy (napríklad v prípade boja proti praniu špinavých peňazí, financovania terorizmu).

Bankové inštitúcie majú napríklad podľa právnych predpisov Únie v oblasti boja proti praniu špinavých peňazí¹⁴⁰ povinnosť preverovať a profilovať klientov z hľadiska trestných činov v oblasti prania špinavých peňazí. Ak banka na plnenie svojich povinností používa systém AI, malo by sa tak diať len na základe údajov uvedených v príslušnom právnom predpise, ktoré sú objektívne a overiteľné, aby sa zabezpečilo, že v prípade osôb klasifikovaných ako podozrivé je odôvodnené predpokladať, že pravdepodobne spáchajú trestné činy v oblasti prania špinavých peňazí. Na predpovede sa musí vzťahovať aj ľudské posúdenie a overenie v súlade s uvedenými právnymi predpismi¹⁴¹ s cieľom zabezpečiť presnosť a vhodnosť takýchto posúdení. Dodržiavaním uvedených právnych predpisov sa zabezpečí, že používanie systému AI na individuálne predvídanie trestnej činnosti na účely boja proti praniu špinavých peňazí nebude patriť do rozsahu pôsobnosti zákazu v článku 5 ods. 1 písm. d) aktu o AI.

210. Avšak vzhľadom na zameranie sa na posúdenie rizika týkajúceho sa konkrétne a výlučne spáchania trestných činov, ktoré vyplýva zo znenia zákazu, ako aj na účel zákazu, ako je vysvetlený v odôvodnení 42, ak súkromný subjekt profiluje zákazníkov na účely svojich bežných obchodných operácií a bezpečnosti alebo na ochranu svojich finančných záujmov (napríklad odhaľovanie finančných nezrovnalostí) bez toho, aby

¹³⁹ Pozri vymedzenie orgánov presadzovania práva v článku 3 bode 45 aktu o AI.

¹⁴⁰ Nariadenie (EÚ) 2024/1624 o boji proti praniu špinavých peňazí z 31. mája 2024.

¹⁴¹ Článok 20 nariadenia (EÚ) 2024/1624.

bolo cieľom posúdiť alebo predvídať riziko, že zákazník spácha konkrétny trestný čin, činnosti súkromných subjektov by sa nemali považovať za činnosti, ktoré patria do rozsahu pôsobnosti zákazu podľa článku 5 ods. 1 písm. d) aktu o AI.

211. Inými slovami, ak súkromné subjekty neboli na základe zákona poverené vykonávať určité osobitné úlohy v oblasti presadzovania práva, ak nekonajú v mene orgánov presadzovania práva alebo ak nepodliehajú osobitným zákonným povinnostiam, ako už bolo opísané, používanie systémov AI na posudzovanie rizík v rámci bežnej činnosti súkromných subjektov a s cieľom chrániť ich súkromné záujmy, pričom skutočnosť, že toto posudzovanie rizík sa môže týkať rizika spáchania trestných činov, je len čisto náhodná a druhotná okolnosť, sa nepovažuje za činnosť, na ktorú sa vzťahuje zákaz.

5.3. Vylúčenie z rozsahu pôsobnosti

5.3.1. Predpovede trestnej činnosti na základe polohy, geopriestorových informácií alebo miesta

212. Predpovede trestnej činnosti na základe polohy, geopriestorových informácií alebo miesta sú založené na mieste alebo polohe spáchania trestného činu alebo na pravdepodobnosti, že v týchto oblastiach bude spáchaný trestný čin. Takéto vykonávanie policajných funkcií v zásade nezahŕňa posudzovanie konkrétnej osoby. Preto uvedené predpovede nepatria do rozsahu pôsobnosti zákazu.

Príklady predpovedí trestnej činnosti na základe polohy, geopriestorových informácií alebo miesta

- Prediktívny policajný systém založený na AI poskytuje skóre vyjadrujúce pravdepodobnosť trestnej činnosti v rôznych oblastiach mesta na základe predchádzajúcej miery trestnej činnosti v jednotlivých oblastiach a ďalších podporných informácií, ako sú mapy ulíc, s cieľom upozorniť na zvýšené riziko konkrétnych druhov trestnej činnosti, napríklad vlámaní, trestných činov s použitím noža atď., a pomôcť orgánom presadzovania práva určiť, kde nasadiť menej alebo viac policajných hliadok/znížiť alebo posilniť prítomnosť polície na vykonávanie policajných funkcií v komunite s cieľom narušiť trestnú činnosť a odrádzať od nej.
- Colný orgán používa nástroje AI na analýzu rizík s cieľom predvídať pravdepodobnosť toho, že sa na určitom mieste nachádzajú drogy alebo nezákonný tovar, napríklad na základe známych trás nezákonného obchodovania.
- Policajné oddelenie používa systémy riadené AI na detekciu výstrelov a určenie miesta strelby v reálnom čase. Systém využíva akustické senzory v mestských oblastiach na identifikáciu zvukov strelby a trianguláciu ich polohy, čím poskytuje policajtom využiteľné údaje na pomoc pri odhaľovaní a vyšetrowaní trestných činov.

213. Nemusi však byť vždy zrejmé, ako odlíšiť systémy na predvídanie trestnej činnosti na základe polohy od individuálnych prediktívnych systémov, ktorými sa posudzuje riziko, že osoba spácha trestný čin. V rozsahu, v akom systém AI zabezpečuje prediktívne vykonávanie policajných funkcií na základe polohy a potom zohľadňuje rizikové skóre určitého miesta ako aspekt pri profilovaní osoby, by sa tento systém mal

považovať za systém zameraný na osoby a v zásade by sa naň mal vzťahovať článok 5 ods. 1 písm. d) aktu o AI, hoci môže patriť mimo rozsahu pôsobnosti zákazu z iných dôvodov.

Napríklad, ak sú informácie o polohe, geopriestorové informácie alebo informácie o mieste spojené s informáciami týkajúcimi sa jednotlivca (napríklad miesto bydliska určitej osoby) a systém AI by posúdil riziko, že táto osoba pravdepodobne spácha trestný čin, výlučne na základe profilovania dotknutej osoby, a to aj na základe jej bydliska, kde je vysoká kriminalita, tento systém by sa mal považovať za systém zameraný na osoby.

5.3.2. Systémy AI, ktoré podporujú ľudské posúdenie založené na objektívnych a overiteľných skutočnostiach spojených s trestnou činnosťou

214. V článku 5 ods. 1 písm. d) aktu o AI sa stanovuje, že zákaz sa nevzťahuje na systémy AI používané na podporu ľudského posúdenia zapojenia fyzickej osoby do trestnej činnosti, ktoré je už založené na objektívnych a overiteľných skutočnostiach priamo spojených s trestnou činnosťou. V takomto prípade by individuálne posúdenia a predpovede rizika trestného činu takisto neboli založené výlučne na profilovaní alebo hodnotení osobných charakteristík, a preto by neboli zakázané.

Medzi príklady systémov AI, ktoré z tohto dôvodu nepatria do rozsahu pôsobnosti zákazu, patrí:

- Použitie systému AI na profilovanie a kategorizáciu skutočného správania, ako je napríklad odôvodnene podozrivé nebezpečné správanie v dave, z ktorého je zrejmé, že niekto pripravuje trestný čin a pravdepodobne ho spácha, pričom existuje zmysluplné ľudské posúdenie klasifikácie využívajúcej AI. V tomto prípade sa posúdenie rizika, ktoré vykonáva človek s podporou AI, nezakladá výlučne na osobných vlastnostiach alebo profilovaní, ale na objektívnych a overiteľných skutočnostiach spojených s hroziacou trestnou činnosťou danej osoby, ktoré pred prijatím opatrení preskúmal človek.
- Polícia vyšetruje riziko možnej ozbrojenej lúpeže a podozrieva dve osoby. Existuje niekoľko overiteľných a objektívnych skutočností, na ktorých sa toto podozrenie zakladá, napríklad overiteľná účasť a komunikácia v chatových skupinách na temnom webe na nákup zbraní. Systém AI kombinujúci geopriestorové alebo miestne informácie na prediktívne vykonávanie policajných funkcií a informácie o automatizovanej registrácii evidenčných čísel vozidiel v súvislosti s vozidlami, ktoré patria podozrivým osobám, podporuje ľudské posúdenie pri vyšetrovaní na základe overiteľných a objektívnych skutočností priamo súvisiacich s konkrétnou trestnou činnosťou.
- Používanie systému AI, ktorým sa posudzuje riziko v súvislosti s predčasným prepustením väzňa. Profil dotknutej osoby alebo posúdenie jej osobnostných vlastností a charakteristík s využitím AI podporuje len ľudské posúdenie objektívnych

a overiteľných skutočností týkajúcich sa trestných činov, ktoré osoba spáchala v minulosti, a preukázaného správania relevantného pre reintegráciu.

- Sudca vykonáva vypočutie osoby obvinenej zo závažného trestného činu na účely vyšetrovacej väzby s cieľom posúdiť, či je možné uplatniť opatrenia, ktoré nezahŕňajú pozbavenie osobnej slobody. Rozhodnutie je založené na posúdení existencie závažných dôvodov na uvalenie vyšetrovacej väzby, ako je pravdepodobnosť, že podozrivá alebo obvinená osoba spácha ďalší trestný čin, ak na ňu nebude uvalená väzba, alebo že utečie či bude brániť riadnemu priebehu vyšetrovania. Na pomoc pri tomto procese sudca používa nástroj na posúdenie rizík využívajúci AI, ktorý je trénovaný na základe údajov, ktoré zahŕňajú trestnú činnosť páchanú jednotlivcami v podobných prípadoch v minulosti, ako aj faktorov, ako sú veková skupina, spoločenské správanie, príjem a postavenie v zamestnaní.
- Systém AI sa používa na podporu ľudského posúdenia zo strany zodpovedného pracovníka s cieľom posúdiť riziko, že osoba, ktorej bol uložený trest nezahŕňajúci odňatie slobody, poruší podmienky prepustenia alebo utečie, a to na základe trestnej činnosti v minulosti a objektívnych skutočností, ktoré sú dôvodom na podozrenie, ako sú dodržiavanie podmienok prepustenia, výsledky psychologického posúdenia a odporúčania iných služieb komunitnej starostlivosti, ktoré môže osoba využívať. Na základe uvedených informácií sa zodpovedný pracovník rozhodne, či sa zachová súčasný stav alebo či sa zmenia podmienky prepustenia.
- Systémy AI, ktoré colné orgány používajú na posúdenie rizika, že tovar vstupujúci do EÚ nie je v súlade s právnymi predpismi platnými na hranici (ktoré môžu zahŕňať napríklad zákaz dovozu nelegálnych drog, porušenie vývozných sankcií alebo inú nezákonnú činnosť), s cieľom identifikovať situácie, v ktorých by sa mala vykonať colná kontrola. Systém AI posudzuje objektívne a overiteľné informácie poskytnuté colným orgánom v súvislosti s tovarom a jeho dodávateľskými reťazcami (napríklad povaha a hodnota tovaru, číslo kontajnera, dopravné prostriedky umožňujúce ukrytie iného tovaru, predchádzajúce poznatky týkajúce sa súladu tovaru s konkrétnym opisom a pôvodom s požiadavkami na jeho dovoz do Únie alebo vývoz z Únie). V určitých prípadoch môže spracúvať aj informácie o predchádzajúcej účasti dovozcu alebo vývozcu na nezrovnalostiach súvisiacich s dovozom tovaru, o jeho príslušnosti k zločineckým organizáciám alebo o záznamoch v registri trestov za obchodovanie s drogami. Takéto systémy nepatria do rozsahu pôsobnosti zákazu, pretože akékoľvek predpovedanie pravdepodobnosti, že fyzická osoba bude zapojená do dovozu alebo vývozu nezákonného tovaru, nie je založené výlučne na profilovaní, ale na objektívnych a overiteľných informáciách týkajúcich sa tovaru a predchádzajúceho zapojenia dovozcu alebo vývozcu do trestnej činnosti a podlieha ľudskému preskúmaniu s cieľom určiť, či si situácia vyžaduje colnú kontrolu alebo opatrenie na zmiernenie rizika.

5.3.3. Systémy umelej inteligencie používané na predvídanie a posudzovanie trestnej činnosti vo vzťahu k právnickým osobám

215. Zákaz v článku 5 ods. 1 písm. d) aktu o AI sa vzťahuje len na individuálne predvídanie a posudzovanie rizík fyzických osôb, čím sa z neho zvyčajne vylučujú systémy na predvídanie trestnej činnosti, ktoré profilujú právnické osoby, ako sú spoločnosti alebo mimovládne organizácie.

Napríklad:

- Daňový alebo colný orgán používa systém AI na analýzu veľkého množstva údajov o transakciách a daňových priznaniach a colných údajov spoločností na posúdenie rizika, že spoločnosť spácha daňový alebo colný podvod, ktorý predstavuje trestný čin.
- Systémy AI, ktoré slúžia na pomoc colným orgánom pri identifikácii situácií, v ktorých by sa mal právnickým osobám vydať pokyn, aby nezasielali nezákonný tovar do EÚ.

216. Zároveň môžu existovať hraničné prípady, keď fyzická osoba koná prostredníctvom právnickej osoby ako „individuálny podnikateľ“ alebo ako nezávislý odborník (napríklad právnik). Za takýchto okolností sa zákaz uvedený v článku 5 ods. 1 písm. d) aktu o AI môže uplatniť za predpokladu, že sú splnené všetky podmienky, keďže systém AI profiluje konkrétnu fyzickú osobu a posudzuje alebo predvída riziko spáchania trestného činu touto osobou, aj keď sa to deje na účely súvisiace s komerčnou činnosťou, ktorú táto fyzická osoba vykonáva.

5.3.4. Systémy AI používané na individuálne predvídanie správnych deliktov

217. Zákaz v článku 5 ods. 1 písm. d) aktu o AI sa vzťahuje len na predvídanie trestných činov, čím sa z jeho pôsobnosti vylučujú správne delikty, ktorých stíhanie v zásade menej zasahuje do základných práv a slobôd ľudí.

Napríklad na orgán verejnej moci, ktorý využíva AI v rámci administratívneho zisťovania na posúdenie rizika, že potenciálni páchatelia spáchajú menej závažné delikty (ako sú drobné dopravné priestupky) alebo nezrovnalosti v daňových, obstarávacích alebo výdavkových procesoch, by sa nevzťahoval rozsah pôsobnosti zákazu v článku 5 ods. 1 písm. d) aktu o AI, a to ani v prípadoch, keď by sa v dôsledku administratívneho zisťovania a kontrol mohli získať informácie o možnom zapojení fyzických osôb do trestných činov.

218. To, či z dôvodu povahy určitého deliktu ide o správny delikt alebo trestný čin, môže závisieť od práva Únie alebo vnútroštátneho práva. V prípade deliktov, ktoré nie sú priamo upravené právom Únie, podlieha vnútroštátna kvalifikácia deliktu preskúmaniu zo strany Súdneho dvora Európskej únie, keďže „trestný čin“ je pojem, ktorý má v rámci práva EÚ autonómny význam a mal by sa v členských štátoch vykladať jednotne. Súdny dvor Európskej únie v inej súvislosti dospel k záveru, že kvalifikácia trestných činov členskými štátmi nie je v tejto súvislosti určujúca¹⁴². Relevantné kritériá

¹⁴²

Pozri napríklad rozsudok Súdneho dvora (veľká komora) zo 14. novembra 2013 v súvislosti s konaním o výkone rozhodnutia o peňažnej sankcii uloženej Mariánovi Balážovi, vec C-60/12, identifikátor ECLI: ECLI:EU:C:2013:733.

používané na posúdenie povahy deliktu (trestného činu alebo iného deliktu) možno nájsť v príslušnej judikatúre Súdneho dvora Európskej únie a Európskeho súdu pre ľudské práva¹⁴³.

5.4. Vzájomný vzťah s inými právnymi aktmi Únie

219. Vzájomný vzťah zákazu v článku 5 ods. 1 písm. d) aktu o AI so smernicou o presadzovaní práva a všeobecným nariadením o ochrane údajov je relevantný pri posudzovaní zákonnosti spracúvania osobných údajov podľa práva Únie v oblasti ochrany údajov, ako sú všeobecné nariadenie o ochrane údajov a smernica o presadzovaní práva. Konkrétne sa článkom 5 ods. 1 písm. d) aktu o AI ukladá orgánom presadzovania práva, iným orgánom verejnej moci a súkromným subjektom, ktoré patria do rozsahu pôsobnosti uvedeného zákazu, osobitný zákaz posudzovať alebo predvídať riziko toho, že fyzická osoba spácha trestný čin, výlučne na základe profilovania fyzickej osoby alebo posúdenia jej osobnostných vlastností a charakteristík. Pokiaľ ide o smernicu o presadzovaní práva, článkom 5 ods. 1 písm. d) aktu o AI nie je dotknutý článok 11 ods. 3 smernice o presadzovaní práva, ktorým sa zakazuje profilovanie vedúce k (priamej alebo nepriamej) diskriminácii.
220. Relevantný je aj vzájomný vzťah zákazu v článku 5 ods. 1 písm. d) aktu o AI a smernice (EÚ) 2016/343 o prezumpcii nevinu, keďže oba akty sa týkajú – priamo v prípade uvedenej smernice a nepriamo v prípade aktu o AI (pozri jeho odôvodnenie 42) – základného práva byť považovaný za nevinného, kým vina nebola preukázaná zákonným spôsobom¹⁴⁴. Zatiaľ čo uvedená smernica sa uplatňuje od okamihu, keď je osoba podozrivá alebo obvinená zo spáchania trestného činu¹⁴⁵, akt o AI má širší rozsah uplatňovania a uplatňuje sa už v štádiu predvídania a predchádzania trestnej činnosti pred začatím formálneho vyšetrovania trestného činu voči konkrétnej osobe a aj v prípadoch, keď takéto predvídanie a posudzovanie rizík

¹⁴³

Podľa judikatúry Súdneho dvora Európskej únie prináleží vnútroštátnym súdom určiť, či sa „netrestná sankcia“, môže považovať za „trestnú“ vzhľadom na tzv. kritériá Engel, pozri: Európsky súd pre ľudské práva, rozsudok z 8. júna 1976, Engel a iní proti Holandsku, sťažnosti č. 5100/71, 5101/71, 5102/71, 5354/72 a 5370/72, CE:ECHR:1976:0608JUD000510071, bod 82. Tieto kritériá, ktoré pôvodne vypracoval Európsky súd pre ľudské práva a následne schválil Súdny dvor Európskej únie, sú alternatívne a nie kumulatívne. Pri skúmaní, či má sankcia trestný charakter, by mal príslušný vnútroštátny súd posúdiť: 1. klasifikáciu príslušných ustanovení podľa vnútroštátneho práva, 2. samotnú povahu porušenia a 3. stupeň príslosti sankcie. Pri posudzovaní deliktu sa okrem iného berie do úvahy, či konanie začal verejný subjekt so zákonnými právomocami na presadzovanie práva; či má právna norma represívny alebo odstrašujúci účel; či sa právna norma snaží chrániť všeobecné záujmy spoločnosti, ktoré sú zvyčajne chránené trestným právom; či uloženie akejkoľvek sankcie závisí od zistenia viny. Pokiaľ ide o prísnosť sankcie, relevantným odkazom je maximálna možná sankcia stanovená vo vnútroštátnom práve. Uvedené kritériá sú alternatívne a nemusia byť kumulatívne. Pozri Európsky súd pre ľudské práva, *Guide on Article 6 of the European Convention on Human Rights, Right to a fair trial (criminal limb)* [Príručka k článku 6 Európskeho dohovoru o ľudských právach, Právo na spravodlivé súdne konanie (trestnoprávny aspekt)], aktualizované 29. februára 2024. Pozri aj Súdny dvor Európskej únie, rozsudok z 5. júna 2012, Bonda, C-489/10, EU:C:2012:319, body 37 a nasl.; Súdny dvor Európskej únie, rozsudok z 26. februára 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, bod 35.

¹⁴⁴

Prezumpcia nevinu je základné právo zakotvené v článku 48 Charty základných práv EÚ.

¹⁴⁵

Ako uviedol Súdny dvor Európskej únie, na uplatnenie smernice sa nevyžaduje, aby príslušné orgány túto osobu informovali o jej postavení podozrivej/obvinenej osoby.

vykonávajú súkromní aktéri, ktorí patria do rozsahu pôsobnosti článku 5 ods. 1 písm. d) aktu o AI, a nie príslušné orgány presadzovania práva vrátane justičných orgánov.

221. Aj v prípadoch, keď sa zákaz uvedený v článku 5 ods. 1 písm. d) aktu o AI neuplatňuje, je dôležité zdôrazniť, že platné právo Únie a vnútroštátne právo sa naďalej uplatňuje v plnom rozsahu, a to vrátane práva v oblasti ochrany údajov, trestného práva procesného a policajného práva a záruk, ktoré môžu ďalej obmedzovať používania systémov AI na individuálne predvídanie trestnej činnosti alebo ukladať v súvislosti s nimi dodatočné podmienky.

6. ČLÁNOK 5 ODS. 1 PÍSM. E) AKTU O AI – NECIELENÁ EXTRAKCIA PODÔB TVÁRE

222. V článku 5 ods. 1 písm. e) aktu o AI sa zakazuje uvádzanie na trh, uvádzanie do prevádzky na tento konkrétny účel alebo používanie systémov AI, ktoré vytvárajú alebo rozširujú databázy na rozpoznávanie tváre prostredníctvom necielenej extrakcie podôb tváre z internetu alebo zo záznamov CCTV.

6.1. Odôvodnenie a ciele

223. Necielenou extrakciou podôb tváre z internetu alebo zo záznamov CCTV sa vážne zasahuje do práva jednotlivcov na súkromie a ochranu údajov a týmto jednotlivcom sa upiera právo zostať v anonymite. V odôvodnení 43 aktu o AI sa preto zákaz stanovený v článku 5 ods. 1 písm. e) aktu o AI odôvodňuje na základe „pocitu hromadného sledovania“ a rizík „hrubého porušenia základných práv vrátane práva na súkromie“.

6.2. Hlavné pojmy a zložky zákazu

V článku 5 ods. 1 písm. e) aktu o AI sa stanovuje

Zakazujú sa tieto praktiky využívajúce AI:

e) uvádzanie na trh, uvádzanie do prevádzky na tento konkrétny účel alebo používanie systémov AI, ktoré vytvárajú alebo rozširujú databázy na rozpoznávanie tváre prostredníctvom necielenej extrakcie podôb tváre z internetu alebo zo záznamov CCTV;

224. Na uplatnenie zákazu podľa článku 5 ods. 1 písm. e) aktu o AI musí byť splnených niekoľko kumulatívnych podmienok:
- i) praktika musí predstavovať „uvádzanie na trh“, „uvádzanie do prevádzky na tento konkrétny účel“ alebo „používanie“ systému AI;
 - ii) na účely vytvárania alebo rozširovania databáz na rozpoznávanie tváre;
 - iii) prostriedkami na naplnenie databázy sú nástroje AI na necielenú extrakciu a
 - iv) podoby tváre pochádzajú z internetu alebo zo záznamov CCTV.
225. Aby sa zákaz uplatnil, musia byť súčasne splnené všetky štyri podmienky. Prvý prvok založený na uvádzaní na trh, uvádzaní do prevádzky alebo používaní systému AI už bola analyzovaný v oddiele 2.3. Zákaz sa preto vzťahuje na poskytovateľov systémov

AI aj subjekty nasadzujúce systémy AI, pričom každý z nich v rámci svojich povinností nesmie takéto systémy AI uvádzať na trh, uvádzať do prevádzky alebo používať. Konkrétne kritériá týkajúce sa zákazu necielenej extrakcie sa ďalej opisujú a analyzujú ďalej. Zákaz sa vzťahuje na nástroje na extrakciu, ktoré sa uvádzajú na trh alebo do prevádzky „na tento konkrétny účel“ necielenej extrakcie podôb tváre z internetu alebo zo záznamov CCTV. Z toho vyplýva, že zákaz sa neuplatňuje na akýkoľvek nástroj na extrakciu, pomocou ktorého možno vytvoriť alebo rozšíriť databázu na rozpoznávanie tvárí, ale len na nástroje na necielenú extrakciu.

6.2.1. Databázy na rozpoznávanie tváre

226. Zákaz v článku 5 ods. 1 písm. e) aktu o AI sa vzťahuje na systémy AI, ktoré slúžia na vytváranie alebo rozširovanie databáz na rozpoznávanie tváre. Pojem „databáza“ by sa mal v tejto súvislosti chápať ako akákoľvek zbierka údajov alebo informácií, ktorá je osobitne usporiadaná na ich rýchle vyhľadávanie a získavanie pomocou počítača. Databáza na rozpoznávanie tváre je schopná priradiť ľudskú tvár z digitálneho obrazu alebo snímky videozáznamu k databáze tvárí, porovnať ju s podobami tvárí v databáze a určiť, či medzi nimi existuje pravdepodobná zhoda. Takáto databáza na rozpoznávanie tváre môže byť dočasná, centralizovaná alebo decentralizovaná. Na základe článku 5 ods. 1 písm. e) sa nevyžaduje, aby jediným účelom databázy bolo jej použitie na rozpoznávanie tváre; postačuje, aby sa databáza dala použiť na rozpoznávanie tváre.

6.2.2. Prostredníctvom necielenej extrakcie podôb tváre

227. „Extrakcia“ sa zvyčajne vzťahuje na používanie vyhľadávacích robotov, botov alebo iných prostriedkov na automatické získavanie údajov alebo obsahu z rôznych zdrojov vrátane CCTV, webových sídiel alebo sociálnych médií. Tieto nástroje sú softvérom naprogramovaným na prehľadávanie databáz, získavanie informácií a ich využívanie na iný účel.
228. „Necielená“ sa vzťahuje na techniku, ktorá funguje ako „vysávač“ tým, že absorbuje čo najviac údajov a informácií bez cielenia na konkrétne a individuálne zamýšľaný (zamýšľané) subjekt (subjekty) extrakcie. Pri extrakcii sa údaje alebo obsah zbierajú bez rozlišovania. Pojem „necielená“ teda znamená, že je bez špecifického zamerania na konkrétneho jednotlivca alebo skupinu jednotlivcov. Rešpektovanie internetových protokolov k odmietnutiu súhlasu, ako je robot.txt, nemá vplyv na necielenú povahu extrakcie.
229. Ak sa nástroju na extrakciu zadá pokyn zhromažďovať obrázky alebo videá obsahujúce ľudské tváre len konkrétnych osôb alebo vopred vymedzenej skupiny osôb, potom sa extrakcia stáva cielenou, napríklad s cieľom nájsť jedného konkrétneho zločinca alebo identifikovať skupinu obetí. Na takúto extrakciu sa nevzťahuje zákaz v článku 5 ods. 1 písm. e) aktu o AI.
230. Zákaz sa nevzťahuje napríklad na cielené zhromažďovanie obrázkov so zameraním na určitú triedu obetí pomocou vyhľadávacích robotov na vyhľadávanie obrázkov obetí, ktoré obchodníci s ľuďmi zverejňujú/propagujú na sociálnych sieťach. Necielená

extrakcia by sa mala vykladať spôsobom, ktorý neumožňuje obchádzanie zákazu. Na extrakciu z internetu alebo zo záznamov CCTV na účely postupného vytvorenia, pričom sa zakaždým vyberú konkrétne skupiny osôb alebo iné kritériá, by sa mal vzťahovať zákaz podľa článku 5 ods. 1 písm. e) aktu o AI, ak je konečný výsledok funkčne rovnaký ako to, keď sa od začiatku vykonáva necielená extrakcia.

231. Ak systémy kombinujú ciele vyhľadávanie obrázkov alebo videí s necieľeným vyhľadávaním, necielená extrakcia je zakázaná.

6.2.3. Z internetu alebo zo záznamov CCTV

232. Aby sa zákaz uvedený v článku 5 ods. 1 písm. e) aktu o AI uplatnil, zdrojom podôb tváre musí byť buď internet, alebo záznamy CCTV. Pokiaľ ide o internet, skutočnosť, že osoba zverejnila svoje podoby tváre na platforme sociálnych médií, neznamena, že dala súhlas na zaradenie týchto snímok do databázy na rozpoznávanie tváre. Medzi príklady extrakcie podôb tváre zo záznamov CCTV patria podoby tváre získané z bezpečnostných kamier prevádzkovaných na miestach, ako sú letiská, ulice, parky atď.

Príklad:

Softvérová spoločnosť na rozpoznávanie tvárí zhromažďuje obrázky tvárí. Fotografie, ktoré spoločnosť uchováva, boli získané zo sociálnych médií (napríklad Facebook, YouTube, Twitter, Venmo) pomocou „automatizovaného nástroja na extrakciu obrázkov“, ktorý prehľadáva internet a rozpoznáva obrázky obsahujúce ľudské tváre. Zhromažďuje tieto obrázky so všetkými súvisiacimi informáciami [ako sú zdroj obrázku (URL), geolokalizácia a niekedy aj mená osôb]. Z obrázkov sa potom extrahujú črty tváre a transformujú sa na matematické vyjadrenia, ktoré sa na účely indexovania a budúceho porovnávania spracujú pomocou hašovacích funkcií. Keď používateľ nahra obrázok osoby do systému AI, tento systém určí, či sa tento obrázok zhoduje s tvárou v databáze. Nahraný obrázok prejde rovnakou matematickou transformáciou ako extrahované obrázky.

233. Ak systém AI prijme obrázok osoby a vyhľadá na internete zhodu s touto tvárou, t. j. použije „internetové vyhľadávače obrázkov využívajúce reverzné inžinierstvo“, bude sa to považovať za cieľnú extrakciu. Okrem toho je otázne, či by sa tieto zhody objavili v „databáze“.

6.3. Vylúčenie z rozsahu pôsobnosti

234. Zákaz v článku 5 ods. 1 písm. e) aktu o AI sa nevzťahuje na necieľnú extrakciu biometrických údajov iných ako podoby tváre (napríklad hlasové vzorky). Zákaz sa nevzťahuje ani na prípady, keď sa na extrakcii nepodieľajú žiadne systémy AI. Do rozsahu pôsobnosti nepatria ani databázy podôb tváre, ktoré sa nepoužívajú na rozpoznávanie osôb, ako napríklad databázy podôb tváre používané na účely tréningu alebo testovania modelov AI, v ktorých nedochádza k identifikácii osôb.
235. Zákaz v článku 5 ods. 1 písm. e) aktu o AI sa nevzťahuje na systémy AI, ktoré získavajú veľké množstvo podôb tváre z internetu na vytváranie modelov AI, ktoré

vytvárajú nové obrázky fiktívnych osôb, pretože takéto systémy by neviedli k rozpoznaní skutočných osôb. Na takéto systémy AI by sa mohli vzťahovať požiadavky na transparentnosť podľa článku 50 aktu o AI.

236. Zákaz v článku 5 ods. 1 písm. e) aktu o AI sa vzťahuje na systémy AI, ktoré slúžia na vytváranie alebo rozširovanie databáz na rozpoznávanie tváre. Pokiaľ ide o existujúce databázy tváří vytvorené pred začatím uplatňovania zákazu, ktoré sa ďalej nerozširujú prostredníctvom necielenej extrakcie využívajúcej AI, tieto databázy a ich používanie musia byť v súlade s platnými pravidlami Únie v oblasti ochrany údajov.
237. Zákaz v článku 5 ods. 1 písm. e) aktu o AI je zameraný na vytváranie alebo rozširovanie databáz na rozpoznávanie tváre. Konkrétny úkon biometrickej identifikácie podlieha osobitným pravidlám v akte o AI a iných príslušných právnych predpisoch Únie.

6.4. Vzájomný vzťah s inými právnymi aktmi Únie

238. Vo vzťahu k právu Únie v oblasti ochrany údajov by necielená extrakcia z internetu alebo zo záznamov CCTV na budovanie alebo rozširovanie databáz na rozpoznávanie tváre, t. j. spracúvanie osobných údajov (zhromažďovanie údajov a používanie databáz), bola nezákonná a nebolo by možné sa odvolávať na žiadny právny základ podľa všeobecného nariadenia o ochrane údajov, nariadenia, ktorým sa stanovujú pravidlá ochrany údajov pre inštitúcie, orgány, úrady a agentúry EÚ, a smernice o presadzovaní práva.

7. ČLÁNOK 5 ODS. 1 PÍSM. F) AKTU O AI – ROZPOZNÁVANIE EMÓCIÍ

239. V článku 5 ods. 1 písm. f) aktu o AI sa zakazuje, aby systémy AI odvodzovali emócie fyzickej osoby v oblasti pracoviska a vzdelávacích inštitúcií s výnimkou prípadov, keď je používanie systému AI zamýšľané zo zdravotných alebo bezpečnostných dôvodov. Systémy na rozpoznávanie emócií, na ktoré sa nevzťahuje zákaz, sa považujú za vysokorizikové podľa bodu 1 písm. c) prílohy III k aktu o AI. V článku 50 ods. 3 aktu o AI sa stanovujú určité požiadavky na transparentnosť pri používaní systémov na rozpoznávanie emócií.

7.1. Odôvodnenie a ciele

240. Technológia rozpoznávania emócií sa rýchlo vyvíja a zahŕňa rôzne technológie a operácie spracovania na detekciu, zhromažďovanie, analýzu, kategorizáciu, reakciu, interakciu v súvislosti s emóciami a učenie sa emócií od osôb. Takáto technológia sa označuje aj ako „afektívna technológia“. Rozpoznávanie emócií možno využiť vo viacerých oblastiach a doménach v širokej škále aplikácií¹⁴⁶, napríklad na analýzu

¹⁴⁶

Využívanie emócií na ekonomické účely sa označuje aj ako „emócionomika“.

správania zákazníkov¹⁴⁷ a cielenú reklamu a neuromarketing¹⁴⁸; v zábavnom priemysle, napríklad na poskytovanie personalizovaných odporúčaní alebo na predpovedanie reakcií na filmy; v medicíne a zdravotníctve, napríklad na odhaľovanie depresie, na prevenciu samovrážd alebo na zisťovanie autizmu, vo vzdelávaní, napríklad na monitorovanie pozornosti alebo interakcie učiacich sa (žiakov a študentov v rôznych vekových kategóriách); v zamestnaní, napríklad ako doplnok náborového procesu, na monitorovanie emócií alebo nudy zamestnancov, ale aj v rámci aplikácií na zlepšenie podmienok na pracovisku na „zvýšenie spokojnosti pracovníkov“¹⁴⁹; na účely presadzovania práva a verejnej bezpečnosti, napríklad pomocou detektorov lži alebo kontroly emócií na veľkých podujatiach a na mnohé ďalšie účely.

241. Účinnosť alebo presnosť rozpoznávania emócií je často predmetom pochybností¹⁵⁰. V odôvodnení 44 aktu o AI sa vysvetľuje, že existujú „vážne obavy v súvislosti s vedeckým základom systémov AI, ktorých cieľom je identifikovať alebo odvodzovať emócie, najmä preto, že prejav emócií sa v jednotlivých kultúrach a situáciách a dokonca aj v prípade jedného jednotlivca značne líši. Medzi hlavné nedostatky takýchto systémov patrí obmedzená spoľahlivosť, nedostatočná špecifickosť a obmedzená možnosť zovšeobecnenia.“ Ďalej sa v ňom vysvetľuje, že rozpoznávanie emócií môže viesť k „diskriminačným výsledkom a môžu zasahovať do práv a slobôd dotknutých osôb“, najmä práva na súkromie, ľudskú dôstojnosť a slobodu myslenia. To zohráva dôležitú úlohu v asymetrických vzťahoch najmä v kontexte pracoviska a vzdelávacích a školiacich inštitúcií, kde sú pracovníci aj študenti v obzvlášť zraniteľnom postavení. Rozpoznávanie emócií v špecifických kontextoch použitia, ako sú napríklad bezpečnosť a lekárska starostlivosť (napríklad liečba a diagnostika), prináša zároveň výhody¹⁵¹.

7.2. Hlavné pojmy a zložky zákazu

- ¹⁴⁷ Pozri napríklad G. Mangano, A. Ferrari, C. Rafale, E. Vezzetti, F. Marcolin, [Willingness of sharing facial data for emotion recognition: a case study in the insurance market](#) (Ochota zdieľať údaje o podobe tváre na rozpoznávanie emócií: prípadová štúdia na poistnom trhu), in: *AI & Society*, Londýn, Springer, 2023.
- ¹⁴⁸ Pozri N. Lee, A. J. Broderick, & L. Chamberlain, [What is 'neuromarketing'? A discussion and agenda for future research](#) (Čo je to „neuromarketing“? Diskusia a program budúceho výskumu), in: *International Journal of Psychophysiology*, 63(2), 2007, s. 199 – 204, v ktorom sa neuromarketing ako oblasť štúdií vymedzuje ako „uplatňovanie neurovedeckých metód na analýzu a pochopenie ľudského správania vo vzťahu k trhom a marketingovým interakciám“ (s. 200).
- ¹⁴⁹ Pozri E. Ackerman, & E. Strickland, *Are you Ready for Workplace Brain Scanning? Extracting and using brain data will make workers happier and more productive, backers say* (Ste pripravení na snímanie mozgu na pracovisku? Podporovatelia tvrdia, že vďaka extrakcii a používaniu údajov o mozgu budú pracovníci šťastnejší a produktívnejší), *IEEE Spectrum*, 19. novembra 2022, <https://spectrum.ieee.org/neurotech-workplace-innereye-emoativ>, kde autori vysvetľujú, že „snímače zisťujú elektrickú aktivitu v rôznych oblastiach mozgu, pričom vzorce tejto aktivity môžu vo všeobecnosti korelovať s rôznymi pocitmi alebo fyziologickými reakciami, ako sú stres, sústredenie alebo reakcia na vonkajšie podnety“.
- ¹⁵⁰ Pozri napríklad J. Stanley, [Experts Say 'Emotion Recognition' lacks Scientific Foundation](#) („Rozpoznávanie emócií“ podľa odborníkov nemá vedecký základ), 18. 7. 2019, ACLU, s odkazom na štúdiu L. Feldmana Barretta a kol., [Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements](#) (Prehodnotenie prejavov emócií: výzvy pri odvodzovaní emócií z ľudských pohybov tváre), *Psychological Science in the Public Interest*, 2019, s. iii-90.
- ¹⁵¹ Pozri napríklad R. El Kaliouby a R. Picard a S. Baron-Cohen, [Affective Computing and Autism](#) (Počítačová analýza emócií a autizmus), *Annals New York Academy of Sciences*, 2007, s. 228 – 248.

V článku 5 ods. 1 písm. f) aktu o AI sa stanovuje:

Zakazujú sa tieto praktiky využívajúce AI:

f) uvádzanie na trh, uvádzanie do prevádzky na tento konkrétny účel alebo používanie systémov AI na odvodzovanie emócií fyzickej osoby v oblasti pracoviska a vzdelávacích inštitúcií s výnimkou prípadov, keď je používanie systému AI určené na uvedenie do prevádzky alebo na trh zo zdravotných alebo bezpečnostných dôvodov;

242. Na uplatnenie zákazu podľa článku 5 ods. 1 písm. f) aktu o AI musí byť splnených niekoľko kumulatívnych podmienok:
- i) praktika musí predstavovať „uvádzanie na trh“, „uvádzanie do prevádzky na tento konkrétny účel“ alebo „používanie“ systému AI;
 - ii) systém AI na odvodzovanie emócií¹⁵²;
 - iii) v oblasti pracoviska alebo vzdelávacích a školiacich inštitúcií a
 - iv) zo zákazu sú vylúčené systémy AI zamýšľané zo zdravotných alebo bezpečnostných dôvodov.
243. Aby sa zákaz uplatnil, musia byť súčasne splnené všetky štyri podmienky. Prvý prvok, t. j. uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému AI, už bol analyzovaný v oddiele 2.3. Zákaz sa preto vzťahuje na poskytovateľov systémov AI aj subjekty nasadzujúce systémy AI, pričom každý z nich v rámci svojich povinností nesmie takéto systémy AI uvádzať na trh, uvádzať do prevádzky alebo používať. Ďalšie podmienky týkajúce sa zákazu sa ďalej opisujú a analyzujú ďalej.

7.2.1. Systémy AI na odvodzovanie emócií

a) Systémy AI na odvodzovanie emócií v porovnaní so systémami na rozpoznávanie emócií

244. V článku 3 bode 39 aktu o AI sa „systémy na rozpoznávanie emócií“ vymedzujú ako systémy AI na účely identifikácie a odvodenia emócií alebo úmyslov fyzických osôb na základe ich biometrických údajov. Zákaz v článku 5 ods. 1 písm. f) aktu o AI sa nevzťahuje na „systémy na rozpoznávanie emócií“, ale len na „systémy AI na odvodzovanie emócií fyzickej osoby“. V odôvodnení 44 sa ďalej objasňuje, že tento zákaz sa vzťahuje na systémy AI, ktorých cieľom je „identifikovať alebo odvodzovať emócie“.
245. Odvodzovanie vo všeobecnosti zahŕňa ako nevyhnutný predpoklad identifikáciu, preto zákaz by sa mal chápať tak, že zahŕňa systémy AI, ktoré identifikujú alebo odvodzujú emócie alebo úmysly¹⁵³. Z dôvodu konzistentnosti je takisto dôležité vykladať zákaz v článku 5 ods. 1 písm. f) aktu o AI tak, že má podobný rozsah pôsobnosti ako pravidlá uplatniteľné na iné systémy na rozpoznávanie emócií [bod 1 písm. c) prílohy III k aktu o AI a článok 50 aktu o AI], a obmedziť ho na odvodzovanie založené na

¹⁵² Alebo technológia schopná odvodiť emócie (t. j. pri uvádzaní na trh).
¹⁵³ Pozri aj odôvodnenie 18 aktu o AI.

biometrických údajoch osoby. Vymedzenie systémov na rozpoznávanie emócií v článku 3 bode 39 aktu o AI by sa preto malo považovať za relevantné vo vzťahu k článku 5 ods. 1 písm. f) aktu o AI.

b) Identifikácia a odvodzovanie emócií alebo úmyslov

246. „Identifikácia“ nastáva vtedy, keď spracovanie biometrických údajov (napríklad hlasu alebo výrazu tváre) fyzickej osoby umožňuje priamo porovnať a identifikovať emóciu s emóciou, ktorá bola predtým naprogramovaná v systéme na rozpoznávanie emócií. „Odvodzovanie“ sa uskutočňuje vyvodením informácií, ktoré sú generované analytickými a inými procesmi, samotným systémom. V takomto prípade sa informácie o emócií nezakladajú výlučne na údajoch zhromaždených o fyzickej osobe, ale sú odvodené z iných údajov vrátane prístupov strojového učenia, ktoré sa z údajov učia, ako zistiť emócie.¹⁵⁴

c) Emócie

247. Na účely článku 5 ods. 1 písm. f) aktu o AI by sa pojem emócie alebo úmysly mal chápať v širokom zmysle a nemal by sa vykladať reštriktívne. V odôvodnení 18 aktu o AI sa uvádzajú niektoré podrobnosti a vymenúvajú sa emócie, „ako sú šťastie, smútok, hnev, prekvapenie, znechutenie, rozpaky, vzrušenie, hanba, pohrdanie, spokojnosť a zábava.“ Tieto príklady nie sú vyčerpávajúce.
248. Zákaz by sa nemal obchádzať odvolávaním sa na postoje a zahŕňa prípady, keď systém AI na základe biometrických údajov zistí, že osoba prejavuje napríklad nahnevaný postoj.
249. V odôvodnení 18 aktu o AI sa objasňuje, že emócie ani úmysly nezahŕňajú „fyzické stavy, ako je bolesť alebo únava vrátane napríklad systémov používaných na zisťovanie stavu únavy profesionálnych pilotov alebo vodičov na účely prevencie nehôd.“ Ďalej sa v ňom objasňuje, že systémy na rozpoznávanie emócií nezahŕňajú „samotné zisťovanie ľahko viditeľných výrazov, gest alebo pohybov, pokiaľ sa nepoužívajú na identifikáciu alebo odvodenie emócií“, čo by sa malo chápať tak, že sa to vzťahuje aj na článok 5 ods. 1 písm. f) aktu o AI. Tieto výrazy môžu byť základnými výrazmi tváre, ako je zamračené alebo úsmev, alebo gestami, ako je pohyb rúk, ramien alebo hlavy, alebo charakteristickými znakmi hlasu osoby, ako je zdvihnutý hlas alebo šepot. Ak sa však tieto ľahko viditeľné výrazy alebo gestá používajú na identifikáciu alebo odvodenie emócií alebo úmyslov, zákaz sa na ne vzťahuje.

Napríklad:

- Spozorovanie, že sa osoba usmieva, nepredstavuje rozpoznávanie emócií.
- Identifikácia toho, či je osoba chorá, nepredstavuje rozpoznávanie emócií.

¹⁵⁴

Pozri odôvodnenie 12 aktu o AI. Odvodené údaje sú preto často aj výsledkom analytických procesov založených na pravdepodobnosti (veľké dáta), ktorých cieľom je nájsť korelácie a vzorce v dátových súboroch.

- To, že televízny vysielateľ používa zariadenie, ktoré umožňuje sledovať, koľkokrát sa jeho moderátori správ usmejú do kamery, nepredstavuje rozpoznávanie emócií.
- Konštatovanie, že osoba je šťastná, predstavuje rozpoznávanie emócií. Systém AI, ktorý odvodzuje, že zamestnanec je nešťastný, smutný alebo nahnevaný na zákazníkov (napríklad z gest tela, zamračeného výrazu alebo chýbajúceho úsmevu), predstavuje „rozpoznávanie emócií“.
- Systémy, ktoré z hlasu alebo gest tela odvodzujú, že študent je rozzúrený a na pokraji prejavu násilného správania, predstavujú „rozpoznávanie emócií“.
- Používanie rozpoznávacích systémov AI na odvolenie únavy profesionálneho pilota alebo vodiča s cieľom upozorniť ho a navrhnuť, kedy sú potrebné prestávky, aby sa predišlo nehodám, nepredstavuje „rozpoznávanie emócií“, pretože rozpoznávanie emócií nezahŕňa fyzické stavy, ako je bolesť alebo únava.

d) Na základe ich biometrických údajov

250. Podľa vymedzenia v článku 3 bode 39 aktu o AI predstavujú systémy na rozpoznávanie emócií len systémy umelej inteligencie, ktoré identifikujú alebo odvodzujú emócie alebo úmysly na základe biometrických údajov.¹⁵⁵
251. Osobné charakteristiky, z ktorých možno získať biometrické údaje, sú fyzické alebo behaviorálne atribúty. Fyziologická biometria využíva fyzické, štrukturálne a relatívne statické atribúty osoby, ako sú odtlačky prstov, vzor dúhovky, kontúry tváre alebo geometria žíl na rukách. Niektoré modality majú mikroskopickú povahu, ale napriek tomu vykazujú biologické a chemické štruktúry, ktoré možno získať a identifikovať, napríklad DNA a telesný pach¹⁵⁶. V prípade behaviorálnej biometrie sa monitorujú osobitné charakteristiky pohybov, gest a motorických zručností jednotlivcov pri vykonávaní úlohy alebo postupnosti úloh. To znamená, že sa zachytávajú a analyzujú pohyby človeka, napríklad kráčanie (analýza chôdze) alebo kontakt prstov s klávesnicou (dynamika písania na klávesnici). Behaviorálna biometria zahŕňa rôzne modality, ktoré vykazujú vedomé aj nevedomé opakované pohyby a s nimi spojené rytmické časovanie/tlaky v súvislosti s časťami tela, a to od podpisov, chôdze, hlasu a dynamiky písania na klávesnici až po sledovanie očí a úderov srdca¹⁵⁷,

¹⁵⁵ V článku 3 bode 34 aktu o AI sa „biometrické údaje“ vymedzujú ako „osobné údaje, ktoré sú výsledkom osobitného technického spracovania týkajúceho sa fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby, ako sú podoba tváre alebo daktyloskopické údaje.“ Pozri aj odôvodnenie 18 aktu o AI v súvislosti s odvodzovaním emócií z hlasu a reči.

¹⁵⁶ [Physiological and Behavioural Biometrics - Biometrics Institute](#) (Fyziologická a behaviorálna biometria – Ústav biometrie).

¹⁵⁷ [Physiological and Behavioural Biometrics - Biometrics Institute](#) (Fyziologická a behaviorálna biometria – Ústav biometrie).

elektroencefalografiu (EEG)¹⁵⁸ alebo elektrokardiogramy (EKG)¹⁵⁹. Biometrický vstup sa môže týkať jednej modalít (napríklad podob tváre) alebo viacerých modalít [napríklad informácie o tvári v kombinácii s elektroencefalogramom (EEG)]. V odôvodnení 18 sa ako príklady uvádzajú výrazy tváre, gestá, napríklad pohyby rúk, alebo charakteristické znaky hlasu osoby.

Napríklad:

- Systém AI, ktorý odvodzuje emócie z písaného textu (analýza obsahu/nálad) s cieľom určiť štýl alebo tón určitého článku, nie je založený na biometrických údajoch, a preto nepatrí do rozsahu pôsobnosti zákazu.
- Systém umelej inteligencie, ktorý odvodzuje emócie zo stláčania klávesov (spôsobu písania), výrazu tváre, držania a pohybov tela, je založený na biometrických údajoch a patrí do rozsahu pôsobnosti zákazu.

252. Vymedzenie biometrických údajov v akte o AI je preto široké a zahŕňa všetky biometrické údaje používané na rozpoznávanie emócií, biometrickú kategorizáciu alebo iné účely.¹⁶⁰

7.2.2. Obmedzenie zákazu na pracoviská a vzdelávacie inštitúcie

253. Zákaz v článku 5 ods. 1 písm. f) aktu o AI je obmedzený na systémy na rozpoznávanie emócií v „oblasti pracoviska a vzdelávacích inštitúcií“. Ako sa objasňuje v odôvodnení 44 aktu o AI, týmto obmedzením sa má riešiť nerovnováha moci v kontexte práce alebo vzdelávania.

a) „Pracovisko“

254. Pojem „pracovisko“ by sa mal vykladať široko. Tento pojem sa vzťahuje na akýkoľvek konkrétny fyzický alebo virtuálny priestor, v ktorom fyzické osoby vykonávajú úlohy a povinnosti, ktoré im pridelil zamestnávateľ alebo organizácia, s ktorou sú prepojené, napríklad v prípade samostatnej zárobkovej činnosti. Patrí sem akékoľvek prostredie, kde sa práca vykonáva, pričom sa môže značne líšiť podľa povahy práce, od vnútorných kancelárskych priestorov, tovární a skladov až po verejne prístupné priestory, ako sú obchody, štadióny alebo múzeá, až po miesta pod holým nebom alebo automobily, ako

¹⁵⁸ Pozri EDPS, [TechDispatch 1/2024 – Neurodata](#), 3. 6. 2024, v ktorom sa diskutuje o používaní údajov o mozgu a súvisiacich technológiách, ako aj o právnych dôsledkoch vrátane návrhu nových „neuropráv“ vrátane duševného súkromia a integrity. In: S. O’Sullivan, H. Chneiweiss, A. Pierucci and K. Rommelfanger, [Neurotechnologies and Human Rights Framework: Do we need new Human Rights?](#) (Neurotechnológie a rámec ľudských práv: potrebujeme nové ľudské práva?), správa, OECD a RE, 9. 11. 2021, s. 33, kde sa diskutuje o súčasnom stave a právnych aspektoch neurotechniky.

¹⁵⁹ Pozri [Hasnul a kol., 2021, *Electrocardiogram-Based Emotion Recognition Systems and Their Applications in Healthcare*](#) (Systémy rozpoznávania emócií na základe elektrokardiogramu a ich využitie v zdravotnej starostlivosti).

¹⁶⁰ V akte o AI nie je súčasťou vymedzenia biometrických údajov formulácia „ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu“ (funkčné využitie biometrických údajov), v čom sa toto vymedzenie líši od vymedzenia biometrických údajov vo všeobecnom nariadení o ochrane údajov, ktoré uvedenú požiadavku obsahuje. Vymedzenie biometrických údajov podľa všeobecného nariadenia o ochrane údajov sa bude uplatňovať podľa pravidiel ochrany údajov v súvislosti so spracúvaním osobných údajov (a keď sa napríklad uplatní článok 9 ods. 1 a 2 všeobecného nariadenia o ochrane údajov).

aj dočasné alebo mobilné pracoviská. Je to nezávislé od postavenia zamestnanca, dodávateľa, stážistu, dobrovoľníka atď.¹⁶¹ Pojem „pracovisko“ v článku 5 ods. 1 písm. f) aktu o AI by sa mal chápať tak, že sa vzťahuje aj na uchádzačov počas procesu výberu a prijímania do zamestnania, a to v súlade s ostatnými ustanoveniami aktu o AI, ktoré sa týkajú uvádzania na trh, uvádzania do prevádzky alebo používania systémov AI v oblasti zamestnanosti, riadenia pracovníkov a prístupu k samostatnej zárobkovej činnosti, keďže v tejto súvislosti existuje nerovnováha moci a rušivý charakter rozpoznávania emócií sa môže uplatňovať už vo fáze náboru.

Napríklad:

- Používanie webových kamier a systémov na rozpoznávanie hlasu v kontaktnom centre na sledovanie emócií zamestnancov, napríklad hnevu, je zakázané¹⁶². Ak sa systémy na rozpoznávanie emócií nasadzujú len na účely osobnej odbornej prípravy, sú povolené, ak sa výsledky neposkytujú zodpovedným osobám v oblasti ľudských zdrojov a nemôžu mať vplyv na hodnotenie, povýšenie atď. osoby, ktorá absolvuje odbornú prípravu, za predpokladu, že sa zákaz neobchádza a používanie systému na rozpoznávanie emócií nemá žiadny vplyv na pracovný pomer.
- Používanie systémov na rozpoznávanie hlasu v kontaktnom centre na sledovanie emócií zákazníkov, ako sú hnev alebo netrpezlivosť, nie je zakázané podľa článku 5 ods. 1 písm. f) aktu o AI (napríklad na pomoc zamestnancom pri zvládaní niektorých nahnevanych zákazníkov).
- Systémy AI, ktoré monitorujú emocionálny tón v hybridných pracovných tímoch prostredníctvom identifikácie a odvodzovania emócií z hlasu a obrazu hybridných videohovorov, ktoré by zvyčajne slúžili na podporu sociálneho povedomia, riadenia emocionálnej dynamiky a predchádzania konfliktom, sú zakázané.
- Používanie systémov AI na rozpoznávanie emócií počas náborového procesu je zakázané.
- Používanie systémov AI na rozpoznávanie emócií počas skúšobnej lehoty je zakázané.
- Používanie kamier supermarketom na sledovanie emócií zamestnancov, napríklad šťastia, je zakázané.
- Používanie kamier supermarketom alebo bankou na odhaľovanie podozrivých zákazníkov, napríklad na zistenie, že sa niekto chystá spáchať lúpež, nie je zakázané podľa článku 5 ods. 1 písm. f) aktu o AI, ak je zabezpečené, že nie sú sledovaní žiadni zamestnanci a existujú dostatočné záruky.

¹⁶¹ Pozri aj odôvodnenia v súvislosti s vysokorizikovými systémami AI na pracovisku, ako je odôvodnenie 56, v ktorom sa uplatňuje široký výklad. Pozri aj zoznam vysokorizikových systémov AI v prílohe III, ktorý sa v bode 4 týka samostatnej zárobkovej činnosti. Na samostatnú zárobkovú činnosť sa v širokom rozsahu vzťahuje aj antidiskriminačné právne predpisy EÚ.

¹⁶² Príklad z Boyd a kol., 2023, „[Automated Emotion Recognition in the Workplace: How Proposed Technologies Reveal Potential Futures of Work](#)“ (Automatizované rozpoznávanie emócií na pracovisku: ako navrhované technológie odhaľujú potenciálnu budúcnosť práce).

b) „Vzdelávacie inštitúcie“

255. Odkaz na **vzdelávacie inštitúcie** je široký a mal by sa chápať tak, že zahŕňa verejné aj súkromné inštitúcie. Neexistuje žiadne obmedzenie, pokiaľ ide o druh alebo vek žiakov alebo študentov alebo o konkrétne prostredie (online, prezenčne, v kombinovanom režime¹⁶³ atď.). Napríklad vzdelávacie a školiace inštitúcie na všetkých úrovniach patria do rozsahu pôsobnosti zákazu v článku 5 ods. 1 písm. f) aktu o AI, a to vrátane odborných škôl, t. j. škôl, v ktorých si študenti osvojujú zručnosti, pri ktorých používajú svoje ruky¹⁶⁴, a kontinuálneho vzdelávania¹⁶⁵. Vzdelávacie inštitúcie sú zvyčajne akreditované alebo schválené príslušnými vnútroštátnymi vzdelávacími orgánmi alebo rovnocennými orgánmi. Kľúčovým prvkom je, že vzdelávacie inštitúcie môžu udeliť diplom (resp. účasť je podmienkou získania diplomu). Zákaz by sa mal chápať tak, že sa uplatňuje aj na uchádzačov počas prijímacieho procesu.

Napríklad:

- Aplikácia založená na AI, ktorá využíva rozpoznávanie emócií na učenie sa jazyka online mimo vzdelávacej inštitúcie, nie je zakázaná podľa článku 5 ods. 1 písm. f) aktu o AI. Naopak, ak vzdelávacia inštitúcia od študentov vyžaduje, aby aplikáciu používali, používanie takéhoto systému na rozpoznávanie emócií je zakázané.
- Ak vzdelávacia inštitúcia pri skúšaní študentov online používa softvér na sledovanie očí založený na AI na sledovanie bodu fixácie a pohybu očí (bod pohľadu, napríklad s cieľom odhaliť, či sa používa nepovolený materiál), nie je to zakázané, pretože systém neidentifikuje ani neodvodzuje emócie. Naopak, ak sa systém používa aj na zisťovanie emócií, napríklad emocionálneho vzrušenia a úzkosti, patrí to do rozsahu pôsobnosti zákazu.
- Používanie systému AI na rozpoznávanie emócií vzdelávacou inštitúciou na odvodzovanie záujmu a pozornosti študentov je zakázané. Naopak, ak sú systémy na rozpoznávanie emócií nasadené len na účely vzdelávania v kontexte hrania rolí (napríklad na odbornú prípravu hercov alebo učiteľov), sú povolené, ak ich výsledky nemôžu ovplyvniť hodnotenie alebo certifikáciu osoby, ktorá odbornú prípravu absolvuje.
- Používanie systému AI na rozpoznávanie emócií vzdelávacou inštitúciou počas prijímacích skúšok nových študentov je zakázané.
- Používanie systému AI, ktorý umožňuje vzdelávacej inštitúcii zachytiť, keď sa študenti medzi sebou rozprávajú prostredníctvom telefónov alebo iných kanálov

¹⁶³ Zmiešané učenie sa má chápať ako využívanie viacerých prístupov v procese vzdelávania a odbornej prípravy vrátane kombinácie digitálnych (vrátane elektronického učenia sa) a nedigitálnych vzdelávacích nástrojov.

¹⁶⁴ Pozri napríklad posúdenie vplyvu priložené k návrhu Komisie, v ktorom sa uvádzajú konkrétne spôsoby použitia AI inštitúciami odborného vzdelávania, ktoré predstavujú intenzívny zásah do širokého spektra základných práv, napríklad pri posudzovaní: Európska komisia, [Pracovný dokument útvarov Komisie. Posúdenie vplyvu. Prílohy, SWD\(2021\)84 final, časť 2/2](#), s. 43. Pozri aj I. Tuomi, *The use of Artificial Intelligence (AI) in education* [Používanie umelej inteligencie (AI) vo vzdelávaní], Európsky parlament, 2020, s. 9 – 10.

¹⁶⁵ Pozri článok 14 charty.

počas online prednášok, nie je zakázané, pretože sa ním neodvodzujú emócie. Naopak, ak sa systém používa aj na zisťovanie emócií, ako sú emocionálne vzrušenie, úzkosť a záujem, patrí do rozsahu pôsobnosti zákazu.

- Využívanie systému AI na rozpoznávanie emócií zo strany vzdelávacej inštitúcie v prípade učiteľov (pracovisko) aj študentov (vzdelávanie) je zakázané.

7.2.3. Výnimky zo zdravotných a bezpečnostných dôvodov

256. Zákaz v článku 5 ods. 1 písm. f) aktu o AI obsahuje výslovnú výnimku pre systémy na rozpoznávanie emócií používané v oblasti pracoviska a vzdelávacích inštitúcií zo zdravotných alebo bezpečnostných dôvodov, ako sú systémy na terapeutické použitie¹⁶⁶. Vzhľadom na cieľ aktu o AI zabezpečiť vysokú úroveň ochrany základných práv by sa táto výnimka mala vykladať úzko.
257. Pod terapeutickým použitím sa rozumie najmä použitie zdravotníckych pomôcok s označením CE. Okrem toho táto výnimka nezahŕňa používanie systémov na rozpoznávanie emócií na zisťovanie všeobecných aspektov blahobytu. Všeobecné monitorovanie úrovne stresu na pracovisku nie je povolené na základe aspektov zdravia alebo bezpečnosti. Napríklad na systém AI určený na zisťovanie vyhorenia alebo depresie na pracovisku alebo vo vzdelávacích inštitúciách by sa výnimka nevzťahovala a bol by aj naďalej zakázaný.
258. Pojem „bezpečnostné dôvody“ v rámci tejto výnimky by sa mal chápať tak, že sa uplatňuje len vo vzťahu k ochrane života a zdravia, a nie na ochranu iných záujmov, napríklad majetku pred krádežou alebo podvodom.
259. Z tohto úzkeho výkladu výnimky vyplýva, že akékoľvek použitie zo zdravotných a bezpečnostných dôvodov by malo byť vždy obmedzené na to, čo je nevyhnutne potrebné a primerané, a to vrátane časových obmedzení, osobného uplatňovania a rozsahu, a malo by byť sprevádzané dostatočnými zárukami. Takéto záruky by mohli zahŕňať napríklad predchádzajúce písomné a odôvodnené odborné stanovisko týkajúce sa konkrétneho prípadu použitia. Nevyhnutnosť by sa mala posudzovať na objektívnom základe vo vzťahu k zdravotnému a bezpečnostnému účelu a nemala by sa zdôvodňovať „potrebami“ zamestnávateľa alebo vzdelávacej inštitúcie. V rámci tohto posúdenia by sa malo zisťovať, či existujú menej rušivé alternatívne prostriedky, ktorými by sa dosiahol rovnaký účel.
260. Zamestnávateľa a edukátori by mali systémy na rozpoznávanie emócií nasadzovať len zo zdravotných a bezpečnostných dôvodov v prípade výslovnej potreby¹⁶⁷. Údaje zhromaždené a spracované v tejto súvislosti sa nesmú použiť na žiadny iný účel. Je to obzvlášť dôležité vzhľadom na to, že sa preukázalo, že používanie softvéru využívajúceho AI na riadenie v práci môže mať potenciálne negatívny vplyv na zdravie

¹⁶⁶ Odôvodnenie 44 aktu o AI.

¹⁶⁷ Ak sa zavádzajú takéto nové technológie, v súlade s pracovným právom EÚ musia zamestnávateľi uskutočniť aj konzultácie s pracovníkmi alebo ich zástupcami, a to v súlade s vnútroštátnymi postupmi. Bez dodržania týchto procesných požiadaviek nemožno takéto systémy zaviesť len s odkazom na akt o AI ako taký. Bude sa pri nich vyžadovať aj súhlas z hľadiska právnych predpisov o ochrane údajov, ktoré sa naďalej uplatňujú.

a bezpečnosť pracovníkov. Priebežné monitorovanie prostredníctvom nositeľných zariadení môže napríklad zvýšiť pracovný stres a zároveň ovplyvniť produktivitu¹⁶⁸.

261. Keďže v odôvodnení 18 aktu o AI sa z vymedzenia pojmu „systémy na rozpoznávanie emócií“ vylučujú fyzické stavy, ako je bolesť alebo únava, viaceré systémy AI používané z bezpečnostných dôvodov by už do tohto vymedzenia pojmu nepatrili, vrátane napríklad systémov používaných pri zisťovaní stavu únavy profesionálnych pilotov alebo vodičov na účely prevencie nehôd.
262. Na systémy na rozpoznávanie emócií, ktoré spĺňajú podmienky výnimky podľa článku 5 ods. 1 písm. f) aktu o AI, sa naďalej vzťahujú iné právne predpisy vrátane pravidiel ochrany údajov¹⁶⁹.
263. Systémy na rozpoznávanie emócií, ktoré sa klasifikujú ako vysokorizikové systémy podľa článku 6 ods. 2 aktu o AI a bodu 1 písm. c) prílohy III k aktu o AI, budú musieť spĺňať požiadavky na vysokorizikové systémy uvedené v kapitole III oddiele 2 aktu o AI a povinnosť v oblasti transparentnosti podľa článku 50 ods. 3 aktu o AI.

Napríklad:

Rozpoznávanie emócií sa môže nasadiť zo zdravotných dôvodov na pomoc zamestnancom alebo študentom s autizmom a na zlepšenie prístupnosti pre nevidiace alebo nepočujúce osoby¹⁷⁰. Na takéto použitie by sa vzťahovala výnimka zo zdravotných dôvodov podľa článku 5 ods. 1 písm. f) aktu o AI.

Naopak, rozpoznávanie emócií na posúdenie blaha študentov alebo zamestnancov, úrovne motivácie a spokojnosti s prácou alebo vzdelávaním sa nepovažuje za „používanie zo zdravotných dôvodov“ a bolo by zakázané.

Zamestnávateľ by mal zakázané nasadzovať na pracovisku zariadenia alebo digitálnych asistentov využívajúcich AI na meranie úzkosti na základe nameranej úrovne stresu alebo na meranie nudy zamestnancov, pokiaľ by zvýšená úroveň stresu/nedostatok koncentrácie nepredstavovali konkrétne nebezpečenstvo, napríklad pri nasadzovaní nebezpečných strojov alebo pri práci s nebezpečnými chemikáliami. Ak by tomu tak bolo, zamestnávateľ by nesmel použiť údaje na iné účely, napríklad na hodnotenie pracovného výkonu zamestnanca.

7.3. Priaznivejšie právne predpisy členských štátov

264. V článku 2 ods. 11 aktu o AI sa stanovuje, že Únia alebo členské štáty môžu zachovať alebo zaviesť „zákony, iné právne predpisy alebo správne opatrenia, ktoré sú pre pracovníkov priaznivejšie z hľadiska ochrany ich práv v súvislosti s používaním

¹⁶⁸ The Interconnection between the AI Act and the EU's Occupational Safety and Health Legal Framework (Vzájomné prepojenie aktu o AI a právneho rámca EÚ pre bezpečnosť a ochranu zdravia pri práci), Global Workplace Law & Policy (kluwerlawonline.com).

¹⁶⁹ Od decembra 2026 sa bude uplatňovať smernica Európskeho parlamentu a Rady (EÚ) 2024/2831 z 23. októbra 2024 o zlepšení pracovných podmienok v oblasti práce pre platformy.

¹⁷⁰ Systémy by mohli byť užitočne využité na pomoc zamestnancom alebo študentom/žiakom pri pochopení emócií kolegov atď.

systémov AI zamestnávateľmi“. Takisto sa môžu povoliť alebo podporiť kolektívne zmluvy, ktoré sú pre pracovníkov priaznivejšie.

Členské štáty môžu napríklad prijať zákony, ktorými sa stanovuje, že používanie systémov na rozpoznávanie emócií v oblasti práce nemožno uplatňovať na lekárske účely.

7.4. Vylúčenie z rozsahu pôsobnosti

265. Ako už bolo uvedené, z rozsahu pôsobnosti sú vylúčené:

- systémy AI odvodzujúce emócie a sentiment nie na základe biometrických údajov,
- systémy AI odvodzujúce fyzické stavy, ako je bolesť a únava.

266. Na systémy na rozpoznávanie emócií používané vo všetkých ostatných oblastiach okrem oblasti pracoviska a vzdelávacích inštitúcií sa nevzťahuje zákaz v článku 5 ods. 1 písm. f) aktu o AI. Takéto systémy sa však považujú za vysokorizikové systémy AI¹⁷¹. Zároveň môžu byť takéto systémy v určitých prípadoch zakázané na základe článku 5 ods. 1 písm. a) a b) aktu o AI (škodlivá manipulácia a zneužívanie) alebo na základe iných právnych predpisov Únie. Na takéto systémy sa naďalej vzťahujú všetky ostatné uplatniteľné právne predpisy, ako sú právne predpisy Únie v oblasti ochrany údajov, ochrany spotrebiteľa atď.

Napríklad:

Na systémy na rozpoznávanie emócií používané v komerčnom kontexte na oslovovanie zákazníkov sa nevzťahuje zákaz podľa článku 5 ods. 1 písm. f) aktu o AI bez ohľadu na to, či sú alebo nie sú založené na biometrických údajoch. Preto sa zákaz nevzťahuje na také príklady, ako sú systémy AI, ktoré umožňujú rozpoznávanie emócií na základe dynamiky písania na klávesnici alebo na základe hlasových správ zákazníkov (napríklad chatové správy, používanie virtuálnych hlasových asistentov), používané v online marketingu na účely aplikácií na zobrazovanie personalizovaných správ a na reklamné účely, a to aj v inteligentných prostrediach („inteligentné bilbordy“).

Napriek tomu sa na takéto praktiky môžu vzťahovať zákazy škodlivej manipulácie a zneužívania v článku 5 ods. 1 písm. a) a b) aktu o AI¹⁷², ak sú splnené všetky podmienky na uplatnenie uvedených zákazov.

a) Ostatné systémy vylúčené z rozsahu pôsobnosti

267. „Kontrola davu“ vo všeobecnosti znamená kontrolu a monitorovanie správania skupín s cieľom udržiavať (verejný) poriadok a bezpečnosť podujatia. Často sa spája s veľkými davovými podujatiami (napríklad futbalové zápasy, koncerty atď.) alebo osobitnými miestami, ako sú letiská alebo vlaky. Systémy na kontrolu davu môžu fungovať bez toho, aby odvodzovali emócie jednotlivých osôb, napríklad v prípade

¹⁷¹ Článok 6 ods. 2 aktu o AI a bod 1 písm. c) prílohy III k aktu o AI.

¹⁷² Tieto situácie môžu byť zakázané aj podľa iných pravidiel, napríklad v oblasti ochrany údajov alebo ochrany spotrebiteľa.

analýzy všeobecnej úrovne hluku a nálady na danom mieste. V takom prípade by systém nepatril do rozsahu pôsobnosti článku 5 ods. 1 písm. f) aktu o AI, pretože neodvodzuje emócie (konkrétnej) fyzickej osoby.

268. Môžu sa však vyskytnúť prípady, keď takéto systémy na kontrolu davu odvodzujú emócie jednotlivcov, napríklad či je v dave veľký počet nahnevaných tvárí. Za normálnych okolností by sa na takéto systémy AI nevzťahoval zákaz podľa článku 5 ods. 1 písm. f) aktu o AI, pretože sa zvyčajne nepoužívajú na pracovisku ani vo vzdelávacích inštitúciách.
269. Do rozsahu pôsobnosti nepatria ani systémy, ktoré sa používajú v zdravotníctve, napríklad opatrovateľské roboty, alebo lekári, ktorí používajú systémy na rozpoznávanie emócií počas vyšetrenia na pracovisku, ani hlasové monitory, ktoré analyzujú tiesňové volania.
270. Takéto systémy často preverujú osoby, ktoré sa tam nachádzajú v pracovnom kontexte, napríklad bezpečnostný personál na futbalovom štadióne alebo na hlavnej stanici (kde sa takéto systémy používajú na rozpoznanie agresívneho správania), alebo zamestnancov v zdravotníctve. V takýchto prípadoch musia nasadzujúce subjekty zabezpečiť záruky, aby sa predišlo preverovaniu zamestnancov. Nemožno sa však úplne vyhnúť tomu, že takéto systémy odvodzujú aj emócie uvedených zamestnancov. Keďže primárny cieľ systému nie je zameraný na posudzovanie emócií zamestnancov, tieto systémy by sa mali považovať za systémy, ktoré nepatria do rozsahu pôsobnosti zákazu. Subjekty nasadzujúce takéto systémy budú aj naďalej zodpovedať za to, aby ich používanie nemalo nepriaznivý vplyv na zamestnancov.

8. ČLÁNOK 5 ODS. 1 PÍSM. G) AKTU O AI: BIOMETRICKÁ KATEGORIZÁCIA PRE URČITÉ „CITLIVÉ“ CHARAKTERISTIKY

271. V článku 5 ods. 1 písm. g) aktu o AI sa zakazujú systémy biometrickej kategorizácie, ktoré jednotlivo kategorizujú fyzické osoby na základe biometrických údajov s cieľom odvodit' alebo vyvodit' ich rasu, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie, sexuálny život alebo sexuálnu orientáciu. Tento zákaz sa nevzťahuje na označovanie, filtrovanie alebo kategorizáciu súborov biometrických údajov získaných v súlade s právom Únie alebo vnútroštátnym právom, ktoré sa môžu používať napríklad na účely presadzovania práva¹⁷³.

8.1. Odôvodnenie a ciele

272. Z biometrických údajov možno extrahovať, odvodiť alebo vyvodit' širokú škálu informácií vrátane „citlivých“ informácií, a to aj bez vedomia dotknutých osôb, s cieľom kategorizovať tieto osoby. To môže viesť k nespravodlivému a diskriminačnému zaobchádzaniu, napríklad dôjde k odmietnutiu služby, pretože sa osoba považuje za príslušníka určitej rasy. Systémy biometrickej kategorizácie založené na AI na účely zaradenia fyzických osôb do osobitných skupín alebo kategórií, ktoré sa týkajú aspektov, ako sú sexuálna alebo politická orientácia alebo rasa, porušujú

¹⁷³

Odôvodnenie 30 aktu o AI.

ľudskú dôstojnosť a predstavujú významné riziko pre iné základné práva, ako je právo na súkromie a nediskrimináciu. Podľa článku 5 ods. 1 písm. g) aktu o AI sú preto zakázané.

8.2. Hlavné pojmy a zložky zákazu

V článku 5 ods. 1 písm. g) aktu o AI sa stanovuje

Zakazujú sa tieto praktiky využívajúce AI:

g) uvádzanie na trh, uvádzanie do prevádzky na tento konkrétny účel alebo používanie systémov biometrickej kategorizácie, ktoré jednotlivo kategorizujú fyzické osoby *na základe ich biometrických údajov* s cieľom odvodiť alebo vyvodiť ich rasu, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie, sexuálny život alebo sexuálnu orientáciu; tento zákaz sa nevzťahuje na žiadne označovanie ani filtrovanie zákonne získaných súborov biometrických údajov, ako sú obrázky, na základe biometrických údajov alebo kategorizácie biometrických údajov v oblasti presadzovania práva;

273. Na uplatnenie zákazu podľa článku 5 ods. 1 písm. g) aktu o AI musí byť splnených niekoľko kumulatívnych podmienok:
- i) praktika musí predstavovať „uvádzanie na trh“, „uvádzanie do prevádzky na tento konkrétny účel“ alebo „používanie“ systému AI;
 - ii) systém musí byť systém biometrickej kategorizácie;
 - iii) musia sa kategorizovať jednotlivé osoby;
 - iv) na základe ich biometrických údajov;
 - v) s cieľom odvodiť alebo vyvodiť ich rasu, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie, sexuálny život alebo sexuálnu orientáciu.
274. Aby sa zákaz uplatnil, musí byť súčasne splnených všetkých päť podmienok. Prvá podmienka, t. j. uvádzanie na trh, uvádzanie do prevádzky alebo používanie systému AI, sa analyzuje v oddiele 2.3. Zákaz sa preto vzťahuje na poskytovateľov systémov AI aj subjekty nasadzujúce systémy AI, pričom každý z nich v rámci svojich povinností nesmie takéto systémy AI uvádzať na trh, uvádzať do prevádzky alebo používať. Ďalšie podmienky uplatňovania zákazu¹⁷⁴ sa ďalej opisujú a analyzujú ďalej.
275. Zákaz sa nevzťahuje na označovanie alebo filtrovanie zákonne získaných súborov biometrických údajov, a to aj na účely presadzovania práva.

8.2.1. Systém biometrickej kategorizácie

276. Kategorizácia jednotlivca biometrickým systémom je zvyčajne proces stanovenia, či biometrické údaje jednotlivca patria do skupiny s určitou vopred vymedzenou charakteristikou. Nejde o identifikáciu jednotlivca ani overenie jeho totožnosti, ale

¹⁷⁴ Pokiaľ ide o kritérium „systému AI“, „uvádzania na trh“, „uvádzania do prevádzky na tento konkrétny účel“ alebo používania, pozri v predchádzajúcom texte.

o zaradenie jednotlivca do určitej kategórie. Napríklad na reklamnom displeji sa môžu zobrazovať rôzne reklamy v závislosti od jednotlivca, ktorý sa naň díva, na základe veku alebo pohlavia.¹⁷⁵ Osoby môžu byť takisto jednoducho zaradené do kategórií zo štatistických dôvodov bez toho, aby boli identifikované a aby bola cieľom ich identifikácia.

277. V článku 3 bode 40 aktu o AI sa systém biometrickej kategorizácie vymedzuje ako systém AI na účely zaraďovania fyzických osôb do špecifických kategórií na základe ich biometrických údajov, pokiaľ to nie je pomocný úkon pre inú komerčnú službu a nevyhnutne potrebné z objektívnych technických dôvodov. Ako je vysvetlené v oddiele 7.2.1 písm. d), „biometrické údaje“ sú vymedzené v článku 3 bode 34 aktu o AI. Biometrické údaje zahŕňajú najmä behaviorálne charakteristické znaky, ktoré sú založené na biometrických znakoch. Z rozsahu biometrickej kategorizácie je vylúčená kategorizácia podľa oblečenia alebo doplnkov, ako sú šatky alebo krížiky, ako aj podľa aktivity na sociálnych sieťach.
278. Biometrická kategorizácia sa môže opierať o kategórie fyzických charakteristických znakov (napríklad črty a tvar tváre, farba pleti), na základe ktorých sa osoby zaraďujú do konkrétnych kategórií. Niektoré z týchto kategórií môžu mať osobitnú „citlivú“ povahu alebo charakteristiky chránené právnymi predpismi Únie v oblasti nediskriminácie, ako je napríklad rasa. Biometrická kategorizácia však môže byť založená aj na DNA alebo na behaviorálnych aspektoch, ako je analýza dynamiky písania na klávesnici alebo chôdze osoby¹⁷⁶.
279. Na to, aby biometrická kategorizácia nepatrila do rozsahu pôsobnosti vymedzenia podľa aktu o AI, musia byť kumulatívne splnené dve podmienky – je to „pomocný úkon pre inú komerčnú službu a nevyhnutne potrebné z objektívnych technických dôvodov“.
280. Podľa odôvodnenia 16 aktu o AI čisto vedľajšia funkcia je funkcia, ktorá je neoddeliteľne spojená s inou komerčnou službou, čo znamená, že táto funkcia sa z objektívnych technických dôvodov nemôže používať bez hlavnej služby, a integrácia uvedenej funkcie alebo funkcionality nie je prostriedkom obchádzania uplatniteľnosti pravidiel aktu o AI.

Podľa článku 5 ods. 1 písm. g) aktu o AI sú povolené napríklad tieto spôsoby používania AI:

– Filtre, ktoré kategorizujú tvárové alebo telesné znaky používané na online trhoch s cieľom umožniť, aby si spotrebiteľ pozrel výrobok na sebe, by mohli predstavovať takúto vedľajšiu funkciu, keďže ich možno použiť len vo vzťahu k hlavnej službe, ktorá spočíva v predaji výrobku.

¹⁷⁵ Pozri [stanovisko 3/2012 k vývoju v oblasti biometrických technológií](#), ktoré vypracovala pracovná skupina zriadená podľa článku 29, WP193, 27. 4. 2012, s. 6.

¹⁷⁶ Pozri napríklad [stanovisko 3/2012 k vývoju v oblasti biometrických technológií](#), ktoré vypracovala pracovná skupina zriadená podľa článku 29, WP193, 27. 4. 2012, s. 16 – 17. Skupina tu odkazuje na „mäkké rozpoznávanie“ (s. 17), t. j. „určovanie správania alebo osobitných potrieb ľudí“.

- Filtre integrované do online služieb sociálnych sietí, ktoré kategorizujú tvárové alebo telesné znaky s cieľom umožniť používateľom pridávať alebo upravovať obrázky alebo videá, by sa takisto mohli považovať za vedľajšiu funkciu, keďže takýto filter nemožno použiť bez hlavnej služby sociálnej siete spočívajúcej v zdieľaní obsahu online.

Naopak, medzi príklady zakázaných spôsobov použitia patria:

- Systém AI, ktorý na základe analýzy biometrických údajov z fotografií nahraných na platforme sociálnych médií kategorizuje osoby, ktoré sú na platforme aktívne, podľa ich predpokladanej politickej orientácie a posiela im ciele politické správy. Hoci takýto systém môže byť len vedľajšou funkciou pre politickú reklamu, nebol by „nevyhnutne potrebný z objektívnych technických dôvodov“, preto nie sú splnené podmienky na jeho vylúčenie z vymedzenia biometrickej kategorizácie.
- Systém AI, ktorý kategorizuje osoby aktívne na platforme sociálnych médií podľa ich predpokladanej sexuálnej orientácie na základe analýzy biometrických údajov z fotografií zdieľaných na tejto platforme a na základe toho týmto osobám doručuje reklamy, by sa považoval za biometrickú kategorizáciu v zmysle aktu o AI. Ani v tomto prípade nie je táto „vedľajšia služba“ nevyhnutne potrebná, a preto sa na ňu nevzťahuje vylúčenie zo zákazu.

8.2.2. Osoby sú individuálne kategorizované na základe ich biometrických údajov

281. Používanie biometrických údajov na kategorizáciu fyzických osôb je základným prvkom pre uplatnenie zákazu [pozri už uvedený oddiel 8.2.1 a oddiel 7.2.1 písm. d)].
282. Okrem toho, aby sa zákaz mohol uplatňovať, musia byť fyzické osoby kategorizované „jednotlivo“. Ak to nie je cieľom alebo výsledkom biometrickej kategorizácie, zákaz sa neuplatňuje, napríklad ak sa kategorizuje celá skupina bez toho, aby sa skúmali jednotlivé osoby.

Príklady jednotlivej kategorizácie zahŕňajú:

- Systémy AI, ktoré vykonávajú „odhad atribútov“ (počítanie demografických údajov) vrátane napríklad „veku, rodu, etnického pôvodu“, napríklad na základe telesných znakov, ako sú tvár, výška alebo farba pleti, očí a vlasov (alebo ich kombinácia).
- Systémy AI schopné kategorizovať jednotlivcov a vyselektovať ich na základe osobitného znaku (napríklad jazvy pod pravým okom) alebo preto, že majú tetovanie na pravej ruke.

Tieto prípady použitia sú príkladmi jednotlivej biometrickej kategorizácie. Na to, aby sa na tieto príklady vzťahoval zákaz podľa článku 5 ods. 1 písm. g) aktu o AI, musia byť splnené všetky podmienky uvedeného ustanovenia.

8.2.3. S cieľom odvodit' alebo vyvodit' ich rasu, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie, sexuálny život alebo sexuálnu orientáciu

283. V článku 5 ods. 1 písm. g) aktu o AI sa zakazujú len systémy biometrickej kategorizácie, ktorých cieľom je odvodiť alebo vyvodit' obmedzený počet citlivých charakteristík: rasu, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie, sexuálny život alebo sexuálnu orientáciu.

Medzi systémy zakázané podľa článku 5 ods. 1 písm. g) aktu o AI patria napríklad:

- systém biometrickej kategorizácie, pri ktorom sa tvrdí, že dokáže odvodiť rasu jednotlivca na základe jeho hlasu (líši sa to od systému, ktorý kategorizuje osoby podľa farby pleti alebo očí, alebo systému, ktorý analyzuje DNA obetí trestných činov z hľadiska ich pôvodu. Uvedené systémy by neboli zakázané),
- systém biometrickej kategorizácie, pri ktorom sa tvrdí, že dokáže odvodiť náboženskú orientáciu jednotlivca z jeho tetovania alebo tváre.

8.3. Vylúčenie z rozsahu pôsobnosti

284. Zákaz v článku 5 ods. 1 písm. g) aktu o AI sa nevzťahuje na systémy AI, ktoré sa zaoberajú označovaním alebo filtrovaním zákonne získaných súborov biometrických údajov, ako sú obrázky, a to aj v oblasti presadzovania práva. Bližšie je to vysvetlené v odôvodnení 30 aktu o AI¹⁷⁷.
285. Označovanie alebo filtrovanie súborov biometrických údajov môžu vykonávať systémy biometrickej kategorizácie práve preto, aby sa zaručilo, že údaje budú rovnako reprezentovať všetky demografické skupiny a nebudú napríklad nadmerne reprezentovať jednu konkrétnu skupinu. Ak sú údaje použité na tréning algoritmu skreslené z hľadiska určitej skupiny (t. j. medzi skupinami existujú systematické rozdiely v údajoch v dôsledku spôsobu zberu údajov alebo sú údaje historicky skreslené), algoritmus môže toto skreslenie replikovať, čo môže viesť k nezákonnej diskriminácii osôb alebo skupín osôb¹⁷⁸. Z tohto dôvodu môže byť pri vysokokvalitných údajoch potrebné označovanie na základe niektorých chránených citlivých informácií, a to práve preto, aby sa zabránilo diskriminácii. Podľa aktu o AI sa môže dokonca vyžadovať, aby operácie označovania spĺňali požiadavky aktu o AI týkajúce sa vysokorizikových systémov AI¹⁷⁹. Takéto označovanie alebo filtrovanie biometrických údajov je preto výslovne vyňaté zo zákazu v článku 5 ods. 1 písm. g) aktu o AI. Zákaz sa uplatňuje len v prípade, keď sa biometrické údaje kategorizujú s cieľom odvodiť rasu, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie, sexuálny život alebo sexuálnu orientáciu.

Medzi príklady prípustného označovania alebo filtrovania patria:

- označovanie biometrických údajov, aby sa predišlo prípadom, keď má príslušník etnickej skupiny nižšiu šancu, že bude pozvaný na pracovný pohovor, pretože

¹⁷⁷ Odôvodnenie 30 aktu o AI: „Tento zákaz by sa nemal vzťahovať na zákonné označovanie, filtrovanie alebo kategorizáciu súborov biometrických údajov získaných v súlade s právom Únie alebo vnútroštátnym právom v oblasti biometrických údajov, ako je triedenie obrázkov podľa farby vlasov alebo farby očí, ktoré možno použiť napríklad v oblasti presadzovania práva.“

¹⁷⁸ Tamže.

¹⁷⁹ Pozri napríklad článok 10 a 17 aktu o AI.

algoritmus bol „trénovaný“ na základe údajov, v ktorých táto konkrétna skupina dosahuje nižšiu výkonnosť, t. j. má horšie výsledky ako iné skupiny¹⁸⁰.

– kategorizácia pacientov pomocou obrázkov podľa farby pleti alebo očí môže byť dôležitá pre diagnostiku, napríklad pre určenie diagnózy v prípade rakoviny.

286. V článku 5 ods. 1 písm. g) aktu o AI sa takisto stanovuje, že zákaz uvedený v tomto ustanovení sa nevzťahuje na označovanie ani filtrovanie zákonne získaných súborov údajov v oblasti presadzovania práva¹⁸¹.

Týka sa to napríklad používania systému AI orgánom presadzovania práva, pričom uvedený systém umožňuje označovanie a filtrovanie súboru údajov, pri ktorom existuje podozrenie, že obsahujú materiál obsahujúci sexuálne zneužívanie detí. V prvom kroku by orgán presadzovania práva použil podporu systémov AI na zistenie citlivých údajov z obrázkov a ich redigovanie. Okrem toho by filtrovanie a označovanie podľa rodu, veku, biometrických údajov, ako sú farba očí a vlasov, jazvy a značky, mohlo pomôcť pri identifikácii obetí alebo vytváraní prepojení s inými prípadmi. Podobne je povolené filtrovanie a označovanie rúk páchatel'ov zneužívania na základe osobitných charakteristických znakov, ako sú dĺžka prstov alebo akékoľvek rozlišovacie znaky alebo tetovania, ktoré pomáhajú pri identifikácii možných podozrivých.

8.4. Vzájomný vzťah s inými právnymi predpismi Únie

287. Systémy AI určené na biometrickú kategorizáciu podľa citlivých atribútov alebo charakteristík chránených podľa článku 9 ods. 1 všeobecného nariadenia o ochrane údajov na základe biometrických údajov, pokiaľ nie sú zakázané podľa tohto nariadenia, sú klasifikované ako vysokorizikové¹⁸² podľa aktu o AI¹⁸³.
288. V článku 5 ods. 1 písm. g) aktu o AI sa ďalej obmedzujú možnosti zákonného spracúvania osobných údajov podľa práva Únie v oblasti ochrany údajov, ako sú všeobecné nariadenie o ochrane údajov, smernica o presadzovaní práva a nariadenie, ktorým sa stanovujú pravidlá ochrany údajov pre inštitúcie, orgány, úrady a agentúry EÚ. Predovšetkým sa podľa článku 5 ods. 1 písm. g) aktu o AI vylučuje možnosť biometrickej kategorizácie fyzických osôb na základe ich biometrických údajov, ako sú vymedzené v akte o AI, s cieľom vyvodiť rasu, politické názory, členstvo v odboroch, náboženské alebo filozofické presvedčenie, sexuálny život alebo sexuálnu orientáciu, s výnimkou označovania alebo filtrovania zákonne získaných súborov biometrických údajov, a to aj v oblasti presadzovania práva, ako sa už opísalo. Zákaz v článku 5 ods. 1 písm. g) aktu o AI je okrem toho v súlade s článkom 11 ods. 3 smernice o presadzovaní práva, v ktorom sa výslovne zakazuje akékoľvek „profilovanie“, ktoré vedie

¹⁸⁰ Agentúra pre základné práva, [# BigData. Discrimination in data supported decision making](#) (#BigData. Diskriminácia pri rozhodovaní na základe údajov), Luxemburg, 2018, 14, s. 5.

¹⁸¹ Pokiaľ ide o používanie systémov biometrickej kategorizácie na účely presadzovania práva, akt o AI vychádza z článku 16 ZFEÚ. Pozri aj odôvodnenie 3 aktu o AI.

¹⁸² Odôvodnenie 54 aktu o AI a bod 1 písm. b) prílohy III k aktu o AI.

¹⁸³ Odôvodnenie 54 aktu o AI a bod 1 písm. b) prílohy III k aktu o AI.

k diskriminácii na základe osobitných kategórií osobných údajov, ako sú rasa, etnický pôvod, sexuálna orientácia, politické názory alebo náboženské presvedčenie.

9. ČLÁNOK 5 ODS. 1 PÍSM. H) AKTU O AI – SYSTÉMY DIAĽKOVEJ BIOMETRICKEJ IDENTIFIKÁCIE V REÁLNOM ČASE NA ÚČELY PRESADZOVANIA PRÁVA

289. V článku 5 ods. 1 písm. h) aktu o AI sa zakazuje používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, až na obmedzené výnimky taxatívne stanovené v akte o AI. Konkrétne sa v článku 5 ods. 1 písm. h) bodoch i) až iii) aktu o AI predpokladajú tri situácie, v ktorých možno povoliť používanie takýchto systémov, ak to povoľujú vnútroštátne právne predpisy a ak sú splnené podmienky a záruky uvedené v článku 5 ods. 2 až 7 aktu o AI.
290. V súlade s článkom 5 ods. 5 aktu o AI sa členské štáty môžu slobodne rozhodnúť, či a v ktorých z uvedených troch situácií je na ich území povolené používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva. Ak neexistujú vnútroštátne právne predpisy, ktoré by takéto používanie umožňovali a upravovali, orgány presadzovania práva a subjekty konajúce v ich mene nesmú takéto systémy nasadzovať na účely presadzovania práva. Predpokladom takéhoto použitia je preto existencia vnútroštátnych právnych predpisov, ktoré sú v súlade s príslušnými požiadavkami aktu o AI.
291. V článku 5 ods. 1 písm. h) aktu o AI sa zakazuje len používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, preto toto ustanovenie sa týka len subjektov nasadzujúcich takéto systémy. Uvádzanie takýchto systémov na trh a do prevádzky, ako aj používanie iných systémov diaľkovej biometrickej identifikácie nie je zakázané, ale podlieha pravidlám pre vysokorizikové systémy AI v súlade s článkom 6 ods. 2 aktu o AI a písmenom a) prílohy III k aktu o AI¹⁸⁴. Ak členský štát povolí používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva na ktorýkoľvek z troch cieľov uvedených v článku 5 ods. 1 písm. h) aktu o AI, pravidlá pre vysokorizikové systémy AI sa uplatňujú aj na toto používanie.
292. Na spätné používanie systémov diaľkovej biometrickej identifikácie na účely presadzovania práva sa vzťahujú osobitné pravidlá. Takéto používanie, ku ktorému nedochádza v reálnom čase, nie je zakázané, ale podlieha dodatočným zárukám pre nasadenie vysokorizikových systémov AI (článok 26 ods. 10 aktu o AI).

9.1. Odôvodnenie a ciele

293. V odôvodnení 32 aktu o AI sa uznáva rušivý charakter systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely

¹⁸⁴ Okrem toho sa na spätné používanie systémov diaľkovej biometrickej identifikácie na účely presadzovania práva vzťahujú osobitné pravidlá (článok 26 ods. 10 aktu o AI).

presadzovania práva, pokiaľ ide o práva a slobody dotknutých osôb, keďže môže ovplyvniť súkromný život veľkej časti obyvateľstva, vyvoláva pocit neustáleho sledovania a nepriamo odrádza od využívania slobody zhromažďovania a iných základných práv. Technické nepresnosti systémov AI určených na diaľkovú biometrickú identifikáciu fyzických osôb môžu viesť ku skresleným výsledkom a mať diskriminačné účinky. Takéto možné skreslené výsledky a diskriminačné účinky sú obzvlášť relevantné z hľadiska veku, etnickej príslušnosti, rasy, pohlavia alebo zdravotného postihnutia. Okrem toho, bezprostrednosť vplyvu a obmedzené možnosti ďalších kontrol alebo opráv v súvislosti s používaním takýchto systémov fungujúcich „v reálnom čase“ so sebou prinášajú zvýšené riziká z hľadiska práv a slobôd dotknutých osôb v súvislosti s činnosťami presadzovania práva alebo v ich dôsledku.

294. Ak je však použitie takýchto systémov nevyhnutne potrebné na dosiahnutie významného verejného záujmu a ak sú situácie, v ktorých môže k takémuto použitiu dôjsť, taxatívne vymenované a úzko vymedzené, toto použitie prevažuje nad rizikami pre základné práva (odôvodnenie 33 aktu o AI). S cieľom zabezpečiť, aby sa takéto systémy používali „zodpovedným a primeraným spôsobom“, podlieha ich používanie zárukám a osobitným povinnostiam a požiadavkám uvedeným v článku 5 ods. 2 až 7 aktu o AI.

9.2. Hlavné pojmy a zložky zákazu

Článok 5 ods. 1 písm. h) aktu o AI

Zakazujú sa tieto praktiky využívajúce AI:

h) používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, pokiaľ takéto použitie nie je nevyhnutne potrebné na jeden z týchto cieľov:

i) cielené pátranie po konkrétnych obetiach únosov, obchodovania s ľuďmi alebo sexuálneho vykorisťovania ľudí, ako aj pátranie po nezvestných osobách;

ii) predchádzanie konkrétnemu, závažnému a bezprostrednému ohrozeniu života alebo fyzickej bezpečnosti fyzických osôb alebo skutočnej a existujúcej alebo skutočnej a predvídateľnej hrozbe teroristického útoku;

iii) lokalizácia alebo identifikácia osoby podozrivej zo spáchania trestného činu na účel vedenia vyšetrovania alebo stíhania trestného činu alebo výkonu trestnej sankcie za trestné činy uvedené v prílohe II, za ktoré možno v dotknutom členskom štáte uložiť trest odňatia slobody alebo ochranné opatrenie obmedzujúce slobodu s hornou hranicou trestnej sadzby najmenej štyri roky.

Prvým pododsekom písm. h) nie je dotknutý článok 9 nariadenia (EÚ) 2016/679 na účely spracúvania biometrických údajov na iné účely ako je presadzovania práva.

295. Na uplatnenie zákazu podľa článku 5 ods. 1 písm. h) aktu o AI musí byť splnených niekoľko kumulatívnych podmienok:

i) systém AI musí byť systém diaľkovej biometrickej identifikácie;

- ii) činnosť spočíva v „používaní“ tohto systému;
 - iii) v „reálnom čase“;
 - iv) vo verejne prístupných priestoroch a
 - v) na účely presadzovania práva.
296. Druhá podmienka, t. j. „používanie“ systému AI, už bola analyzovaná v oddiele 2.3 týchto usmernení. Ďalšie uvedené podmienky sa bližšie opisujú a analyzujú v nasledujúcom texte.

9.2.1. Pojem diaľkovej biometrickej identifikácie

297. Technológie na biometrické rozpoznávanie zisťujú, zachytávajú a transformujú merateľné fyzické charakteristické znaky (ako sú vzdialenosť a veľkosť očí, dĺžka nosa atď.) alebo behaviorálne charakteristické znaky (ako sú chôdza alebo hlas) na strojovo čitateľné biometrické údaje [pozri oddiel 7.2.1 písm. d)]. Tieto údaje sú k dispozícii v rôznych formách: ako obrazy alebo vzory, ktoré sú matematickou reprezentáciou významných znakov jednotlivca a používajú sa na účely rozpoznávania. Technológie na biometrické rozpoznávanie sa používajú na účely overovania a identifikácie¹⁸⁵.
298. Podľa článku 3 bodu 41 aktu o AI systém diaľkovej biometrickej identifikácie je
- systém AI na účely identifikácie fyzických osôb bez ich aktívneho zapojenia, zvyčajne na diaľku prostredníctvom porovnania biometrických údajov osoby s biometrickými údajmi obsiahnutými v referenčnej databáze.*
299. Toto vymedzenie zahŕňa len identifikačnú funkciu systémov na biometrické rozpoznávanie, ktorá predpokladá absenciu aktívneho zapojenia dotknutých osôb (t. j. žiadnu aktívnu účasť) a vedie k zachytávaniu charakteristických znakov týchto osôb zvyčajne na diaľku. Na účely identifikácie sa zachytené biometrické údaje porovnávajú s biometrickými údajmi, ktoré sú už uložené v referenčnej databáze (ktorou môže byť úložisko, napríklad kriminálna databáza obsahujúca podoby tváre alebo vzory týkajúce sa podozrivých osôb).

a) Len na účely identifikácie

300. Pojem „biometrická identifikácia“ sa vymedzuje v článku 3 bode 35 aktu o AI ako
- automatizované rozpoznávanie fyzických, fyziologických a behaviorálnych alebo psychologických znakov človeka na účely stanovenia totožnosti fyzickej osoby porovnaním biometrických údajov daného jednotlivca s biometrickými údajmi jednotlivcov uloženými v databáze.*
301. V odôvodnení 15 aktu o AI sa ďalej objasňuje, že takéto znaky človeka môžu zahŕňať
- tvár, pohyb očí, tvar tela, hlas, reč, chôdza, držanie tela, srdcová frekvencia, tlak krvi, vôňa, dynamika písania na klávesnici.*

¹⁸⁵

Ako je vymedzené biometrickou komunitou v norme ISO/IEC 2382-37:2022 Informačné technológie. Slovník. Biometria, pojem 37.01.03.

302. Do vymedzenia biometrickej identifikácie možno zahrnúť aj systémy AI používané na sledovanie fyzických osôb, napríklad na zistenie, ktorým smerom uniká podozrivý. Možno to vyvodiť z článku 5 ods. 1 písm. h) bodu iii) aktu o AI, na základe ktorého sa umožňuje lokalizácia osôb podozrivých z trestných činov. Lokalizácia je možná, keď je osoba sledovaná.
303. Systémy AI, ktoré sú určené na biometrické overovanie, nepatria do rozsahu pôsobnosti zákazu v článku 5 ods. 1 písm. h) aktu o AI¹⁸⁶. Biometrické overenie (alebo autentifikácia) sa skladá z porovnávaní údajov zadaných na snímači s iným súborom predtým zaznamenaných údajov uložených v zariadení, ako sú smartfón, pas alebo preukaz totožnosti. Účelom biometrického overenia je overiť, či je konkrétna osoba osobou, o ktorej tvrdí, že ňou je.

Príkladom biometrického overenia je porovnanie tváre cestujúceho naskenovanej na elektronickej bráne s podobou tváre v jeho pase.

b) Činnosť na diaľku

304. Podľa článku 3 bodu 41 aktu o AI činnosť na diaľku znamená schopnosť biometrických systémov identifikovať osoby bez ich aktívneho zapojenia, zvyčajne na diaľku prostredníctvom porovnania biometrických údajov osoby s biometrickými údajmi obsiahnutými v referenčnej databáze.
305. Používanie biometrických systémov na potvrdenie totožnosti fyzickej osoby výlučne na účely prístupu k službe, odomknutia zariadenia alebo získania bezpečnostného prístupu do priestorov je vylúčené z pojmu „na diaľku“ (odôvodnenie 15 aktu o AI). Táto modalita sa používa napríklad pri kontrole prístupu¹⁸⁷.

Napríklad systém na identifikáciu tváre je nasadený na zabezpečenie vstupu do vyhradených priestorov (napríklad do priestorov elektrárne) prostredníctvom technológie skenovania tváre; systém porovnáva tvár osoby snímanú vstupnou kamerou s referenčnou podobou obsiahnutou v referenčnej databáze osôb s povoleným vstupom do budovy.

306. V odôvodnení 17 aktu o AI sa objasňuje, že toto vylúčenie z rozsahu pôsobnosti zákazu je odôvodnené skutočnosťou, že takéto systémy majú pravdepodobne malý vplyv na základné práva fyzických osôb v porovnaní so systémami diaľkovej biometrickej identifikácie, ktoré sa môžu použiť na spracúvanie biometrických údajov veľkého počtu osôb bez ich aktívneho zapojenia. V odôvodnení sa ďalej objasňuje, že systémy diaľkovej biometrickej identifikácie sa zvyčajne používajú na vnímanie viacerých osôb alebo ich správania súčasne, a to s cieľom výrazne uľahčiť identifikáciu fyzických osôb bez ich aktívneho zapojenia. Na aktívnu zapojenie nestačí, aby boli osoby informované

¹⁸⁶ Odôvodnenie 17 aktu o AI.

¹⁸⁷ Napríklad Ross A, Jain AK (2015) *Biometrics, Overview* (Biometria, prehľad), in: Li S.Z. a Jain A.K. (eds), *Encyclopedia of Biometrics*, (1. vydanie Springer Science, New York), s. 289 – 294.

o prítomnosti kamier, ale musia aktívne a vedome vstúpiť pred kameru, ktorá je nainštalovaná spôsobom podporujúcim aktívne zapojenie.

Napríklad:

– Systémy diaľkovej biometrickej identifikácie, ktoré sa používajú v kamerách inštalovaných na stenách alebo strope staníc metra na účely sledovania. Takýto systém spĺňa podmienku činnosti na diaľku.

– Systémy, ktoré sa používajú na umožnenie vstupu do stanice metra, ako sú biometrické lístky na metro, kde sa osoby aktívne zapájajú a vedome pristupujú k biometrickému snímaču, aby im bol umožnený vstup, túto podmienku nespĺňajú.

307. Systémy na biometrické rozpoznávanie, ktoré spracúvajú (bezkontaktné) odtlačky prstov, chôdzu, hlas, DNA, dynamiku písania na klávesnici a iné (biometrické) behaviorálne signály, môžu takisto predstavovať systémy diaľkovej biometrickej identifikácie¹⁸⁸.

Napríklad:

– Na identifikáciu hovoriacej osoby sa môže nasadiť systém hlasovej biometrie. Pomocou mikrofónu sa potom získa biometrická vzorka.

– Systém na rozpoznávanie chôdze sa môže používať prostredníctvom CCTV a videozáznamy sa automaticky kontrolujú na zistenie výskytu zhôd s predtým zachytenými vzormi.

– Biometrická technológia dynamiky písania na klávesnici sa môže použiť na identifikáciu osoby, ktorá píše podvodnú správu.

Skutočnosť, že tieto systémy sú uvedené ako príklady systémov diaľkovej biometrickej identifikácie, neznamená, že sú zakázané podľa článku 5 aktu o AI.

308. V prípade telových kamier umožňujúcich diaľkovú biometrickú identifikáciu, ktoré môžu používať jednotliví príslušníci orgánov presadzovania práva, sa necielené filmovanie napríklad počas demonštrácie so stovkami účastníkov bude považovať za splnenie podmienky činnosti na diaľku.

c) Referenčná databáza

309. Identifikácia nie je možná bez referenčnej databázy obsahujúcej biometrické údaje na účely porovnania. Existencia referenčnej databázy je teda **nevyhnutná** na vykonanie porovnania na účely identifikácie¹⁸⁹.

¹⁸⁸ Spoločné stanovisko EDPB a EDPS 5/2021, s. 11; Rada Európskej únie, „Stanovisko právneho servisu“, 12302/22, 12. septembra 2022, bod 33, a odôvodnenie 15 aktu o AI.

¹⁸⁹ Odôvodnenie 34 aktu o AI.

Napríklad v prípade nezvestných osôb by sa databáza Schengenského informačného systému¹⁹⁰ mohla použiť ako referenčná databáza na účely rozpoznávania tváre (po uvedení do prevádzky).

9.2.2. V reálnom čase

310. V reálnom čase znamená, že systém zachytáva a ďalej spracováva biometrické údaje „okamžite, takmer okamžite alebo v každom prípade bez výrazného časového odstupu“¹⁹¹. Všetky kroky spracovania, t. j. zachytenie, porovnanie a identifikácia biometrických údajov, prebiehajú súčasne alebo takmer súčasne, čo môže zahŕňať „limitované menšie oneskorenie“, aby sa zabránilo obchádzaniu zákazu prostredníctvom spätného používania systémov diaľkovej biometrickej identifikácie¹⁹². Pojem „bez výrazného časového odstupu“ nie je v akte o AI vymedzený; bude potrebné posúdenie od prípadu k prípadu. Keďže zariadenia používané na identifikáciu v reálnom čase alebo na následnú diaľkovú identifikáciu sú čoraz častejšie jedno a to isté s rôznymi funkciami, rozlišovanie je na základe času. Vo všeobecnosti je odstup významný aspoň vtedy, keď možno predpokladať, že osoba pravdepodobne opustila miesto, kde boli biometrické údaje zachytené.
311. Systémy v reálnom čase sa vo všeobecnosti používajú na danom mieste na uľahčenie rýchlej reakcie a nie na spätnú identifikáciu osôb. Používateľovi systému poskytujú prostriedky na sledovanie pohybu sledovaných osôb a ich monitorovanie.

- a) Systém AI kontroluje všetkých prichádzajúcich návštevníkov na mieste konania koncertu: diaľková biometrická identifikácia v reálnom čase.
- b) Systém nahráva všetkých prichádzajúcich návštevníkov koncertu na videozáznam. Na koncerte sa stane incident. Po koncerte sa na videozázname spustí identifikačný systém s cieľom identifikovať páchatel'a: následná diaľková biometrická identifikácia.

312. Ak orgán presadzovania práva tajne odфотографuje osobu prostredníctvom mobilného zariadenia a odošle ju do databázy na okamžité vyhľadanie, môže sa na to v závislosti od okolností vzťahovať zákaz podľa článku 5 ods. 1 písm. h) aktu o AI.

9.2.3. Vo verejne prístupných priestoroch

313. V článku 3 bode 44 aktu o AI sa **verejne prístupné priestory** vymedzujú ako
- akékoľvek fyzické miesto vo verejnom alebo v súkromnom vlastníctve prístupné neurčenému počtu fyzických osôb bez ohľadu na to, či možno uplatniť určité podmienky prístupu, a bez ohľadu na možné obmedzenia kapacity.*

¹⁹⁰ Zápisy o nezvestných osobách (článok 32 rozhodnutia o SIS II); rozhodnutie Rady 2007/533/SVV z 12. júna 2007 o zriadení, prevádzke a využívaní Schengenského informačného systému druhej generácie (SIS II).

¹⁹¹ Odôvodnenie 17 aktu o AI.

¹⁹² V článku 3 bode 42 aktu o AI.

314. V odôvodnení 19 aktu o AI sa uvádza niekoľko prvkov, ktoré charakterizujú takéto priestory:

- Prístupnosť pre neurčený počet osôb, nezávisle od potenciálnych kapacitných alebo bezpečnostných obmedzení, ako sú kúpa vstupenky alebo cestovného lístka, predchádzajúca registrácia alebo určitá veková hranica. Možnosť prístupu do priestoru cez nezamknuté dvere neznamena, že priestor je verejne prístupný, ak existujú náznaky alebo okolnosti, ktoré naznačujú opak (napríklad označenie obmedzujúce prístup). Prístup do priestoru môže byť okrem toho obmedzený na určité osoby, ako sa vymedzuje v právnych predpisoch, a to v súvislosti s verejnou bezpečnosťou alebo ochranou, alebo rozhodnutím osoby, ktorá má nad priestorom príslušné právomoci.

V zásade sú verejne prístupné priestory napríklad:

- miesto konania koncertu, na ktorom účastníci platia vstupné,
- miesto, kde sa organizuje veľtrh zameraný na účastníkov starších ako 50 rokov.

Priestor uzavretý bránou, aj keď je odomknutá, ako napríklad vstup do oplotenej obytnej zóny niekoľkých domov, sa obvykle nepovažuje za verejne prístupný priestor. Naopak, park v uzavretej obytnej zóne s otváracími hodinami pre verejnosť bez obmedzenia prístupu počas týchto hodín bude vo všeobecnosti predstavovať verejne prístupný priestor počas týchto hodín a uzavretý priestor mimo uvedených hodín.

- Irelevantnosť vlastníctva, t. j. priestor nemusí byť vo verejnom vlastníctve, aby sa považoval za verejne prístupný priestor.

Priestor môže napríklad vlastníť súkromný subjekt alebo verejný subjekt, prípadne ho môže vlastníť verejný subjekt a spravovať súkromný subjekt, pričom to nemá vplyv na charakter priestoru.

- Nie je určená špecifická činnosť, na ktorú sa priestor využíva; verejne prístupný priestor nemusí byť nevyhnutne priestor spojený s verejnou službou. Okrem toho priestor spojený s verejnou službou môže zahŕňať aj priestory, ktoré nie sú verejne prístupné, t. j. kancelárie zamestnancov verejnej správy pracujúcich v rámci obce.

Verejne prístupné priestory sa môžu využívať napríklad na obchodovanie, ako napríklad predajne, reštaurácie, kaviarne atď., pre služby, ako napríklad banky, profesionálne činnosti (ordinácia lekára, ako aj kancelária účtovníka), ubytovacie a pohostinské služby (napríklad hotel) atď., na šport, ako napríklad plavecké bazény, posilňovne, štadióny atď., pre dopravu, ako napríklad autobusové zastávky, stanice metra a železničné stanice, letiská, dopravné prostriedky atď., na zábavu, ako

napríklad kiná, divadlá, múzeá, koncertné a konferenčné sieni atď., alebo na voľný čas alebo iné činnosti, ako napríklad verejné cesty a námestia, parky, lesy, ihriská¹⁹³.

315. Nasledujúce priestory nepredstavujú verejne prístupné priestory v zmysle článku 5 ods. 1 písm. h) aktu o AI:

- online priestory, pretože nepredstavujú fyzický priestor v zmysle článku 3 bodu 44 aktu o AI,

Z rozsahu pôsobnosti zákazu sú preto vylúčené napríklad chatové miestnosti, sociálne médiá, online platformy atď.

- určité priestory určené na prístup obmedzenému počtu osôb, ako sú továrne, spoločnosti a pracoviská s kontrolou prístupu alebo obmedzením na príslušných zamestnancov alebo poskytovateľov služieb, pretože do nich majú prístup len príslušní zamestnanci a poskytovatelia služieb¹⁹⁴.

Napríklad pracovisko prístupné prostredníctvom preukazu sa v zásade nepovažuje za verejne prístupný priestor, zatiaľ čo kancelária bez kontroly prístupu ním môže byť.

- **väznice a hraničná kontrola** nie sú verejne prístupné priestory¹⁹⁵.

316. Napríklad hraničný priechod nie je verejne prístupným priestorom, zatiaľ čo ulica vedúca k hraničnému priechodu alebo les v jeho blízkosti ním zvyčajne je.

317. Niektoré priestory môžu mať dvojakú funkciu. Napríklad letisko sa vo všeobecnosti považuje za verejne prístupný priestor, pokiaľ ide o jeho spoločné priestory, ale priestor určený na hraničnú kontrolu (kde stoja colníci a kde prebieha kontrola pasov alebo dokladov totožnosti) je z rozsahu pôsobnosti zákazu vylúčený.

318. Ako je objasnené v odôvodnení 19 aktu o AI, to, či je priestor prístupný verejnosti, by sa malo posudzovať od prípadu k prípadu.

9.2.4. Na účely presadzovania práva

319. Zákaz v článku 5 ods. 1 písm. h) aktu o AI sa vzťahuje na používanie systémov diaľkovej biometrickej identifikácie na účely presadzovania práva bez ohľadu na subjekt, orgán alebo inštitúciu, ktoré vykonávajú činnosti presadzovania práva.

320. Presadzovanie práva je vymedzené v článku 3 bode 46 aktu o AI ako „činnosti vykonávané orgánmi presadzovania práva alebo v ich mene na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo na účely výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania

¹⁹³ Odôvodnenie 19 aktu o AI.

¹⁹⁴ Odôvodnenie 19 aktu o AI.

¹⁹⁵ Odôvodnenie 19 aktu o AI. V inom kontexte bola kontrola hraníc vymedzená ako činnosť vykonávaná na hraniciach na účely nariadenia (EÚ) 2016/399 (Kódex schengenských hraníc) a v súlade s ním, výlučne v nadväznosti na úmysel prekročiť takúto hranicu alebo na prekročenie takejto hranice. Nepatrí sem takzvaná pohraničná oblasť, ktorá sa môže rozprestierať maximálne do 50 kilometrov na oboch stranách hranice.

takémuto ohrozeniu.“ Tieto účely sú rovnaké ako účely uvedené v článku 1 smernice o presadzovaní práva¹⁹⁶. Akýkoľvek výklad týchto účelov vo vzťahu k smernici o presadzovaní práva môže byť preto relevantný aj na účely výkladu pojmu „presadzovanie práva“ použitého v akte o AI.

321. Účely presadzovania práva zahŕňajú vyšetrovanie, odhaľovanie a stíhanie trestných činov. Zahŕňajú aj činnosti súvisiace s predchádzaním trestným činom vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu, a to pred tým, ako bol akýkoľvek trestný čin skutočne spáchaný. Polícia môže napríklad prijať „donucovacie opatrenia pri demonštráciách, významných športových podujatiach alebo nepokojoch“ v rámci predchádzania trestnej činnosti¹⁹⁷. Napokon tieto činnosti zahŕňajú výkon sankcií, ako je napríklad výkon trestu.
322. Podľa článku 3 bodu 46 aktu o AI sa činnosti presadzovania práva môžu vykonávať orgánmi presadzovania práva alebo v ich mene. Orgány presadzovania práva sú ďalej vymedzené v článku 3 bode 45 aktu o AI rovnakým spôsobom, ako sú vymedzené príslušné vnútroštátne orgány v smernici o presadzovaní práva¹⁹⁸. Toto vymedzenie zahŕňa orgány presadzovania práva a poverené orgány alebo subjekty (ktorými môžu byť súkromné subjekty):

- a) *každý orgán verejnej moci príslušný v oblasti predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania, alebo v oblasti výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu, alebo*

Medzi takéto orgány verejnej moci patria napríklad policajné orgány a orgány trestnej justície (napríklad prokurátori), keď vykonávajú úlohu v oblasti presadzovania práva.

- b) *každý iný orgán alebo subjekt, ktorý bol právom členského štátu poverený vykonávať verejnú moc a verejné právomoci na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu;*

323. Podľa aktu o AI môžu iné subjekty, orgány alebo osoby vykonávať činnosti presadzovania práva po tom, ako boli právom členského štátu poverené vykonávať verejnú moc a verejné právomoci na už uvedené účely.
324. „V mene“ znamená, že orgán presadzovania práva poveril výkonom činnosti v oblasti presadzovania práva (alebo jej časti) iný subjekt alebo osobu vrátane súkromných

¹⁹⁶ Niektoré činnosti orgánov presadzovania práva sú vylúčené z rozsahu pôsobnosti smernice o presadzovaní práva, napríklad keď vykonávajú administratívne úlohy (napríklad v oblasti ľudských zdrojov), tieto činnosti sa vykonávajú mimo rámca presadzovania práva. Patria do rozsahu pôsobnosti všeobecného nariadenia o ochrane údajov. Pozri odôvodnenie 19 všeobecného nariadenia o ochrane údajov.

¹⁹⁷ Odôvodnenie 12 smernice o presadzovaní práva.

¹⁹⁸ Článok 3 bod 7 smernice o presadzovaní práva.

subjektov, alebo v konkrétnych prípadoch požiadal iný subjekt alebo osobu, aby konala na podporu činností presadzovania práva. V oboch prípadoch musia orgány presadzovania práva poučiť druhý subjekt o všetkých hlavných aspektoch a dohliadať naň, keďže táto požiadavka je neoddeliteľnou súčasťou pojmu konania „v mene“ určitej osoby.

Delegovanie úloh na iné orgány môže zahŕňať napríklad:

- keď orgány presadzovania práva požiadajú podniky verejnej dopravy, aby zaistili bezpečnosť v sieťach verejnej dopravy podľa ich pokynov a pod ich dohľadom,
- keď orgány presadzovania práva požiadajú športové federácie, aby konali podľa ich pokynov a pod ich dohľadom v záujme zaistenia bezpečnosti na športových podujatiach,
- keď orgány presadzovania práva požiadajú banky, aby vykonali určité opatrenia na „boj proti určitým trestným činom v konkrétnych prípadoch“ podľa pokynov a pod dohľadom orgánov presadzovania práva.

Tieto činnosti patria pod vymedzenie pojmu „na účely presadzovania práva“, keďže tieto subjekty konajú „v mene“ orgánov presadzovania práva. Ak uvedené subjekty pri odhaľovaní trestných činov (napríklad podvod, pranie špinavých peňazí) a boji proti nim konajú „vo vlastnom mene“, nebudú sa považovať za subjekty, na ktoré sa vzťahuje zákaz podľa článku 5 ods. 1 písm. h) aktu o AI.

325. Činnosti týchto iných orgánov alebo subjektov patria pod vymedzenie pojmu „presadzovanie práva“, iba ak boli tieto iné orgány alebo subjekty poverené konkrétnou úlohou presadzovania práva.

9.3. Výnimky zo zákazu

326. V akte o AI sa stanovujú tri výnimky zo všeobecného zákazu používania diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva. V článku 5 ods. 1 písm. h) bodoch i) až iii) aktu o AI sú taxatívne vymenované tri ciele, na ktoré možno povoliť diaľkovú biometrickú identifikáciu v reálnom čase, zatiaľ čo v článku 5 ods. 2 až 7 aktu o AI sú stanovené podmienky a záruky pre takéto povolenie. Ustanovenia v článku 5 ods. 1 písm. h) bodoch i) až iii) aktu o AI samy osebe nepredstavujú právny základ pre používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch. Použitie diaľkovej biometrickej identifikácie v reálnom čase môže umožniť len vnútroštátne právo členského štátu, ktoré spĺňa najmä požiadavky článku 5 ods. 2 až 7 aktu o AI, ako sa uvádza v článku 5 ods. 2 aktu o AI. Ak teda neexistujú právne predpisy členského štátu, ktoré by povoľovali používanie diaľkovej biometrickej identifikácie v reálnom čase na jeden alebo viacero z uvedených cieľov, takéto používanie je od 2. februára 2025 zakázané.

9.3.1. Odôvodnenie a ciele

327. Cieľmi stanovenými v článku 5 ods. 1 písm. h) bodoch i) až iii) aktu o AI sa má umožniť používanie určitých nástrojov AI a vyšetrovacích nástrojov na účely presadzovania práva. Medzi tieto ciele patrí:

i) cielené pátranie po obetiach troch konkrétnych závažných trestných činov a po nezvestných osobách [ochrana];

ii) predchádzanie bezprostrednému ohrozeniu života alebo fyzickej bezpečnosti alebo skutočnej hrozbe teroristických útokov [predchádzanie] a

iii) lokalizácia alebo identifikácia podozrivých osôb a páchatel'ov určitých závažných trestných činov uvedených v prílohe II [stíhanie/vyšetrovanie].

328. V uvedených scenároch zákonodarca Únie vyvážil bezpečnostné potreby spoločnosti s rizikom, ktoré systémy diaľkovej biometrickej identifikácie v reálnom čase predstavujú pre základné práva jednotlivcov, na ktorých uvedené systémy pôsobia. Podľa odôvodnenia 33 aktu o AI ciele, na ktoré je povolené používanie systémov diaľkovej biometrickej identifikácie v reálnom čase na účely presadzovania práva vo verejne prístupných priestoroch, musia byť prísne, taxatívne a úzko vymedzené a uplatniť sa, ak existuje „nevyhnutná potreba“ dosiahnuť „významný verejný záujem“, ktorý „prevažuje nad rizikami“, ktoré to predstavuje pre základné práva. Akékoľvek iné používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, ktoré nie je uvedené v článku 5 ods. 1 písm. h) bodoch i) až iii) aktu o AI, je zakázané.

Napríklad používanie systémov diaľkovej biometrickej identifikácie v reálnom čase políciou na identifikáciu zlodca v obchode a porovnanie podoby jeho tváre s databázami trestných činov je zakázané, pretože nepatrí pod žiadny z cieľov uvedených v článku 5 ods. 1 písm. h) bodoch i) až iii) aktu o AI.

9.3.2. Cielené pátranie po obetiach troch závažných trestných činov a po nezvestných osobách

329. Podľa článku 5 ods. 1 písm. h) bodu i) aktu o AI je používanie diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva povolené, ak je nevyhnutne potrebné a ak sú splnené podmienky uvedené v článku 5 ods. 2 až 7 aktu o AI, na cielené pátranie po obetiach únosov, obchodovania s ľuďmi alebo sexuálneho vykorisťovania ľudí, ako aj na pátranie po nezvestných osobách.

a) Cielené pátranie po obetiach troch druhov trestných činov

330. Cieľom scenára opísaného v článku 5 ods. 1 písm. h) bode i) aktu o AI je pomôcť orgánom presadzovania práva pri pátraní po obetiach troch závažných trestných činov.

331. Cielené pátranie by zahŕňalo lokalizáciu a identifikáciu obetí.

Tri druhy trestných činov

332. Scenár uvedený v článku 5 ods. 1 písm. h) bode i) aktu o AI sa vzťahuje na ciele pátranie po konkrétnych obetiach troch závažných trestných činov: únosov ľudí, obchodovania s ľuďmi a sexuálneho vykorisťovania ľudí¹⁹⁹.

Ak dôjde napríklad k únosu dieťaťa a existujú konkrétne indície, že únosca má v úmysle dopraviť dieťa z jedného miesta na druhé autom, polícia môže použiť systém diaľkovej biometrickej identifikácie v reálnom čase na ciele pátranie po tomto dieťati, ale musí vymedziť rozsah jeho nasadenia a trvanie použitia na identifikáciu dieťaťa.

b) Pátranie po nezvestných osobách

333. Prvý scenár zahŕňa aj pátranie po nezvestnej osobe²⁰⁰.
334. Možno rozlišovať medzi nezvestnými deťmi a nezvestnými dospelými osobami, pretože dobrovoľné zmiznutie nezvestnej dospelé osoby nepovedie vždy k začatiu pátrania. Platné pravidlá týkajúce sa nezvestných detí sa v jednotlivých členských štátoch značne líšia²⁰¹. V každom prípade možno podľa článku 5 ods. 1 písm. h) bodu i) aktu o AI používať systém diaľkovej biometrickej identifikácie v reálnom čase len na pátranie po nezvestných osobách na účely presadzovania práva.
335. Zmiznutie dospelé osoby nemusí vždy viesť k policajnému pátraniu po tejto osobe, pretože dospelé osoby majú právo zmiznúť. Pátranie by mohlo súvisieť s právnym postavením osoby (keď sa uplatňuje opatrovníctvo), jej zdravotným stavom (duševná choroba), existenciou správy vyjadrujúcej samovražedný úmysel, ale aj odchodom bez osobných vecí. Ak sú okolnosti zmiznutia dôvodom na obavy, zmiznutie sa môže nahlásiť na políciu, aby sa mohlo začať pátranie.
336. V niektorých členských štátoch sa pátranie po nezvestnej osobe môže uskutočniť v rámci administratívneho postupu a nie na účely presadzovania práva. Ak je napríklad zraniteľná osoba nezvestná, ale neexistuje podozrenie z trestného činu ani žiadny iný účel presadzovania práva, použitie systémov diaľkovej biometrickej identifikácie v reálnom čase na pátranie po tejto osobe by sa nepovažovalo za použitie na účely

¹⁹⁹ Únos, obchodovanie s ľuďmi a sexuálne vykorisťovanie sú tri trestné činy, ktoré môžu viesť k vydaniu európskeho zatýkacieho rozkazu na zatknutie osoby podozrivej zo spáchania uvedených trestných činov alebo odsúdené osoby a jej odovzdanie do krajiny, ktorá európsky zatýkací rozkaz vydala. Tieto tri trestné činy sa týkajú najmä, nie však výlučne, žien a detí. Podľa Generálneho riaditeľstva Európskej komisie pre migráciu a vnútorné záležitosti takmer 40 % obetí tvoria občania EÚ a väčšina z nich sú ženy a deti, ktoré sa stali obeťami obchodovania s ľuďmi na účely sexuálneho vykorisťovania. Počet obetí z radov mužov sa za desať rokov takmer zdvojnásobil. Obchoduje sa s nimi na účely nútenej práce a núteného žobrania, zatiaľ čo s väčšinou žien a detí sa obchoduje na účely sexuálneho vykorisťovania. https://home-affairs.ec.europa.eu/policies/internal-security/organised-crime-and-human-trafficking/together-against-trafficking-human-beings_sk.

²⁰⁰ Pojem „nezvestná osoba“ nie je na úrovni EÚ vymedzený. V záveroch Rady z decembra 2021 o zintenzívnení cezhraničnej policajnej spolupráce v oblasti nezvestných osôb sa však Rada odvoláva na vymedzenie nezvestnej osoby v odporúčaní Rady Európy CM/Rec (2009) 12, ako aj vo vnútroštátnych právnych predpisoch. Závery Rady (2021) 14808/21, bod 11, strana 4.

²⁰¹ Európska komisia, Európska migračná sieť, *How do EU Member States treat cases of missing unaccompanied minors?* (Ako členské štáty EÚ riešia prípady nezvestných maloletých osôb bez sprievodu?), EMN Inform, 2020.

presadzovania práva, a preto by sa naň vzťahovali pravidlá takéhoto použitia podľa všeobecného nariadenia o ochrane údajov.

9.3.3. Predchádzanie bezprostrednému ohrozeniu života alebo teroristickým útokom

337. V článku 5 ods. 1 písm. h) bode ii) aktu o AI sa uvádza druhý scenár, v ktorom je povolené používanie diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, a to za predpokladu, že je to nevyhnutne potrebné a že sú splnené podmienky stanovené v článku 5 ods. 2 až 7 aktu o AI

predchádzanie konkrétnemu, závažnému a bezprostrednému ohrozeniu života alebo fyzickej bezpečnosti fyzických osôb alebo skutočnej a existujúcej alebo skutočnej a predvídateľnej hrozbe teroristického útoku.

a) Konkrétne, závažné a bezprostredné ohrozenie života alebo fyzickej bezpečnosti fyzických osôb

338. Podľa článku 2 charty, ktorým sa zaručuje právo na život, musia Únia a jej členské štáty poskytovať záruky pre životy jednotlivcov, a teda ich chrániť. Na základe kritérií v článku 5 ods. 1 písm. h) bode ii) aktu o AI týkajúcich sa ohrozenia života sa na povolenie používania systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch vyžaduje existencia 1. konkrétneho, 2. závažného a 3. bezprostredného ohrozenia života alebo fyzickej bezpečnosti 4. fyzických osôb. Hrozba nemusí byť obmedzená na identifikovaných jednotlivcov alebo skupinu, pretože sa týka fyzických osôb vo všeobecnosti.
339. V odôvodnení 33 aktu o AI sa objasňuje, že bezprostredné ohrozenie života alebo fyzickej bezpečnosti fyzických osôb môže zahŕňať aj bezprostredné ohrozenie kritickej infraštruktúry²⁰², „ak by narušenie alebo zničenie takejto kritickej infraštruktúry viedlo k bezprostrednému ohrozeniu života alebo fyzickej bezpečnosti osoby, a to aj v dôsledku vážnej ujmy na poskytovaní základných dodávok pre obyvateľstvo alebo výkone základných funkcií štátu.“

Napríklad:²⁰³

Bezprostredné ohrozenie života alebo fyzickej bezpečnosti osoby môže vyplývať aj zo závažného narušenia a zničenia kritickej infraštruktúry (napríklad elektrárne, zásobovania vodou alebo nemocnice), ak dôjde k vážnej ujme v podobe zastavenia základných dodávok pre obyvateľstvo (nedostatok elektrickej energie alebo pitnej vody počas dlhého obdobia, v mimoriadne teplom alebo chladnom počasí atď.)

340. To, čo predstavuje bezprostredné ohrozenie života alebo fyzickej bezpečnosti fyzických osôb, sa v konečnom dôsledku vymedzuje a posudzuje na úrovni členského štátu na základe jeho vnútroštátnych právnych predpisov v súlade s právom EÚ, najmä

²⁰² Ako sa vymedzuje v článku 2 bode 4 smernice 2022/2557.
²⁰³ Odôvodnenie 33 aktu o AI.

s prihliadnutím na kľúčové prvky a odôvodnenie článku 5 aktu o AI. Bude sa to musieť stanoviť, resp. budú sa na to musieť uviesť odkazy v zákonoch, ktoré musia členské štáty prijať, aby mohli využívať výnimky zo zákazu používania diaľkovej biometrickej identifikácie v reálnom čase na účely presadzovania práva vo verejne prístupných priestoroch.

341. **Bezprostredné** ohrozenie života alebo fyzickej bezpečnosti je ohrozenie, ktorá môže nastať v ktoromkoľvek okamihu a vyžaduje si „**prijatie okamžitých opatrení**“²⁰⁴. **Závažné** ohrozenie fyzickej bezpečnosti sa týka vážnych zranení.
342. Konkrétne ohrozenie znamená, že ohrozenie je jasne vymedzené, individualizované a špecifické, teda že by nemalo byť hypotetické alebo sa týkať určitých nebezpečenstiev vo všeobecnosti.

Polícia napríklad získa informáciu, že bývalý študent plánuje smrtiaci útok na svojej bývalej univerzite, pretože sa chce pomstiť niekoľkým bývalým spolužiakom. Polícia dostane informácie o bezprostrednej hrozbe útoku, o škole, ktorá má byť cieľom útoku, a o zbraniach, ktoré plánuje použiť na uskutočnenie svojich plánov.

343. Konkrétne ohrozenie nemusí byť úmyselné. Aj neúmyselné konanie by mohlo viesť k ohrozeniu života alebo fyzickej bezpečnosti.

b) Skutočná a existujúca alebo skutočná a predvídateľná hrozba teroristického útoku

344. Táto časť druhého scenára opísaného v článku 5 ods. 1 písm. h) bode ii) aktu o AI sa skladá z niekoľkých prvkov: existencia hrozby teroristického útoku a charakteristiky hrozby, ktorá musí byť skutočná a existujúca alebo skutočná a predvídateľná.

Hrozba teroristického útoku

345. Posúdenie existencie a závažnosti hrozby sa vykonáva na vnútroštátnej úrovni pri posudzovaní skutočných okolností opatrenia, ktoré sa má prijať na zaistenie národnej bezpečnosti a konkrétnejšie v prípade teroristického útoku. **Úroveň teroristickej hrozby je vymedzená na vnútroštátnej úrovni** a v jednotlivých členských štátoch sa líši. Napríklad Holandsko stanovilo päť úrovní hrozby²⁰⁵, Belgicko štyri²⁰⁶, Francúzsko tri²⁰⁷ a Švédsko päť²⁰⁸. Pojem „skutočná a existujúca alebo skutočná a predvídateľná hrozba“, ako sa používa v článku 5 ods. 1 písm. h) bode ii), je však autonómnym pojmom práva Únie, a preto by sa mal v zásade posudzovať nezávisle od vnútroštátneho vymedzenia. Hrozba sa netýka terorizmu vo všeobecnosti, ale konkrétne hrozby teroristického útoku.

Charakteristika hrozby: skutočná a existujúca alebo skutočná a predvídateľná

²⁰⁴ Odôvodnenie 37 nariadenia (EÚ) 2023/1543.

²⁰⁵ <https://www.government.nl/topics/counterterrorism-and-national-security/risk-of-an-attack-threat-level>.

²⁰⁶ <https://cuta.belgium.be>; <https://crisiscenter.be/en/risks-belgium/security-risks/terrorism-and-extremism>.

²⁰⁷ <https://www.sgdsn.gouv.fr/vigipirate#>; <https://www.sgdsn.gouv.fr/files/files/Vigipirate/20160130-np-sgdsn-pse-tackling-terrorism-together.pdf>.

²⁰⁸ <https://www.krisinformation.se/en/hazards-and-risks/terrorism>.

346. Hranica závažnosti, ktorú musí hrozba dosiahnuť, aby bolo možné používať systémy diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, bola inšpirovaná judikatúrou Súdneho dvora Európskej únie týkajúcou sa opatrení v oblasti uchovávaní údajov a záznamov o cestujúcich, ktorých cieľom je ochrana národnej bezpečnosti, najmä pred teroristickými útokmi. Podľa Súdneho dvora Európskej únie v uvedených súvislostiach „musí byť hrozba pre národnú bezpečnosť skutočná a aktuálna, alebo prinajmenšom predvídateľná, čo predpokladá existenciu dostatočne konkrétnych okolností.“²⁰⁹

Predchádzanie

347. Na rozdiel od článku 5 ods. 1 písm. h) bodu i) a článku 5 ods. 1 písm. h) bodu iii) aktu o AI sa v scenári opísanom v článku 5 ods. 1 písm. h) bode ii) neuvádza, že použitie diaľkovej biometrickej identifikácie v reálnom čase je povolené na lokalizáciu alebo identifikáciu konkrétnej osoby. Jeho účelom je predchádzanie konkrétnemu ohrozeniu. Scenár sa preto môže vzťahovať aj na použitie diaľkovej biometrickej identifikácie v reálnom čase na odhaľovanie a sledovanie „teroristov v pohybe“, t. j. viacerých osôb spojených s tou istou hrozbou, ak existujú konkrétne náznaky, že tieto osoby plánujú spáchať teroristický útok, ale nie je jasné kde.

Diaľková biometrická identifikácia v reálnom čase na predchádzanie teroristickému útoku v parku

Polícia dostala informáciu, že po parku pobehuje osoba, ktorá hľadá ľudí, na ktorých by mohla zaútočiť nožom, pričom vykrikuje násilné extrémistické heslá, ktoré sa zvyčajne spájajú s teroristickými útokmi a teroristickými skupinami. Ak členský štát povolil používanie diaľkovej biometrickej identifikácie v reálnom čase v scenári opísanom v článku 5 ods. 1 písm. h) bode ii) aktu o AI, orgány presadzovania práva môžu použiť diaľkovú biometrickú identifikáciu v reálnom čase na identifikáciu a lokalizáciu osoby v parku a jeho okolí s cieľom zabrániť útoku, ak sú splnené ostatné podmienky článku 5 ods. 2 až 7 aktu o AI.

9.3.4. Lokalizácia a identifikácia osôb podozrivých z niektorých trestných činov

348. Podľa článku 5 ods. 1 písm. h) bodu iii) aktu o AI sa povoľuje používanie diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na „lokalizáci[u] alebo identifikáci[u] osoby podozrivej zo spáchania trestného činu na účel vedenia vyšetrovania alebo stíhania trestného činu alebo výkonu trestnej sankcie za trestné činy uvedené v prílohe II, za ktoré možno v dotknutom členskom štáte uložiť trest odňatia slobody alebo ochranné opatrenie obmedzujúce slobodu s hornou hranicou trestnej sadzby najmenej štyri roky.“

²⁰⁹

Rozsudok Súdneho dvora z 20. septembra 2022, SpaceNet, C-793/19 (spojené veci C-793/19, C-794/19), ECLI:EU:C:2022:702, bod 93.

V prílohe II k aktu o AI sa uvádza taxatívny zoznam závažných trestných činov, pri ktorých možno povoliť použitie diaľkovej biometrickej identifikácie v reálnom čase na už uvedený účel. Ide o tieto trestné činy:

- terorizmus,
- obchodovanie s ľuďmi,
- sexuálne vykorisťovanie detí a detská pornografia,
- nedovolené obchodovanie s omamnými alebo psychotropnými látkami,
- nedovolené obchodovanie so zbraňami, strelivom alebo s výbušninami,
- vražda, ťažká ujma na zdraví,
- nedovolené obchodovanie s ľudskými orgánmi alebo tkanivami,
- nedovolené obchodovanie s jadrovými alebo rádioaktívnymi materiálmi,
- únos, obmedzovanie osobnej slobody alebo branie rukojemníka,
- trestné činy podliehajúce právomoci Medzinárodného trestného súdu,
- nezákonné ovládnutie lietadla alebo plavidla,
- znásilnenie,
- trestné činy proti životnému prostrediu,
- organizovaná alebo ozbrojená lúpež,
- sabotáž,
- účasť v zločineckej organizácii zapojenej do jedného alebo viacerých vyššie uvedených trestných činov.

a) Lokalizácia a identifikácia

349. Členský štát môže povoliť používanie diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva s cieľom lokalizovať a identifikovať osobu podozrivú z trestného činu na účely vedenia vyšetrovania trestného činu, stíhania tejto osoby za spáchaný trestný čin alebo výkonu existujúceho trestu.

b) Podozrivé osoby a páchatelia

350. Článok 5 ods. 1 písm. h) bod iii) aktu o AI sa vzťahuje na dve kategórie osôb: podozrivé osoby a páchatel'ov. Podozrivá osoba je osoba, v súvislosti s ktorou existujú závažné dôvody domnievať sa, že spáchala trestný čin, a o zapojení tejto osoby do trestného činu už boli zhromaždené dostatočné dôkazy. Páchatel' je osoba, ktorá je obvinená zo spáchania trestného činu alebo odsúdená za spáchanie trestného činu. Rovnaké podmienky (trestný čin uvedený v prílohe II a horná hranica trestnej sadzby najmenej štyri roky) platia aj v prípade lokalizácie alebo identifikácie spolupáchatel'a trestných činov uvedených v prílohe II k aktu o AI.

c) Zoznam závažných trestných činov

351. Používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva je opodstatnené len pri závažných trestných činoch.
352. Prvých päť trestných činov uvedených v prílohe II k aktu o AI je rovnakých ako „únijné trestné činy“ uvedené v článku 83 ZFEÚ, zatiaľ čo ostatné trestné činy predstavujú priority spolupráce v oblasti presadzovania práva²¹⁰. Niektoré z nich (napríklad únos, nedovolené obchodovanie s jadrovými alebo rádioaktívnymi materiálmi) môžu byť spojené s terorizmom²¹¹.
353. Hoci všetky trestné činy uvedené v prílohe II môžu viesť k vydaniu európskeho zatýkacieho rozkazu na podozrivú osobu alebo páchatel'a, použitie diaľkovej biometrickej identifikácie v reálnom čase na lokalizáciu a identifikáciu osoby podozrivej zo spáchania niektorého z týchto závažných trestných činov si nevyžaduje vydanie európskeho zatýkacieho rozkazu.
354. Okrem toho, aby bolo možné na tento účel použiť diaľkovú biometrickú identifikáciu v reálnom čase, musí byť za príslušný trestný čin možné v dotknutom členskom štáte uložiť trest odňatia slobody alebo ochranné opatrenie obmedzujúce slobodu s hornou hranicou trestnej sadzby najmenej štyri roky.

Počas rušného festivalu v meste nasadia policajné orgány technológie na rozpoznávanie tvárí naživo s cieľom monitorovať okolie festivalu a identifikovať hľadané osoby s vydanými zatykačmi za nedovolené obchodovanie s drogami a sexuálne trestné činy. Pri rôznych vstupoch na festival polícia využíva živé videozáznamy ľudí, ktorí prechádzajú pred mobilnou kamerou, a porovnáva ich tváre s operatívnym spisom, ktorý obsahuje tváre hľadaných osôb.

Po prvé, pokiaľ ide o typy trestných činov, diaľkovú biometrickú identifikáciu možno použiť v prípade nedovoleného obchodovania s drogami. Sexuálne trestné činy však nie sú uvedené v zozname trestných činov, pokiaľ sa netýkajú sexuálneho vykorisťovania detí, materiálu obsahujúceho sexuálne zneužívanie detí alebo znásilnenia. Polícia nesmie nasadzovať technológie na rozpoznávanie tváre v reálnom čase plošne a bez cieleného zamerania, t. j. v nádeji, že nájde hľadaných zločincov a zabráni ich prítomnosti v uliciach.

Iný prípad nastane, ak polícia dostane fyzický opis s fotografiou hľadanej osoby, na ktorú je vydaný európsky zatýkací rozkaz za obchodovanie s drogami, a má dôvody domnievať sa, že uvedená osoba bude prítomná na festivale. Za uvedených okolností sa na nasadenie technológií na rozpoznávanie tváre v reálnom čase s cieľom identifikovať zacieleného jednotlivca môže vzťahovať článok 5 ods. 1 písm. h) bod iii) aktu o AI.

²¹⁰ Priority Europolu.

²¹¹ Pozri odôvodnenie 33 a pozri vymedzenie trestných činov terorizmu v článku 3 smernice (EÚ) 2017/541.

Po závažnom teroristickom útoku na vianočnom trhu s 12 obeťami polícia využíva technológie na rozpoznávanie tváre v reálnom čase, aby identifikovala páchateľa a zistila, kam uniká. V tejto súvislosti využíva aj technológie na rozpoznávanie tváří v reálnom čase na blízkej železničnej stanici a na cieľových staniciach vlakov, ktoré odtiaľ odchádzajú krátko po útoku. V prípade teroristického útoku môže byť takéto použitie povolené podľa článku 5 ods. 1 písm. h) bodu iii) aktu o AI.

355. Prepojenie medzi článkom 5 ods. 1 písm. h) bodom i) a článkom 5 ods. 1 písm. h) bodom iii) aktu o AI možno vytvoriť v prípade trestných činov, na ktoré sa vzťahuje scenár opísaný v článku 5 ods. 1 písm. h) bode i) aktu o AI. Zatiaľ čo systémy diaľkovej biometrickej identifikácie v reálnom čase možno použiť na nájdenie obete alebo nezvestnej osoby, uvedené systémy sa môžu použiť aj na lokalizáciu a identifikáciu páchateľa alebo osoby podozrivej z obchodovania s ľuďmi, sexuálneho vykorisťovania, pokiaľ ide o deti (ako sa uvádza v prílohe II), a únosu [pokiaľ sa únos uvedený v článku 5 ods. 1 písm. h) bode i) aktu o AI kvalifikuje ako únos, ako je uvedené v prílohe II k aktu o AI]. Prepojenie možno vytvoriť aj medzi článkom 5 ods. 1 písm. h) bodmi ii) a iii) aktu o AI: systémy diaľkovej biometrickej identifikácie v reálnom čase možno použiť na predchádzanie ohrozeniu, ktoré patrí do rozsahu pôsobnosti článku 5 ods. 1 písm. h) bodu ii), a ak sa toto ohrozenie naplní, možno uvedené systémy použiť na identifikáciu/lokalizáciu páchateľa „v pohybe“.

10. ZÁRUKY A PODMIENKY PRE VÝNIMKY (ČLÁNOK 5 ODS. 2 AŽ 7 AKTU O AI)

10.1. Zacielený jednotlivec a záruky (článok 5 ods. 2 aktu o AI)

V článku 5 ods. 2 aktu o AI sa stanovuje:

„Systémy diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch sa na účely presadzovania práva na dosiahnutie ktoréhokoľvek z cieľov uvedených v odseku 1 prvom pododseku písm. h) nasadzujú na účely stanovené v uvedenej písmene, len aby sa potvrdila totožnosť špecificky zacieleného jednotlivca, pričom sa zohľadnia tieto skutočnosti:

- a) povaha situácie, ktorá viedla k možnému použitiu, najmä závažnosť, pravdepodobnosť a rozsah ujmy, ktorá by bola spôsobená v prípade nepoužitia systému;
- b) dôsledky použitia systému pre práva a slobody všetkých dotknutých osôb, najmä závažnosť, pravdepodobnosť a rozsah týchto dôsledkov.

Používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva na dosiahnutie ktoréhokoľvek z cieľov uvedených v odseku 1 prvom pododseku písm. h) tohto článku musí okrem toho byť v súlade s nevyhnutnými a primeranými zárukami a podmienkami týkajúcimi sa tohto používania, a to podľa vnútroštátnych právnych predpisov oprávňujúcich ich použitie, najmä pokiaľ ide o časové, geografické a osobné

obmedzenia. Používanie systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch sa povolí len vtedy, ak orgán presadzovania práva dokončil posúdenie vplyvu na základné práva, ako sa stanovuje v článku 27, a zaregistroval systém v databáze Únie podľa článku 49. V riadne odôvodnených naliehavých prípadoch sa však používanie takýchto systémov môže začať bez registrácie v databáze Únie za predpokladu, že sa takáto registrácia dokončí bez zbytočného odkladu.“

356. Používanie systémov diaľkovej biometrickej identifikácie v reálnom čase na jeden z cieľov uvedených v článku 5 ods. 1 písm. h) bodoch i) až iii) aktu o AI podlieha určitým zárukám a podmienkam, ktoré sú podrobne uvedené v článku 5 ods. 2 až 7 aktu o AI.
357. Po prvé, používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva je povolené, len „aby sa potvrdila totožnosť špecificky zacieleného jednotlivca“. Cieľom tejto prvej podmienky je vyvážiť závažnosť situácie a ujmy vyplývajúce z nepoužívania systému s vplyvom technológie na práva a slobody jednotlivcov. Jej cieľom je zabrániť masovému sledovaniu tým, že sa v prípade nasadenia diaľkovej biometrickej identifikácie v reálnom čase cieľi na jednotlivca. V dôsledku toho by sa nasadenie systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva malo povoliť len v prípade zacielených jednotlivcov.
358. Použitie výrazu „potvrdenie totožnosti“ na rozdiel od výrazu „identifikácia“ má slúžiť ako dodatočná záruka z hľadiska základných práv obmedzujúca riziko nerozlišujúceho sledovania a znamená, že identifikácia jednotlivca v zmysle článku 5 ods. 1 písm. h) aktu o AI musí byť cieleňá. Uvedený výraz by sa mal chápať tak, že použitie diaľkovej biometrickej identifikácie v reálnom čase sa môže začať len na účely pátrania po konkrétnych osobách, v prípade ktorých majú orgány presadzovania práva dôvody domnievať sa alebo sú informované, že sú obeťami trestných činov uvedených v článku 5 ods. 1 písm. h) bode i) aktu o AI alebo sú zapojené do jedného zo scenárov opísaných v článku 5 ods. 1 písm. h) bode ii) alebo v článku 5 ods. 1 písm. h) bode iii) aktu o AI. V praxi to znamená porovnanie údajov zozbieraných v reálnom čase s údajmi obsiahnutými v referenčnej databáze. Pokiaľ ide o používanie systému diaľkovej biometrickej identifikácie v reálnom čase v scenároch opísaných v článku 5 ods. 1 písm. h) bode ii) aktu o AI a na vedenie vyšetrovania trestného činu v zmysle článku 5 ods. 1 písm. h) bodu iii) aktu o AI, orgány presadzovania práva nemusia pred použitím systému nevyhnutne poznať totožnosť osôb, po ktorých pátrajú. Ak majú skutkové zistenia a informácie o plánovanom teroristickom útoku teroristickej skupiny (bez toho, aby vedeli, kto plán vykoná) v určitom čase a na určitom mieste, systém diaľkovej biometrickej identifikácie sa môže použiť na identifikáciu páchatel'a z teroristickej skupiny za predpokladu, že orgány presadzovania práva vytvorili referenčnú databázu obsahujúcu biometrické údaje osôb, ktoré sú súčasťou teroristickej skupiny. Vo všetkých troch scenároch opísaných v článku 5 ods. 1 písm. h) bodoch i) až iii) aktu o AI môže „potvrdenie totožnosti“ zahŕňať aj lokalizáciu príslušnej osoby.

359. Po druhé, pred použitím systému by sa mala posúdiť povaha situácie, ktorá vedie k možnému použitiu, najmä závažnosť, pravdepodobnosť a rozsah ujmy pre fyzické osoby, spoločnosť a účely presadzovania práva, ktorá by bola spôsobená v prípade nepoužitia systému, v porovnaní s dôsledkami použitia systému pre práva a slobody dotknutých osôb, najmä závažnosť, pravdepodobnosť a rozsah týchto dôsledkov. To by malo zahŕňať posúdenie, či orgány presadzovania práva alebo subjekty konajúce v ich mene majú k dispozícii menej rušivé alternatívne riešenia.

Orgány presadzovania práva majú napríklad zakázané používať systémy na rozpoznávanie tváre v reálnom čase na ulici na základe všeobecných obáv týkajúcich sa bezpečnosti, predchádzania trestnej činnosti a preplnenosti, pretože by to zahŕňalo neustále monitorovanie a sledovanie všetkých osôb, ktoré nie je časovo obmedzené, a preto by to nespĺňalo kritériá pre výnimku zo zákazu stanovenú v článku 5 ods. 1 písm. h) aktu o AI.

360. Kritérium „**závažnosti**“, ktoré sa tu uplatňuje v súvislosti s možnou ujmov a dôsledkami, znamená rôznu mieru zásahu do dotknutých základných práv, čo súvisí so zásadou proporcionality²¹². Pokiaľ ide o zásahy do základných práv, niektoré zásahy sa považujú za závažnejšie ako iné.
361. Kritérium „**rozsahu**“ sa vzťahuje najmä na počet a kategórie osôb, ktoré sú zásahom dotknuté (vrátane detí a zraniteľných alebo marginalizovaných osôb).
362. Napokon „**pravdepodobnosť**“ znamená to, nakoľko možno predpokladať, že udalosť nastane.
363. Posúdenie závažnosti, rozsahu a pravdepodobnosti ujmy a následkov by malo byť súčasťou posúdenia vplyvu na základné práva, ktoré je orgán presadzovania práva povinný vykonať (pozri ďalej). Toto posúdenie sa bude vykonávať od prípadu k prípadu.
364. Po tretie, používanie diaľkovej biometrickej identifikácie v reálnom čase by malo byť jasne obmedzené z hľadiska geografického rozsahu, trvania a cieľovej osoby. Tým sa zabezpečí, aby sa systém diaľkovej biometrickej identifikácie používal, len keď je to nevyhnutne potrebné.
365. Pokiaľ ide o **geografické obmedzenie**, môže sa vzťahovať na jednu alebo viacero geografických oblastí na základe „objektívnych a nediskriminačných faktorov“. V prípade biometrickej identifikácie to znamená, že geografické obmedzenie sa vzťahuje na jasne vymedzenú hranicu, pre ktorú existujú indície, že v rámci nej dôjde k udalosti. Takéto vymedzenie by za zvyčajných okolností nemalo zahŕňať celé mesto alebo krajinu, ale malo by byť cielennejšie.

²¹² Rozsudok Súdneho dvora z 2. októbra 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788, bod 55, v ktorom Súdny dvor uvádza, že „prístup musí byť priamo úmerný závažnosti zásahu do dotknutých základných práv“.

366. Ďalšia záruka sa týka **osobného rozsahu** opatrenia, t. j. vymedzenia **kategórií dotknutých osôb**. Tým by sa vylúčila necielená, nerozlišujúca identifikácia osôb bez ďalších indícií incidentu.
367. Nakoniec, **lehota** je časové obdobie obmedzené na to, čo je nevyhnutne potrebné, ktoré však možno v prípade potreby predĺžiť v súlade s platnými pravidlami. Systémy diaľkovej biometrickej identifikácie v reálnom čase sa preto nemôžu používať počas neobmedzeného alebo neurčitého časového obdobia. Obdobie je potrebné určiť vzhľadom na konkrétne indície, ktoré vedú k používaniu systémov diaľkovej biometrickej identifikácie.
368. Po štvrté, pred nasadením musí orgán presadzovania práva, ktorý nasadzuje systém diaľkovej biometrickej identifikácie v reálnom čase, ukončiť posúdenie vplyvu na základné práva a zaregistrovať systém v databáze EÚ (okrem riadne odôvodnených prípadov).

10.1.1. Posúdenie vplyvu na základné práva

369. Posúdenie vplyvu na základné práva vykonávané v rámci uplatňovania článku 5 ods. 2 aktu o AI musí byť v súlade s podmienkami stanovenými v článku 27 aktu o AI. V uvedenom ustanovení sa stanovujú požiadavky týkajúce sa posúdenia vplyvu na základné práva, ktoré sa vzťahujú na vysokorizikové systémy AI.
370. V období, keď sa už začnú uplatňovať zákazy v článku 5 aktu o AI (po 2. februári 2025), ale ustanovenia o vysokorizikových systémoch AI sa ešte neuplatňujú (pred 2. augustom 2026), by mali požiadavky na posúdenie vplyvu na základné práva stanovené v článku 27 aktu o AI uplatňovať subjekty nasadzujúce systémy diaľkovej biometrickej identifikácie v reálnom čase, ktoré spĺňajú podmienky na využitie jednej alebo viacerých výnimiek uvedených v článku 5 ods. 1 písm. h) aktu o AI. Nasledujúce predbežné usmernenie sa týka len používania diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva v období, kým sa nezačnú uplatňovať povinnosti pre vysokorizikové systémy AI a kým Komisia neprijme vzor pre posúdenie vplyvu na základné práva a neposkytne ďalšie usmernenia k povinnosti podľa článku 27 aktu o AI.
371. Posúdenie vplyvu na základné práva je nový typ posúdenia vplyvu, ktorého cieľom je identifikovať vplyv, ktorý môžu mať určité vysokorizikové systémy AI vrátane systémov diaľkovej biometrickej identifikácie na základné práva. Posúdenie vplyvu na základné práva je nástrojom zodpovednosti. Posúdenie vplyvu na základné práva nenahrádza existujúce posúdenie vplyvu na ochranu údajov, ktoré musia vykonať prevádzkovatelia (t. j. tí, ktorí sú zodpovední za spracúvanie osobných údajov) podľa článku 27 smernice o presadzovaní práva, článku 35 všeobecného nariadenia o ochrane údajov alebo článku 39 nariadenia, ktorým sa stanovujú pravidlá ochrany údajov pre inštitúcie, orgány, úrady a agentúry EÚ.

Posúdenie vplyvu na ochranu údajov sa musí vykonať napríklad vtedy, keď sa biometrické údaje spracúvajú prostredníctvom nových technológií, pri ktorých možno predpokladať, že povedú k vysokému riziku pre práva a slobody fyzických osôb
--

(napríklad CCTV, rozpoznávanie tváre pomocou AI a kamery nosené na tele) vo verejne prístupných priestoroch.

372. Zatiaľ čo posúdenie vplyvu na ochranu údajov sa zameriava na riziká pre práva a slobody jednotlivcov vyplývajúce zo spracúvania ich osobných údajov, posúdenie vplyvu na základné práva sa všeobecnejšie týka možného vplyvu systémov AI na základné práva jednotlivcov. Rozsah pôsobnosti posúdenia vplyvu na základné práva je preto širší, pokiaľ ide o zahrnuté činnosti a posudzované základné práva. Ak sa osobné údaje spracúvajú systémom AI (čo je prípad systémov diaľkovej biometrickej identifikácie), posúdením vplyvu na základné práva by sa malo doplniť posúdenie vplyvu na ochranu údajov, ktoré vykonal nasadzujúci subjekt ako prevádzkovateľ²¹³, bez toho, aby sa vzťahovalo na aspekty, ktoré sa už riešili v posúdení vplyvu na ochranu údajov, aby sa zabránilo prekryvaniu. Analýza posúdenia vplyvu na základné práva v týchto usmerneniach sa obmedzuje na povolené používanie diaľkovej biometrickej identifikácie v reálnom čase a má slúžiť ako predbežné usmernenie pre nasadzujúce subjekty v tomto prechodnom období pred tým, ako úrad pre AI poskytne vzor²¹⁴.
373. Povinnosť vykonať posúdenie vplyvu na základné práva podľa článku 5 ods. 2 aktu o AI sa ukladá subjektom nasadzujúcim systém diaľkovej biometrickej identifikácie, a nie subjektom alebo orgánom, resp. komukoľvek inému, kto koná v ich mene. Ak v mene nasadzujúceho subjektu/orgánu presadzovania práva konajú iní aktéri, budú musieť prispieť k príprave posúdenia vplyvu na základné práva všetkými relevantnými informáciami, aby sa zabezpečilo jeho riadne vykonanie.
374. Posúdenie vplyvu na základné práva sa musí vykonať pred nasadením povoleného systému diaľkovej biometrickej identifikácie v reálnom čase.
375. Podľa článku 27 aktu o AI by posúdenie vplyvu na základné práva malo obsahovať tieto informácie:
- Opis používania diaľkovej biometrickej identifikácie a procesov nasadzujúceho subjektu v súvislosti s týmto používaním, spolu s jeho zamýšľaným účelom

Tento opis by mal zahŕňať:

- názov nasadzujúceho subjektu,
- účel (účely) presadzovania práva, na ktorý (ktoré) sa bude systém diaľkovej biometrickej identifikácie v reálnom čase používať,
- opis referenčnej databázy, s ktorou sa bude biometrická identifikácia porovnávať, vrátane zdrojov biometrických údajov (podoby tváre, hlasové vzorky atď.), ktoré sa použijú,

²¹³ Článok 27 bod 4 aktu o AI.

²¹⁴ Analýza sa teda nevzťahuje na prípad vysokorizikových systémov AI vo všeobecnosti.

- opis technológie, na ktorej je systém založený, s cieľom vysvetliť jeho fungovanie (odkazom na dostupnú dokumentáciu poskytnutú poskytovateľom a na jej názov)²¹⁵,
- právny základ, na ktorom bude diaľková biometrická identifikácia v reálnom čase nasadená.

- Časový úsek a frekvencia používania

Každé jednotlivé použitie systému diaľkovej biometrickej identifikácie v reálnom čase pre jednu z povolených výnimiek musí byť pred jeho nasadením povolené justičným orgánom alebo iným nezávislým orgánom podľa článku 5 ods. 3 aktu o AI. Naopak, v prípade posúdenia vplyvu na základné práva musia nasadzujúce subjekty poskytnúť všeobecný údaj o plánovanom časovom úseku používania a jeho očakávanej frekvencii.

- Kategórie osôb a skupín, ktoré sú systémom dotknuté

Na účely výnimky v článku 5 ods. 1 písm. h) aktu o AI by sa v posúdení vplyvu na základné práva malo rozlišovať medzi:

- zacielenou osobou, ktorá môže byť obeťou trestného činu, páchatelom alebo podozrivou osobou,
- osobami, ktorých biometrické údaje sú zahrnuté v referenčnej databáze, a
- kategóriami osôb, ktoré sa nachádzajú v okolitých oblastiach, kde bude systém diaľkovej biometrickej identifikácie nasadený.

Používaním systémov diaľkovej biometrickej identifikácie v reálnom čase budú dotknuté nielen základné práva zacieleného jednotlivca. Dotknuté budú aj práva iných osôb, ktorých biometrické údaje sa používajú na účely porovnania, okoloidúcich a osôb, ktoré sa náhodne nachádzajú v oblasti pátrania. Opis geografického rozsahu oblasti (oblastí) pátrania, na ktorú (ktoré) sa vzťahuje systém diaľkovej biometrickej identifikácie v reálnom čase, ovplyvní počet osôb, ktoré sú systémom dotknuté.

- Konkrétne riziká ujmy pre dotknuté osoby

376. Medzi základné práva, ktoré môžu byť dotknuté používaním diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, patria najmä:

- právo na súkromný a rodinný život vrátane primeraného očakávania anonymity ľudí vo verejných priestoroch,
- právo na ochranu údajov, keďže systémy diaľkovej biometrickej identifikácie sa pri identifikácii konkrétnych osôb spoliehajú na spracovanie biometrických údajov a iných osobných údajov (napríklad mien, identifikačných čísel, ako aj citlivých údajov, ako je etnický pôvod),

²¹⁵

Po nadobudnutí účinnosti pravidiel týkajúcich sa vysokorizikového systému AI to možno vykonať na základe odkazu na registračné číslo systému v databáze EÚ a dostupných informácií o systéme, ktoré sú v nej uvedené.

- sloboda myslenia, svedomia a náboženského vyznania, sloboda prejavu a sloboda zhromažďovania a združovania vo verejných priestoroch, v ktorých sa vykonáva pátranie, na ktoré by používanie systémov diaľkovej biometrickej identifikácie mohlo mať odrádzajúci účinok, čím by sa jednotlivcom bránilo v plnom uplatňovaní ich práv a slobôd, pretože ak jednotlivci vedia, že sú monitorovaní, mohli by zmeniť svoje správanie alebo sa dokonca vyhýbať určitému správaniu,
- právo na účinný prostriedok nápravy a na spravodlivý proces,
- právo na nediskrimináciu, ak systém zahŕňa skreslenia (napríklad rodové, etnické alebo rasové) a vedie k nesprávnej identifikácii podozrivej osoby alebo páchatel'a,
- právo na ľudskú dôstojnosť v dôsledku pocitu, že jednotlivec je redukovaný na objekt systému,
- prezumpcia nevinoty a právo na obhajobu, pretože žiadne rozhodnutie, ktoré by malo nepriaznivý vplyv na jednotlivca, sa nesmie prijímať výlučne na základe výstupu systému diaľkovej biometrickej identifikácie v reálnom čase,
- práva dieťaťa v prípade, že obeť, nezvestná osoba alebo podozrivá osoba je maloletá,
- práva starších osôb v prípade nezvestnej osoby.

Na posúdenie konkrétnych rizík ujmy, ktoré môžu mať vplyv na identifikovanú (identifikované) dotknutú (dotknuté) osobu (osoby) alebo skupinu (skupiny), sa musia v rámci posúdenia vplyvu na základné práva identifikovať základné práva týchto osôb a posúdiť vplyv na ich základné práva vrátane závažnosti vplyvu a jeho rozsahu s prihliadnutím na potenciálne dotknuté osoby.

Táto časť posúdenia vplyvu na základné práva by mala zahŕňať aj posúdenie, či je použitie systému diaľkovej biometrickej identifikácie v reálnom čase potrebné a primerané vzhľadom na ciele a okolnosti, za ktorých je zamýšľané, vrátane existencie alebo neexistencie menej rušivých alternatív. V posúdení vplyvu na základné práva by sa mala opisovať úroveň výkonnosti a presnosti systému na základe technickej dokumentácie a tréningových údajov, ak sú k dispozícii, na ktorých bola technológia testovaná a vyvinutá, aby sa zabránilo skresleniam a diskriminácii.

V posúdení vplyvu na základné práva by sa mal identifikovať aj vplyv používania systému diaľkovej biometrickej identifikácie v reálnom čase na základné práva všetkých potenciálne dotknutých jednotlivcov, najmä podozrivej osoby alebo páchatel'a, obeť, po ktorej sa pátra, a ďalších jednotlivcov nachádzajúcich sa vo verejne prístupných priestoroch, ktoré sú predmetom pátrania. V rozsahu, v akom systém spracúva biometrické údaje týchto jednotlivcov, budú ovplyvnené ich práva na súkromný a rodinný život a na ochranu údajov, čo sa posúdi v rámci posúdenia vplyvu na ochranu údajov, pokiaľ ide o činnosti spracúvania údajov. V prípade iných činností súvisiacich s používaním systémov diaľkovej biometrickej identifikácie v reálnom čase a vplyvom na iné základné práva sa bude posúdením vplyvu na základné práva dopĺňať posúdenie vplyvu na ochranu údajov. V závislosti od kontextu nasadenia môžu byť

ovplyvnené ďalšie základné práva týchto jednotlivcov, napríklad ich právo na ľudskú dôstojnosť, slobodu myslenia, svedomia a náboženského vyznania, slobodu zhromažďovania alebo slobodu prejavu, právo na účinný prostriedok nápravy a spravodlivý proces, prezumpcia nevinu a právo na obhajobu, práva dieťaťa.

Posúdenie vplyvu na základné práva by sa malo vykonať na abstraktnej úrovni pred prvým uvedením systému AI do prevádzky. Konkrétne úvahy závislé od kontextu, ktoré určujú vplyv použitia systému diaľkovej biometrickej identifikácie v reálnom čase v každom jednotlivom prípade, by mali byť podrobnejšie rozpracované v individuálnej žiadosti o povolenie každého použitia systému diaľkovej biometrickej identifikácie zo strany justičného orgánu alebo nezávislého správneho orgánu (pozri oddiel 10.23.8.3).

- Opatrenia na zabezpečenie ľudského dohľadu

V súlade s článkom 5 ods. 3 aktu o AI sa žiadne rozhodnutie, ktoré by malo nepriaznivý vplyv na jednotlivca, nesmie prijať výlučne na základe výstupu systému diaľkovej biometrickej identifikácie v reálnom čase. V dôsledku toho by sa v posúdení vplyvu na základné práva mali opisovať postupy, ktoré sa budú dodržiavať počas prevádzky systému, a spôsob interpretácie výstupov v kontexte rozhodovacieho procesu. V rámci uvedených postupov by sa mali poskytnúť pokyny na nasadenie systému diaľkovej biometrickej identifikácie, objasniť úloha ľudského činiteľa pri overovaní a interpretácii výstupov a poskytnúť odbornú prípravu na obsluhu systému. Osoba zodpovedná za ľudský dohľad by mala mať dostatočnú „gramotnosť v oblasti AI, odbornú prípravu a právomoc“²¹⁶, aby pochopila, ako systém funguje a kedy je jeho výkon nedostatočný alebo dochádza k jeho zlyhaniu.

Relevantné sú aj ďalšie úvahy o ľudskom dohľade a monitorovaní podľa článkov 14 a 26 aktu o AI, ktoré by sa mali opísať.

- Opatrenia na zmiernenie rizika

Okrem vykonávania opatrení na zabezpečenie ľudského dohľadu (vrátane zabránenia diskriminačným opatreniam) by mal nasadzujúci subjekt vysvetliť nápravné opatrenia v prípade, že sa riziko naplní, vrátane postupov riadenia a mechanizmov riešenia sťažností (napríklad v prípade nesprávnej identifikácie).

10.1.2. Registrácia povolených systémov diaľkovej biometrickej identifikácie

377. Na základe článku 5 ods. 2 aktu o AI sa subjektu nasadzujúcemu systém diaľkovej biometrickej identifikácie v reálnom čase, ktorý sa používa vo verejne prístupných priestoroch na účely presadzovania práva, ukladá aj povinnosť zaregistrovať systém v databáze EÚ stanovenej v článku 49 aktu o AI. V riadne odôvodnených naliehavých situáciách (ako je bezprostredné ohrozenie) sa však nasadenie môže začať aj pred registráciou, ak orgán presadzovania práva registruje systém bez zbytočného odkladu. Bez zbytočného odkladu by sa malo chápať ako „čo najskôr“ vzhľadom na okolnosti naliehavej situácie, ktorá zabránila registrácii systému pred jeho použitím.

²¹⁶

Odôvodnenie 91 aktu o AI.

To, či registrácia spĺňa toto kritérium, si vyžaduje posúdenie od prípadu k prípadu. Nemožno ho *a priori* presne časovo vymedziť. Odklad by nemal byť spôsobený úmyselným konaním. Podľa článku 49 ods. 4 aktu o AI budú systémy diaľkovej biometrickej identifikácie používané na účely presadzovania práva zaregistrované v zabezpečenej neverejnej časti databázy s obmedzenými informáciami a obmedzeným prístupom k týmto informáciám.

Napríklad žiadosť orgánov presadzovania práva o registráciu systému diaľkovej biometrickej identifikácie do 24 hodín od použitia by sa mohla považovať za primeraný odklad, ak bol systém nasadený v situácii bezprostredného ohrozenia života, napríklad v prípade aktívneho strelca.

10.2. Potreba predchádzajúceho povolenia

378. V článku 5 ods. 3 aktu o AI sa vyžaduje **predchádzajúce povolenie** každého jednotlivého použitia systému diaľkovej biometrickej identifikácie v reálnom čase a zakazuje sa automatizované rozhodovanie **výlučne na základe výstupu takéhoto systému**, ktoré má nepriaznivé právne účinky.

V článku 5 ods. 3 aktu o AI sa stanovuje:

Na účely odseku 1 prvého pododseku písm. h) a odseku 2 podlieha každé použitie systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva predchádzajúcemu povoleniu, ktoré udeľuje justičný orgán alebo nezávislý správny orgán, ktorého rozhodnutie je záväzné, členského štátu, v ktorom sa má použitie uskutočniť, vydanému na základe odôvodnenej žiadosti a v súlade s podrobnými pravidlami vnútroštátneho práva uvedenými v odseku 5. V riadne odôvodnenej naliehavej situácii sa však použitie takéhoto systému môže začať bez povolenia za predpokladu, že sa o takéto povolenie požiada bez zbytočného odkladu, najneskôr však do 24 hodín. Ak sa takéto povolenie zamietne, používanie sa s okamžitou účinnosťou zastaví a všetky údaje, ako aj výsledky a výstupy tohto používania sa okamžite vyradia a vymažú.

Príslušný justičný orgán alebo nezávislý správny orgán, ktorého rozhodnutie je záväzné, udelí povolenie len vtedy, ak sa na základe objektívnych dôkazov alebo jasných indícií, ktoré mu boli predložené, presvedčí, že použitie predmetného systému diaľkovej biometrickej identifikácie v reálnom čase je potrebné a primerané na dosiahnutie niektorého z cieľov uvedených v odseku 1 prvom pododseku písm. h), ako sa uvádza v žiadosti, a najmä je naďalej obmedzené na to, čo je striktné nevyhnutné, pokiaľ ide o časový a geografický rozsah a rozsah týkajúci sa osobných aspektov. Pri rozhodovaní o žiadosti tento orgán zohľadní skutočnosti uvedené v odseku 2. Žiadne rozhodnutie, ktoré má pre osobu nepriaznivé právne účinky, sa nesmie prijať výlučne na základe výstupu systému diaľkovej biometrickej identifikácie v reálnom čase.

10.2.1. Cieľ

379. Cieľom požiadavky na predchádzajúce povolenie („povolenie *ex ante*“) na akékoľvek použitie systému diaľkovej biometrickej identifikácie „v reálnom čase“ vo verejne prístupných priestoroch na účely presadzovania práva je potreba posúdenia a rozhodnutia, či je akékoľvek plánované použitie takéhoto systému na takéto účely:
- potrebné a primerané na dosiahnutie niektorého z cieľov uvedených v článku 5 ods. 1 písm. h) bodoch i) až iii), t. j. na cielené pátranie po konkrétnych obetiach, predchádzanie konkrétnym ohrozeniam alebo lokalizáciu či identifikáciu páchateľov, a
 - obmedzené na to, čo je striktne nevyhnutné, pokiaľ ide o časový a geografický rozsah a rozsah týkajúci sa osobných aspektov.
380. Dôsledkom týchto požiadaviek je, že pred nasadením akéhokoľvek systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva by sa malo vykonať dvojité posúdenie nevyhnutnosti a proporcionality. Po prvé, používateľ by mal pri vykonávaní posúdenia vplyvu na základné práva vykonať posúdenie, ako sa vyžaduje v článku 5 ods. 2 aktu o AI. Po druhé, v súlade s článkom 5 ods. 3 aktu o AI musí justičný alebo nezávislý správny orgán takisto posúdiť potrebnosť a proporcionalitu použitia takéhoto systému v medziach vnútroštátneho práva, ktorým sa poskytuje právny základ pre každé takéto použitie, pričom zohľadní chartu a iné právo Únie. V dôsledku toho sa každý takýto systém môže používať len 1. po posúdení vplyvu na základné práva a 2. v prípade, že takéto používanie povolil príslušný vnútroštátny orgán.
381. Článok 5 ods. 3 aktu o AI sa musí vykladať a chápať v spojení s článkom 5 ods. 5 aktu o AI: aby bolo používanie systému diaľkovej biometrickej identifikácie v reálnom čase povolené, musí existovať vnútroštátny právny predpis prijatý v dotknutých členských štátoch, ktorým sa takéto používanie oprávňuje²¹⁷. Niektoré členské štáty už majú zavedený systém predchádzajúceho povolenia na používanie biometrických systémov podľa iných právnych predpisov Únie alebo vnútroštátnych právnych predpisov, ako sú napríklad právne predpisy o ochrane údajov.

10.2.2. Hlavná zásada: predchádzajúce povolenie justičného orgánu alebo nezávislého správneho orgánu

382. Používanie systémov diaľkovej biometrickej identifikácie v reálnom čase, ktorým sa sleduje jeden z cieľov uvedených v článku 5 ods. 1 písm. h) bodoch i) až iii) aktu o AI a ktoré bolo stanovené vo vnútroštátnom práve dotknutých členských štátov, musí **pred použitím** povoliť justičný orgán alebo nezávislý správny orgán. Toto je hlavná zásada.
383. V naliehavých prípadoch však existuje výnimka. Výnimka musí byť **riadne odôvodnená**²¹⁸. Naliehavé situácie **sa opisujú ako** také, „v ktorých je natoľko potrebné použiť predmetné systémy, že je **naozaj objektívne nemožné získať povolenie pred**

²¹⁷ Pozri aj článok 5 ods. 2 aktu o AI: „[...] podľa vnútroštátnych právnych predpisov oprávňujúcich ich použitie [...]“.

²¹⁸ To znamená, že „orgán presadzovania práva [by] mal v takýchto situáciách požiadať o takéto povolenie a zároveň uviesť dôvody, prečo oň nemohol požiadať skôr, a to bez zbytočného odkladu a najneskôr do 24 hodín“ (odôvodnenie 35 aktu o AI).

začatím použitia systému AI“²¹⁹. V takomto naliehavom prípade „by sa používanie systému AI malo obmedziť na **absolútne nevyhnutné minimum** a malo by **podliehať primeraným zárukám a podmienkam** stanoveným vo vnútroštátnom práve a špecifikovaným v kontexte každého jednotlivého naliehavého prípadu použitia samotným orgánom presadzovania práva“.

10.2.2.1. Predchádzajúca a odôvodnená žiadosť v súlade s vnútroštátnymi procesnými pravidlami

a) Kto podáva žiadosť?

384. Hoci to nie je špecifikované, možno predpokladať, že žiadosť bude obvykle iniciovať nasadzujúci subjekt, t. j. **príslušný orgán (presadzovania práva)**. Podľa vymedzenia orgánu presadzovania práva podľa článku 3 bodu 45 písm. b) aktu o AI sa „každý iný orgán alebo subjekt, ktorý bol právom členského štátu poverený vykonávať verejnú moc a verejné právomoci na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu“, považuje za orgán presadzovania práva a mohol by byť „príslušným orgánom“, aj pokiaľ ide o predloženie žiadosti o predchádzajúce povolenie.
385. Na používanie systému diaľkovej biometrickej identifikácie v reálnom čase na činnosti, ktoré nepatria do rozsahu pôsobnosti aktu o AI, sa nevyžaduje povolenie podľa článku 5 ods. 3 aktu o AI. Ak by sa následne takýto systém používal na účely presadzovania práva, takéto použitie by patrilo do rozsahu pôsobnosti aktu o AI a vyžadovalo by sa povolenie, ak sú splnené požiadavky článku 5 ods. 1 písm. h) aktu o AI.

b) Žiadosť na aké použitie?

386. Na používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch **na účely presadzovania práva** je potrebné predchádzajúce povolenie, a to aj v prípade, že tieto systémy prevádzkujú iné strany v mene orgánov presadzovania práva, napríklad športové kluby alebo nákupné centrá.

Napríklad:

– Organizácia, ktorej boli zverené prostriedky na pátranie po nezvestných deťoch, sa rozhodne používať systém diaľkovej biometrickej identifikácie v reálnom čase. Nemá mandát na vykonávanie verejnej moci a verejných právomocí ani na predchádzanie trestným činom alebo vykonávanie úloh v oblasti predchádzania ohrozeniu verejnej bezpečnosti. Na takéto použitie sa nevzťahuje zákaz stanovený v článku 5 ods. 1 písm. h) aktu o AI, pretože nie je určené na účely presadzovania práva. Uvedený systém však bude kategorizovaný ako „vysokorizikový“ [bod 1 písm. a) prílohy III] a môže byť potrebná vyhovieť požiadavke na predchádzajúcu konzultáciu s dozorným orgánom podľa článku 36 všeobecného nariadenia o ochrane údajov. V závislosti od uplatniteľného vnútroštátneho práva a od toho, či sa uplatňuje niektorá z výnimiek z článku 9 ods. 1 všeobecného nariadenia o ochrane údajov, sa na takéto spracúvanie môže vyžadovať aj predchádzajúce povolenie. Naopak, ak by tú istú organizáciu

požiadali orgány presadzovania práva, aby v ich mene konala pri pátraní po nezvestných deťoch v kontexte presadzovania práva a pod dohľadom a podľa pokynov príslušných orgánov presadzovania práva, bolo by potrebné predchádzajúce povolenie podľa článku 5 ods. 3 aktu o AI.

- Súkromná organizácia poverená poskytovaním prostriedkov na pomoc osobám, ktorým hrozí, že sa stanú obeťami prírodnej katastrofy²²⁰, sa na tento účel rozhodne používať systém diaľkovej biometrickej identifikácie v reálnom čase. Na takéto použitie sa nevzťahuje zákaz stanovený v článku 5 ods. 1 písm. h) aktu o AI, pretože nie je určené na účely presadzovania práva. Uvedený systém však bude kategorizovaný ako „vysokorizikový“ [bod 1 písm. a) prílohy III] a môže byť potrebná vyhovieť požiadavke na predchádzajúcu konzultáciu s dozorným orgánom podľa článku 36 všeobecného nariadenia o ochrane údajov. V závislosti od uplatniteľného vnútroštátneho práva a od toho, či sa uplatňuje niektorá z výnimiek z článku 9 ods. 1 všeobecného nariadenia o ochrane údajov, sa na takéto spracúvanie môže vyžadovať aj predchádzajúce povolenie.

c) Kedy? „Každé použitie“

387. V súlade s článkom 5 ods. 3 aktu o AI je potrebné predchádzajúce povolenie pre „každé použitie“. Z toho vyplýva, že rozhodujúcim momentom pre získanie takéhoto povolenia nie je moment pred inštaláciou systémov diaľkovej biometrickej identifikácie v reálnom čase, ale každé ich konkrétne použitie.

Napríklad:

- polícia nainštaluje na hlavnej železničnej stanici v meste kamery CCTV pripravené na biometrické spracúvanie (nie je potrebné povolenie podľa aktu o AI, ale biometrický systém musí spĺňať požiadavky na vysokorizikové systémy, pred prvým použitím sa musí vypracovať posúdenie vplyvu na základné práva a pred každým jednotlivým použitím systému je potrebné individuálne povolenie justičného alebo nezávislého správneho orgánu).

Polícia má konkrétne informácie o tom, že do mesta príde vlakom terorista (na identifikáciu v reálnom čase je potrebné predchádzajúce povolenie).

d) Motivovaná žiadosť

388. Podľa článku 5 ods. 3 aktu o AI sa vyžaduje, aby každá jednotlivá žiadosť na použitie diaľkovej biometrickej identifikácie v reálnom čase bola „odôvodnená“, a teda podložená a motivovaná.
389. Niektoré členské štáty umožňujú podávanie takýchto žiadostí online²²¹. V súlade s článkom 5 ods. 5 aktu o AI by sa vo vnútroštátnom práve mali stanoviť požiadavky týkajúce sa presného obsahu žiadosti, pričom by sa mali v plnej miere zohľadniť už uvedené požiadavky vrátane dostatočných dôkazov na určenie nevyhnutnej potrebnosti

²²⁰

Medzi prírodné katastrofy patria povodne alebo prírodné požiare.

²²¹

Pozri napríklad žiadosti o povolenie adresované francúzskemu orgánu pre ochranu údajov CNIL.

a primeranosti použitia diaľkovej biometrickej identifikácie v reálnom čase a ďalších relevantných aspektov, ktoré odrážajú výnimočnú povahu povolenia takéhoto použitia.

10.2.2.2. Povolenie justičného orgánu alebo nezávislého správneho orgánu

390. Povolenie môže udeliť len justičný alebo nezávislý správny orgán, ktorého rozhodnutie je záväzné.

a) Nezávislý orgán

391. Súdny dvor Európskej únie vykladá pojem „nezávislosť“ v rôznych kontextoch. Napríklad vo veci HK/Prokuratuur Súdny dvor Európskej únie vysvetlil, že nezávislosť znamená, že orgán zachováva „*neutrálny postoj*“²²². Súdny dvor Európskej únie spresnil, že orgán zapojený do predchádzajúcich vyšetrovaní, v tomto prípade prokurátor, takúto nezávislosť nemá. Podobné úvahy sa môžu uplatniť, pokiaľ ide o nezávislosť požadovanú v článku 5 ods. 3 aktu o AI, čo znamená, že povolujujúci orgán musí byť nezávislý od orgánu, ktorý používa systém diaľkovej biometrickej identifikácie. To by sa týkalo nielen polície, ale aj prípadov vyšetrovajúcich sudcov alebo prokurátorov, ktorí vykonávajú dohľad nad prácou polície a používaním diaľkovej biometrickej identifikácie, na ktoré sa žiada povolenie.

392. Vo veci Komisia/Poľsko, v ktorej sa posudzovala otázka, kedy možno orgán považovať za nezávislý v kontexte bezpečnosti železníc, Súdny dvor Európskej únie konštatoval, že „pokiaľ [...] ide o verejné orgány, nezávislosť obvykle označuje postavenie, ktoré dotknutému orgánu zabezpečuje možnosť konať úplne slobodne vo vzťahu k subjektom, voči ktorým musí byť zabezpečená jeho nezávislosť, a to bez akýchkoľvek pokynov a nátlaku“²²³. Podobné aspekty sa môžu uplatniť v súvislosti s článkom 5 ods. 3 aktu o AI.

393. Justičné orgány v demokratickej spoločnosti sú vo všeobecnosti takisto nezávislé orgány. Justícia zohráva dôležitú úlohu vtedy, keď je nezávislá od orgánu (orgánov) výkonnej moci a od zákonodarcu, pričom samostatne a nezávisle zastrešuje a kontroluje uplatňovanie právnych predpisov a základných práv a slobôd. Nezávislosť súdnictva je jedným z kľúčových aspektov právneho štátu a je zaručená článkom 47 (charta) a článkom 6 ods. 1 Európskeho dohovoru o ľudských právach²²⁴.

b) Orgán miesta, kde sa použitie uskutoční

394. Povolenie musí byť adresované orgánu, ktorý je príslušný podľa vnútroštátneho práva²²⁵.

²²² Rozsudok Súdneho dvora z 2. marca 2021, Prokuratuur, C-746/18, ECLI:EU:C:2021:152, bod 54.

²²³ Rozsudok Súdneho dvora z 13. júna 2018, Komisia/Pol'sko, C-530/16, ECLI:EU:C:2018:430, bod 67.

²²⁴ Pozri R. Manko, *Judicial independence in the case law of the European Court of Human Rights* (Nezávislosť súdnictva v judikatúre Európskeho súdu pre ľudské práva), briefing, Výskumná služba Európskeho parlamentu (EPRS), 2022, s. 12; X, *ECJ case law on judicial independence. Chronological overview* (Judikatúra Súdneho dvora Európskej únie k nezávislosti súdnictva. Chronologický prehľad), briefing, Výskumná služba Európskeho parlamentu (EPRS), 2023, s. 12.

²²⁵ Pozri rozsudok Súdneho dvora zo 6. októbra 2015, Schrems, C-362/14, <https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:62014CJ0362>, ECLI:EU:C:2015:650, bod 44.

c) Povolenie len vtedy, ak je „potrebné a primerané“ na dosiahnutie niektorého z cieľov stanovených vo výnimkách

395. Pri každom povolení na používanie diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva sa musí posúdiť, či sú splnené požiadavky článku 5 ods. 3 aktu o AI.

Veľmi rušivé

396. V súvislosti s ochranou údajov sa Európsky výbor pre ochranu údajov vo svojich usmerneniach 5/2022 a európsky dozorný úradník pre ochranu údajov domnievajú, že používaním biometrických údajov, najmä technológie na rozpoznávanie tváre, sú dotknuté viaceré základné práva a slobody. S týmto názorom súhlasí aj Agentúra Európskej únie pre základné práva a Rada Európy²²⁶. Súdny dvor Európskej únie²²⁷ aj Európsky súd pre ľudské práva²²⁸ potvrdili citlivú povahu spracúvania biometrických údajov.

397. Každý zásah do **základných práv a slobôd musí vždy rešpektovať ich podstatu**. Vyplýva to z článku 52 ods. 1 charty.

398. Pojem „podstata“ základných práv a slobôd bol rozvinutý v judikatúre Súdneho dvora Európskej únie a predstavuje samostatnú hodnotu v právnom poriadku Únie. Ak sa nerešpektuje podstata základného práva alebo slobody, znamená to, že právo alebo sloboda sú opatrením neprimerane dotknuté, takže zásah do nich sa vopred nepovolí.

Len „ak je to potrebné a primerané“

399. Na každý zásah do základných práv a slobôd sa vyžaduje „zákon“, ktorým by sa mala v zásade rešpektovať potrebnosť a proporcionalita podľa článku 52 charty. (Pozri ďalej v článku 5 ods. 5 aktu o AI.) V článku 5 ods. 3 aktu o AI sa vyžaduje, aby sa vo vnútroštátnom práve povoľujúcim používanie diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva stanovilo, že povolenie na takéto používanie je prípustné „len vtedy, ak sa [orgán] presvedčí, že použitie [...] je potrebné a primerané na dosiahnutie niektorého z cieľov uvedených“ v článku 5 ods. 1 písm. h) aktu o AI. Vnútroštátne orgány musia overiť, či je biometrická identifikácia nevyhnutne potrebná²²⁹. V tomto posúdení by sa malo vychádzať z posúdenia vplyvu na základné práva, ktoré by už malo zahŕňať posúdenie potrebnosti a proporcionality všeobecným spôsobom pred podaním žiadosti o povolenie pre každé použitie na základe konkrétnych okolností.

²²⁶ Poradný výbor Dohovoru o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (ETS 108), *Usmernenia k rozpoznávaniu tváre*, 2021.

²²⁷ Rozsudok Súdneho dvora z 26. januára 2023, Ministerstvo na vatreshnite raboti, C-205/21, ECLI:EU:C:2023:49, body 60 až 76 a 116 až 134.

²²⁸ Rozsudok Európskeho súdu pre ľudské práva zo 4. júla 2023, Glukhin/Rusko, sťažnosť č. 11519/20, ECLI:CE:ECHR:2023:0704JUD001151920, body 88 a 90 (ďalej len „rozsudok Glukhin/Rusko“).

²²⁹ Na účely zberu údajov pozri aj: rozsudok Súdneho dvora z 28. novembra 2024, Ministerstvo na vatreshnite raboti, C-80/23, ECLI:EU:C:2024:991.

10.2.2.3. Výnimka z požiadavky na predchádzajúce povolenie: žiadosť do 24 hodín a dôsledky v prípade zamietnutia

400. V naliehavých prípadoch môže používateľ podať žiadosť o povolenie do 24 hodín od okamihu, keď sa začne používať systém diaľkovej biometrickej identifikácie v reálnom čase. V praxi to bude spravidla okamih, keď sa „zapnú“ a nasadia kamery pripravené na biometrické spracúvanie alebo schopné biometrického spracúvania a vykoná sa prvé biometrické porovnanie so systémom. Orgánu by sa malo sprístupniť logovanie činností spracúvania, aby bolo možné zdôvodniť včasnosť žiadosti²³⁰.
401. V takom prípade by sa v žiadosti malo zdôvodniť, prečo nebola pred začatím používania systému predložená predchádzajúca žiadosť.

10.2.2.4. Okamžité zastavenie v prípade zamietnutia žiadosti o povolenie a vymazanie údajov

402. V článku 5 ods. 3 aktu o AI sa ďalej stanovuje, že ak sa žiadosť o povolenie v naliehavom prípade zamietne, používanie systému diaľkovej biometrickej identifikácie v reálnom čase by sa malo s okamžitou účinnosťou ukončiť. V takýchto prípadoch sa musia všetky údaje vrátane výsledkov a výstupov tohto používania okamžite vyradiť a vymazať²³¹. Článok 5 ods. 3 aktu o AI je v tejto súvislosti výslovný bez výnimky. Nasadzujúci subjekt bude mať:
- a) referenčnú databázu, ktorá obsahuje biometrické informácie (napríklad podoby tváre, úryvky hlasu, ...) a prípadne súvisiace identifikačné informácie, na základe ktorých
 - b) sa porovnávajú sa zachytené biometrické informácie od jednotlivcov prítomných vo verejne prístupnom priestore s cieľom identifikovať a selektovať týchto jednotlivcov.
 - c) Na základe tohto porovnania sa vytvorí výsledok porovnania.
403. Požiadavka vyradiť a vymazať zozbierané a spracované údaje znamená aj to, že je potrebné odstrániť a vymazať referenčnú (referenčné) databázu (databázy) použitú (použité) na nepovolenú biometrickú identifikáciu, ak boli vytvorené osobitne na účely sporného vyhľadávania. Databázu používanú na identifikáciu možno zachovať len v prípade, že ju orgány presadzovania práva vytvorili a mali v úmysle udržiavať *zákonným spôsobom* na *iné* legitímne účely ako na nepovolené používanie diaľkovej biometrickej identifikácie v reálnom čase.
404. Okrem vymazania akejkoľvek (nezákonnej) databázy s biometrickými údajmi sa musia vymazať aj všetky zozbierané obrázky a iné osobné údaje vrátane metaúdajov, údaje o technickom spracovaní vrátane vzorov a iných osobných údajov a iné porovnávacie

²³⁰ Automaticky generované logy údajov sa v prípade vysokorizikových systémov AI musia uchovávať najmenej šesť mesiacov a v prípade vysokorizikových systémov uvedených v bode 1 písm. a) prílohy III musia pre každé použitie obsahovať dátum a čas začiatku a ukončenia. Pozri článok 12 ods. 3 písm. a) a článok 19 aktu o AI.

²³¹ Dozorné orgány by mali mať aj právomoci na vykonávanie následného overenia a kontroly uvedených skutočností. Pozri článok 5 ods. 5 aktu o AI.

a výstupné údaje získané počas nezákonného používania systému diaľkovej biometrickej identifikácie v reálnom čase.

405. Ak orgán presadzovania práva napadne zamietnutie, tieto údaje môže uchovávať správca až do prijatia konečného rozhodnutia o žiadosti. Počas tohto obdobia by sa uvedené údaje za normálnych okolností nemali sprístupniť orgánu presadzovania práva³¹⁰.

10.2.2.5. Žiadne rozhodovanie výlučne na základe výstupu systému diaľkovej biometrickej identifikácie v reálnom čase

406. V súlade s článkom 5 ods. 3 aktu o AI, aj keď subjekt nasadzujúci systém diaľkovej biometrickej identifikácie v reálnom čase získa povolenie, žiadne rozhodnutie, ktoré má pre osobu nepriaznivé právne účinky, sa nesmie prijať výlučne na základe výstupu systému diaľkovej biometrickej identifikácie „v reálnom čase“.

Napríklad:

– Osoba je zatknutá a uväznená za závažný trestný čin výlučne na základe identifikácie pomocou systému na rozpoznávanie tváre bez akýchkoľvek ďalších kontrol. Je to nad rámec požiadavky na ľudský dohľad podľa článku 14 aktu o AI. Kontroly sa môžu týkať napríklad otázky, či daná osoba bola na inom mieste alebo takisto či existujú iné dôvody, pre ktoré daná osoba nemôže byť osobou, ktorá je predmetom pátrania.

Požiadavky na ľudský dohľad podľa článku 14 aktu o AI

407. Na používanie diaľkovej biometrickej identifikácie v reálnom čase, ktoré je povolené, pretože sa ním sleduje jeden z cieľov uvedených v článku 5 ods. 1 písm. h) a je v súlade s článkom 5 ods. 2 až 6 aktu o AI, sa aj naďalej vzťahujú pravidlá pre vysokorizikové systémy. V súlade s článkom 14 aktu o AI vysokorizikové systémy AI „musia byť dizajnované a vyvinuté tak, aby nad nimi počas obdobia ich používania mohli fyzické osoby vykonávať účinný dohľad, a to aj pomocou vhodných nástrojov rozhrania človek – stroj“. Podľa článku 14 ods. 5 aktu o AI nasadzujúci subjekt na základe identifikácie vyplývajúcej zo systému nesmie konať ani prijať žiadne rozhodnutie, „pokiaľ takáto identifikácia nebola zvlášť overená a potvrdená aspoň dvoma fyzickými osobami, ktoré majú potrebnú spôsobilosť, odbornú prípravu a právomoc,“ alebo pokiaľ „sa podľa práva Únie alebo vnútroštátneho práva uplatňovanie tejto požiadavky považuje za neprimerané“. V článku 4 aktu o AI sa predpisujú opatrenia týkajúce sa gramotnosti v oblasti AI pre poskytovateľov a používateľov systémov AI na „zabezpečenie dostatočnej úrovne gramotnosti v oblasti AI svojich zamestnancov a ostatných osôb, ktoré sa [...] zaoberajú prevádzkou a používaním systémov AI“, pričom sa berú do úvahy osoby, na ktorých sa majú systémy AI používať.
408. Ako uviedol Európsky výbor pre ochranu údajov v súvislosti s ochranou údajov, na to, aby bol ľudský dohľad účinný, je nevyhnutné „umožniť tejto osobe pochopiť systém [v tomto prípade na rozpoznávanie tváre] a jeho obmedzenia, ako aj správne interpretovať jeho výsledky. Takisto je potrebné vytvoriť pracovné miesto a organizáciu, ktoré budú pôsobiť proti účinkom nadmernej dôvery v automatizáciu a budú predchádzať podpore

nekritickej akceptácie výsledkov, napríklad z dôvodu časového tlaku, náročných postupov, potenciálne škodlivých účinkov na kariéru atď.“²³² Podobné úvahy sa môžu uplatniť v súvislosti s aktom o AI.

10.3. Oznámenie orgánom o každom použití systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva

V článku 5 ods. 4 aktu o AI sa stanovuje:

Bez toho, aby bol dotknutý odsek 3, každé použitie systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva sa oznámi príslušnému orgánu dohľadu nad trhom a vnútroštátnemu orgánu pre ochranu údajov v súlade s vnútroštátnymi pravidlami uvedenými v odseku 5. Oznámenie obsahuje aspoň informácie uvedené v odseku 6 a neobsahuje citlivé operačné údaje.

409. Každé použitie systému diaľkovej biometrickej identifikácie, ktorým sa sleduje jeden z cieľov uvedených v článku 5 ods. 1 písm. h) bodoch i) až iii) aktu o AI, sa oznámi príslušnému orgánu dohľadu nad trhom a vnútroštátnemu orgánu pre ochranu údajov. Oznámenie sa musí uskutočniť po každom použití, aby bolo možné podať správu o počte povolení a ich výsledku. Oznámenie nemusí obsahovať citlivé operačné údaje. Podľa článku 3 bodu 38 aktu o AI „citlivé operačné údaje“ sú operačné údaje súvisiace s činnosťami presadzovania práva (predchádzanie trestným činom, ich odhaľovanie, vyšetrovanie alebo stíhanie), ktorých zverejnenie by mohlo ohroziť integritu trestného konania.
410. Podrobnosti o požiadavke na podávanie správ nájdete v oddiele 10.6.

10.4. Potreba vnútroštátnych právnych predpisov v medziach výnimiek zo aktu o AI

10.4.1. Zásada: vyžaduje sa, aby vnútroštátne právo poskytovalo právny základ pre povolenie všetkých alebo niektorých výnimiek

411. Na začatie používania systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva sú potrebné vnútroštátne právne predpisy. Zároveň sa v článku 5 ods. 5 aktu o AI stanovuje, že členské štáty sa môžu slobodne rozhodnúť, či takéto vnútroštátne právne predpisy prijímú. Ak sa prijme vnútroštátny právny predpis, ktorým sa povoľuje používanie diaľkovej biometrickej identifikácie v reálnom čase, v akte o AI sa uvádzajú vecné prvky, ktoré musia vnútroštátne právne predpisy obsahovať, aby boli v súlade s požiadavkami stanovenými v akte o AI.

Článok 5 ods. 5 aktu o AI

²³²

Európsky výbor pre ochranu údajov, *Usmernenia 05/2022 o používaní technológie rozpoznávania tváre v oblasti presadzovania práva*, verzia 2.0, 26. apríla 2023, s. 22.

Členský štát sa môže rozhodnúť, že na účely presadzovania práva v rámci obmedzení a za podmienok uvedených v odseku 1 prvom pododseku písm. h) a odsekoch 2 a 3 stanoví možnosť úplne alebo čiastočne povoliť používanie systému diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch. Dotknuté členské štáty vo svojom vnútroštátnom práve stanovia potrebné podrobné pravidlá na podávanie žiadostí o povolenia uvedené v odseku 3, ich vydávanie a výkon, ako aj pre dohľad nad nimi a podávanie správ o nich. V týchto pravidlách sa takisto uvedie, v súvislosti s ktorým z cieľov uvedených v odseku 1 prvom pododseku písm. h) a s ktorým z trestných činov uvedených v bode iii) uvedeného písmena h) môžu byť príslušné orgány oprávnené používať tieto systémy na účely presadzovania práva. Členské štáty oznámia tieto pravidlá Komisii najneskôr 30 dní po ich prijatí. Členské štáty môžu v súlade s právom Únie zaviesť prísnejšie právne predpisy o používaní systémov diaľkovej biometrickej identifikácie.

10.4.2. Vo vnútroštátnom práve sa rešpektujú obmedzenia a podmienky článku 5 ods. 1 písm. h) aktu o AI

412. Keďže používanie systémov diaľkovej biometrickej identifikácie „v reálnom čase“ vo verejne prístupných priestoroch na účely presadzovania práva sa považuje za zásah do základných práv, v článku 5 ods. 5 aktu o AI stanovuje, že takéto používanie sa v členských štátoch stanoví vnútroštátnym právom. Tieto vnútroštátne právne predpisy poskytujú právny základ pre používanie takýchto systémov.
413. Vnútroštátnymi právnymi predpismi sa nesmú prekročiť obmedzenia stanovené v článku 5 ods. 1 písm. h) aktu o AI a musia sa rešpektovať všetky ďalšie súvisiace podmienky stanovené v akte o AI. Z toho vyplýva, že členské štáty nesmú rozšíriť ciele, na ktoré možno používať diaľkovú biometrickú identifikáciu v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, nad rámec cieľov uvedených v článku 5 ods. 1 písm. h) bodoch i) až iii) aktu o AI²³³.
414. Členské štáty oznámia tieto vnútroštátne právne predpisy Komisii najneskôr 30 dní po ich prijatí. Samotným takýmto oznámením sa nepredpokladá súlad práva členských štátov s aktom o AI. Úrad pre AI po prijatí oznámenia odošle potvrdenie o prijatí. Členské štáty sa takisto vyzývajú, aby pred prijatím zaslali úradu pre AI predbežnú verziu navrhovaného vnútroštátneho (alebo regionálneho) právneho predpisu. V každom prípade neoznámenie úradu pre AI v zákonnej lehote 30 dní od prijatia stanovenej v článku 5 ods. 5 môže znamenať, že daný vnútroštátny právny predpis je v súdnom konaní nepoužiteľný, ako sa rozhodlo v rôznych kontextoch²³⁴. Komisia zverejní právne predpisy členských štátov na verejnom webovom sídle.

²³³ Pozri rozsudok Súdneho dvora z 5. apríla 2022, Commissioner of An Garda Síochána, C-140/20, ECLI:EU:C:2022:258, bod 54: „Na účely splnenia požiadavky proporcionality musí vnútroštátna právna úprava stanoviť jasné a presné pravidlá, ktoré budú upravovať rozsah a uplatnenie predmetného opatrenia a ukladať minimálne požiadavky[.]“.

²³⁴ Pozri analogicky rozsudok Súdneho dvora z 19. decembra 2019, Airbnb Ireland, C-390/18, EU:C:2019:1112, body 96 až 97.

415. Členské štáty môžu v súlade s právom Únie zaviesť prísnejšie právne predpisy, t. j. právne predpisy s prísnejšími požiadavkami, než sú požiadavky stanovené v článku 5 ods. 1 písm. h) a v článku 5 ods. 2 až 7 aktu o AI.

10.4.3. Podrobné vnútroštátne právne predpisy týkajúce sa podávania žiadostí o povolenia, ich vydávania a výkonu

416. Pokiaľ ide o podrobné pravidlá, ktoré sa vzťahujú na podávanie žiadosti o povolenie, jeho vydávania a výkonu, tieto pravidlá sa určia vo vnútroštátnom práve. Každý členský štát, ktorý chce povoliť používanie predmetných systémov, musí vo svojich vnútroštátnych právnych predpisoch stanoviť také pravidlá, ktorých cieľom je poskytnúť povoľujúcemu orgánu relevantné a úplné informácie o používaní systémov diaľkovej biometrickej identifikácie v reálnom čase, aby mohol rozhodnúť o nevyhnutnej potrebnosti a proporcionality takéhoto používania.

Vnútroštátnym právom povoľujúcim používanie systémov diaľkovej biometrickej identifikácie v reálnom čase sa môže upravovať napríklad:

- ktoré sú príslušné orgány podľa článku 5 ods. 1 písm. h) aktu o AI a nezávislé orgány v členskom štáte príslušné na vydanie (alebo zamietnutie) povolenia,
- podrobný rozsah cieľov, na ktoré možno použiť diaľkovú biometricкую identifikáciu v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva [bez toho, aby sa prekročili ciele uvedené v článku 5 ods. 1 písm. h) bodoch i) až iii), ale prípadne aby sa ešte zúžili],
- povinnosť, že žiadosti musia mať písomnú podobu a musia obsahovať podrobné vysvetlenie konkrétneho použitia a zamýšľaného účelu použitia na konkrétny trestný čin/situáciu, ktorá odôvodňuje jeho použitie,
- požiadavka odôvodnenia a predloženia podporných dôkazov (a v relevantných prípadoch potrebu ich prekladu) na odôvodnenie použitia systému, ktorým sa sledujú ciele uvedené v článku 5 ods. 1 písm. h) bodoch i) až iii) aktu o AI, najmä pokiaľ ide o miesto, obdobie a osobný rozsah, a odôvodnenie nevyhnutnej potrebnosti a proporcionality vrátane relevantnosti, dostatočnosti a účinnosti použitia systému a neexistencie menej rušivých prostriedkov,
- opis technológie, ktorá sa použije, a miesta zberu údajov,
- minimálna spoľahlivosť, použitá prahová hodnota a miera presnosti použitých systémov,
- možnosť auditu predložených informácií vrátane technických údajov a kritérií presnosti zo strany povoľujúceho orgánu kedykoľvek *ex ante* a *ex post*,
- špecifikáciu použitých referenčných databáz,
- trvanie uchovávania zachytených údajov a všetkých ostatných použitých súvisiacich osobných údajov,
- bezpečnostné opatrenia vrátane opatrení proti nezákonnému prístupu k údajom,

- iné záruky (v relevantných prípadoch),
- opis akejkolvek spolupráce so súkromnými subjektmi alebo s orgánmi verejnej moci, a to aj v iných krajinách, a prenosi a výmeny údajov,
- výsledovateľnosť procesu,
- mená zodpovedných osôb nasadzujúcich subjektov,

V súvislosti s vydaním, *pokiaľ ide o ostatné formálne prvky*

- možnosť písomného postupu doplneného o vypočutie,
- dôvody zamietnutia,
- práva osôb, v prípade ktorých sa vykonáva pátranie, práva osôb, ktorých údaje sa zachytávajú, a možné práva tretích strán²³⁵,
- lehoty, v rámci ktorých budú musieť orgány prijať rozhodnutie,
- akákoľvek potreba formálnych oznámení pri udelení/zamietnutí povolenia,
- sankcie za nedodržanie (formálnych a vecných) požiadaviek,
- právo odvolať sa proti zamietnutiu povolenia,

V súvislosti s výkonom

- registrácia používania systémov diaľkovej biometrickej identifikácie v reálnom čase v centrálnom registri so súhrnom vecných prvkov,
- prípadné ďalšie povinnosti týkajúce sa podávania správ,
- postup predĺženia alebo zmeny povolenia.

10.4.4. Podrobné vnútroštátne právne predpisy týkajúce sa dohľadu a podávania správ vo vzťahu k povoleniu

417. V článku 70 aktu o AI sa členským štátom ukladá povinnosť „zriadi[t] [...] aspoň jeden notifikujúci orgán a aspoň jeden orgán dohľadu nad trhom“. V článku 74 ods. 8 aktu o AI sa stanovuje, že „členské štáty určia za orgány dohľadu nad trhom na účely tohto nariadenia buď príslušné dozorné orgány pre ochranu údajov podľa nariadenia (EÚ) 2016/679 alebo smernice (EÚ) 2016/680, alebo akýkoľvek iný orgán určený podľa rovnakých podmienok stanovených v článkoch 41 až 44 smernice (EÚ) 2016/680.“
418. Táto povinnosť je nad rámec určenia povoľujúceho orgánu, ktorý bude musieť členský štát zriadiť pred tým, ako bude môcť povoliť používanie systémov diaľkovej biometrickej identifikácie v reálnom čase na ktorýkoľvek z cieľov uvedených v článku 5 ods. 1 písm. h) bodoch i) až iii) aktu o AI.

10.5. Výročné správy vnútroštátnych orgánov dohľadu nad trhom a vnútroštátnych orgánov pre ochranu údajov členských štátov

²³⁵

Pozri napríklad Európsky výbor pre ochranu údajov, *Usmernenia 05/2022 o používaní technológie rozpoznávania tváre v oblasti presadzovania práva*, verzia 2.0, 26. apríla 2023, s. 24 a nasl.

V článku 5 ods. 6 aktu o AI sa stanovuje:

Vnútroštátne orgány dohľadu nad trhom a vnútroštátne orgány pre ochranu údajov členských štátov, ktorým bolo oznámené používanie systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva podľa odseku 4, predkladajú Komisii výročné správy o takomto používaní. Na tento účel Komisia poskytne členským štátom a vnútroštátnym orgánom dohľadu nad trhom a orgánom pre ochranu údajov vzor vrátane informácií o počte rozhodnutí prijatých príslušnými justičnými orgánmi alebo nezávislým správny orgánom, ktorého rozhodnutie je záväzné v nadväznosti na žiadosti o povolenie v súlade s odsekom 3, a o ich výsledku.

419. Vnútroštátne orgány dohľadu nad trhom a vnútroštátne orgány pre ochranu údajov členských štátov, ktoré boli informované nasadzujúcimi subjektmi o používaní systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva (pozri článok 5 ods. 4), musia Komisii predkladať výročné správy o takomto používaní. Tieto správy sa vypracúvajú na základe vzoru poskytnutého Komisiou. Uvedený vzor bude vytvorený vo vhodnom čase.
420. Ak je nasadzujúcim subjektom inštitúcia, orgán alebo agentúra EÚ, európsky dozorný úradník pre ochranu údajov je povinný každoročne informovať Komisiu o systémoch diaľkovej biometrickej identifikácie v reálnom čase používaných vo verejne prístupných priestoroch na účely presadzovania práva.
421. Iba správa vnútroštátneho orgánu pre ochranu údajov sa bude vzťahovať na obdobie od 2. februára 2025 do 2. augusta 2025, keďže v akte o AI sa od členských štátov nevyžaduje, aby vymenovali vnútroštátny orgán dohľadu nad trhom pred 2. augustom 2025.
422. Vnútroštátne orgány dohľadu nad trhom a vnútroštátne orgány pre ochranu údajov sa môžu slobodne rozhodnúť, či chcú predložiť individuálne správy alebo spoločnú správu za každý členský štát.

10.6. Výročné správy Komisie

V článku 5 ods. 7 aktu o AI sa stanovuje:

Komisia uverejňuje výročné správy o používaní systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva, pričom vychádza zo súhrnných údajov z členských štátov na základe výročných správ uvedených v odseku 6. Tieto výročné správy nesmú obsahovať citlivé operačné údaje o súvisiacich činnostiach v oblasti presadzovania práva.

423. V akte o AI sa od Komisie vyžaduje, aby na základe súhrnných údajov uverejňovala výročné správy o využívaní systémov diaľkovej biometrickej identifikácie v reálnom čase vo verejne prístupných priestoroch na účely presadzovania práva v členských štátoch a inštitúciami, agentúrami a orgánmi Únie. Tieto správy budú vychádzať z informácií oznámených vnútroštátnymi orgánmi podľa článku 5 ods. 6 aktu o AI.

424. Výročná správa Komisie neobsahuje citlivé operačné údaje. Citlivé operačné údaje sú „operačné údaje súvisiace s činnosťami predchádzania trestným činom, ich odhaľovania, vyšetrovania alebo stíhania, ktorých zverejnenie by mohlo ohroziť integritu trestného konania“²³⁶. To by mohlo znamenať, že sa nesmú zverejňovať konkrétne podrobnosti, ktoré odhaľujú prebiehajúce alebo minulé vyšetrovania, napríklad miesta, použité kamery.

10.7. Vylúčenie z rozsahu pôsobnosti

425. Všetky ostatné použitia systémov diaľkovej biometrickej identifikácie, na ktoré sa nevzťahuje zákaz podľa článku 5 ods. 1 písm. h) aktu o AI, patria do kategórie vysokorizikových systémov AI, ako sú vymedzené v článku 6 a uvedené v bode 1 písm. a) prílohy III k aktu o AI, ak patria do rozsahu pôsobnosti aktu o AI.
426. Systémy diaľkovej biometrickej identifikácie, ktoré nepatria do rozsahu pôsobnosti zákazu v článku 5 ods. 1 písm. h) aktu o AI, zahŕňajú systémy na biometrické overenie/autentifikáciu a spätné používanie systémov (následnej) diaľkovej biometrickej identifikácie vo verejne prístupných priestoroch na účely presadzovania práva. Napríklad policajné orgány môžu byť na základe vnútroštátneho práva oprávnené vykonávať spätné rozpoznávanie tváre s cieľom porovnať podoby osôb podozrivých zo spáchania trestných činov so zaznamenanými podobami tváre v databáze trestných činov²³⁷. Ďalším použitím, ktoré nepatrí do rozsahu pôsobnosti zákazu, je použitie systémov diaľkovej biometrickej identifikácie v reálnom čase na účely presadzovania práva buď v súkromnom priestore (napríklad u niekoho doma), alebo v online priestore (napríklad použitie chatovej miestnosti alebo online hry na identifikáciu osoby podozrivej zo šírenia materiálu obsahujúceho sexuálne zneužívanie detí). Napokon do rozsahu pôsobnosti zákazu nepatrí používanie systémov diaľkovej biometrickej identifikácie súkromnými aktérmi v reálnom čase aj spätne (napríklad používanie technológie na rozpoznávanie tváre naživo supermarketom na identifikáciu známych zlodějov, používanie technológie na rozpoznávanie tváre v naživo športovou arénou na identifikáciu osôb, ktorým bol zakázaný vstup do arény, alebo používanie technológie na rozpoznávanie tváre naživo v školách na účely bezpečnosti a školskej dochádzky).
427. Okrem pravidiel, ktoré sa vzťahujú na vysokorizikové systémy AI vo všeobecnosti, sa na **spätne používanie systémov diaľkovej biometrickej identifikácie** na účely presadzovania práva vzťahujú dodatočné podmienky a záruky v súlade s článkom 26 ods. 10 aktu o AI (uplatňuje sa od 2. augusta 2026)²³⁸.
428. Použitie na **iné účely ako na presadzovanie práva** musí byť v každom prípade v súlade s **pravidlami ochrany údajov**. Ďalej uvedené prípady ilustrujú výklad

²³⁶ Článok 3 bod 38 aktu o AI.

²³⁷ Napríklad databáza *Traitement des Antécédents Judiciaires* vo Francúzsku, vytvorená na základe dokumentu *Décret no. 2012-652 du 4 mai 2012 relatif au Traitement des Antécédents Judiciaires* (dekrét 2012-652).

²³⁸ Článok 26 ods. 10 a odôvodnenie 94 aktu o AI.

článku 9 ods. 2 všeobecného nariadenia o ochrane údajov v prípadoch takéhoto použitia a výnimky zo spracúvania biometrických údajov.

Napríklad:

- Francúzsky správny súd rozhodol, že skúšanie technológie na rozpoznávanie tváre naživo v dvoch verejných školách na účely kontroly prístupu a bezpečnosti nebolo nevyhnutné ani primerané (podľa pravidiel ochrany údajov). K dispozícii boli alternatívne riešenia, ktoré boli pre študentov menej rušivé, napríklad používanie preukazov. Okrem toho neboli splnené podmienky výslovného súhlasu. Preto sa súhlas nemohol použiť ako platný právny základ na skúšanie technológie na rozpoznávanie tváre na stredných školách²³⁹.
- V Holandsku nebolo supermarketu povolené používať technológiu na rozpoznávanie tváre naživo s cieľom predchádzať krádežiam. Bez výslovného súhlasu zákazníka alebo bez právneho základu, ktorý by umožňoval spracúvanie na základe významného verejného záujmu (napríklad na bezpečnostné účely), by supermarket nemohol spracúvať biometrické údaje, a teda nasadiť technológiu na rozpoznávanie tváre²⁴⁰.
- Používanie technológie na rozpoznávanie tváre naživo pri vstupe do futbalového klubu na identifikáciu fanúšikov bolo zakázané vo Francúzsku²⁴¹ a na zaistenie bezpečnosti divákov bolo zakázané v Španielsku²⁴².

10.8. Príklady použitia

Polícia inštaluje mobilné kamery CCTV vybavené technológiami na rozpoznávanie tváre založenými na AI na policajnú dodávku v okolí hlavného vchodu futbalového štadióna počas zápasu majstrovstiev Európy s cieľom zabezpečiť oblasť a identifikovať osoby, ktorých tváre sú zaznamenané v ad hoc databáze hľadaných osôb v operatívnom spise. Tento operatívny spis obsahuje osoby podozrivé zo spáchania trestného činu (od závažných trestných činov až po podvody a vlámnia), osoby, ktoré by mohli byť predmetom záujmu na spravodajské účely, a zraniteľné osoby s duševnými problémami. Používanie technológií na rozpoznávanie tváre naživo zo strany polície nie je spojené s informáciami o prítomnosti konkrétnej osoby na podujatí. Hoci možno predpokladať, že v operatívnom spise sú osoby, pri pátraní po ktorých by mohlo byť povolené použitie diaľkovej biometrickej identifikácie v reálnom čase, tento operatívny spis je príliš nekonkrétny a nesúvisí s podujatím, ktorým je futbalový zápas. Takéto použitie by sa preto malo zakázať.

²³⁹ TA Marseille (Správny súd v Marseille) 27. februára 2020, č. 1901249.

²⁴⁰ <https://www.autoriteitpersoonsgegevens.nl/en/current/dutch-dpa-issues-formal-warning-to-supermarket-for-use-of-facial-recognition-technology>.

²⁴¹ <https://www.cnil.fr/fr/reconnaissance-faciale-et-interdiction-commerciale-de-stade-la-cnil-adresse-un-avertissement-un-club>.

²⁴² <https://www.biometricupdate.com/202401/spanish-data-authority-opposes-facial-recognition-for-football-stadium-access>.

Pomocou systému biometrickej identifikácie (nie diaľkovej) sa overuje, či majú osoby prístup do jadrovej elektrárne. Keď sa ľudia dostavia pred (viditeľnú) kameru a systém im odoprie prístup, systém sa následne pokúsi zistiť, či je daná osoba v operatívnom spise so zoznamom teroristov. Systém nefunguje ako diaľkový. Osoby sa aktívne zúčastňovali na overení, aby získali povolenie na vstup do elektrárne. Na tento prípad použitia sa nevzťahuje zákaz podľa článku 5 aktu o AI.

Policačné orgány v rušnom meste nasadzujú kamery CCTV využívajúce AI, ktoré dokážu využívať technológie na rozpoznávanie tváre naživo. Je možné, že sa k rozpoznávaniu tváre sa pridávajú rôzne funkcie, ako sú napríklad detekcia objektov a pohybu v dave.

Tieto kamery umiestnili na viacerých miestach vrátane miest, kde sa konajú bohoslužby, na viacerých miestach navštevovaných komunitou LGBT+, v ordináciách lekára, lekárňach a rôznych reštauráciách a baroch. Inštalácia kamier pripravených na biometrické spracúvanie ako taká nie je podľa aktu o AI zakázaná. Niektoré spôsoby použitia vrátane nešpecifikovanej a nerozlišujúcej identifikácie fyzických osôb sú však zakázané.

Počas letných prázdnin došlo v obytnej štvrti k niekoľkým vlámaniam. Polícia získala opis podozrivej osoby od očitých svedkov, ktorí ju vo štvrti videli v rôznych okamihoch pred lúpežami. Na identifikáciu a zatknutie podozrivej osoby používa polícia počas víkendu na rôznych miestach vo štvrti technológiu na rozpoznávanie tváre naživo. Na základe indícií od očitých svedkov polícia vytvorila podobizeň tváre podozrivej osoby a z databázy zadržaných osôb extrahovala niekoľko fotografií osôb, ktoré sa podobajú na uvedenú podobizeň tváre.

Aj keď polícia používa technológiu na rozpoznávanie tváre naživo proti zacielenej podozrivej osobe a vymedzí rozsah a čas použitia, takéto použitie nie je povolené v prípade trestného činu, ktorý nie je uvedený v prílohe II k aktu o AI.

Polícia kontroluje emócie fanúšikov na futbalovom štadióne pomocou systému na biometrické rozpoznávanie. Systém zaznamená potenciálnu agresiu a okamžite nasadí v danej časti štadióna diaľkovú biometrickú identifikáciu v reálnom čase s cieľom identifikovať výtržníkov, ktorí sa v minulosti správali násilne.

Kontrola emócií na štadióne nie je podľa aktu o AI zakázaná (patrí však do vysokorizikovej kategórie podľa aktu o AI). Uplatňovanie diaľkovej biometrickej identifikácie v reálnom čase by však bolo podľa aktu o AI zakázané, najmä ak ide o biometrický systém, ktorý rozhoduje o potrebe identifikácie osôb na účely presadzovania práva.

S cieľom identifikovať politického demonštranta, ktorý zorganizoval hromadný protest v uliciach, sa polícia spolieha na sieť CCTV nainštalovanú v meste a v rámci metra. V dotknutom členskom štáte musia organizátori hromadných protestov, ktoré sa konajú na verejných komunikáciách a vo verejných priestoroch, ako sú ulice,

oznámiť plánovaný protest obecným orgánom tri dni vopred, aby sa predišlo narušeniu verejného poriadku a násiliu. Neoznámenie je trestným činom, za ktorý hrozí trest odňatia slobody až na šesť mesiacov a pokuta až 8 000 EUR. Na identifikáciu demonštranta polícia získava videozáznamy z kamier CCTV nainštalovaných v uliciach a vykonáva spätné rozpoznávanie tváre porovnávaním získaných záberov s fotografiami zverejnenými v sociálnych médiách.

Na základe aktu o AI nie je zakázané **spätné používanie technológie na rozpoznávanie tváre**. Takéto používanie sa považuje za vysokorizikové a malo by byť v súlade s požiadavkami aktu o AI pre takéto systémy²⁴³.

Ďalšie príklady praktík, ktoré NIE SÚ zakázané:

- Hotely využívajú diaľkovú biometrickú identifikáciu v reálnom čase na rozpoznávanie VIP hostí. Nejde o presadzovanie práva.
- Nákupné centrá využívajúce diaľkovú biometrickú identifikáciu v reálnom čase na vyhľadávanie zlodejov. Nejde o presadzovanie práva.

Zakázané:

Nákupné centrum využíva diaľkovú biometrickú identifikáciu v reálnom čase na vyhľadávanie zlodejov na základe poverenia polície. Systém je nasadený na účely presadzovania práva vo verejne prístupnom priestore. Použitie je zakázané, pretože na pátranie po zlodejov sa nevzťahuje žiadna z výnimiek uvedených v článku 5 ods. 1 písm. h) aktu o AI.

11. ZAČIATOK UPLATŇOVANIA

429. Podľa článku 113 aktu o AI sa článok 5 aktu o AI uplatňuje od 2. februára 2025. Zákazy uvedené v tomto ustanovení sa budú v zásade vzťahovať na všetky systémy AI bez ohľadu na to, či boli uvedené na trh alebo do prevádzky pred týmto dátumom alebo po ňom²⁴⁴.
430. Zároveň sa 2. augusta 2025 začnú uplatňovať kapitoly o správe a riadení a sankciách. V dôsledku toho sa ustanovenia o sankciách za nedodržanie zákazov uvedených v článku 5 aktu o AI nebudú uplatňovať pred 2. augustom 2025. V tomto prechodnom

²⁴³ Na spracúvanie biometrických údajov na účely presadzovania práva sa naďalej vzťahuje článok 10 smernice o presadzovaní práva, ktorý sa musí vykonávať na vnútroštátnej úrovni. Ich spracúvanie na účely spätného použitia technológie na rozpoznávanie tváre by malo byť povolené len vtedy, ak je to nevyhnutne potrebné, a malo by podliehať primeraným zárukám. Je otázne, či je spätné použitie technológie na rozpoznávanie tváre nevyhnutne potrebné na identifikáciu demonštranta. V rozsudku vo veci Glukhin/Rusko, ktorý slúži ako základ pre tento scenár, Európsky súd pre ľudské práva rozhodol, že hoci odhaľovanie trestnej činnosti môže byť legitímnym cieľom, použitie technológie na rozpoznávanie tváre, spätne aj naživo, bolo neprimerané, keďže neexistovali žiadne riziká z hľadiska verejného poriadku alebo bezpečnosti dopravy. Súdny dvor zdôraznil „vysoko rušivý“ charakter technológií na rozpoznávanie tváre. V tomto prípade súd dospel k záveru, že používanie technológie na rozpoznávanie tváre nie je reakciou na naliehavú spoločenskú potrebu, ani nie je nevyhnutné v demokratickej spoločnosti.

²⁴⁴ Pozri článok 111 ods. 1 a 2 aktu o AI, v ktorom sa uvádza, že doložkou o zachovaní predchádzajúceho stavu nie je dotknuté uplatňovanie článku 5 aktu o AI, ako sa uvádza v článku 113 ods. 3 písm. a) aktu o AI.

období nebudú k dispozícii ani orgány dohľadu nad trhom, ktoré by monitorovali, či sa zákazy riadne dodržiavajú.

431. Aj v tomto prechodnom období sú však zákazy plne uplatniteľné a povinné pre poskytovateľov systémov AI a subjekty nasadzujúce systémy AI. Títo prevádzkovatelia by preto mali prijať potrebné opatrenia na zabezpečenie toho, aby neuvádzali na trh, neuvádzali do prevádzky ani nepoužívali systémy AI, ktoré by mohli predstavovať zakázané praktiky podľa článku 5 aktu o AI. Aj keď sa ustanovenia o monitorovaní a pokutách začnú uplatňovať až neskôr, samotné zákazy majú priamy účinok, a tak umožňujú dotknutým stranám domáhať sa ich uplatňovania na vnútroštátnych súdoch a žiadať o predbežné súdne príkazy, ktorými sa ukladá povinnosť zdržať sa zakázaných praktík.

12. PRESKÚMANIE A AKTUALIZÁCIA USMERNENÍ KOMISIE

432. Tieto usmernenia predstavujú prvý výklad s praktickými príkladmi zákazov uvedených v článku 5 aktu o AI. Komisia bude prevádzkovateľom a orgánom poskytovať ďalšiu podporu v súvislosti s tým, ako chápať uvedené zákazy, a priebežne bude zhromažďovať ďalšie praktické prípady použitia s príspevom poskytovateľov systémov AI a subjektov nasadzujúcich systémy AI, Rady pre AI a ďalších príslušných zainteresovaných strán.
433. Komisia preskúma tieto usmernenia hneď, ako to bude potrebné vzhľadom na praktické skúsenosti získané pri vykonávaní zákazov a tempo technologického, spoločenského a regulačného vývoja v tejto oblasti. Patria sem aj všetky relevantné skúsenosti z opatrení na presadzovanie v oblasti dohľadu nad trhom a výklady, ktoré poskytol Súdny dvor Európskej únie v súvislosti so zákazmi a inými ustanoveniami aktu o AI, ktoré sa skúmajú v týchto usmerneniach. Počas takéhoto preskúmania môže Komisia rozhodnúť o zrušení alebo zmene týchto usmernení. Komisia vyzýva poskytovateľov systémov AI a subjekty nasadzujúce systémy AI, vnútroštátne orgány dohľadu nad trhom prostredníctvom Rady pre AI, poradné fórum pre AI, výskumnú komunitu a organizácie občianskej spoločnosti, aby prispeli k tomuto procesu reakciou na budúce výzvy na verejnú konzultáciu.

