EVROPSKÁ
KOMISE

V Bruselu dne 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

KTERÝM SE STANOVÍ HARMONIZOVANÁ PRAVIDLA PRO UMĚLOU INTELIGENCI (AKT O UMĚLÉ INTELIGENCI) A MĚNÍ URČITÉ LEGISLATIVNÍ AKTY UNIE

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

DŮVODOVÁ ZPRÁVA

1. SOUVISLOSTI NÁVRHU

1.1. Odůvodnění a cíle návrhu

Tato důvodová zpráva doprovází návrh nařízení, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (dále jen „akt o umělé inteligenci“). Umělá inteligence (UI) je rychle se vyvíjející skupina technologií, které mohou přinést širokou škálu výhod hospodářství i společnosti v celém spektru průmyslových odvětví a společenského života. Díky zlepšení predikcí, optimalizaci operací a přidělování zdrojů, jakož i personalizaci poskytování služeb, může využívání umělé inteligence podporovat výsledky přínosné z hlediska společnosti i životního prostředí a poskytovat klíčové konkurenční výhody společnostem i evropskému hospodářství. Tato opatření jsou potřebná obzvláště v odvětvích s vysokými dopady, například v oblasti změny klimatu, životního prostředí a zdraví, veřejného sektoru, financí, mobility, vnitřních věcí a zemědělství. Stejné prvky a techniky, které jsou motorem socioekonomických přínosů UI, však mohou rovněž přinášet nová rizika nebo negativní důsledky pro jednotlivce nebo pro společnost. S ohledem na rychlost technologických změn a na potenciální výzvy je EU odhodlána usilovat o vyvážený přístup. Je v zájmu Unie zachovat vedoucí postavení EU v oblasti technologií a zajistit, aby Evropané mohli využívat výhod nových technologií vyvinutých a fungujících v souladu s hodnotami, základními právy a zásadami Unie.

Tento návrh vychází z politického závazku předsedkyně von der Leyenové, která ve svých politických směrech pro Komisi na období 2019–2024 nazvaných „Unie, která si klade vyšší cíle“[1] oznámila, že Komise předloží právní předpisy pro koordinovaný evropský přístup k lidským a etickým důsledkům UI. V návaznosti na toto oznámení zveřejnila Komise dne 19. února 2020 bílou knihu o UI – evropský přístup k excelenci a důvěře[2]. Tato bílá kniha nastiňuje politické možnosti k dosažení dvojího cíle: podporovat zavádění UI a zabývat se riziky spojenými s některými způsoby využívání této technologie. Návrh usiluje o realizaci druhého cíle vytvoření ekosystému důvěry tím, že navrhne právní rámec pro důvěryhodnou UI. Tento návrh je založen na hodnotách a základních právech EU a jeho cílem je poskytnout lidem a ostatním uživatelům důvěru v přijímání řešení založených na UI a zároveň podporovat podniky v tom, aby tato řešení rozvíjely. UI by měla být nástrojem pro lidi a pozitivní silou pro dobro společnosti, jejímž konečným cílem je zvýšit kvalitu života lidí. Pravidla pro UI dostupnou na trhu Unie nebo jinak ovlivňující obyvatele Unie by se proto měla zaměřovat na člověka, aby lidé mohli důvěřovat tomu, že se tato technologie používá bezpečným způsobem a v souladu s právními předpisy, včetně dodržování základních práv. Po zveřejnění bílé knihy zahájila Komise rozsáhlé konzultace se zúčastněnými stranami, které se setkaly s velkým zájmem značného počtu zúčastněných stran; ty do značné míry podporovaly regulační zásahy s cílem řešit výzvy a obavy v souvislosti se vzrůstajícím využíváním UI.

Návrh reaguje rovněž na výslovné žádosti Evropského parlamentu (EP) a Evropské rady, které opakovaně vyjádřily výzvy k přijetí legislativních opatření s cílem zajistit dobře fungující vnitřní trh systémů umělé inteligence (dále jen „systémy UI“), kde jsou přínosy i rizika UI odpovídajícím způsobem řešeny na úrovni Unie. Podporuje cíl Unie zastávat v celosvětovém kontextu čelnou pozici, pokud jde o rozvoj bezpečné, důvěryhodné a etické

[1] https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_cs_0.pdf.

[2] Evropská komise, bílá kniha Komise o umělé inteligenci – evropský přístup k excelenci a důvěře, COM(2020) 65 final, 2020.

umělé inteligence, který vytyčila Evropská rada[3], a zajišťuje ochranu etických zásad, kterou výslovně požadoval Evropský parlament[4].

V roce 2017 zdůraznila Evropská rada potřebu „reagovat neodkladně na nové trendy“, kdy se jedná „například o otázky umělé inteligence […], přičemž je současně třeba zajistit vysokou úroveň ochrany údajů, digitálních práv a etických norem“[5]. Ve svých závěrech z roku 2019 o koordinovaném plánu rozvoje a používání umělé inteligence vytvořené v Evropě[6] Rada dále zdůraznila, že je důležité zajistit úplné dodržování práv evropských občanů, a vyzvala k tomu, aby byly přezkoumány příslušné stávající právní předpisy s cílem zajistit, že splňují svůj účel z hlediska nových příležitostí a výzev spojených s UI. Evropská rada rovněž vyzvala k jasnému vymezení aplikací UI, které by měly být považovány za vysoce rizikové[7].

Nejnovější závěry ze dne 21. října 2020 dále vyzvaly k vyrovnání se s výzvami, jako je neprůhlednost, komplexní povaha, předpojatost, jistá míra nepředvídatelnosti a částečně autonomní chování určitých systémů UI, aby bylo možno zajistit jejich kompatibilitu se základními právy a usnadnit prosazování právních předpisů[8].

Významné množství práce v oblasti UI vykonal také Evropský parlament. V říjnu 2020 přijal celou řadu usnesení o UI, týkajících se mimo jiné etiky[9], odpovědnosti[10] a autorského práva[11]. Po nich v roce 2021 následovala usnesení o UI v trestních věcech[12] a v oblasti vzdělávání, kultury a v audiovizuálním odvětví[13]. Usnesení Evropského parlamentu o rámci pro etické aspekty umělé inteligence, robotiky a souvisejících technologií výslovně doporučuje Komisi, aby navrhla legislativní opatření s cílem využít příležitostí a přínosů UI, ale také zajistit ochranu etických zásad. Toto usnesení obsahuje znění legislativního návrhu nařízení etických zásad pro vývoj, zavádění a používání UI, robotiky a souvisejících technologií. V souladu s politickým závazkem předsedkyně von der Leyenové, který učinila ve svých politických směrech ohledně usnesení přijatých Evropským parlamentem podle článku 225 SFEU, zohledňuje tento návrh výše uvedené usnesení Evropského parlamentu za plného respektování zásad proporcionality, subsidiarity a zlepšování právní úpravy.

V této politické souvislosti Komise předkládá navrhovaný regulační rámec pro umělou inteligenci s těmito **konkrétními cíli**:

---

3 Evropská rada, mimořádné zasedání Evropské rady (1. a 2. října 2020) – závěry, EUCO 13/20, 2020, s. 6.

4 Usnesení Evropského parlamentu ze dne 20. října 2020 obsahující doporučení Komisi k rámci pro etické aspekty umělé inteligence, robotiky a souvisejících technologií, 2020/2012(INL).

5 Evropská rada, *zasedání Evropské rady (19. října 2017) – závěry*, EUCO 14/17, 2017, s. 8.

6 Rada Evropské unie, *Umělá inteligence b) Závěry o koordinovaném plánu v oblasti umělé inteligence – přijetí* 6177/19, 2019.

7 Evropská rada, *mimořádné zasedání Evropské rady Evropské rady (1. a 2. října 2020) – závěry*, EUCO 13/20, 2020.

8 Rada Evropské unie, *Závěry předsednictví – Listina základních práv se zřetelem k umělé inteligenci a digitálním změnám*, 11481/20, 2020.

9 Usnesení Evropského parlamentu ze dne 20. října 2020 o rámci pro etické aspekty umělé inteligence, robotiky a souvisejících technologií, 2020/2012(INL).

10 Usnesení Evropského parlamentu ze dne 20. října 2020 o režimu občanskoprávní odpovědnosti za umělou inteligenci, 2020/2014(INL).

11 Usnesení Evropského parlamentu ze dne 20. října 2020 o právech duševního vlastnictví při vývoji technologií umělé inteligence, 2020/2015(INI).

12 Návrh zprávy Evropského parlamentu o umělé inteligenci v trestním právu a jejím využívání policií a soudními orgány v trestních věcech, 2020/2016(INI).

13 Návrh zprávy Evropského parlamentu o umělé inteligenci ve vzdělávání, kultuře a audiovizuálním odvětví, 2020/2017(INI). V tomto ohledu přijala Komise akční plán digitálního vzdělávání 2021–2027: Nové nastavení vzdělávání a odborné přípravy pro digitální věk, který předpokládá vypracování etických pokynů pro UI a využívání dat ve vzdělávání – sdělení Komise COM(2020) 624 final.

- zajistit, aby systémy UI, které budou uváděny na trh Unie a používány, byly bezpečné a aby byly v souladu se stávajícími právními předpisy o základních právech a hodnotách Unie,
- zajistit právní jistotu s cílem usnadnit investice a inovace v oblasti UI,
- zlepšit správu a účinné vymáhání stávajících právních předpisů upravujících základní práva a bezpečnostní požadavky platné pro systémy UI,
- usnadnit rozvoj jednotného trhu pro zákonné, bezpečné a důvěryhodné aplikace UI a zamezit roztříštění trhu.

Z hlediska dosažení těchto cílů představuje tento návrh vyvážený a přiměřený horizontální regulační přístup k UI, který je omezen na minimální požadavky nezbytné k řešení rizik a problémů souvisejících s UI, aniž by nepřiměřeně omezoval technologický rozvoj nebo mu bránil, případně jinak neúměrně zvyšoval náklady na uvádění řešení v oblasti UI na trh. Návrh stanoví spolehlivý a pružný právní rámec. Na jedné straně jsou jeho základní regulační rozhodnutí komplexní a obstojí v budoucnosti, včetně požadavků založených na zásadách, které by systémy UI měly splňovat. Na druhé straně zavádí přiměřený regulační systém soustředěný na přesně definovaný regulační přístup založený na rizicích, který nevytváří zbytečná omezení obchodu, přičemž právní zásah je přizpůsoben konkrétním situacím, v nichž existuje oprávněný důvod k obavám nebo kdy lze tyto obavy v blízké budoucnosti důvodně předpokládat. Tento právní rámec zároveň zahrnuje pružné mechanismy, které umožňují jeho dynamické přizpůsobování v souladu s vývojem technologie a vznikem nových znepokojujících situací.

Návrh stanoví harmonizovaná pravidla pro vývoj systémů UI, jejich uvádění na trh a používání v Unii na základě vyváženého přístupu založeného na posouzení rizik. Navrhuje jedinou definici UI, která obstojí i v budoucnosti. Některé obzvláště škodlivé praktiky v oblasti UI jsou zakázány vzhledem k tomu, že jsou v rozporu s hodnotami Unie, a současně jsou navrhována konkrétní omezení a záruky v souvislosti s určitými použitími systémů biometrické identifikace na dálku pro účely vymáhání práva. Návrh stanoví spolehlivou metodiku řízení rizik s cílem definovat „vysoce rizikové“ systémy UI, které představují významná rizika pro zdraví a bezpečnost nebo základní práva osob. Než bude možné tyto systémy UI uvést na trh Unie, bude nutné, aby splňovaly soubor povinných horizontálních požadavků na důvěryhodnou UI a dodržovaly postupy posuzování shody. Předvídatelné, přiměřené a jasné povinnosti jsou kladeny rovněž na poskytovatele a uživatele těchto systémů, aby byla zajištěna bezpečnost a dodržování stávajících právních předpisů chránících základní práva během celého životního cyklu systémů UI. U některých konkrétních systémů UI jsou navrhovány pouze minimální povinnosti transparentnosti, zejména pokud se používají chatboty nebo tzv. deep fakes (realistické fotomontáže a videomontáže).

Navrhovaná pravidla budou prosazována prostřednictvím systému správy na úrovni členských států, který vychází z již existujících struktur, a mechanismu spolupráce na úrovni Unie na základě zřízení Evropské rady pro umělou inteligenci. Jsou rovněž navrhována dodatečná opatření na podporu tzv. regulačních pískovišť umělé inteligence a další opatření ke snížení regulační zátěže a na podporu malých a středních podniků a začínajících podniků.

1.2. Soulad s platnými předpisy v této oblasti politiky

Horizontální povaha návrhu vyžaduje plný soulad se stávajícími právními předpisy Unie použitelnými v odvětvích, kde jsou vysoce rizikové systémy UI již používány nebo je jejich používání pravděpodobné v blízké budoucnosti.

Je rovněž zajištěn soulad s Listinou základních práv EU a se stávajícími sekundárními právními předpisy Unie o ochraně údajů, ochraně spotřebitele, zákazu diskriminace a rovnosti žen a mužů. Tímto návrhem není dotčeno obecné nařízení o ochraně osobních údajů (nařízení (EU) 2016/679) ani směrnice o prosazování práva (směrnice (EU) 2016/680) a návrh je doplňuje o soubor harmonizovaných pravidel pro navrhování, vývoj a používání některých vysoce rizikových systémů UI a omezení některých použití systémů biometrické identifikace na dálku. Návrh rovněž doplňuje stávající právní předpisy Unie o zákazu diskriminace o zvláštní požadavky, jejichž cílem je minimalizovat riziko algoritmické diskriminace, zejména pokud jde o navrhování a kvalitu souborů dat používaných pro vývoj systémů UI, a které jsou doplněny o povinnosti týkající se testování, řízení rizik, dokumentace a lidského dohledu v průběhu celého životního cyklu systémů UI. Tímto návrhem není dotčeno uplatňování právních předpisů Unie v oblasti hospodářské soutěže.

Pokud jde o vysoce rizikové systémy UI, které jsou bezpečnostními součástmi produktů, bude tento návrh začleněn do stávajících odvětvových právních předpisů v oblasti bezpečnosti s cílem zajistit soudržnost, zabránit zdvojování a minimalizovat další zátěž. Zejména pokud jde o vysoce rizikové systémy UI v souvislosti s produkty, na které se vztahují právní předpisy nového legislativního rámce (NLR) (například strojní zařízení, zdravotnické prostředky, hračky), budou požadavky na systémy UI stanovené v tomto návrhu kontrolovány v rámci stávajících postupů posuzování shody podle příslušných právních předpisů NLR. Pokud jde o vzájemné působení požadavků, požadavky tohoto návrhu by sice měly pokrýt bezpečnostní rizika specifická pro systémy UI, avšak cílem právních předpisů NLR je zajistit celkovou bezpečnost konečného produktu, a proto mohou obsahovat zvláštní požadavky týkající se bezpečného začlenění systému UI do konečného produktu. Tento přístup plně odráží návrh nařízení o strojních zařízeních, který je přijat ve stejný den jako tento návrh. Tento návrh by se přímo nevztahoval na vysoce rizikové systémy UI související s produkty, na něž se vztahují příslušné právní předpisy starého přístupu (například letectví, automobily). Při přijímání příslušných prováděcích právních předpisů nebo právních předpisů v přenesené pravomoci podle těchto aktů však bude nutno zohlednit základní požadavky *ex ante* na vysoce rizikové systémy UI uvedené v tomto návrhu.

Pokud jde o systémy UI poskytované nebo používané regulovanými úvěrovými institucemi, měly by být jako příslušné orgány pro dohled nad požadavky tohoto návrhu určeny orgány odpovědné za dohled nad právními předpisy Unie v oblasti finančních služeb s cílem zajistit soudržné prosazování povinností podle tohoto návrhu a právních předpisů Unie v oblasti finančních služeb, jimiž jsou systémy UI do určité míry implicitně regulovány ve vztahu k vnitřnímu systému správy úvěrových institucí. V zájmu dalšího posílení soudržnosti jsou jak postup posuzování shody, tak některé procesní povinnosti poskytovatelů podle tohoto návrhu začleněny do postupů podle směrnice 2013/36/EU o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu[14].

Tento návrh je rovněž v souladu s platnými právními předpisy Unie o službách, včetně zprostředkovatelských služeb, regulovaných směrnicí o elektronickém obchodu 2000/31/ES[15] a nedávným návrhem aktu o digitálních službách, který předložila Komise[16].

---

[14] Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES, text s významem pro EHP (Úř. věst. L 176, 27.6.2013, s. 338).

[15] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“) (Úř. věst. L 178, 17.7.2000, s. 1).

Pokud jde o systémy UI, které jsou součástí rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva řízeném Agenturou Evropské unie pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva (eu-LISA), nebude se tento návrh vztahovat na systémy UI, které byly uvedeny na trh nebo do provozu před uplynutím jednoho roku ode dne použití tohoto nařízení, ledaže by nahrazení nebo změna těchto právních aktů vedla k zásadní změně koncepce nebo určeného účelu dotčeného systému nebo systémů UI.

1.3. Soulad s ostatními politikami Unie

Návrh je součástí širšího komplexního balíčku opatření zabývajícího se problémy vyvolanými rozvojem a využíváním umělé inteligence, které zkoumá bílá kniha o UI. Je tedy zajištěna soudržnost a doplňkovost s dalšími probíhajícími nebo plánovanými iniciativami Komise, jejichž cílem je rovněž řešit tyto problémy, včetně revize odvětvových právních předpisů týkajících se konkrétních výrobků (například směrnice o strojních zařízeních a směrnice o obecné bezpečnosti výrobků), a s iniciativami, které se zabývají otázkami odpovědnosti souvisejícími s novými technologiemi, včetně systémů UI. Tyto iniciativy budou vycházet z tohoto návrhu a doplňovat jej s cílem vyjasnit právní předpisy a podpořit rozvoj ekosystému důvěry v UI v Evropě.

Tento návrh je rovněž v souladu s celkovou digitální strategií Komise, pokud jde o její příspěvek k podpoře technologií, které slouží lidem, což je jeden ze tří hlavních pilířů politické orientace a cílů oznámených ve sdělení „Formování digitální budoucnosti Evropy“[17]. Stanoví soudržný, účinný a přiměřený rámec pro zajištění rozvoje umělé inteligence způsobem, který respektuje lidská práva a získává jejich důvěru, zajišťuje připravenost Evropy na digitální věk a mění příštích deset let v **digitální dekádu**[18].

Podpora inovací založených na UI je navíc úzce spojena s **aktem o správě dat**[19]**, se směrnicí o otevřených datech**[20] a s dalšími iniciativami v rámci **strategie EU pro data**[21], které zavedou důvěryhodné mechanismy a služby pro opakované použití, sdílení a slučování dat, která jsou nezbytná pro vývoj vysoce kvalitních modelů umělé inteligence založených na datech.

Návrh rovněž významně posiluje úlohu Unie, která se podílí na formování globálních norem a standardů a prosazuje důvěryhodnou UI, která je v souladu s hodnotami a zájmy Unie. Poskytuje Unii pevný základ pro další jednání s jejími externími partnery, včetně třetích zemí, a pro účast na mezinárodních fórech v otázkách týkajících se umělé inteligence.

---

16 Viz návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY o jednotném trhu digitálních služeb (akt o digitálních službách) a o změně směrnice 2000/31/ES, COM/2020/825 final.

17 Sdělení Komise, Formování digitální budoucnosti Evropy, COM(2020)67 final.

18 Digitální kompas 2030:Evropské pojetí digitální dekády.

19 Návrh nařízení o evropské správě dat (akt o správě dat) COM/2020/767.

20 Směrnice Evropského parlamentu a Rady (EU) 2019/1024 ze dne 20. června 2019 o otevřených datech a opakovaném použití informací veřejného sektoru, PE/28/2019/REV/1 (Úř. věst. L 172, 26.6.2019, s. 56).

21 Sdělení Komise Evropská strategie pro data, COM(2020) 66 final.

2. PRÁVNÍ ZÁKLAD, SUBSIDIARITA A PROPORCIONALITA

2.1. Právní základ

Právním základem tohoto návrhu je v prvé řadě článek 114 Smlouvy o fungování Evropské unie (SFEU), který stanoví přijetí opatření nezbytných pro vytvoření a fungování vnitřního trhu.

Tento návrh představuje hlavní součást strategie EU pro jednotný digitální trh. Prvořadým cílem tohoto návrhu je zajistit řádné fungování vnitřního trhu stanovením harmonizovaných pravidel, zejména pokud jde o vývoj produktů a služeb využívajících technologie UI nebo poskytovaných jako samostatné systémy UI, jejich uvádění na trh Unie a používání. Některé členské státy již nyní zvažují taková vnitrostátní pravidla, která by zajišťovala, že UI bude bezpečná a že bude vyvíjena a používána v souladu s povinnostmi v oblasti základních práv. To pravděpodobně povede ke dvěma hlavním problémům: i) k roztříštěnosti vnitřního trhu, pokud jde o podstatné prvky, týkající se zejména požadavků na produkty a služby umělé inteligence, jejich uvádění na trh, jejich používání, odpovědnost za ně a dohled nad nimi ze strany veřejných orgánů; a ii) podstatnému snížení právní jistoty jak pro poskytovatele, tak pro uživatele systémů UI ohledně toho, jak se budou na tyto systémy v Unii vztahovat stávající a nová pravidla. Vzhledem ke značnému objemu přeshraničního oběhu produktů a služeb představují optimální řešení těchto dvou problémů harmonizující právní předpisy EU.

Návrh totiž definuje společné povinné požadavky na návrh a vývoj určitých systémů UI před jejich uvedením na trh, které budou dále rozvedeny prostřednictvím harmonizovaných technických norem. Návrh rovněž řeší situaci po uvedení systémů UI na trh tím, že harmonizuje způsob provádění kontrol *ex post*.

Navíc vzhledem k tomu, že tento návrh obsahuje určitá zvláštní pravidla ochrany fyzických osob v souvislosti se zpracováním osobních údajů, zejména omezení používání systémů UI pro biometrickou identifikaci na dálku v reálném čase na veřejně přístupných místech pro účely prosazování práva, je vhodné založit toto nařízení, pokud jde o tato zvláštní pravidla, na článku 16 SFEU.

2.2. Subsidiarita (v případě nevýlučné pravomoci)

Povaha umělé inteligence, která se často opírá o rozsáhlé a rozmanité datové soubory a která může být začleněna do jakéhokoli produktu nebo služby, které volně obíhají v rámci vnitřního trhu, znamená, že cílů tohoto návrhu nelze účinně dosáhnout pouze na úrovni jednotlivých členských států. Vznikající různorodá regulace potenciálně rozdílných vnitrostátních pravidel bude navíc brzdit bezproblémový oběh produktů a služeb souvisejících se systémy UI v celé EU a bude neúčinná při zajišťování bezpečnosti a ochrany základních práv a hodnot Unie v jednotlivých členských státech. Vnitrostátní přístupy k řešení těchto problémů vytvoří pouze další právní nejistotu a překážky a zpomalí pronikání umělé inteligence na trh.

Cílů tohoto návrhu lze lépe dosáhnout na úrovni Unie, aby se zabránilo dalšímu tříštění jednotného trhu na potenciálně protichůdné vnitrostátní rámce, které brání volnému oběhu zboží a služeb obsahujících UI. Pevný evropský regulační rámec pro důvěryhodnou UI také zajistí rovné podmínky a ochranu všech občanů, přičemž zároveň posílí konkurenceschopnost a průmyslovou základnu Evropy v oblasti umělé inteligence. Pouze společný postup na úrovni Unie může rovněž ochránit digitální suverenitu Unie a využívat její nástroje a regulační pravomoci k utváření globálních pravidel a norem.

2.3. Proporcionalita

Návrh vychází ze stávajících právních rámců a je přiměřený a nezbytný k dosažení svých cílů, protože se řídí přístupem založeným na posouzení rizik a ukládá regulační zátěž pouze tehdy, je-li pravděpodobné, že daný systém UI představuje vysoké riziko pro základní práva a bezpečnost. U jiných systémů UI, které nejsou vysoce rizikové, jsou ukládány pouze velmi omezené povinnosti transparentnosti, například pokud jde o poskytování informací umožňujících upozornit na používání systému UI při interakci s lidmi. U vysoce rizikových systémů UI jsou požadavky na vysoce kvalitní údaje, dokumentaci a sledovatelnost, transparentnost, lidský dohled, přesnost a spolehlivost nezbytným předpokladem zmírňování rizik pro základní práva a bezpečnost, které tato UI představuje a na něž se nevztahují jiné platné právní rámce. Harmonizované normy a podpůrné nástroje poskytující pokyny a umožňující dodržování předpisů pomohou poskytovatelům a uživatelům splnit požadavky stanovené v návrhu a minimalizovat náklady. Náklady vzniklé provozovatelům jsou úměrné dosahovaným cílům, hospodářským přínosům a výhodám vyplývajícím z dobré pověsti, které mohou provozovatelé od tohoto návrhu očekávat.

2.4. Volba nástroje

Volba nařízení jako právního nástroje je odůvodněna potřebou jednotného uplatňování nových pravidel, jako je například definice UI, zákaz některého škodlivého jednání, které používání UI umožňuje, a klasifikace určitých systémů UI. Přímá použitelnost nařízení v souladu s článkem 288 SFEU omezí právní roztříštěnost a usnadní rozvoj jednotného trhu s legálními, bezpečnými a důvěryhodnými systémy UI. Toho bude dosaženo zejména zavedením harmonizovaného souboru základních požadavků na systémy UI klasifikované jako vysoce rizikové a povinností poskytovatelů a uživatelů těchto systémů, které zlepší ochranu základních práv a poskytnou právní jistotu stejnou měrou provozovatelům i spotřebitelům.

Ustanovení tohoto nařízení zároveň nejsou příliš normativní a ponechávají prostor pro různé úrovně opatření členských států v případě prvků, které neohrožují cíle této iniciativy, zejména vnitřní organizace systému dozoru nad trhem a zavádění opatření na podporu inovací.

3. VÝSLEDKY HODNOCENÍ *EX POST*, KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

3.1. Konzultace se zúčastněnými stranami

Tento návrh je výsledkem rozsáhlých konzultací se všemi hlavními zúčastněnými stranami, při nichž byly ze strany Komise uplatněny obecné zásady a minimální standardy pro konzultace zúčastněných stran.

Dne 19. února 2020 byla současně se zveřejněním bílé knihy o umělé inteligenci zahájena **on-line veřejná konzultace**, která trvala do 14. června 2020. Cílem této konzultace bylo shromáždit názory a stanoviska k této bílé knize. Konzultace se zaměřila na všechny zúčastněné strany z veřejného i soukromého sektoru, včetně vlád, místních orgánů, komerčních i nekomerčních organizací, sociálních partnerů, odborníků, akademických pracovníků a občanů. Komise po provedení analýzy všech obdržených odpovědí zveřejnila souhrn výsledků a jednotlivé odpovědi na svých internetových stránkách[22].

Celkem bylo obdrženo 1 215 příspěvků, z toho 352 od společností nebo obchodních organizací/sdružení, 406 od jednotlivců (92 % jednotlivců z EU), 152 jménem

[22] Všechny výsledky konzultací jsou dostupné zde.

akademických/výzkumných institucí a 73 od orgánů veřejné moci. Hlasy občanské společnosti zastupovalo 160 respondentů (z toho 9 organizací spotřebitelů, 129 nevládních organizací a 22 odborových svazů) a 72 respondentů přispělo jako „ostatní“. Z 352 zástupců podniků a průmyslu bylo 222 společností a zástupců podniků, přičemž 41,5 % z nich představovaly mikropodniky a malé a střední podniky. Zbytek představovala hospodářská sdružení. Celkem 84 % odpovědí zástupců podniků a průmyslu pocházelo ze zemí EU-27. V závislosti na položené otázce využilo 81 až 598 respondentů při vkládání komentářů možnost vepsat libovolný text. Prostřednictvím internetových stránek „EU Survey“ bylo předloženo přes 450 stanovisek, a to jak navíc k odpovědi na dotazník (více než 400), tak jako samostatné příspěvky (více než 50).

Celkově se zúčastněné strany všeobecně shodují na tom, že je třeba jednat. Velká většina zúčastněných stran se shoduje na tom, že existují legislativní mezery, případně že je zapotřebí vytvořit nové právní předpisy. Několik zúčastněných stran však upozorňuje Komisi na nutnost vyhnout se zdvojování, protichůdným závazkům a nadměrné regulaci. V řadě komentářů byl zdůrazněn význam technologicky neutrálního a přiměřeného regulačního rámce.

Zúčastněné strany většinou požadovaly úzkou, jednoznačnou a přesnou definici UI. Zúčastněné strany rovněž zdůraznily, že kromě vyjasnění pojmu „umělá inteligence“ je důležité definovat rovněž pojmy „riziko“, „vysoké riziko“, „nízké riziko“, „biometrická identifikace na dálku“ a „újma“.

Většina respondentů výslovně podporuje přístup založený na posouzení rizik. Používání rámce založeného na posouzení rizik bylo považováno za lepší alternativu než plošná regulace všech systémů UI. Typy rizik a hrozeb by měly být založeny na individuálním přístupu podle jednotlivých odvětví a jednotlivých případů. Výpočet rizik by měl zohledňovat rovněž dopad na práva a na bezpečnost.

Pro podporu UI by mohla být velmi užitečná regulační pískoviště a některé zúčastněné strany, zejména hospodářská sdružení, je vítají.

Přes 50 % respondentů, zejména z řad hospodářských sdružení, kteří vyjádřili názor na modely prosazování, se u vysoce rizikových systémů UI vyslovilo pro kombinaci posuzování rizik vlastními silami *ex ante* a prosazování *ex post*.

3.2. Sběr a využití výsledků odborných konzultací

Návrh vychází z analýzy prováděné po dobu dvou let a z úzkého zapojení zúčastněných stran, včetně akademických pracovníků, podniků, sociálních partnerů, nevládních organizací, členských států a občanů. Přípravné práce byly zahájeny v roce 2018 zřízením **odborné skupiny na vysoké úrovni pro UI**, jejíž inkluzivní a široké složení zahrnovalo 52 známých odborníků, kteří byli pověřeni poradenstvím Komisi při provádění její strategie pro umělou inteligenci. V dubnu 2019 Komise podpořila[23] klíčové požadavky stanovené v etických pokynech odborné skupiny na vysoké úrovni pro důvěryhodnou UI[24], které byly revidovány tak, aby zohledňovaly více než 500 připomínek zúčastněných stran. Tyto klíčové požadavky odrážejí rozšířený a společný přístup, o kterém svědčí nepřeberné množství etických kodexů a zásad vypracovaných celou řadou soukromých a veřejných organizací v Evropě i mimo ni, a podle něhož by se vývoj a používání UI měly řídit určitými základními zásadami

[23] Evropská komise, *Budování důvěry v umělou inteligenci zaměřenou na člověka*, COM(2019) 168.

[24] Odborná skupina na vysoké úrovni pro umělou inteligenci, *Etické pokyny pro zajištění důvěryhodnosti UI*, 2019.

zaměřenými na hodnotu. Kontrolní seznam pro důvěryhodnou umělou inteligenci (ALTAI)[25] tyto požadavky uvedl do praxe v pilotním procesu zahrnujícím více než 350 organizací.

Navíc byla vytvořena **Aliance pro umělou inteligenci**[26] jako platforma pro přibližně 4 000 zúčastněných stran, která jim umožňuje diskutovat o technologických a společenských důsledcích UI a která vrcholí každoročním shromážděním pro UI.

Tento inkluzivní přístup dále rozvinula **bílá kniha** o UI, která podnítila připomínky více než 1 250 zúčastněných stran, včetně více než 450 dalších stanovisek. V důsledku toho Komise zveřejnila počáteční posouzení dopadů, k němuž bylo opět zasláno více než 130 připomínek[27]. Byla rovněž uspořádána **další pracovní setkání a akce zúčastněných stran**, jejichž výsledky podporují analýzu provedenou v rámci posouzení dopadů a politická rozhodnutí přijatá v tomto návrhu[28]. Bylo také zadáno vypracování **externí studie**, jejímž cílem bylo posloužit jako podklad pro posouzení dopadů.

3.3. Posouzení dopadů

Komise provedla v souladu se svou politikou „zlepšování právní úpravy“ posouzení dopadů tohoto návrhu, které přezkoumal Výbor Komise pro kontrolu regulace. Dne 16. prosince 2020 se konalo setkání s Výborem pro kontrolu regulace, po němž následovalo vydání záporného stanoviska. Po podstatné revizi posouzení dopadů s cílem zohlednit připomínky a po opětovném předložení posouzení dopadů vydal Výbor pro kontrolu regulace dne 21. března 2021 kladné stanovisko. Stanoviska Výboru pro kontrolu regulace, doporučení a vysvětlení toho, jakým způsobem byla zohledněna, jsou uvedena v příloze 1 posouzení dopadů.

Komise zkoumala různé politické možnosti dosažení obecného cíle návrhu, kterým je **zajistit řádné fungování jednotného trhu** vytvořením podmínek pro rozvoj a používání důvěryhodné UI v Unii.

Byly posouzeny čtyři politické možnosti s různými stupni regulačních zásahů:

- **možnost č. 1**: legislativní nástroj EU zavádějící dobrovolný systém označování,
- **možnost č. 2**: odvětvový „*ad hoc*“ přístup,
- **možnost č. 3**: horizontální legislativní nástroj EU využívající přiměřený přístup založený na posouzení rizik,
- **možnost č. 3+**: horizontální legislativní nástroj EU využívající přiměřený přístup založený na posouzení rizik + kodexy chování pro systémy UI, které nejsou vysoce rizikové,
- **možnost č. 4**: horizontální legislativní nástroj EU stanovující závazné požadavky pro všechny systémy UI bez ohledu na riziko, které představují.

Podle zavedené metodiky Komise byla každá z těchto politických možností hodnocena na základě hospodářských a společenských dopadů se zvláštním zaměřením na dopady na základní práva. Upřednostňovanou možností je možnost č. 3+, tj. regulační rámec pouze pro

[25] Odborná skupina na vysoké úrovni pro umělou inteligenci, *Kontrolní seznam pro důvěryhodnou umělou inteligenci (ALTAI) pro účely posouzení vlastními silami*, 2020.

[26] Aliance pro UI je fórum mnoha zúčastněných stran, které bylo zahájeno v červnu 2018; Aliance pro UI https://ec.europa.eu/digital-single-market/en/european-ai-alliance.

[27] Evropská komise, *Počáteční posouzení dopadů k návrhu právního aktu Evropského parlamentu a Rady, kterým se stanoví požadavky na umělou inteligenci.*

[28] Podrobné informace o všech provedených konzultacích viz příloha 2 posouzení dopadů.

vysoce rizikové systémy UI s možností, aby se všichni poskytovatelé systémů UI, které nejsou vysoce rizikové, řídili určitým kodexem chování. Tyto požadavky se budou týkat údajů, dokumentace a sledovatelnosti, poskytování informací a transparentnosti, lidského dohledu, spolehlivosti a přesnosti a pro vysoce rizikové systémy UI by byly povinné. Společnosti, které zavedly kodexy chování pro jiné systémy UI, by tak činily dobrovolně.

Tato upřednostňovaná možnost byla považována za vhodnou z hlediska co nejúčinnějšího řešení cílů tohoto návrhu. Tím, že tato upřednostňovaná možnost vyžaduje od vývojářů a uživatelů UI omezený, ale účinný soubor opatření, omezuje rizika porušování základních práv a bezpečnosti lidí a podporuje účinný dohled a vymáhání, neboť zaměřuje požadavky pouze na systémy, kde existuje vysoké riziko tohoto porušování. Tato možnost tak stlačuje náklady na dodržování předpisů na minimum, čímž brání zbytečnému zpomalování zavádění umělé inteligence v důsledku vyšších cen a nákladů na dodržování předpisů. Za účelem řešení možných nevýhod pro malé a střední podniky zahrnuje tato možnost několik ustanovení na podporu souladu těchto podniků a snižování jejich nákladů, včetně vytváření regulačních pískovišť a povinnosti zohledňovat zájmy malých a středních podniků při stanovování poplatků souvisejících s posuzováním shody.

Upřednostňovaná možnost zvýší důvěru lidí v UI, společnosti získají větší právní jistotu a členské státy nebudou mít důvod přijímat jednostranná opatření, která by mohla vést k roztříštění jednotného trhu. Vyšší poptávka založená na vyšší důvěře, dostupnější nabídky vzhledem k právní jistotě a absence překážek přeshraničního pohybu systémů UI pravděpodobně povedou k prosperitě jednotného trhu UI. Evropská unie bude i nadále rozvíjet rychle rostoucí ekosystém UI v oblasti inovativních služeb a produktů, v nichž je vestavěna technologie UI, nebo samostatných systémů UI, což povede ke zvýšení digitální autonomie.

Podniky nebo veřejné orgány, které vyvíjejí nebo používají aplikace UI představující vysoké riziko pro bezpečnost nebo základní práva občanů, by musely dodržovat zvláštní požadavky a povinnosti. Soulad s těmito požadavky by znamenal: do roku 2025 náklady v přibližné výši 6 000 až 7 000 EUR na dodávku průměrného vysoce rizikového systému UI v hodnotě přibližně 170 000 EUR. Uživatelé UI by v závislosti na případu použití tam, kde by to bylo vhodné, každoročně rovněž vynakládali náklady na čas strávený zajišťováním lidského dohledu. Ty by dle odhadu činily přibližně 5 000 až 8 000 EUR ročně. Náklady na ověření pro dodavatele vysoce rizikové UI by mohly činit dalších 3 000 až 7 500 EUR. Podniky nebo orgány veřejné moci, které vyvíjejí nebo používají jakékoli aplikace UI, které nejsou klasifikovány jako vysoce rizikové, by měly pouze minimální informační povinnosti. Mohly by se však rozhodnout připojit se k ostatním, společně přijmout kodex chování s cílem řídit se vhodnými požadavky a zajistit, aby jejich systémy UI byly důvěryhodné. V tomto případě by náklady byly maximálně stejně vysoké jako u vysoce rizikových systémů UI, s největší pravděpodobností by však byly nižší.

Dopady politických možností na jednotlivé kategorie zúčastněných stran (hospodářské subjekty/podniky; subjekty posuzování shody, normalizační orgány a jiné veřejné subjekty; jednotlivce/občany; výzkumné pracovníky) jsou podrobně vysvětleny v příloze 3 posouzení dopadů předloženého na podporu tohoto návrhu.

3.4. Účelnost právních předpisů a zjednodušování

Tento návrh stanoví povinnost, která se bude vztahovat na poskytovatele a uživatele vysoce rizikových systémů UI. Vytvoří právní jistotu pro poskytovatele, kteří tyto systémy vyvíjejí a uvádějí na trh Unie, a zajistí, aby nevznikla žádná překážka pro přeshraniční poskytování služeb a produktů souvisejících s umělou inteligencí. U společností využívajících UI bude podporovat důvěru mezi jejich zákazníky. U vnitrostátních orgánů veřejné správy bude

podporovat důvěru veřejnosti ve využívání UI a posilovat donucovací mechanismy (zavedením evropského koordinačního mechanismu, zajištěním vhodných kapacit a usnadněním auditů systémů UI s novými požadavky na dokumentaci, sledovatelnost a transparentnost). Tento rámec bude navíc obsahovat zvláštní opatření na podporu inovací, včetně regulačních pískovišť a zvláštních opatření na podporu malých uživatelů a poskytovatelů vysoce rizikových systémů UI při dodržování nových pravidel.

Návrh je rovněž konkrétně zaměřen na posílení evropské konkurenceschopnosti a průmyslové základny v oblasti UI. Je zajištěn plný soulad se stávajícími odvětvovými právními předpisy Unie použitelnými na systémy UI (týkajícími se například produktů a služeb), které dále vyjasní a zjednoduší prosazování nových pravidel.

3.5. Základní práva

Využívání UI s jejími specifickými vlastnostmi (například neprůhlednost, složitost, závislost na datech či autonomní chování) může nepříznivě ovlivnit řadu základních práv zakotvených v Listině základních práv Evropské unie (dále jen „Listina“). Snahou tohoto návrhu je zajistit vysokou úroveň ochrany těchto základních práv a jeho cílem je řešit různé zdroje rizik prostřednictvím jasně definovaného přístupu založeného na posouzení rizik. Návrh obsahuje soubor požadavků na důvěryhodnou UI a přiměřené povinnosti pro všechny účastníky hodnotového řetězce, čímž posílí a podpoří ochranu práv chráněných Listinou: právo na lidskou důstojnost (článek 1), na respektování soukromého života a ochranu osobních údajů (články 7 a 8), na zákaz diskriminace (článek 21) a na rovnost žen a mužů (článek 23). Jeho cílem je zabránit odrazujícímu účinku na právo na svobodu projevu (článek 11) a svobodu shromažďování (článek 12) a zajistit ochranu práva na účinnou právní ochranu a spravedlivý proces, práva na obhajobu a presumpci neviny (články 47 a 48), jakož i obecnou zásadu řádné správy. Návrh navíc v určitých oblastech pozitivně ovlivní práva celé řady zvláštních skupin, jako jsou například práva pracovníků na slušné a spravedlivé pracovní podmínky (článek 31), vysoká úroveň ochrany spotřebitele (článek 28), práva dítěte (článek 24) a začlenění osob se zdravotním postižením (článek 26). Relevantní je rovněž právo na vysokou úroveň ochrany životního prostředí a zvyšování jeho kvality (článek 37), a to i ve vztahu ke zdraví a bezpečnosti lidí. Dodržování dalších základních práv usnadní rovněž povinnosti týkající se testování *ex ante*, řízení rizik a lidského dohledu, které budou minimalizovat riziko chybných nebo zkreslených rozhodnutí přijatých s podporou UI v kritických oblastech, jako je například vzdělávání a odborná příprava, zaměstnání, důležité služby, prosazování práva a soudnictví. V případě, že bude i přesto docházet k porušování základních práv, budou dotčeným osobám umožněna účinná náprava zajištěním transparentnosti a sledovatelnosti systémů UI ve spojení s přísnými kontrolami *ex post*.

Tento návrh ukládá určitá omezení svobody podnikání (článek 16) a svobody umění a věd (článek 13) s cílem zajistit dodržování naléhavých důvodů veřejného zájmu, jako je zdraví, bezpečnost, ochrana spotřebitele a ochrana dalších základních práv („odpovědné inovace“), při vývoji a používání vysoce rizikové technologie UI. Tato omezení jsou přiměřená a omezují se na minimum nezbytné k prevenci a zmírnění závažných bezpečnostních rizik a pravděpodobného porušování základních práv.

Zpřísnění povinností v souvislosti s transparentností rovněž nepřiměřeně neovlivní právo na ochranu duševního vlastnictví (čl. 17 odst. 2) vzhledem k tomu, že tyto povinnosti budou omezeny pouze na minimum informací nezbytných pro výkon práva jednotlivců na účinnou právní ochranu a na nezbytnou transparentnost vůči orgánům dozoru a donucovacím orgánům v souladu s jejich pověřeními. Jakékoli zveřejnění informací bude provedeno v souladu s příslušnými právními předpisy v dané oblasti, včetně směrnice 2016/943 o ochraně nezveřejněného know-how a obchodních informací (obchodního tajemství) před jejich

neoprávněným získáním, využitím a zpřístupněním. Pokud je nutné umožnit orgánům veřejné moci a oznámeným subjektům přístup k důvěrným informacím nebo ke zdrojovým kódům s cílem ověřit soulad s podstatnými povinnostmi, vztahují se na ně závazné povinnosti zachování důvěrnosti.

4. ROZPOČTOVÉ DŮSLEDKY

Členské státy budou povinny určit dozorové úřady, jejichž úkolem bude provádění legislativních požadavků. Jejich dozorčí funkce by mohla vycházet ze zavedených struktur, například pokud jde o subjekty posuzování shody nebo dozor nad trhem, avšak vyžadovala by dostatečné odborné znalosti a lidské a finanční zdroje. V závislosti na zavedené struktuře v jednotlivých členských státech by se mohlo jednat o 1 až 25 zaměstnanců v přepočtu na plný úvazek na členský stát.

Podrobný přehled souvisejících nákladů je uveden ve „finančním výkazu“ souvisejícím s tímto návrhem.

5. OSTATNÍ PRVKY

5.1. Plány provádění a způsoby monitorování, hodnocení a podávání zpráv

Zavedení spolehlivého mechanismu monitorování a hodnocení má zásadní význam pro zajištění účinného dosahování konkrétních cílů návrhu. Za monitorování účinků návrhu bude odpovídat Komise. Vytvoří systém pro registraci samostatných vysoce rizikových aplikací UI do veřejné databáze na úrovni celé EU. Tato registrace rovněž umožní příslušným orgánům, uživatelům a dalším zájemcům ověřit, zda daný vysoce rizikový systém UI splňuje požadavky stanovené v návrhu, a posílit výkon dohledu nad systémy UI, které představují vysoké riziko pro základní práva. Poskytovatelé UI budou pro potřeby této databáze povinni poskytovat smysluplné informace o svých systémech a o posuzování shody prováděném u těchto systémů.

Poskytovatelé UI budou rovněž povinni informovat příslušné vnitrostátní orgány o závažných incidentech nebo chybném fungování, které představují porušení povinností v oblasti základních práv, jakmile se o nich dovědí, jakož i o jakémkoli stažení systémů UI z oběhu nebo z trhu. Příslušné vnitrostátní orgány poté tyto závažné incidenty nebo chybné fungování prošetří, shromáždí všechny potřebné informace a budou je pravidelně předávat Komisi společně s příslušnými metadaty. Komise tyto informace o závažných incidentech doplní komplexní analýzou celkového trhu s umělou inteligencí.

Komise zveřejní zprávu obsahující hodnocení a přezkum navrhovaného rámce UI pět let po datu jeho použitelnosti.

5.2. Podrobné vysvětlení konkrétních ustanovení návrhu

5.2.1. OBLAST PŮSOBNOSTI A DEFINICE (HLAVA I)

Hlava I stanoví předmět nařízení a oblast působnosti nových pravidel, která se týkají uvádění systémů UI na trh a do provozu a jejich používání. Vymezuje rovněž definice používané v rámci celého nástroje. Cílem definice systému UI v tomto právním rámci je dosáhnout maximální možné technologické neutrality a použitelnosti i v budoucnu s přihlédnutím k rychlému technologickému vývoji a vývoji trhu v souvislosti s UI. Pro zajištění potřebné právní jistoty doplňuje hlavu I příloha I, která obsahuje podrobný seznam přístupů a technik pro rozvoj UI, který bude Komise upravovat v souladu s novým technologickým vývojem. Pro účely zajištění rovných podmínek jsou rovněž jednoznačně definováni klíčoví účastníci

celého hodnotového řetězce UI, jako jsou například poskytovatelé a uživatelé systémů UI, mezi něž se řadí veřejní i soukromí provozovatelé.

5.2.2. ZAKÁZANÉ POSTUPY V OBLASTI UMĚLÉ INTELIGENCE (HLAVA II)

Hlava II stanoví seznam zakázaných praktik v oblasti UI. Toto nařízení se řídí přístupem založeným na posouzení rizik, který rozlišuje mezi použitími UI vytvářejícími i) nepřijatelné riziko; ii) vysoké riziko a iii) nízké nebo minimální riziko. Seznam zakázaných praktik v hlavě II zahrnuje všechny systémy UI, jejichž používání je považováno za nepřijatelné z důvodu rozporu s hodnotami Unie, například v důsledku porušování základních práv. Tyto zákazy se týkají praktik, které mají významný potenciál manipulovat s osobami prostřednictvím podprahových technik bez jejich vědomí, případně zneužívají zranitelnosti konkrétních zranitelných skupin, jako jsou děti nebo osoby se zdravotním postižením, s cílem podstatně ovlivnit jejich chování způsobem, který by mohl jim nebo jiné osobě způsobit psychickou nebo fyzickou újmu. Na jiné manipulativní nebo vykořisťovatelské praktiky týkající se dospělých, které by mohly systémy UI umožňovat, by se mohly vztahovat stávající právní předpisy o ochraně údajů, ochraně spotřebitele a digitálních službách, které zaručují, že fyzické osoby budou řádně informovány a budou mít svobodnou volbu nebýt předmětem profilování ani jiných praktik, které by mohly ovlivnit jejich chování. Návrh rovněž zakazuje přidělování sociálního kreditu na základě UI pro obecné účely prováděné orgány veřejné moci. A konečně je až na určité omezené výjimky zakázáno rovněž používání biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva.

5.2.3. VYSOCE RIZIKOVÉ SYSTÉMY UI (HLAVA III)

Hlava III obsahuje zvláštní pravidla pro systémy UI, které představují vysoké riziko pro zdraví a bezpečnost nebo pro základní práva fyzických osob. Tyto vysoce rizikové systémy UI jsou v souladu s přístupem založeným na posouzení rizik na evropském trhu povoleny pod podmínkou, že budou splňovat určité závazné požadavky a že bude provedeno posouzení shody *ex ante*. Klasifikace systému UI jako vysoce rizikového je založena na určeném účelu daného systému UI v souladu se stávajícími právními předpisy upravujícími bezpečnost výrobků. Klasifikace systému UI jako vysoce rizikového proto nezávisí pouze na funkci, kterou tento systém vykonává, ale také na konkrétním účelu a způsobech, pro které se tento systém používá.

Kapitola 1 hlavy III stanoví klasifikační pravidla a vymezuje dvě hlavní kategorie vysoce rizikových systémů UI:

- systémy UI určené k použití jako bezpečnostní součást produktů, na které se vztahuje posouzení shody *ex ante* třetí stranou,
- jiné samostatné systémy UI s důsledky převážně pro základní práva, které jsou výslovně uvedeny v příloze III.

Tento seznam vysoce rizikových systémů UI v příloze III obsahuje omezený počet systémů UI, jejichž rizika se již projevila nebo se pravděpodobně projeví v blízké budoucnosti. Aby Komise zajistila, že nařízení bude možno přizpůsobit nově vznikajícím použitím a aplikacím UI, může rozšířit seznam vysoce rizikových systémů UI používaných v určitých předem definovaných oblastech uplatněním souboru kritérií a metodiky posuzování rizik

Kapitola 2 stanoví právní požadavky na vysoce rizikové systémy UI, pokud jde o údaje a správu údajů, dokumentaci a uchovávání záznamů, transparentnost a poskytování informací uživatelům, lidský dohled, spolehlivost, přesnost a bezpečnost. U řady provozovatelů postupujících s řádnou péčí odpovídají navrhované minimální požadavky nejnovějším

poznatkům již nyní a jsou výsledkem dvouletých přípravných prací, odvozených z etických pokynů odborné skupiny na vysoké úrovni pro umělou inteligenci[29], jejichž pilotního provozu se účastní více než 350 organizací[30]. Jsou rovněž do značné míry v souladu s dalšími mezinárodními doporučeními a zásadami, což zajišťuje slučitelnost navrhovaného rámce pro UI s rámcem přijatým mezinárodními obchodními partnery EU. Konkrétní technická řešení pro dosažení souladu s těmito požadavky mohou být uvedena v normách nebo v jiných technických specifikacích, případně vyvinuta jiným způsobem v souladu s obecnými technickými nebo vědeckými poznatky podle uvážení poskytovatele systému UI. Tato flexibilita je mimořádně důležitá, protože poskytovatelům systémů UI umožňuje volbu způsobu splnění jejich požadavků s přihlédnutím k nejnovějšímu vývoji a technologickému a vědeckému pokroku v této oblasti.

Kapitola 3 ukládá poskytovatelům vysoce rizikových systémů UI jednoznačný soubor horizontálních povinností. Přiměřené povinnosti jsou kladeny rovněž na uživatele a na další účastníky v celém hodnotovém řetězci UI (například na dovozce, distributory a zplnomocněné zástupce).

Kapitola 4 stanoví rámec pro zapojení oznámených subjektů jako nezávislých třetích stran do postupů posuzování shody, zatímco kapitola 5 podrobně vysvětluje postupy posuzování shody, které je třeba dodržovat u jednotlivých typů vysoce rizikových systémů UI. Cílem přístupu posuzování shody je minimalizovat zátěž hospodářských subjektů i oznámených subjektů, jejichž kapacitu je třeba v průběhu času postupně zvyšovat. Systémy UI určené k použití jako bezpečnostní součásti produktů, které se řídí právními předpisy podle nového legislativního rámce (například strojní zařízení, hračky, zdravotnické prostředky atd.), budou podléhat stejným mechanismům posuzování shody *ex ante* a *ex post* a mechanismu prosazování jako produkty, jejichž součást tvoří. Klíčovým rozdílem je, že mechanismy posuzování shody *ex ante* a *ex post* zajistí dodržování nejen požadavků stanovených odvětvovými právními předpisy, ale také požadavků stanovených tímto nařízením.

Pokud jde o samostatné vysoce rizikové systémy UI uvedené v příloze III, bude zaveden nový systém dodržování a prosazování právních předpisů. Tento postup se řídí vzorem právních předpisů nového legislativního rámce prováděným na základě vnitřní kontroly zajišťované poskytovateli s výjimkou systémů biometrické identifikace na dálku, na které by se vztahovalo posuzování shody třetími stranami. Komplexní posuzování shody *ex ante* prostřednictvím interních kontrol v kombinaci s účinným prosazováním *ex post* by mohlo být vzhledem k rané fázi regulačního zásahu a skutečnosti, že odvětví UI je velmi inovativní a odborné znalosti v oblasti auditu jsou získávány teprve nyní, pro tyto systémy účinným a rozumným řešením. Posuzování „samostatných“ vysoce rizikových systémů UI na základě interních kontrol by vyžadovalo úplné, účinné a řádně zdokumentované posouzení shody všech požadavků nařízení *ex ante*, posouzení shody spolehlivých systémů řízení kvality a rizik a monitorování po uvedení na trh. Poté, co poskytovatel provede příslušné posouzení shody, měl by tyto samostatné vysoce rizikové systémy UI zaregistrovat do databáze EU, kterou bude spravovat Komise s cílem zvýšit transparentnost a veřejný dohled a posílit dohled příslušných orgánů *ex post*. Naproti tomu posuzování shody systémů UI, které jsou bezpečnostními součástmi produktů, se bude z důvodu souladu s platnými právními předpisy o bezpečnosti výrobků řídit systémem založeným na postupech posuzování shody třetími stranami, které jsou již stanoveny v příslušných odvětvových právních předpisech upravujících bezpečnost výrobků. V případě podstatných změn systémů UI (zejména změn,

[29] Odborná skupina na vysoké úrovni pro umělou inteligenci, *Etické pokyny pro zajištění důvěryhodnosti UI*, 2019.

[30] Komise je podpořila rovněž ve svém sdělení z roku 2019 o přístupu k UI zaměřeném na člověka.

které přesahují rámec toho, co poskytovatel předem stanovil ve své technické dokumentaci a co bylo předmětem kontroly v okamžiku posuzování shody *ex ante*) bude zapotřebí provést nové opětovné posouzení shody *ex ante*.

5.2.4. POVINNOSTI TRANSPARENTNOSTI URČITÝCH SYSTÉMŮ UI (HLAVA IV)

Hlava IV se týká určitých systémů UI s cílem zohlednit specifická rizika manipulace, která představují. Povinnosti transparentnosti se budou vztahovat na systémy, které i) komunikují s lidmi; ii) se používají k detekci emocí nebo k určování spojení se (sociálními) kategoriemi na základě biometrických údajů nebo iii) generují obsah nebo s ním manipulují (tzv. deep fakes). Pokud osoby komunikují se systémem UI, případně jsou-li jejich emoce nebo vlastnosti rozpoznávány automatizovanými prostředky, musí být o této skutečnosti informovány. Pokud je systém UI používán k vytváření obrazového, zvukového nebo video obsahu, který se výrazně podobá obsahu autentickému, případně k manipulaci s ním, měla by existovat povinnost zveřejnit, že tento obsah je generován automatizovanými prostředky, kromě výjimek pro legitimní účely (prosazování práva, svoboda projevu). To umožňuje osobám činit informovaná rozhodnutí nebo se dané situace nezúčastnit.

5.2.5. OPATŘENÍ NA PODPORU INOVACÍ (HLAVA V)

Hlava V přispívá k cíli vytvoření právního rámce, který je vstřícný k inovacím, použitelný i v budoucnosti a odolný vůči narušení. Za tímto účelem vybízí příslušné vnitrostátní orgány k vytváření regulačních pískovišť a stanoví základní rámec v oblasti správy, dohledu a odpovědnosti. Regulační pískoviště UI vytvářejí kontrolované prostředí pro testování inovativních technologií po omezenou dobu na základě testovacího plánu dohodnutého s příslušnými orgány. Hlava V obsahuje rovněž opatření ke snížení regulační zátěže pro malé a střední podniky a začínající podniky.

5.2.6. SPRÁVA A PROVÁDĚNÍ (HLAVA VI, VII A VII)

Hlava VI zřizuje správní systémy na úrovni Unie a na úrovni jednotlivých států. Na úrovni Unie návrh zřizuje Evropskou radu pro umělou inteligenci (dále jen „rada“) složenou ze zástupců členských států a Komise. Tato rada usnadní plynulé, účinné a harmonizované provádění tohoto nařízení tím, že přispěje k účinné spolupráci vnitrostátních dozorových úřadů a Komise a bude Komisi poskytovat rady a odborné znalosti. Bude rovněž v rámci členských států shromažďovat a sdílet osvědčené postupy.

Na vnitrostátní úrovni budou členské státy povinny pro účely dohledu nad uplatňováním a prováděním nařízení určit jeden nebo více příslušných vnitrostátních orgánů, k nimž bude patřit i vnitrostátní dozorový orgán. Jako orgán příslušný k dohledu nad orgány, institucemi a jinými subjekty Unie, které spadají do oblasti působnosti tohoto nařízení, bude působit evropský inspektor ochrany údajů.

Hlava VII si klade za cíl usnadnit monitorovací práci Komise a vnitrostátních orgánů vytvořením celoevropské databáze samostatných vysoce rizikových systémů UI, které mají dopady především na základní práva. Tuto databázi bude provozovat Komise a údaje do ní budou dodávat poskytovatelé systémů UI, kteří budou povinni registrovat své systémy dříve, než je uvedou na trh nebo jinak uvedou do provozu.

Hlava VIII stanoví povinnosti poskytovatelů systémů UI v oblasti monitorování a oznamování, pokud jde o monitorování a oznamování po uvedení na trh a oznamování vyšetřování nežádoucích příhod a chybného fungování v souvislosti s umělou inteligencí. Úkolem orgánů dozoru nad trhem je rovněž kontrolovat trh a vyšetřovat soulad všech vysoce rizikových systémů UI, které již byly uvedeny na trh, s povinnostmi a požadavky. Orgány dozoru nad trhem mají mít veškeré pravomoci podle nařízení (EU) 2019/1020 o dozoru nad trhem. Uplatňování standardů *ex post* by mělo zajistit, že jakmile bude systém UI uveden na

trh, budou mít orgány veřejné moci k dispozici dostatečné pravomoci a zdroje umožňující zasáhnout v případě, že systémy UI způsobí neočekávaná rizika, což je zárukou rychlé reakce. Budou rovněž monitorovat dodržování příslušných povinností provozovatelů v souladu s tímto nařízením. Návrh nepředpokládá automatické vytváření dalších subjektů nebo orgánů na úrovni členských států. Členské státy proto mohou jmenovat stávající odvětvové orgány (a využívat jejich odborných znalostí) a svěřit jim rovněž pravomoci monitorovat a vymáhat ustanovení tohoto nařízení.

Ničím z toho není dotčen stávající systém a rozdělení pravomocí v členských státech při prosazování povinností v oblasti základních práv *ex post*. Pokud je to pro jejich pověření nezbytné, budou mít stávající orgány dozoru a donucovací orgány také pravomoc vyžádat si jakoukoli dokumentaci vedenou podle tohoto nařízení a mít k ní přístup, a v případě potřeby požádat orgány dozoru nad trhem, aby za pomoci technických prostředků zorganizovaly testování vysoce rizikového systému UI.

5.2.7. KODEXY CHOVÁNÍ (HLAVA IX)

Hlava IX vytváří rámec pro vypracování kodexů chování, jejichž cílem je povzbudit poskytovatele systémů UI, které nejsou vysoce rizikové, k dobrovolnému uplatňování povinných požadavků na vysoce rizikové systémy UI (stanovených v hlavě III). Poskytovatelé systémů UI, které nejsou vysoce rizikové, si mohou kodexy chování sami vytvořit a zavést. Tyto kodexy mohou zahrnovat rovněž dobrovolné závazky týkající se například udržitelnosti životního prostředí, přístupnosti pro osoby se zdravotním postižením, účasti zúčastněných stran na navrhování a vývoji systémů UI a rozmanitosti vývojových týmů.

5.2.8. ZÁVĚREČNÁ USTANOVENÍ (HLAVA X, XI A XII)

Hlava X zdůrazňuje povinnost všech stran respektovat důvěrný charakter informací a údajů a stanoví pravidla pro výměnu informací získaných při provádění tohoto nařízení. Hlava X rovněž zahrnuje opatření, jejichž cílem je zajistit účinné provádění tohoto nařízení prostřednictvím účinných, přiměřených a odrazujících sankcí za porušení příslušných ustanovení.

Hlava XI stanoví pravidla pro způsob přenesení pravomocí a jejich provádění. Návrh zmocňuje Komisi, aby případně přijímala prováděcí akty s cílem zajistit jednotné uplatňování tohoto nařízení nebo aktů v přenesené pravomoci za účelem aktualizace nebo doplnění seznamů uvedených v přílohách I až VII.

Hlava XII obsahuje povinnost Komise pravidelně posuzovat potřebu aktualizace přílohy III a vypracovávat pravidelné zprávy o hodnocení a přezkumu tohoto nařízení. Stanoví rovněž závěrečná ustanovení, včetně diferencovaného přechodného období, pro počáteční datum použitelnosti nařízení s cílem usnadnit bezproblémové provádění pro všechny dotčené strany.

2021/0106 (COD)

Návrh

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY,

KTERÝM SE STANOVÍ HARMONIZOVANÁ PRAVIDLA PRO UMĚLOU INTELIGENCI (AKT O UMĚLÉ INTELIGENCI) A MĚNÍ URČITÉ LEGISLATIVNÍ AKTY UNIE

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na články 16 a 114 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru[31],

s ohledem na stanovisko Výboru regionů[32],

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) Účelem tohoto nařízení je zlepšit fungování vnitřního trhu stanovením jednotného právního rámce zejména pro vývoj umělé inteligence, její uvádění na trh a využívání v souladu s hodnotami Unie. Toto nařízení sleduje řadu naléhavých důvodů veřejného zájmu, jako je například vysoká úroveň ochrany zdraví, bezpečnosti a základních práv, a zajišťuje volný pohyb zboží a služeb založených na UI přes hranice, čímž brání členským státům ukládat omezení vývoje, uvádění na trh a používání systémů UI, pokud to není tímto nařízením výslovně povoleno.

(2) Systémy umělé inteligence (systémy UI) lze snadno uplatnit v řadě hospodářských a společenských odvětví, včetně přeshraničních, a mohou obíhat v celé Unii. Některé členské státy již zkoumají možnost přijetí vnitrostátních pravidel, která by zajišťovala, že umělá inteligence bude bezpečná a že bude vyvíjena a používána v souladu s povinnostmi v oblasti základních práv. Rozdílné vnitrostátní předpisy mohou vést k roztříštěnosti vnitřního trhu a ke snížení právní jistoty pro provozovatele, kteří systémy UI vyvíjejí nebo používají. Proto je třeba zajistit jednotnou a vysokou úroveň ochrany v celé Unii a zároveň zabránit rozdílům, které jsou překážkou volného oběhu systémů UI a souvisejících produktů a služeb na vnitřním trhu, tím, že budou stanoveny jednotné povinnosti provozovatelů a bude zaručena jednotná ochrana naléhavých důvodů obecného zájmu a práv osob na celém vnitřním trhu na základě článku 114 Smlouvy o fungování Evropské unie (SFEU). V rozsahu, v němž toto nařízení obsahuje zvláštní pravidla ochrany fyzických osob v souvislosti se zpracováním osobních údajů, která se týkají omezení používání systémů UI pro biometrickou identifikaci na dálku v „reálném čase“ na veřejně přístupných místech

[31] Úř. věst. C […], […], s. […].
[32] Úř. věst. C […], […], s. […].

pro účely prosazování práva, je vhodné, aby se ve vztahu k těmto zvláštním pravidlům zakládalo na článku 16 SFEU. S ohledem na tato zvláštní pravidla a na použití článku 16 SFEU je vhodné provést konzultace s Evropským sborem pro ochranu osobních údajů.

(3) Umělá inteligence je rychle se vyvíjející skupina technologií, které mohou přispět k široké škále hospodářských a společenských přínosů v celém spektru průmyslových odvětví a sociálních aktivit. Díky zlepšení predikcí, optimalizaci provozu a přidělování zdrojů a personalizaci digitálních řešení dostupných pro jednotlivce a organizace může využívání umělé inteligence poskytnout společnostem klíčové konkurenční výhody a podpořit sociálně a environmentálně prospěšné výsledky, například v oblasti zdravotnictví, zemědělství, vzdělávání a odborné přípravy, správy infrastruktury, energetiky, dopravy a logistiky, veřejných služeb, bezpečnosti, spravedlnosti, účinného využívání zdrojů a energetické účinnosti a zmírňování změny klimatu a přizpůsobování se této změně.

(4) Umělá inteligence může zároveň v závislosti na okolnostech týkajících se jejího konkrétního uplatňování a využívání vytvářet rizika a působit újmu veřejným zájmům a právům, které jsou chráněny právem Unie. Tato újma může být hmotná nebo nehmotná.

(5) Je proto nezbytné zavést právní rámec Unie, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci, s cílem podpořit vývoj, využívání a zavádění umělé inteligence na vnitřním trhu, který by zároveň splňoval vysokou úroveň ochrany veřejných zájmů, jako je například zdraví, bezpečnost a ochrana základních práv, která jsou uznávána a chráněna právem Unie. K dosažení tohoto cíle by měla být stanovena pravidla, která budou regulovat uvádění určitých systémů UI na trh a do provozu a tím zajišťovat bezproblémové fungování vnitřního trhu a umožňovat, aby tyto systémy měly prospěch ze zásady volného pohybu zboží a služeb. Stanovením těchto pravidel toto nařízení podporuje cíl Unie zastávat v celosvětovém kontextu čelnou pozici, pokud jde o rozvoj bezpečné, důvěryhodné a etické umělé inteligence, který vytyčila Evropská rada[33], a zajišťuje ochranu etických zásad, kterou výslovně požadoval Evropský parlament[34].

(6) Je třeba jednoznačně definovat pojem „systém UI“ s cílem zajistit právní jistotu a zároveň poskytnout flexibilitu umožňující přizpůsobit se budoucímu technologickému vývoji. Tato definice by měla být založena na klíčových funkčních vlastnostech tohoto softwaru, zejména na jeho schopnosti generovat pro danou sadu člověkem definovaných cílů výstupy, jako je například obsah, predikce, doporučení nebo rozhodnutí, které ovlivňují prostředí, s nímž systém komunikuje, ať už ve fyzické, nebo digitální dimenzi. Systémy UI mohou být navrženy tak, aby fungovaly s různou úrovní samostatnosti a aby mohly být použity buď samostatně, nebo jako součást určitého produktu bez ohledu na to, zda je systém do tohoto produktu fyzicky zabudován (vestavěný systém), nebo zda napomáhá funkčnosti tohoto produktu, aniž by do něho byl zabudován (nevestavěný systém). Definici systému UI by měl doplňovat seznam konkrétních technik a přístupů využívaných při jeho vývoji, který by měl být průběžně aktualizován s ohledem na vývoj trhu a technologií

[33] Evropská rada, mimořádné zasedání Evropské rady (1. a 2. října 2020) – závěry, EUCO 13/20, 2020, s. 6.

[34] Usnesení Evropského parlamentu ze dne 20. října 2020 obsahující doporučení Komisi k rámci pro etické aspekty umělé inteligence, robotiky a souvisejících technologií, 2020/2012(INL).

prostřednictvím přijímání aktů v přenesené pravomoci Komisí za účelem změny uvedeného seznamu.

(7) Pojem „biometrické údaje“ používaný v tomto nařízení je v souladu s pojmem „biometrické údaje“ definovaným v čl. 4 bodě 14 nařízení Evropského parlamentu a Rady (EU) 2016/679[35], v čl. 3 bodě 18 nařízení Evropského parlamentu a Rady (EU) 2018/1725[36] a v čl. 3 bodě 13 směrnice Evropského parlamentu a Rady (EU) 2016/680[37] a měl by být vykládán konzistentně s nimi.

(8) Pojem „systém biometrické identifikace na dálku“ používaný v tomto nařízení by měl být definován funkčně jako systém UI určený k identifikaci fyzických osob na dálku prostřednictvím porovnání biometrických údajů dané osoby s biometrickými údaji obsaženými v referenční databázi a bez předchozích znalostí, zda bude cílová osoba přítomna a zda ji bude možné identifikovat, bez ohledu na konkrétní technologii, procesy nebo typy použitých biometrických údajů. Vzhledem k jejich různým vlastnostem a způsobům, jimiž jsou používány, jakož i různým souvisejícím rizikům, je třeba rozlišovat mezi systémy biometrické identifikace na dálku, která probíhá „v reálném čase“ a „zpětně“. V případě systémů provádějících identifikaci „v reálném čase“ probíhá jak zaznamenání biometrických údajů, tak porovnání a identifikace okamžitě, téměř okamžitě nebo v každém případě bez významného zpoždění. V tomto ohledu by neměl existovat žádný prostor pro obcházení pravidel tohoto nařízení o používání dotčených systémů UI „v reálném čase“ stanovením menších zpoždění. Systémy fungující „v reálném čase“ zahrnují použití materiálu „živě“ nebo jen „s malým časovým posunem“ jako jsou například videozáznamy generované kamerou nebo jiným zařízením s podobnými funkcemi. Naproti tomu v případě systémů, ve kterých identifikace probíhá „zpětně,“ dochází k porovnání a identifikaci zachycených údajů až se značným zpožděním. Jedná se o materiály, jako jsou například fotografie nebo videozáznamy generované kamerami s uzavřeným televizním okruhem nebo soukromými zařízeními, které byly vytvořeny před použitím tohoto systému ve vztahu k dotčeným fyzickým osobám.

(9) Pro účely tohoto nařízení by se pod pojmem „veřejně přístupné místo“ mělo rozumět jakékoli fyzické místo, které je přístupné veřejnosti, bez ohledu na to, zda je dané místo v soukromém nebo veřejném vlastnictví. Tento pojem proto nezahrnuje místa, která jsou soukromé povahy a obvykle nejsou volně přístupná třetím stranám, včetně donucovacích orgánů, pokud k tomu tyto strany nebyly výslovně vyzvány nebo oprávněny, jako jsou například domácnosti, soukromé kluby, kanceláře, sklady a továrny. Tento pojem nezahrnuje ani on-line prostory, protože se nejedná o prostory fyzické. Pouhá skutečnost, že pro přístup do konkrétního prostoru může být nezbytné splnění určitých podmínek, jako jsou například vstupenky nebo věková omezení, však

---

35 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

36 Nařízení Evropského parlamentu a Rady (EU) 2018/1725 ze dne 23. října 2018 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES (Úř. věst. L 295, 21.11.2018, s. 39).

37 Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV (směrnice o prosazování práva) (Úř. věst. L 119, 4.5.2016, s. 89).

neznamená, že daný prostor není veřejně přístupný ve smyslu tohoto nařízení. V důsledku toho jsou kromě veřejných prostor, jako jsou ulice, příslušné části státních budov a většina dopravní infrastruktury, zpravidla veřejně přístupné také prostory jako kina, divadla, obchody a nákupní centra. To, zda je daný prostor přístupný veřejnosti, by však mělo být určováno případ od případu s ohledem na zvláštnosti dané konkrétní situace.

(10) V zájmu zajištění rovných podmínek a účinné ochrany práv a svobod jednotlivců v celé Unii by se pravidla stanovená tímto nařízením měla vztahovat na poskytovatele systémů UI nediskriminačním způsobem bez ohledu na to, zda jsou usazeni v Unii nebo ve třetí zemi, a na uživatele systémů UI usazené v Unii.

(11) Do oblasti působnosti tohoto nařízení by měly spadat i určité systémy UI s ohledem na svou digitální povahu, i když nejsou uvedeny ani na trh, ani do provozu, ani nejsou používány v Unii. Jedná se například o provozovatele usazeného v Unii, který smluvně zadává určité služby provozovateli usazenému mimo Unii v souvislosti s činností, kterou má provádět systém UI, jejž by bylo možno označit jako vysoce rizikový a jehož účinky mají dopad na fyzické osoby nacházející se v Unii. Za těchto okolností by systém UI používaný provozovatelem mimo Unii mohl zpracovávat údaje zákonně shromážděné v Unii a převáděné z Unie a poskytovat zadávajícímu provozovateli v Unii výstup z tohoto systému UI vyplývající z tohoto zpracování, aniž by byl tento systém UI uveden na trh nebo do provozu v Unii nebo v ní byl používán. Aby se předešlo obcházení tohoto nařízení a aby byla zajištěna účinná ochrana fyzických osob nacházejících se v Unii, mělo by se toto nařízení vztahovat také na poskytovatele a uživatele systémů UI, kteří jsou usazeni ve třetí zemi, v rozsahu, v jakém jsou výstupy vytvořené těmito systémy používány v Unii. S ohledem na již existující ujednání a na zvláštní potřeby spolupráce se zahraničními partnery, s nimiž probíhá výměna informací a důkazů, by se však toto nařízení nemělo vztahovat na veřejné orgány třetí země a na mezinárodní organizace, pokud jednají v rámci mezinárodních dohod týkajících se prosazování práva a justiční spolupráce s Unií nebo s jejími členskými státy, uzavřených na vnitrostátní nebo evropské úrovni. Tyto dohody byly uzavřeny dvoustranně mezi členskými státy a třetími zeměmi nebo mezi Evropskou unií, Europolem a dalšími agenturami EU a třetími zeměmi a mezinárodními organizacemi.

(12) Toto nařízení by se mělo vztahovat také na instituce, úřady, orgány a agentury Unie, pokud jednají jako poskytovatel nebo uživatel systému UI. Systémy UI vyvinuté nebo používané výhradně pro vojenské účely by měly být z oblasti působnosti tohoto nařízení vyloučeny, pokud toto použití spadá do výlučné působnosti společné zahraniční a bezpečnostní politiky upravené v hlavě V Smlouvy o EU (SEU). Tímto nařízením by neměla být dotčena ustanovení týkající se odpovědnosti poskytovatelů zprostředkovatelských služeb stanovená ve směrnici Evropského parlamentu a Rady 2000/31/ES [ve znění aktu o digitálních službách].

(13) V zájmu zajištění jednotné a vysoké úrovně ochrany veřejných zájmů, pokud jde o zdraví, bezpečnost a základní práva, by měly být pro všechny vysoce rizikové systémy UI stanoveny společné normativní standardy. Tyto standardy by měly být v souladu s Listinou základních práv Evropské unie (dále jen „Listina“) a se závazky Unie v oblasti mezinárodního obchodu a měly by být nediskriminační.

(14) Aby bylo možné zavést přiměřený a účinný soubor závazných pravidel pro systémy UI, měl by být dodržován jasně definovaný přístup založený na posouzení rizik. Tento přístup by měl přizpůsobit typ a obsah těchto pravidel intenzitě a rozsahu rizik, která

mohou systémy UI vytvářet. Je proto nezbytné zakázat některé postupy v oblasti UI a stanovit požadavky na vysoce rizikové systémy UI a povinnosti příslušných provozovatelů, jakož i povinnosti transparentnosti pro určité systémy UI.

(15) Na jedné straně přináší využívání umělé inteligence celou řadu výhod, avšak tuto technologii lze používat i nesprávně a může se stát zdrojem nových a výkonných nástrojů umožňujících manipulativní a vykořisťovatelské praktiky a praktiky v oblasti sociální kontroly. Tyto praktiky jsou mimořádně škodlivé a měly by být zakázány, protože jsou v rozporu s hodnotami Unie v oblasti úcty k lidské důstojnosti, svobody, rovnosti, demokracie a právního státu a se základními právy Unie, včetně práva na zákaz diskriminace, na ochranu údajů a soukromí a práva dítěte.

(16) Mělo by být zakázáno uvádění na trh, uvádění do provozu nebo využívání určitých systémů UI určených k ovlivňování lidského chování, které by mohly způsobit fyzickou nebo psychickou újmu. Tyto systémy UI využívají součásti uplatňující podprahové techniky, které jednotlivci nejsou schopni vnímat, případně zneužívají zranitelnosti dětí a jiných osob v důsledku jejich věku nebo fyzické nebo mentální nezpůsobilosti. Činí tak s úmyslem podstatně ovlivnit chování určité osoby, a to takovým způsobem, který této nebo jiné osobě působí nebo by mohl způsobit újmu. Tento záměr nelze předpokládat, pokud je lidské chování ovlivněno v důsledku faktorů nesouvisejících se systémem UI, které jsou mimo kontrolu poskytovatele nebo uživatele. Uvedený zákaz by neměl bránit výzkumu těchto systémů UI pro legitimní účely, pokud se dotčený výzkum nezaměřuje na využívání systému UI ve vztazích člověk-stroj, které vystavuje fyzické osoby újmě, a pokud je prováděn v souladu s uznávanými etickými standardy vědeckého výzkumu.

(17) Systémy UI provádějící hodnocení sociálního kreditu fyzických osob pro obecné účely ze strany veřejných orgánů nebo jejich jménem mohou vést k diskriminačním výsledkům a k vyloučení určitých skupin. Mohou porušovat právo na důstojnost a zákaz diskriminace a hodnoty rovnosti a spravedlnosti. Tyto systémy UI hodnotí nebo klasifikují důvěryhodnost fyzických osob na základě jejich sociálního chování v různých kontextech nebo známých či předvídaných osobních či osobnostních vlastností. Sociální kredit získaný na základě těchto systémů UI může vést ke znevýhodňujícímu nebo nepříznivému zacházení s fyzickými osobami nebo s celými skupinami těchto osob v sociálních kontextech nesouvisejících s kontextem, ve kterém byly dané údaje původně vytvořeny nebo shromážděny, případně ke znevýhodňujícímu zacházení, které je nepřiměřené nebo neodůvodněné s ohledem na závažnost jejich sociálního chování. Tyto systémy UI by proto měly být zakázány.

(18) Využívání systémů UI pro biometrickou identifikaci fyzických osob na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva je považováno za zvláště rušivý zásah do práv a svobod dotčených osob, neboť může ovlivnit soukromý život velké části populace, vyvolávat pocit neustálého sledování a nepřímo odrazovat od využívání svobody shromažďování a dalších základních práv. Bezprostřednost dopadu a omezené možnosti dalších kontrol nebo oprav v souvislosti s používáním těchto systémů fungujících „v reálném čase“ s sebou navíc nesou zvýšené riziko z hlediska práv a svobod osob, kterých se týkají činnosti v oblasti prosazování práva.

(19) Používání těchto systémů pro účely prosazování práva by proto mělo být zakázáno s výjimkou tří taxativně vyjmenovaných a úzce definovaných situací, kdy je toto použití nezbytně nutné k dosažení významného veřejného zájmu, jehož význam převažuje nad uvedenými riziky. Tyto situace zahrnují hledání potenciálních obětí

trestných činů, včetně pohřešovaných dětí; některé případy ohrožení života nebo fyzické bezpečnosti fyzických osob nebo hrozby teroristického útoku a odhalování, lokalizaci, identifikaci nebo stíhání pachatelů nebo osob podezřelých z trestných činů uvedených v rámcovém rozhodnutí Rady 2002/584/SVV[38], pokud lze tyto trestné činy v dotčeném členském státě potrestat trestem odnětí svobody nebo ochranným opatřením spojeným s odnětím osobní svobody s horní hranicí sazby v délce nejméně tři roky a jsou-li vymezeny právem tohoto členského státu. Tato hranice pro trest odnětí svobody nebo ochranné opatření spojené s odnětím osobní svobody v souladu s vnitrostátními právními předpisy přispívá k zajištění toho, že použití systémů biometrické identifikace na dálku „v reálném čase“ bude možno potenciálně odůvodnit jen dostatečnou závažností daného trestného činu. Je navíc pravděpodobné, že některé z 32 trestných činů uvedených v rámcovém rozhodnutí Rady 2002/584/SVV budou v praxi relevantnější než jiné v tom smyslu, že nezbytnost a přiměřenost využívání biometrické identifikace na dálku „v reálném čase“ bude pravděpodobně velmi různorodá jak z hlediska praktické snahy o odhalování, lokalizaci, identifikaci nebo stíhání pachatelů jednotlivých uvedených trestných činů nebo osob podezřelých z jejich spáchání, tak s ohledem na pravděpodobné rozdíly v závažnosti, pravděpodobnosti a rozsahu způsobené újmy nebo možných negativních důsledků.

(20) Aby bylo zajištěno odpovědné a přiměřené používání těchto systémů, je rovněž důležité stanovit, že v každé z těchto tří taxativně vyjmenovaných a úzce definovaných situací je třeba zohlednit určité prvky, zejména pokud jde o povahu situace, která vedla k předložení žádosti, o důsledky užití těchto systémů pro práva a svobody všech dotčených osob a o záruky a podmínky zajištěné při tomto použití. Na využívání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva by se navíc měla vztahovat vhodná časová a prostorová omezení, zejména s ohledem na důkazy nebo náznaky týkající se daných hrozeb, obětí nebo pachatele. Pro každý případ použití v každé ze tří výše uvedených situací by mělo být vhodné využití referenční databáze osob.

(21) Každé použití systému biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva by mělo podléhat výslovnému a konkrétnímu povolení justičního orgánu nebo nezávislého správního orgánu členského státu. Toto povolení by mělo být v zásadě získáno před tímto použitím s výjimkou řádně odůvodněných naléhavých situací, tj. situací, kdy je potřeba použít dotyčné systémy tak naléhavá, že je účinně a objektivně nemožné získat povolení před zahájením tohoto použití. V těchto naléhavých situacích by použití mělo být omezeno na absolutně nezbytné minimum a mělo by podléhat příslušným zárukám a podmínkám, které stanoví vnitrostátní právo a specifikuje samotný donucovací orgán v kontextu každého jednotlivého případu naléhavého použití. Donucovací orgán by měl v těchto situacích rovněž usilovat o co nejvčasnější získání povolení a měl by uvést důvody, proč o něj nemohl požádat již dříve.

(22) Dále je vhodné v rámci taxativně vymezeném tímto nařízením stanovit, že toto použití na území členského státu v souladu s tímto nařízením by mělo být možné pouze tehdy a do té míry, do níž se dotčený členský stát rozhodl výslovně stanovit možnost povolit toto použití ve své podrobné vnitrostátní úpravě. V důsledku toho se členské státy mohou podle tohoto nařízení i nadále dle vlastního uvážení rozhodnout, že tuto

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

možnost vůbec nestanoví, případně že ji stanoví pouze ve vztahu k některým cílům, které mohou povolené použití určené v tomto nařízení odůvodnit.

(23) Využívání systémů UI pro biometrickou identifikaci fyzických osob na dálku „v reálném“ čase na veřejně přístupných místech pro účely prosazování práva nutně zahrnuje i zpracování biometrických údajů. Pravidla tohoto nařízení, která toto použití až na určité výjimky zakazují a která jsou založena na článku 16 SFEU, by se měla použít jako *lex specialis*, pokud jde o pravidla zpracování biometrických údajů uvedená v článku 10 směrnice (EU) 2016/680, což by toto použití a zpracování biometrických údajů vyčerpávajícím způsobem regulovalo. Toto použití a zpracování by proto mělo být možné jen v případě, že bude slučitelné s rámcem stanoveným tímto nařízením, a mimo tento rámec by neměl existovat prostor pro to, aby příslušné orgány jednající za účelem prosazování práva používaly tyto systémy a zpracovávaly tyto údaje v souvislosti s nimi z důvodů uvedených v článku 10 směrnice (EU) 2016/680. V této souvislosti není cílem tohoto nařízení poskytnout právní základ zpracování osobních údajů podle článku 8 směrnice 2016/680. Na používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro jiné účely než prosazování práva, a to i příslušnými orgány, by se však neměl vztahovat zvláštní rámec týkající se tohoto použití pro účely prosazování práva, stanovený tímto nařízením. Toto použití pro jiné účely než pro účely prosazování práva by proto nemělo podléhat požadavku na povolení podle tohoto nařízení a použitelným podrobným pravidlům vnitrostátního práva, která ho případně mohou uvést v účinnost.

(24) Jakékoli zpracování biometrických údajů a dalších osobních údajů související s používáním systémů UI pro účely biometrické identifikace jinak než v souvislosti s používáním systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva podle tohoto nařízení, včetně případů, kdy tyto systémy používají příslušné orgány na veřejně přístupných místech pro jiné účely než pro účely prosazování práva, by mělo i nadále splňovat všechny případné požadavky vyplývající z čl. 9 odst. 1 nařízení (EU) 2016/679, z čl. 10 odst. 1 nařízení (EU) 2018/1725 a z článku 10 směrnice (EU) 2016/680.

(25) V souladu s článkem 6a Protokolu č. 21 o postavení Spojeného království a Irska s ohledem na prostor svobody, bezpečnosti a práva, připojeného ke Smlouvě o EU a Smlouvě o fungování EU, není Irsko vázáno pravidly stanovenými v čl. 5 odst. 1 písm. d) a čl. 5 odst. 2 a 3 tohoto nařízení přijatého na základě článku 16 Smlouvy o fungování EU, která se týkají zpracování osobních údajů členskými státy, vykonávají-li činnosti spadající do oblasti působnosti části třetí hlavy V kapitoly 4 nebo 5 Smlouvy o fungování EU, pokud není Irsko vázáno pravidly Unie upravujícími formy justiční spolupráce v trestních věcech nebo policejní spolupráce, v jejichž rámci musí být dodržována pravidla přijatá na základě článku 16 Smlouvy o fungování EU.

(26) V souladu s články 2 a 2a Protokolu č. 22 o postavení Dánska, připojeného ke Smlouvě o EU a Smlouvě o fungování EU, nejsou pro Dánsko závazná ani použitelná pravidla stanovená v čl. 5 odst. 1 písm. d) a v čl. 5 odst. 2 a 3 tohoto nařízení přijatého na základě článku 16 Smlouvy o fungování EU, která se týkají zpracování osobních údajů členskými státy, vykonávají-li činnosti spadající do oblasti působnosti části třetí hlavy V kapitoly 4 nebo 5 Smlouvy o fungování EU.

(27) Vysoce rizikové systémy UI by měly být uváděny na trh Unie nebo do provozu pouze tehdy, splňují-li určité závazné požadavky. Tyto požadavky by měly zajistit, aby vysoce rizikové systémy UI, které jsou dostupné v Unii nebo jejichž výstupy jsou v Unii jinak využívány, nepředstavovaly nepřijatelné riziko pro důležité veřejné zájmy

Unie uznané a chráněné právem Unie. Systémy UI označené jako vysoce rizikové by měly být omezeny na systémy, které mají významný škodlivý dopad na zdraví, bezpečnost a základní práva osob v Unii, a toto omezení minimalizuje jakékoli případné omezení mezinárodního obchodu.

(28) Systémy UI by mohly mít nepříznivé účinky na zdraví a bezpečnost osob, zejména pokud tyto systémy fungují jako součásti produktů. V souladu s cíli harmonizačních právních předpisů Unie, které mají usnadnit volný pohyb produktů na vnitřním trhu a zajistit, aby se na trh dostávaly pouze bezpečné a jinak vyhovující produkty, je důležitá náležitá prevence a zmírňování bezpečnostních rizik, která mohou případně vyplývat z produktu jako celku v důsledku jeho digitálních prvků, včetně systémů UI. Například stále autonomnější roboti, ať už v kontextu výroby, nebo osobní asistence a péče, by měli být schopni bezpečně fungovat a vykonávat své funkce ve složitých prostředích. Obdobně ve zdravotnictví, kde existuje obzvláště vysoké riziko v oblasti života a zdraví, by měly být stále sofistikovanější diagnostické systémy a systémy podporující lidská rozhodnutí spolehlivé a přesné. Míra nepříznivého dopadu systému UI na základní práva chráněná Listinou je obzvláště důležitá v případě, že je systém UI klasifikován jako vysoce rizikový. Tato práva zahrnují právo na lidskou důstojnost, respektování soukromého a rodinného života, ochranu osobních údajů, svobodu projevu a informací, svobodu shromažďování a sdružování a zákaz diskriminace, ochranu spotřebitele, práva pracovníků, práva osob s postižením, právo na účinnou právní ochranu a spravedlivý proces, právo na obhajobu a presumpci neviny a právo na řádnou správu. Kromě těchto práv je třeba zdůraznit zvláštní práva dětí zakotvená v článku 24 Listiny základních práv EU a v Úmluvě OSN o právech dítěte (ve vztahu k digitálním prostředí dále rozpracovaná v obecné připomínce č. 25 k Úmluvě o právech dítěte), které v obou případech vyžadují zohlednění zranitelnosti dětí a poskytnutí této ochrany a péče, která je nezbytná pro jejich blaho. Při posuzování závažnosti újmy, kterou může systém UI způsobit, a to i ve vztahu ke zdraví a bezpečnosti osob, by mělo být zohledněno také základní právo na vysokou úroveň ochrany životního prostředí zakotvené v Listině a provedené do politik Unie.

(29) Pokud jde o vysoce rizikové systémy UI, které jsou bezpečnostními součástmi produktů nebo systémů, případně které jsou samy produkty nebo systémy spadajícími do působnosti nařízení Evropského parlamentu a Rady (ES) č. 300/2008[39], nařízení Evropského parlamentu a Rady (EU) č. 167/2013[40], nařízení Evropského parlamentu a Rady (EU) č. 168/2013[41], směrnice Evropského parlamentu a Rady 2014/90/EU[42], směrnice Evropského parlamentu a Rady (EU) 2016/797[43], nařízení Evropského parlamentu a Rady (EU) 2018/858[44], nařízení Evropského parlamentu a Rady (EU)

---

39 Nařízení Evropského parlamentu a Rady (ES) č. 300/2008 ze dne 11. března 2008 o společných pravidlech v oblasti ochrany civilního letectví před protiprávními činy a o zrušení nařízení (ES) č. 2320/2002 (Úř. věst. L 97, 9.4.2008, s. 72).

40 Nařízení Evropského parlamentu a Rady (EU) č. 167/2013 ze dne 5. února 2013 o schvalování zemědělských a lesnických vozidel a dozoru nad trhem s těmito vozidly (Úř. věst. L 60, 2.3.2013, s. 1).

41 Nařízení Evropského parlamentu a Rady (EU) č. 168/2013 ze dne 15. ledna 2013 o schvalování dvoukolových nebo tříkolových vozidel a čtyřkolek a dozoru nad trhem s těmito vozidly (Úř. věst. L 60, 2.3.2013, s. 52).

42 Směrnice Evropského parlamentu a Rady 2014/90/EU ze dne 23. července 2014 o lodní výstroji a o zrušení směrnice Rady 96/98/ES (Úř. věst. L 257, 28.8.2014, s. 146).

43 Směrnice Evropského parlamentu a Rady (EU) 2016/797 ze dne 11. května 2016 o interoperabilitě železničního systému v Evropské unii (Úř. věst. L 138, 26.5.2016, s. 44).

44 Nařízení Evropského parlamentu a Rady (EU) 2018/858 ze dne 30. května 2018 o schvalování motorových vozidel a jejich přípojných vozidel, jakož i systémů, konstrukčních částí a samostatných

2018/1139[45] a nařízení Evropského parlamentu a Rady (EU) 2019/2144[46], je vhodné tyto akty pozměnit s cílem zajistit, aby Komise při přijímání jakýchkoli budoucích relevantních aktů v přenesené pravomoci nebo prováděcích aktů na základě výše uvedených aktů zohledňovala povinné požadavky na vysoce rizikové systémy UI stanovené v tomto nařízení na základě technických a regulačních specifik jednotlivých odvětví, aniž by zasahovala do stávajících mechanismů správy, posuzování shody a prosazování ani do orgánů zřízených v rámci uvedených aktů.

(30) Pokud jde o systémy UI, které jsou bezpečnostními součástmi produktů nebo jsou produkty samy o sobě, a které spadají do oblasti působnosti některých harmonizačních právních předpisů Unie, je vhodné je podle tohoto nařízení klasifikovat jako vysoce rizikové, pokud u daného produktu provádí postup posuzování shody subjekt, který vykonává činnosti posuzování shody jakožto třetí strana podle příslušných harmonizačních právních předpisů Unie. Těmito produkty jsou zejména strojní zařízení, hračky, výtahy, zařízení a ochranné systémy určené k použití v prostředí s nebezpečím výbuchu, rádiová zařízení, tlaková zařízení, zařízení pro rekreační plavidla, lanové dráhy, spotřebiče plynných paliv, zdravotnické prostředky a diagnostické zdravotnické prostředky *in vitro*.

(31) Klasifikace systému UI jako vysoce rizikového podle tohoto nařízení by neměla nutně znamenat, že produkt, jehož je daný systém UI bezpečnostní součástí, případně tento samotný systém UI jako produkt, je považován za „vysoce rizikový“ podle kritérií stanovených v příslušných harmonizačních právních předpisech Unie, které se na tento produkt vztahují. To platí zejména pro nařízení Evropského parlamentu a Rady (EU) 2017/745[47] a nařízení Evropského parlamentu a Rady (EU) 2017/746[48], kde je pro produkty se středním a vysokým rizikem vyžadováno posuzování shody subjektem, který vykonává činnosti posuzování shody jakožto třetí strana.

(32) Pokud jde o samostatné systémy UI, jimiž se rozumí vysoce rizikové systémy UI s výjimkou těch, které představují bezpečnostní součásti produktů nebo které jsou samy produkty, je vhodné je klasifikovat jako vysoce rizikové, pokud s ohledem na

---

technických celků určených pro tato vozidla a o dozoru nad trhem s nimi, o změně nařízení (ES) č. 715/2007 a č. 595/2009 a o zrušení směrnice 2007/46/ES (Úř. věst. L 151, 14.6.2018, s. 1).

[45] Nařízení Evropského parlamentu a Rady (EU) 2018/1139 ze dne 4. července 2018 o společných pravidlech v oblasti civilního letectví a o zřízení Agentury Evropské unie pro bezpečnost letectví, kterým se mění nařízení (ES) č. 2111/2005, (ES) č. 1008/2008, (EU) č. 996/2010, (EU) č. 376/2014 a směrnice Evropského parlamentu a Rady 2014/30/EU a 2014/53/EU a kterým se zrušuje nařízení Evropského parlamentu a Rady (ES) č. 552/2004 a (ES) č. 216/2008 a nařízení Rady (EHS) č. 3922/91 (Úř. věst. L 212, 22.8.2018, s. 1).

[46] Nařízení Evropského parlamentu a Rady (EU) 2019/2144 ze dne 27. listopadu 2019 o požadavcích pro schvalování typu motorových vozidel a jejich přípojných vozidel a systémů, konstrukčních částí a samostatných technických celků určených pro tato vozidla z hlediska obecné bezpečnosti a ochrany cestujících ve vozidle a zranitelných účastníků silničního provozu, o změně nařízení Evropského parlamentu a Rady (EU) 2018/858 a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 78/2009, (ES) č. 79/2009 a (ES) č. 661/2009 a nařízení Komise (ES) č. 631/2009, (EU) č. 406/2010, (EU) č. 672/2010, (EU) č. 1003/2010, (EU) č. 1005/2010, (EU) č. 1008/2010, (EU) č. 1009/2010, (EU) č. 19/2011, (EU) č. 109/2011, (EU) č. 458/2011, (EU) č. 65/2012, (EU) č. 130/2012, (EU) č. 347/2012, (EU) č. 351/2012, (EU) č. 1230/2012 a (EU) 2015/166 (Úř. věst. L 325, 16.12.2019, s. 1).

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

[48] Nařízení Evropského parlamentu a Rady (EU) 2017/746 ze dne 5. dubna 2017 o diagnostických zdravotnických prostředcích in vitro a o zrušení směrnice 98/79/ES a rozhodnutí Komise 2010/227/EU (Úř. věst. L 117, 5.5.2017, s. 176).

určený účel představují vysoké riziko újmy na zdraví a bezpečnosti nebo na základních právech osob s přihlédnutím jak k závažnosti možné újmy, tak k pravděpodobnosti, že nastane, a pokud jsou využívány v celé řadě oblastí uvedených v tomto nařízení, které jsou výslovně definovány předem. Identifikace těchto systémů je založena na stejné metodice a kritériích, jaké se předpokládají i u jakýchkoli budoucích změn seznamu vysoce rizikových systémů UI.

(33) Technické nepřesnosti systémů UI určených pro biometrickou identifikaci fyzických osob na dálku mohou vést ke zkresleným výsledkům a mít diskriminační účinky. To je relevantní zejména v případě věku, etnického původu, pohlaví nebo zdravotních postižení. Proto by měly být systémy biometrické identifikace na dálku „v reálném čase“ i „zpětně“ klasifikovány jako vysoce rizikové. S ohledem na rizika, která oba typy systémů biometrické identifikace na dálku představují, by se na ně měly vztahovat zvláštní požadavky v oblasti schopnosti zaznamenávání dat a lidského dohledu.

(34) Pokud jde o správu a provoz kritické infrastruktury, je vhodné klasifikovat jako vysoce rizikové takové systémy UI, které jsou určeny k použití jako bezpečnostní součásti při řízení a provozu silniční dopravy a při zásobování vodou, plynem, teplem a elektřinou, protože jejich porucha nebo chybné fungování může ohrozit život a zdraví osob ve velkém rozsahu a vést ke značnému narušení běžného provozování sociálních a hospodářských činností.

(35) Za vysoce rizikové by měly být považovány systémy UI používané ve vzdělávání nebo v odborné přípravě, zejména při určování přístupu osob do školských institucí a institucí odborného vzdělávání, jejich přidělování do těchto institucí nebo pro hodnocení osob v testech jako součásti nebo jako předpokladu jejich vzdělávání, protože mohou určovat vzdělávací a profesní průběh života lidí a tak ovlivňovat jejich schopnost zajišťovat si živobytí. Pokud budou tyto systémy navrženy a používány nesprávně, mohou porušovat právo na vzdělávání a odbornou přípravu i právo nebýt diskriminován a fixovat historické vzorce diskriminace.

(36) Jako vysoce rizikové mohou být klasifikovány systémy UI používané při zaměstnávání, řízení pracovníků a při přístupu k samostatné výdělečné činnosti, zejména při náboru a výběru osob, při rozhodování o povýšení nebo propuštění a při přidělování úkolů, monitorování nebo hodnocení osob ve smluvních pracovněprávních vztazích, protože mohou významně ovlivnit budoucí kariérní vyhlídky a živobytí těchto osob. Příslušné smluvní pracovněprávní vztahy by měly zahrnovat zaměstnance a osoby poskytující služby prostřednictvím platforem, jak je uvedeno v pracovním programu Komise na rok 2021. Tyto osoby by v zásadě neměly být považovány za uživatele ve smyslu tohoto nařízení. Tyto systémy mohou v průběhu celého procesu náboru a při hodnocení, povyšování nebo udržování osob ve smluvních pracovněprávních vztazích fixovat historické vzorce diskriminace, například vůči ženám, určitým věkovým skupinám, osobám se zdravotním postižením nebo osobám určitého rasového nebo etnického původu nebo sexuální orientace. Systémy UI používané k monitorování výkonnosti a chování těchto osob mohou ovlivnit rovněž jejich práva na ochranu údajů a soukromí.

(37) Další oblastí, ve které si používání systémů UI zaslouží zvláštní pozornost, je přístup k určitým základním soukromým a veřejným službám a výhodám nezbytným pro plné zapojení osob do společnosti nebo pro zlepšení jejich životní úrovně. Jako vysoce rizikové systémy UI by měly být klasifikovány zejména systémy UI používané k hodnocení rizika úvěrů nebo úvěruschopnosti fyzických osob, protože určují přístup

těchto osob k finančním zdrojům nebo k základním službám, jako je bydlení, elektřina a telekomunikační služby. Systémy UI používané k tomuto účelu mohou vést k diskriminaci osob nebo skupin a fixovat historické vzorce diskriminace, například na základě rasového nebo etnického původu, zdravotního postižení, věku a sexuální orientace, nebo vytvářet nové formy diskriminačních dopadů. Vzhledem k velmi omezenému rozsahu tohoto dopadu a dostupným alternativám na trhu je vhodné stanovit výjimku pro systémy UI užívané pro účely posouzení úvěruschopnosti a hodnocení rizika úvěrů, pokud je uvedou do provozu malí poskytovatelé pro svou vlastní potřebu. Fyzické osoby, které žádají o dávky sociálního zabezpečení a veřejné asistenční služby u orgánů veřejné správy, případně kterým jsou tyto dávky a služby poskytovány, jsou zpravidla na těchto dávkách a službách závislé a nacházejí se ve vztahu k odpovědným orgánům ve zranitelném postavení. Využívání systémů UI k určování toho, zda by tyto orgány měly tyto výhody a služby zamítnout, omezit, zrušit nebo žádat jejich navrácení, může mít významný dopad na živobytí daných osob a může porušovat jejich základní práva, jako je právo na sociální ochranu, na zákaz diskriminace, na lidskou důstojnost nebo na účinnou právní ochranu. Tyto systémy by proto měly být klasifikovány jako vysoce rizikové. Toto nařízení by však nemělo bránit rozvoji a využívání inovativních přístupů ve veřejné správě, pro kterou by mohlo být širší využívání vyhovujících a bezpečných systémů UI prospěšné, pokud tyto systémy nepředstavují vysoké riziko pro právnické a fyzické osoby. A konečně by měly být jako vysoce rizikové klasifikovány rovněž systémy UI používané při dispečinku pohotovostních služeb nebo stanovení priorit při tomto dispečinku, protože rozhodují v situacích, které jsou velmi kritické pro život a zdraví osob a jejich majetek.

(38) Opatření donucovacích orgánů zahrnující určitá použití systémů UI se vyznačují značným stupněm nerovnováhy sil a mohou vést ke sledování fyzické osoby, jejímu zatčení nebo zbavení svobody, jakož i k dalším nepříznivým dopadům na základní práva zaručená Listinou. Zejména v případě, že systém UI nebyl trénován na vysoce kvalitních datech, nesplňuje odpovídající požadavky na přesnost nebo spolehlivost nebo není před uvedením na trh nebo jiným uvedením do provozu řádně navržen a otestován, může dojít k vyčleňování osob diskriminačním nebo jinak nesprávným nebo nespravedlivým způsobem. Kromě toho by mohl být omezen výkon důležitých základních procesních práv, jako je právo na účinnou právní ochranu a na spravedlivý proces, jakož i právo na obhajobu a presumpce neviny, zejména pokud tyto systémy UI nejsou dostatečně transparentní, vysvětlitelné a zdokumentované. Je proto vhodné označit za vysoce rizikové celou řadu systémů UI určených k použití v kontextu prosazování práva, kde je přesnost, spolehlivost a transparentnost obzvláště důležitá, s cílem zabránit nepříznivým dopadům, zachovat důvěru veřejnosti a zajistit odpovědnost a účinné opravné prostředky. S ohledem na povahu dotčených činností a na rizika s nimi spojená by tyto vysoce rizikové systémy UI měly zahrnovat zejména systémy UI určené k využívání donucovacími orgány k individuálnímu hodnocení rizik, polygrafy a podobné nástroje, případně systémy užívané k detekci emočního stavu fyzických osob, k odhalování tzv. deep fakes, k vyhodnocování spolehlivosti důkazů v trestním řízení, k predikci výskytu nebo opakování skutečné nebo potenciální trestné činnosti na základě profilování fyzických osob nebo k posuzování osobnostních a povahových rysů nebo předchozí trestné činnosti fyzických osob nebo skupin, k profilování v průběhu odhalování, vyšetřování nebo stíhání trestných činů, jakož i k analýze trestné činnosti ve vztahu k fyzickým osobám. Systémy UI výslovně určené k použití daňovými a celními orgány při správním řízení by neměly být

považovány za vysoce rizikové systémy UI používané donucovacími orgány za účelem prevence, odhalování, vyšetřování a stíhání trestných činů.

(39) Systémy UI využívané pro účely migrace, azylu a řízení ochrany hranic ovlivňují osoby, které jsou často v obzvláště zranitelném postavení a jsou závislé na výsledku činnosti příslušných orgánů veřejné moci. Přesnost, nediskriminační povaha a transparentnost systémů UI používaných v těchto kontextech jsou proto obzvláště důležité pro zajištění dodržování základních práv dotčených osob, zejména jejich práva na volný pohyb, na zákaz diskriminace, na ochranu soukromého života a osobních údajů, na mezinárodní ochranu a na řádnou správu. Je proto vhodné označit jako vysoce rizikové ty systémy UI, které jsou určeny k použití příslušnými orgány veřejné moci pověřenými úkoly v oblasti migrace, azylu a řízení ochrany hranic, jako jsou například polygrafy a podobné nástroje, případně nástroje určené k detekci emočního stavu fyzické osoby; k posuzování určitých rizik, která představují fyzické osoby vstupující na území členského státu nebo žádající o vízum nebo azyl; k ověření pravosti příslušných dokladů fyzických osob; jako pomoc příslušným orgánům veřejné správy při posuzování žádostí o azyl, vízum a povolení k pobytu a souvisejících stížností, pokud jde o cíl, jímž je zjištění způsobilosti fyzických osob žádajících o určitý status. Systémy UI v oblasti migrace, azylu a řízení ochrany hranic, na které se vztahuje toto nařízení, by měly splňovat příslušné procesní požadavky stanovené směrnicí Evropského parlamentu a Rady 2013/32/EU[49], nařízením Evropského parlamentu a Rady (ES) č. 810/2009[50] a dalšími příslušnými právními předpisy.

(40) Určité systémy UI určené k výkonu spravedlnosti a demokratických procesů by měly být klasifikovány jako vysoce rizikové s ohledem na jejich potenciálně významný dopad na demokracii, právní stát a individuální svobody, jakož i na právo na účinnou právní ochranu a na spravedlivý proces. Jako vysoce rizikové je vhodné kvalifikovat systémy UI, jejichž cílem je poskytovat pomoc justičním orgánům při zkoumání a výkladu skutečností a práva a při uplatňování práva na konkrétní soubor skutečností, zejména z důvodu řešení rizik možného zkreslení, chyb a neprůhlednosti. Tato kvalifikace by se však neměla vztahovat na systémy UI určené pro čistě pomocné správní činnosti, které neovlivňují faktický výkon spravedlnosti v jednotlivých případech, jako je například anonymizace nebo pseudonymizace soudních rozhodnutí, dokumentů nebo údajů, komunikace mezi zaměstnanci, administrativní úkoly nebo přidělování zdrojů.

(41) Skutečnost, že daný systém UI je podle tohoto nařízení klasifikován jako vysoce rizikový, by neměla být vykládána v tom smyslu, že používání tohoto systému musí být nezbytně zákonné podle jiných aktů práva Unie nebo podle vnitrostátních právních předpisů slučitelných s právem Unie, které se týkají například ochrany osobních údajů, používání polygrafů a podobných nástrojů nebo jiných systémů ke zjišťování emočního stavu fyzických osob. K jakémukoli takovému využívání by mělo i nadále docházet pouze v souladu s příslušnými požadavky vyplývajícími z Listiny a z příslušných aktů sekundárního práva Unie a vnitrostátního práva. Toto nařízení by nemělo být chápáno tak, že poskytuje právní základ pro zpracování osobních údajů, případně včetně zvláštních kategorií osobních údajů.

---

[49] Směrnice Evropského parlamentu a Rady 2013/32/EU ze dne 26. června 2013 o společných řízeních pro přiznávání a odnímání statusu mezinárodní ochrany (Úř. věst. L 180, 29.6.2013, s. 60).

[50] Nařízení Evropského parlamentu a Rady (ES) č. 810/2009 ze dne 13. července 2009 o kodexu Společenství o vízech (vízový kodex) (Úř. věst. L 243, 15.9.2009, s. 1).

(42) Ke zmírnění rizik, která vyplývají uživatelům a dotčeným osobám z vysoce rizikových systémů UI uváděných na trh Unie nebo jinak uváděných do provozu na tomto trhu, by měly být uplatňovány určité povinné požadavky s přihlédnutím k určenému účelu používání tohoto systému a v souladu se systémem řízení rizik, který stanoví poskytovatel.

(43) Na vysoce rizikové systémy UI by se měly vztahovat požadavky týkající se kvality použitých souborů dat, technické dokumentace a uchovávání záznamů, transparentnosti a poskytování informací uživatelům, lidského dohledu a spolehlivosti, přesnosti a kybernetické bezpečnosti. Tyto požadavky jsou nezbytným předpokladem účinného zmírňování rizik pro zdraví, bezpečnost a základní práva v závislosti na určeném účelu tohoto systému; žádná další opatření méně omezující obchod nejsou rozumně dostupná, a tudíž nedochází k bezdůvodným omezením obchodu.

(44) Pro výkonnost celé řady systémů UI má zásadní význam vysoká kvalita dat, zejména pokud jsou používány techniky zahrnující trénování modelů s cílem zajistit, aby vysoce rizikový systém UI fungoval dle předpokladu a bezpečně a aby se nestal zdrojem diskriminace, kterou právo Unie zakazuje. Soubory vysoce kvalitních tréninkových dat, dat pro ověřování platnosti a testovacích dat vyžadují zavedení vhodných postupů správy a řízení dat. Soubory tréninkových dat, dat pro ověřování platnosti a testovacích dat by měly být dostatečně relevantní, reprezentativní, bez chyb a úplné s ohledem na určený účel systému. Měly by rovněž vykazovat příslušné statistické vlastnosti, včetně údajů o osobách nebo skupinách osob, pro které má být daný vysoce rizikový systém UI používán. Soubory tréninkových dat, dat pro ověřování platnosti a testovacích dat by měly s ohledem na svůj určený účel zohledňovat zejména rysy, vlastnosti nebo prvky, které jsou specifické pro konkrétní zeměpisné, behaviorální nebo funkční prostředí nebo kontext, ve kterém má být systém UI používán. V zájmu ochrany práva jiných osob na zabránění diskriminaci, která by mohla vyplynout ze zkreslení v rámci systémů UI, by poskytovatelé měli mít možnost zpracovávat také zvláštní kategorie osobních údajů jako záležitost významného veřejného zájmu s cílem zajistit sledování, detekci a opravu tohoto zkreslení ve vztahu k vysoce rizikovým systémům UI.

(45) Při vývoji vysoce rizikových systémů UI by měli mít některé subjekty, jako jsou poskytovatelé, oznámené subjekty a další příslušné subjekty, například centra pro digitální inovace, pokusná zkušební zařízení a výzkumní pracovníci, přístup k vysoce kvalitním datovým souborům ve svých příslušných oborech činnosti, které souvisejí s tímto nařízením. Zásadní význam pro zajištění důvěryhodného, odpovědného a nediskriminačního přístupu k vysoce kvalitním datům pro účely trénování, ověřování a testování systémů UI budou mít společné evropské datové prostory vytvořené Komisí, jakož i usnadnění sdílení údajů ve veřejném zájmu mezi podniky a s vládou. Například v oblasti zdraví umožní společný evropský prostor pro data z oblasti veřejného zdraví nediskriminační přístup k údajům o zdraví a trénování algoritmů umělé inteligence na těchto souborech dat, a to způsobem, který bude chránit soukromí, bude bezpečný, včasný, transparentní a důvěryhodný a bude u něj zajištěna vhodná institucionální správa. Poskytování vysoce kvalitních dat pro účely trénování, ověřování a testování systémů UI mohou podporovat rovněž odpovídající příslušné orgány, včetně odvětvových, které poskytují nebo podporují přístup k datům.

(46) Pro ověření souladu s požadavky tohoto nařízení má zásadní význam, aby byly k dispozici informace, jak byly vysoce rizikové systémy UI vytvořeny a jak fungují po celou dobu své životnosti. To vyžaduje vedení záznamů a dostupnost technické dokumentace obsahující informace nezbytné k posouzení souladu daného systému UI

s příslušnými požadavky. Tyto informace by měly zahrnovat obecné vlastnosti, schopnosti a omezení tohoto systému, použité algoritmy, data, postupy při trénování, testování a ověřování, jakož i dokumentaci příslušného systému řízení rizik. Technická dokumentace by měla být průběžně aktualizována.

(47) Aby se vyřešila neprůhlednost, kvůli níž mohou být určité systémy UI pro fyzické osoby nepochopitelné nebo příliš složité, je u vysoce rizikových systémů UI zapotřebí určitá míra transparentnosti. Uživatelé by měli být schopni interpretovat výstup systému a používat jej vhodným způsobem. K vysoce rizikovým systémům UI by proto měla být připojena příslušná dokumentace a návod k použití a měly by obsahovat stručné a jasné informace, včetně informací týkajících se potenciálního rizika pro základní práva a rizika diskriminace.

(48) Vysoce rizikové systémy UI by měly být navrženy a vyvinuty tak, aby na jejich fungování mohly dohlížet fyzické osoby. Za tímto účelem by měl poskytovatel systému před uvedením systému na trh nebo do provozu stanovit vhodná opatření lidského dohledu. Tato opatření by případně měla zajistit zejména to, aby byla do systému zabudována provozní omezení, která samotný systém není schopen překonat a která reagují na lidskou obsluhu, a aby fyzické osoby, které byly pověřeny lidským dohledem, měly odbornou způsobilost, odbornou přípravu a pravomoc nezbytné k výkonu této funkce.

(49) Vysoce rizikové systémy UI by měly po celou dobu svého životního cyklu fungovat konzistentně a splňovat příslušnou úroveň přesnosti, spolehlivosti a kybernetické bezpečnosti v souladu s obecně uznávaným nejnovějším vývojem. Uživatelé by měli být informováni o úrovni a měřítkách přesnosti.

(50) U vysoce rizikových systémů UI je klíčovým požadavkem technická spolehlivost. Tyto systémy by měly být odolné vůči rizikům souvisejícím s omezeními systému (například chyby, poruchy, nekonzistentnost, neočekávané situace), jakož i vůči svévolným zásahům, které mohou ohrozit bezpečnost systému UI a vést ke škodlivému nebo jinak nežádoucímu chování. Neschopnost ochrany před těmito riziky by mohla vést k dopadům na bezpečnost nebo negativně ovlivnit základní práva, například v důsledku chybných rozhodnutí nebo nesprávných či zkreslených výstupů systému UI.

(51) Zásadní úlohu při zajišťování odolnosti systémů UI proti pokusům o změnu jejich použití, chování nebo výkonnosti nebo o ohrožení jejich bezpečnostních vlastností třetími stranami, které se škodlivým záměrem zneužívají zranitelných míst tohoto systému, hraje kybernetická bezpečnost. Kybernetické útoky na systémy UI mohou využívat aktiva specifická pro UI, jako jsou například soubory tréninkových dat (například tzv. data poisoning) nebo trénované modely (například nepřátelské útoky), nebo zneužívat slabých míst digitálních aktiv daného systému UI nebo příslušné infrastruktury IKT. Pro zajištění úrovně kybernetické bezpečnosti odpovídající těmto rizikům by proto poskytovatelé vysoce rizikových systémů UI měli přijmout vhodná opatření, případně současně zohlednit i příslušnou infrastrukturu IKT.

(52) V rámci harmonizačních právních předpisů Unie by měla být pravidla použitelná pro uvádění na trh, uvádění do provozu a používání vysoce rizikových systémů UI

stanovena v souladu s nařízením Evropského parlamentu a Rady (ES) č. 765/2008[51], kterým se stanoví požadavky na akreditaci a dozor nad trhem s výrobky, s rozhodnutím Evropského parlamentu a Rady č. 768/2008/ES[52] o společném rámci pro uvádění výrobků na trh a s nařízením Evropského parlamentu a Rady (EU) 2019/1020[53] o dozoru nad trhem a souladu výrobků s předpisy („nový legislativní rámec pro uvádění výrobků na trh“).

(53) Je vhodné, aby za uvedení vysoce rizikového systému UI na trh nebo do provozu převzala odpovědnost konkrétní fyzická nebo právnická osoba definovaná jako poskytovatel bez ohledu na to, zda je tato fyzická nebo právnická osoba totožná s osobou, která tento systém navrhla nebo vyvinula.

(54) Poskytovatel by měl zavést spolehlivý systém řízení jakosti, zajistit provedení požadovaného postupu posuzování shody, vypracovat příslušnou dokumentaci a zavést spolehlivý systém monitorování po uvedení na trh. Orgány veřejné moci, které uvádějí do provozu vysoce rizikové systémy UI pro vlastní potřebu, mohou přijímat a provádět pravidla pro systém řízení jakosti jako součást systému řízení jakosti přijatého na vnitrostátní nebo regionální úrovni, případně s přihlédnutím ke zvláštnostem daného odvětví a k pravomocím a organizaci příslušného orgánu veřejné moci.

(55) Pokud není vysoce rizikový systém UI, který je bezpečnostní součástí produktu, na nějž se vztahují příslušné odvětvové právní předpisy nového legislativního rámce, uveden na trh nebo do provozu nezávisle na tomto produktu, měl by výrobce konečného produktu definovaného v příslušných právních předpisech nového legislativního rámce splňovat povinnosti poskytovatele stanovené v tomto nařízení a zejména zajistit, aby systém UI zabudovaný do konečného produktu splňoval požadavky tohoto nařízení.

(56) Aby bylo umožněno prosazování tohoto nařízení a byly vytvořeny rovné podmínky pro provozovatele, a rovněž s přihlédnutím k různým formám zpřístupňování digitálních produktů, je důležité zajistit, aby osoby usazené v Unii mohly za všech okolností poskytnout orgánům veškeré nezbytné informace o souladu systému UI. Poskytovatelé usazení mimo Unii proto v případě, že dodávají do Unie systémy UI, u nichž nelze identifikovat dovozce, předem jmenují formou písemného pověření svého zplnomocněného zástupce usazeného v Unii.

(57) V souladu se zásadami nového legislativního rámce by měly být stanoveny konkrétní povinnosti příslušných hospodářských subjektů, jako jsou dovozci a distributoři, s cílem zajistit právní jistotu a usnadnit těmto příslušným provozovatelům dodržování předpisů.

(58) Vzhledem k povaze systémů UI a rizikům z hlediska bezpečnosti a základních práv, která mohou souviset s jejich používáním, a to i pokud jde o potřebu zajistit řádné monitorování výkonnosti daného systému UI v reálných podmínkách, je vhodné

---

[51] Nařízení Evropského parlamentu a Rady (ES) č. 765/2008 ze dne 9. července 2008, kterým se stanoví požadavky na akreditaci a dozor nad trhem týkající se uvádění výrobků na trh a kterým se zrušuje nařízení (EHS) č. 339/93 (Úř. věst. L 218, 13.8.2008, s. 30).

[52] Rozhodnutí Evropského parlamentu a Rady č. 768/2008/ES ze dne 9. července 2008 o společném rámci pro uvádění výrobků na trh a o zrušení rozhodnutí Rady 93/465/EHS (Úř. věst. L 218, 13.8.2008, s. 82).

[53] Nařízení Evropského parlamentu a Rady (EU) 2019/1020 ze dne 20. června 2019 o dozoru nad trhem a souladu výrobků s předpisy a o změně směrnice 2004/42/ES a nařízení (ES) č. 765/2008 a (EU) č. 305/2011 (Text s významem pro EHP) (Úř. věst. L 169, 25.6.2019, s. 1).

stanovit konkrétní odpovědnost uživatelů. Uživatelé by zejména měli vysoce rizikové systémy UI využívat v souladu s návodem k použití a měly by být stanoveny některé další povinnosti týkající se monitorování fungování systémů UI a případně uchovávání záznamů.

(59) Je vhodné předjímat, že uživatelem systému UI by měla být fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, pod jehož vedením je systém UI provozován, s výjimkou případů, kdy je systém používán v rámci osobní neprofesionální činnosti.

(60) S ohledem na složitost hodnotového řetězce umělé inteligence by měly příslušné třetí strany, zejména ty, které se podílejí na prodeji a dodávkách softwaru, softwarových nástrojů a součástí a předtrénovaných modelů a dat, případně strany, které jsou poskytovateli síťových služeb, podle potřeby spolupracovat s poskytovateli a uživateli s cílem umožnit jim dodržování povinností podle tohoto nařízení, jakož i s příslušnými orgány zřízenými podle tohoto nařízení.

(61) Klíčovou úlohu při poskytování technických řešení zajišťujících dodržování tohoto nařízení poskytovatelům by měla hrát normalizace. Jeden z prostředků, které poskytovatelům umožní prokázat soulad s požadavky tohoto nařízení, by mělo představovat dodržování harmonizovaných norem definovaných v nařízení Evropského parlamentu a Rady (EU) č. 1025/2012[54]. V oblastech, kde harmonizované normy buď neexistují, nebo jsou nedostatečné, by však Komise mohla přijmout společné technické specifikace.

(62) Aby byla zajištěna vysoká úroveň důvěryhodnosti vysoce rizikových systémů UI, mělo by být u těchto systémů před jejich uvedením na trh nebo do provozu provedeno posouzení shody.

(63) V případě vysoce rizikových systémů UI vztahujících se k produktům upraveným stávajícími harmonizačními právními předpisy Unie v souladu s přístupem nového legislativního rámce je v zájmu minimalizace zátěže provozovatelů a předcházení případnému zdvojování vhodné, aby byl soulad těchto systémů UI s požadavky tohoto nařízení posuzován v rámci posuzování shody, které uvedené právní předpisy již upravují. Použitelnost požadavků tohoto nařízení by tedy neměla mít vliv na konkrétní logiku, metodiku nebo obecnou strukturu posuzování shody podle příslušných zvláštních právních předpisů nového legislativního rámce. Tento přístup se plně odráží ve vzájemném vztahu mezi tímto nařízením a [nařízením o strojních zařízeních]. Bezpečnostní rizika systémů UI zajišťujících bezpečnostní funkce u strojních zařízení jsou sice řešena v rámci požadavků tohoto nařízení, avšak [nařízení o strojních zařízeních] obsahuje některé konkrétní požadavky zajišťující bezpečné začlenění daného systému UI do strojního zařízení obecně, aby nedocházelo k ohrožení bezpečnosti daného strojního zařízení jako celku. [Nařízení o strojních zařízeních] používá stejnou definici systému UI jako toto nařízení.

(64) Vzhledem k rozsáhlejším zkušenostem profesionálních ověřovatelů před uvedením na trh v oblasti bezpečnosti produktů a k odlišné povaze souvisejících rizik je vhodné alespoň v počáteční fázi uplatňování tohoto nařízení omezit oblast působnosti

[54] Nařízení Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci, změně směrnic Rady 89/686/EHS a 93/15/EHS a směrnic Evropského parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES, a kterým se ruší rozhodnutí Rady 87/95/EHS a rozhodnutí Evropského parlamentu a Rady č. 1673/2006/ES (Úř. věst. L 316, 14.11.2012, s. 12).

posuzování shody vysoce rizikových systémů UI třetími stranami v případech, které se netýkají produktů. Posuzování shody těchto systémů by proto měl provádět zpravidla poskytovatel na vlastní odpovědnost s jedinou výjimkou, kterou tvoří systémy UI určené pro biometrickou identifikaci osob na dálku, u nichž by mělo být předpokládáno zapojení oznámeného subjektu do posuzování shody, pokud nejsou tyto systémy zakázány.

(65) Příslušné vnitrostátní orgány by v souladu s tímto nařízením měly určit oznámené subjekty pro účely posouzení shody systémů UI určených pro biometrickou identifikaci osob na dálku třetími stranami pod podmínkou, že splňují určitý soubor požadavků, zejména požadavku na nezávislost, způsobilost a neexistenci střetu zájmů.

(66) V souladu s obecně zavedeným pojmem „podstatná změna“ u produktů regulovaných harmonizačními právními předpisy Unie je vhodné provést nové posouzení shody systému UI pokaždé, když dojde ke změně, která může ovlivnit soulad daného systému s tímto nařízením, nebo pokud se změní určený účel tohoto systému. U systémů UI, které se i po uvedení na trh nebo do provozu dále „učí“ (tj. automaticky přizpůsobují způsob výkonu funkcí), je navíc nezbytné stanovit pravidla určující, že změny algoritmu a jeho výkonnosti, které byly předem stanoveny poskytovatelem a posouzeny v okamžiku posuzování shody, by neměly představovat podstatnou změnu.

(67) Vysoce rizikové systémy UI by měly být opatřeny označením CE prokazujícím jejich shodu s tímto nařízením, aby jim byl umožněn volný pohyb v rámci vnitřního trhu. Členské státy by neměly vytvářet neodůvodněné překážky uvádění na trh nebo do provozu u vysoce rizikových systémů UI, které jsou v souladu s požadavky stanovenými v tomto nařízení a jsou opatřeny označením CE.

(68) Rychlá dostupnost inovativních technologií může mít za určitých podmínek zásadní význam pro zdraví a bezpečnost osob i pro společnost jako celek. Je proto vhodné, aby členské státy mohly z výjimečných důvodů veřejné bezpečnosti nebo ochrany života a zdraví fyzických osob a ochrany průmyslového a obchodního vlastnictví povolit uvedení na trh nebo do provozu v případě systémů UI, u nichž nebylo provedeno posouzení shody.

(69) Z důvodu usnadnění práce Komise a členských států v oblasti umělé inteligence a zvýšení transparentnosti vůči veřejnosti by poskytovatelé vysoce rizikových systémů UI s výjimkou těch, které se vztahují k produktům spadajícím do oblasti působnosti příslušných stávajících harmonizačních právních předpisů Unie, měli mít povinnost zaregistrovat svůj vysoce rizikový systém UI do databáze EU, kterou zřídí a bude spravovat Komise. Komise by měla být správcem této databáze v souladu s nařízením Evropského parlamentu a Rady (EU) 2018/1725[55]. Aby byla zajištěna plná funkčnost této databáze při jejím zavedení, měl by postup při vytváření databáze zahrnovat vypracování funkčních specifikací ze strany Komise a nezávislou zprávu o auditu.

(70) Určité systémy UI určené k interakci s fyzickými osobami nebo ke generování obsahu mohou představovat specifická rizika vydávání se za jinou osobu nebo podvodu bez ohledu na to, zda je lze či nelze označit za vysoce rizikové. Na používání těchto systémů by se proto měly za určitých okolností vztahovat zvláštní povinnosti

[55] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (Úř. věst. L 119, 4.5.2016, s. 1).

transparentnosti, aniž by tím byly dotčeny požadavky a povinnosti kladené na vysoce rizikové systémy UI. Zejména fyzické osoby by měly být upozorněny, že komunikují se systémem UI, pokud to není zřejmé z okolností a kontextu použití. Fyzické osoby by navíc měly být informovány v případě, že jsou vystaveny systému rozpoznávání emocí nebo systému biometrické kategorizace. Tyto informace a oznámení by měly být poskytovány ve formátech přístupných pro osoby se zdravotním postižením. Uživatelé, kteří používají systém UI k vytváření obrazového, zvukového nebo video obsahu, který se znatelně podobá existujícím osobám, místům nebo událostem a určité osobě by se mohl nepravdivě jevit jako autentický, případně s tímto obsahem manipulují, by měli zveřejnit, že tento obsah byl uměle vytvořen nebo s ním bylo manipulováno, tím, že daný výstup umělé inteligence odpovídajícím způsobem označí a odhalí jeho umělý původ.

(71) Umělá inteligence je rychle se vyvíjející skupina technologií, která vyžaduje nové formy regulačního dohledu a bezpečný prostor pro experimentování při současném zajištění odpovědné inovace a integrace vhodných záruk a opatření ke zmírnění rizika. K zajištění právního rámce příznivého pro vznik inovací, použitelného i v budoucnosti a odolného vůči narušení je třeba podporovat příslušné vnitrostátní orgány jednoho nebo více členských států ve vytváření regulačních pískovišť umělé inteligence s cílem usnadnit vývoj a testování inovativních systémů UI pod přísným regulačním dohledem dříve, než budou tyto systémy uvedeny na trh nebo jinak uvedeny do provozu.

(72) Cílem těchto regulačních pískovišť by měla být podpora inovací UI na základě vytvoření kontrolovaného experimentálního a testovacího prostředí ve fázi vývoje a před uvedením na trh s cílem zajistit soulad inovativních systémů UI s tímto nařízením a s dalšími příslušnými právními předpisy Unie a členských států; dále posílení právní jistoty inovátorů, dohledu příslušných orgánů a jejich porozumění příležitostem, vznikajícím rizikům a dopadům používání UI, jakož i urychlení přístupu na trhy, mimo jiné odstraněním překážek pro malé a střední podniky a začínající podniky. Aby bylo zajištěno jednotné provádění v celé Unii a úspory z rozsahu, je vhodné stanovit společná pravidla pro zavádění regulačních pískovišť a rámec spolupráce mezi příslušnými orgány, které se podílejí na dohledu nad těmito pískovišti. Toto nařízení by mělo poskytnout právní základ pro použití osobních údajů shromážděných pro jiné účely k vývoji určitých systémů UI ve veřejném zájmu v rámci regulačního pískoviště UI v souladu s čl. 6 odst. 4 nařízení (EU) 2016/679 a s článkem 6 nařízení (EU) 2018/1725, aniž je dotčen čl. 4 odst. 2 směrnice (EU) 2016/680. Účastníci pískoviště by měli zajistit vhodné záruky a spolupracovat s příslušnými orgány, mimo jiné tím, že budou postupovat podle jejich pokynů a budou jednat rychle a v dobré víře s cílem zmírnit veškerá vysoká rizika pro bezpečnost a základní práva, která případně vzniknou v průběhu vývoje a experimentování v rámci pískoviště. Chování účastníků pískoviště by mělo být zohledněno při rozhodování příslušných orgánů o tom, zda uloží správní pokutu podle čl. 83 odst. 2 nařízení 2016/679 a podle článku 57 směrnice 2016/680.

(73) V zájmu podpory a ochrany inovací je důležité, aby byly obzvláště zohledněny zájmy malých poskytovatelů a uživatelů systémů UI. Za tímto účelem by členské státy měly vyvíjet iniciativy zaměřené na tyto provozovatele, a to včetně zvyšování povědomí a informační komunikace. Oznámené subjekty by navíc měly zohledňovat zvláštní zájmy a potřeby malých poskytovatelů při stanovování poplatků za posuzování shody. Značné náklady pro poskytovatele a další provozovatele, zejména jedná-li se o poskytovatele a provozovatele menšího rozsahu, mohou představovat náklady na překlady související s povinnou dokumentací a s komunikací s úřady. Členské státy by

případně měly zajistit, aby jedním z jazyků, který určí a přijmou pro účely dokumentace příslušných poskytovatelů a komunikace s provozovateli, byl jazyk, kterému obecně rozumí co nejvyšší počet přeshraničních uživatelů.

(74) K provádění tohoto nařízení s cílem minimalizovat rizika v oblasti provádění vyplývající z nedostatku věcných a odborných znalostí na trhu, jakož i usnadnit dodržování povinností poskytovatelů a oznámených subjektů podle tohoto nařízení, by mohly potenciálně přispět platformy pro UI na vyžádání, evropská centra pro digitální inovace a zkušební a experimentální zařízení zřízená Komisí a členskými státy na vnitrostátní úrovni nebo na úrovni EU. Tyto organizace mohou poskytovatelům a oznámeným subjektům poskytovat zejména technickou a vědeckou podporu v rámci svých úkolů a oblastí působnosti.

(75) Je vhodné, aby Komise v maximální možné míře usnadnila přístup ke zkušebním a experimentálním zařízením orgánům, skupinám nebo laboratořím, které jsou zřízeny nebo akreditovány podle příslušných harmonizačních právních předpisů Unie a které plní úkoly v souvislosti s posuzováním shody produktů nebo zařízení, na něž se uvedené harmonizační právní předpisy Unie vztahují. To platí zejména pro odborné skupiny, odborné laboratoře a referenční laboratoře v oblasti zdravotnických prostředků podle nařízení (EU) 2017/745 a nařízení (EU) 2017/746.

(76) V zájmu usnadnění hladkého, účinného a harmonizovaného provádění tohoto nařízení by měla být zřízena Evropská rada pro umělou inteligenci. Tato rada by měla odpovídat za řadu poradenských úkolů, včetně vydávání stanovisek, doporučení, rad nebo pokynů v záležitostech souvisejících s prováděním tohoto nařízení, včetně technických specifikací nebo stávajících norem týkajících se požadavků stanovených v tomto nařízení a poskytování poradenství a pomoci Komisi v konkrétních otázkách týkajících se umělé inteligence.

(77) Při uplatňování a prosazování tohoto nařízení hrají klíčovou roli členské státy. V tomto ohledu by měl každý členský stát určit jeden nebo více příslušných vnitrostátních orgánů pro účely dohledu nad uplatňováním a prováděním tohoto nařízení. V zájmu zvýšení efektivity organizace na straně členských států a stanovení oficiálního kontaktního místa pro veřejnost a další protistrany na úrovni členských států a Unie by měl každý členský stát určit jeden vnitrostátní orgán jako vnitrostátní dozorový orgán.

(78) Všichni poskytovatelé vysoce rizikových systémů UI by měli mít zaveden systém monitorování po uvedení na trh s cílem zajistit, že budou schopni zohlednit zkušenosti s používáním vysoce rizikových systémů UI při zlepšování svých systémů a procesu návrhu a vývoje, případně že budou schopni včas přijmout veškerá případná nápravná opatření. Tento systém je rovněž klíčovým předpokladem zajištění účinnějšího a včasnějšího řešení potenciálních rizik vyplývajících ze systémů UI, které se po uvedení na trh nebo do provozu dále „učí“. Poskytovatelé by měli mít v této souvislosti rovněž povinnost zavést systém hlášení veškerých závažných incidentů nebo porušení vnitrostátních právních předpisů a právních předpisů Unie na ochranu základních práv, k nimž dojde v důsledku používání jejich systémů UI, příslušným orgánům.

(79) V zájmu zajištění náležitého a účinného vymáhání požadavků a povinností stanovených tímto nařízením, které představuje harmonizační právní předpis Unie, by se měl v plném rozsahu uplatňovat systém dozoru nad trhem a souladu výrobků s předpisy stanovený nařízením (EU) 2019/1020. Vnitrostátní orgány veřejné správy nebo veřejnoprávní subjekty dohlížející na uplatňování právních předpisů Unie na

ochranu základních práv, včetně orgánů pro rovné zacházení, by rovněž měly mít přístup k veškeré dokumentaci vytvořené podle tohoto nařízení, pokud je to nutné pro výkon jejich pověření.

(80) Právní předpisy Unie týkající se finančních služeb zahrnují pravidla a požadavky vnitřní správy a řízení rizik, které se vztahují na regulované finanční instituce v průběhu poskytování těchto služeb, včetně případů, kdy využívají systémy UI. V zájmu zajištění jednotného uplatňování a vymáhání povinností vyplývajících z tohoto nařízení a příslušných pravidel a požadavků právních předpisů Unie o finančních službách by měly být jako příslušné orgány pro účely dohledu nad prováděním tohoto nařízení, včetně činností dozoru nad trhem ve vztahu k systémům UI poskytovaným nebo používaným finančními institucemi, které jsou předmětem regulace nebo dozoru, určeny orgány odpovědné za dohled nad právními předpisy o finančních službách a jejich vymáhání, tam, kde je to relevantní, včetně Evropské centrální banky. V zájmu dalšího posílení souladu mezi tímto nařízením a pravidly platnými pro úvěrové instituce podléhající směrnici Evropského parlamentu a Rady 2013/36/EU[56] je rovněž vhodné začlenit postup posuzování shody a některé procesní povinnosti poskytovatelů v souvislosti s řízením rizik, monitorováním po uvedení na trh a dokumentací do stávajících povinností a postupů podle směrnice 2013/36/EU. Aby nedocházelo k překrývání, je třeba počítat rovněž s omezenými výjimkami ve vztahu k systému řízení kvality poskytovatelů a k povinnosti monitorování uložené uživatelům vysoce rizikových systémů UI v rozsahu, v jakém se vztahují na úvěrové instituce podléhající směrnici 2013/36/EU.

(81) Vývoj systémů UI s výjimkou vysoce rizikových systémů UI v souladu s požadavky tohoto nařízení může vést k rozsáhlejšímu zavádění důvěryhodné umělé inteligence v Unii. Poskytovatelé systémů UI, které nejsou vysoce rizikové, by měli být vybízeni k vytváření kodexů chování určených k podpoře dobrovolného uplatňování povinných požadavků platných pro vysoce rizikové systémy UI. Poskytovatelé by také měli být povzbuzováni k tomu, aby dobrovolně uplatňovali další požadavky týkající se například udržitelnosti životního prostředí, přístupnosti pro osoby se zdravotním postižením, zapojení zúčastněných stran do návrhu a vývoje systémů UI a rozmanitosti vývojových týmů. Komise může vyvíjet iniciativy, včetně iniciativ odvětvové povahy, s cílem usnadnit snižování technických překážek bránících přeshraniční výměně dat pro účely rozvoje UI, a to i ohledně infrastruktury pro přístup k datům a sémantické a technické interoperability různých druhů dat.

(82) Je důležité, aby systémy UI související s produkty, které podle tohoto nařízení nejsou vysoce rizikové, a proto nemusí splňovat požadavky, které jsou v něm stanoveny, byly při uvedení na trh nebo do provozu přesto bezpečné. Jako záchranná síť pro přispění k tomuto cíli by se uplatnila směrnice Evropského parlamentu a Rady 2001/95/ES[57].

(83) V zájmu zajištění důvěryhodné a konstruktivní spolupráce příslušných orgánů na úrovni Unie a na vnitrostátní úrovni by měly všechny strany zapojené do uplatňování tohoto nařízení respektovat důvěrnost informací a údajů získaných při plnění svých úkolů.

---

[56] Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES (Úř. věst. L 176, 27.6.2013, s. 338).

[57] Směrnice Evropského parlamentu a Rady 2001/95/ES ze dne 3. prosince 2001 o obecné bezpečnosti výrobků (Úř. věst. L 11, 15.1.2002, s. 4).

(84) Členské státy by měly přijmout veškerá nezbytná opatření k zajištění toho, aby byla ustanovení tohoto nařízení prováděna, a to i stanovením účinných, přiměřených a odrazujících sankcí za jejich porušení. U určitých konkrétních porušení by členské státy měly zohlednit rozpětí a kritéria stanovená v tomto nařízení. Evropský inspektor ochrany údajů by měl být oprávněn ukládat pokuty orgánům, institucím a subjektům Unie spadajícím do oblasti působnosti tohoto nařízení.

(85) Za účelem zajištění toho, že v případě potřeby bude možné regulační rámec upravit, by měla být na Komisi přenesena pravomoc přijímat akty v souladu s článkem 290 Smlouvy o fungování EU, pokud jde o změnu technik a přístupů uvedených v příloze I pro účely definice systémů UI, harmonizačních právních předpisů Unie uvedených v příloze II, vysoce rizikových systémů UI uvedených v příloze III, ustanovení týkajících se technické dokumentace uvedených v příloze IV, obsahu EU prohlášení o shodě uvedeného v příloze V, ustanovení týkajících se postupů posuzování shody v přílohách VI a VII a ustanovení zavádějících vysoce rizikové systémy UI, na které by se měl vztahovat postup posuzování shody založený na posouzení systému řízení kvality a posouzení technické dokumentace. Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni, a aby tyto konzultace probíhaly v souladu se zásadami stanovenými v interinstitucionální dohodě o zdokonalení tvorby právních předpisů ze dne 13. dubna 2016[58]. Pro zajištění rovné účasti na vypracovávání aktů v přenesené pravomoci obdrží Evropský parlament a Rada veškeré dokumenty současně s odborníky z členských států a jejich odborníci mají automaticky přístup na setkání skupin odborníků Komise, jež se věnují přípravě aktů v přenesené pravomoci.

(86) Za účelem zajištění jednotných podmínek k provedení tohoto nařízení by měly být Komisi svěřeny prováděcí pravomoci. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011[59].

(87) Jelikož cíle tohoto nařízení nemůže být uspokojivě dosaženo na úrovni členských států a spíše jich z důvodu rozsahu nebo účinků může být lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o EU. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje toto nařízení rámec toho, co je nezbytné pro dosažení tohoto cíle.

(88) Toto nařízení by se mělo použít ode dne … [*Úřad pro publikace – vložte datum uvedené v článku 85*]. Infrastruktura související se správou a se systémem posuzování shody by však měla být funkční již před tímto datem, a proto by se ustanovení o oznámených subjektech a o struktuře řízení měla použít ode dne … [*Úřad pro publikace – vložte datum – tři měsíce od vstupu tohoto nařízení v platnost*]. Kromě toho by členské státy měly stanovit pravidla ukládání sankcí, včetně správních pokut, a oznámit je Komisi a zajistit, aby byla řádně a účinně provedena do data použitelnosti tohoto nařízení. Ustanovení o sankcích by proto měla platit ode dne [*Úřad pro publikace – vložte datum – dvanáct měsíců od vstupu tohoto nařízení v platnost*].

(89) V souladu s čl. 42 odst. 2 nařízení (EU) 2018/1725 byl konzultován evropský inspektor ochrany údajů a Evropský sbor pro ochranu osobních údajů, a jejich stanovisko bylo vydáno dne […].

---

58 Úř. věst. L 123, 12.5.2016, s. 1.

59 Nařízení Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí (Úř. věst. L 55, 28.2.2011, s. 13).

PŘIJALY TOTO NAŘÍZENÍ:

HLAVA I

OBECNÁ USTANOVENÍ

Článek 1
Předmět

Toto nařízení stanoví:

a) harmonizovaná pravidla pro uvádění systémů umělé inteligence (dále jen „systémy UI“) na trh a do provozu a pro jejich používání v Unii;

b) zákaz určitých postupů v oblasti umělé inteligence;

c) zvláštní požadavky na vysoce rizikové systémy UI a povinnosti provozovatelů těchto systémů;

d) harmonizovaná pravidla transparentnosti pro systémy UI určené k interakci s fyzickými osobami, pro systémy rozpoznávání emocí a pro systémy biometrické kategorizace, jakož i pro systémy UI používané k vytváření obrazového, zvukového nebo video obsahu nebo k manipulaci s ním;

e) pravidla monitorování trhu a dozoru nad ním.

Článek 2
Oblast působnosti

1. Toto nařízení se vztahuje na:

a) poskytovatele, kteří uvádějí na trh nebo do provozu systémy UI v Unii bez ohledu na to, zda jsou tito poskytovatelé usazeni v Unii nebo ve třetí zemi;

b) uživatele systémů UI nacházející se v Unii;

c) poskytovatele a uživatele systémů UI, kteří se nacházejí ve třetí zemi, pokud se výstup systému používá v Unii.

2. Pro vysoce rizikové systémy UI, které představují bezpečnostní součásti produktů nebo systémů nebo které jsou samy o sobě produkty nebo systémy a které spadají do oblasti působnosti následujících aktů, se použije pouze článek 84 tohoto nařízení:

a) nařízení (ES) č. 300/2008;

b) nařízení (EU) č. 167/2013;

c) nařízení (EU) č. 168/2013;

d) směrnice 2014/90/EU;

e) směrnice (EU) 2016/797;

f) nařízení (EU) 2018/858;

g) nařízení (EU) 2018/1139;

h) nařízení (EU) 2019/2144.

3. Toto nařízení se nevztahuje na systémy UI vyvinuté nebo používané výhradně pro vojenské účely.

4. Toto nařízení se nevztahuje na orgány veřejné moci ve třetí zemi ani na mezinárodní organizace spadající do oblasti působnosti tohoto nařízení podle odstavce 1, pokud tyto orgány nebo organizace používají systémy UI v rámci mezinárodních dohod o prosazování práva a o justiční spolupráci s Unií nebo s jedním či více členskými státy.

5. Tímto nařízením není dotčeno uplatňování ustanovení o odpovědnosti poskytovatelů zprostředkovatelských služeb uvedených v kapitole II oddíle IV směrnice Evropského parlamentu a Rady 2000/31/ES[60] [*bude nahrazeno odpovídajícími ustanoveními aktu o digitálních službách*].

Článek 3
Definice

Pro účely tohoto nařízení se rozumí:

1) „systémem umělé inteligence“ (systém UI) software, který je vyvinut pomocí jedné nebo více technik a přístupů uvedených v příloze I, a který může pro danou sadu cílů definovaných člověkem generovat výstupy, jako je například obsah, predikce, doporučení nebo rozhodnutí ovlivňující prostředí, s nimiž komunikují;

2) „poskytovatelem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, které vyvíjí nebo nechávají vyvíjet systém UI za účelem jeho uvedení na trh nebo do provozu pod svým vlastním jménem nebo ochrannou známkou, ať už za úplatu, nebo zdarma;

3) „malým poskytovatelem“ poskytovatel, který je mikropodnikem nebo malým podnikem ve smyslu doporučení Komise 2003/361/ES[61];

4) „uživatelem“ jakákoli fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, které v rámci své pravomoci využívají systém UI, s výjimkou případů, kdy je tento systém UI využíván při osobní neprofesionální činnosti;

5) „zplnomocněným zástupcem“ jakákoli fyzická nebo právnická osoba usazená v Unii, která obdržela od poskytovatele systému UI písemné pověření k tomu, aby jeho jménem plnila povinnosti a prováděla postupy stanovené tímto nařízením;

6) „dovozcem“ jakákoli fyzická nebo právnická osoba usazená v Unii, která uvádí na trh nebo do provozu systém UI označený jménem nebo ochrannou známkou fyzické nebo právnické osoby usazené mimo Unii;

7) „distributorem“ fyzická nebo právnická osoba v dodavatelském řetězci, jiná než poskytovatel nebo dovozce, která dodává systém UI na trh Unie, aniž by ovlivňovala jeho vlastnosti;

8) „provozovatelem“ poskytovatel, uživatel, zplnomocněný zástupce, dovozce a distributor;

9) „uvedením na trh“ první dodání systému UI na trh Unie;

---

60 Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu) (Úř. věst. L 178, 17.7.2000, s. 1).

61 Doporučení Komise ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).

10) „dodáním na trh“ dodání systému UI k distribuci nebo použití na trhu Unie v rámci obchodní činnosti, ať už za úplatu, nebo zdarma;

11) „uvedením do provozu“ dodání systému UI k prvnímu použití přímo uživateli nebo pro vlastní použití na trhu Unie za určeným účelem;

12) „určeným účelem“ použití systému UI určené poskytovatelem, včetně konkrétního kontextu a podmínek použití, které jsou uvedeny v informacích dodaných poskytovatelem v návodu k použití, v propagačních nebo prodejních materiálech a prohlášeních, jakož i v technické dokumentaci;

13) „důvodně předvídatelným nesprávným použitím“ použití systému UI způsobem, který není v souladu s jeho určeným účelem, avšak může vyplývat z důvodně předvídatelného lidského chování nebo z interakce s jinými systémy;

14) „bezpečnostní součástí produktu nebo systému“ součást produktu nebo systému, která plní bezpečnostní funkci pro daný produkt nebo systém, případně jejíž porucha nebo chybné fungování ohrožuje zdraví a bezpečnost osob nebo majetku;

15) „návodem k použití“ informace poskytnuté poskytovatelem, které uživatele informují zejména o určeném účelu a řádném použití daného systému UI, včetně konkrétního geografického, behaviorálního nebo funkčního prostředí, ve kterém má být tento vysoce rizikový systém UI používán;

16) „stažením systému UI z oběhu“ jakékoli opatření, jehož cílem je dosáhnout, aby byl systém UI zpřístupněný uživatelům navrácen poskytovateli;

17) „stažením systému UI z trhu“ jakékoli opatření, jehož cílem je zabránit distribuci, vystavování a nabízení systému UI;

18) „výkonností systému UI“ schopnost systému UI dosáhnout svého určeného účelu;

19) „oznamujícím orgánem“ vnitrostátní orgán odpovědný za stanovení a provádění postupů nezbytných pro posuzování, jmenování a oznamování subjektů posuzování shody a za jejich monitorování;

20) „posuzováním shody“ postup ověřování toho, zda byly splněny požadavky stanovené v hlavě III kapitole 2 tohoto nařízení týkající se systému UI;

21) „subjektem posuzování shody“ subjekt, který vykonává činnosti posuzování shody jakožto třetí strana, včetně testování, certifikace a inspekce;

22) „oznámeným subjektem“ subjekt posuzování shody určený v souladu s tímto nařízením a dalšími příslušnými harmonizačními právními předpisy Unie;

23) „podstatnou změnou“ změna systému UI po jeho uvedení na trh nebo do provozu, která ovlivňuje soulad systému UI s požadavky stanovenými v hlavě III kapitole 2 tohoto nařízení nebo vede ke změně určeného účelu, podle kterého byl systém UI posuzován;

24) „označením shody CE“ nebo „označením CE“ označení, kterým poskytovatel vyjadřuje, že systém UI je ve shodě s požadavky stanovenými v hlavě III kapitole 2 tohoto nařízení a v dalších příslušných právních předpisech Unie harmonizujících uvádění produktů na trh („harmonizační právní předpisy Unie“), které upravují jeho umísťování;

25) „monitorováním po uvedení na trh“ veškeré činnosti prováděné poskytovateli systémů UI s cílem aktivně shromažďovat a přezkoumávat zkušenosti získané v souvislosti s využíváním systémů UI, které dodávají na trh nebo uvádějí do

provozu za účelem určení potřeby okamžitého uplatnění jakýchkoliv nezbytných nápravných nebo preventivních opatření;

26) „orgánem dozoru nad trhem“ vnitrostátní orgán provádějící činnosti a přijímající opatření podle nařízení (EU) 2019/1020;

27) „harmonizovanou normou“ evropská norma podle definice v čl. 2 odst. 1 písm. c) nařízení (EU) č. 1025/2012;

28) „společnými specifikacemi“ dokument jiný než norma, který obsahuje technická řešení sloužící jako nástroj pro plnění některých požadavků a povinností stanovených v tomto nařízení;

29) „tréninkovými daty“ data používaná pro trénování systému UI přizpůsobováním jeho parametrů, které se lze naučit, včetně vah neuronové sítě;

30) „daty pro ověřování platnosti“ data používaná pro vyhodnocení trénovaného systému UI a pro vyladění jeho parametrů, které se nelze naučit, a jeho procesu učení, mimo jiné s cílem zabránit přeučení; přičemž soubor dat pro ověřování platnosti může být samostatný soubor dat nebo součást souboru tréninkových dat, ať už jako pevné, nebo variabilní rozdělení;

31) „testovacími daty“ data používaná k zajištění nezávislého vyhodnocení trénovaného a ověřeného systému UI za účelem potvrzení očekávané výkonnosti tohoto systému před jeho uvedením na trh nebo do provozu;

32) „vstupními daty“ data poskytovaná systému UI nebo přímo získaná tímto systémem, na jejichž základě tento systém vytváří výstup;

33) „biometrickými údaji“ osobní údaje vyplývající z konkrétního technického zpracování, týkající se fyzických či fyziologických znaků nebo znaků chování fyzické osoby, které umožňují nebo potvrzují její jedinečnou identifikaci, například zobrazení obličeje nebo daktyloskopické údaje;

34) „systémem rozpoznávání emocí“ systém UI pro účely zjišťování nebo odvozování emocí nebo záměrů fyzických osob na základě jejich biometrických údajů;

35) „systémem biometrické kategorizace“ systém UI pro účely zařazení fyzických osob do určitých kategorií podle pohlaví, věku, barvy vlasů, barvy očí, tetování, etnického původu nebo sexuální či politické orientace, na základě jejich biometrických údajů;

36) „systémem biometrické identifikace na dálku“ systém UI pro účely identifikace fyzických osob na dálku na základě porovnání biometrických údajů dané osoby s biometrickými údaji obsaženými v referenční databázi, aniž by uživatel systému UI předem věděl, zda bude daná osoba přítomna a zda ji bude možné identifikovat;

37) „systémem biometrické identifikace na dálku, v reálném čase‘“ systém biometrické identifikace na dálku, kdy zachycení biometrických údajů, porovnání a identifikace probíhá bez významné prodlevy. To zahrnuje nejen okamžitou identifikaci, ale také omezená krátká zpoždění, jejichž cílem je zabránit obcházení systému;

38) „systémem ‚zpětné‘ biometrické identifikace na dálku“ systém biometrické identifikace na dálku jiný než systém biometrické identifikace na dálku „v reálném čase“;

39) „veřejně přístupným místem“ jakékoli fyzické místo přístupné veřejnosti bez ohledu na to, zda pro něj platí určité podmínky přístupu;

40) „donucovacím orgánem“

a) jakýkoliv orgán veřejné moci příslušný k prevenci, vyšetřování, odhalování či stíhání trestných činů či výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení, nebo

b) jakýkoliv jiný orgán nebo subjekt pověřený právem členského státu plnit veřejnou funkci a vykonávat veřejnou moc pro účely prevence, vyšetřování, odhalování či stíhání trestných činů či výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení;

41) „prosazováním práva“ činnosti prováděné donucovacími orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení;

42) „vnitrostátním dozorovým orgánem“ orgán, kterému členský stát svěřuje odpovědnost za provádění a uplatňování tohoto nařízení, za koordinaci činností svěřených danému členskému státu, za to, že funguje jako jednotné kontaktní místo pro Komisi a za zastupování daného členského státu v Evropské radě pro umělou inteligenci;

43) „příslušným vnitrostátním orgánem“ vnitrostátní dozorový orgán, oznamující orgán a orgán dozoru nad trhem;

44) „závažným incidentem“ incident, který přímo nebo nepřímo vede, mohl vést nebo může vést k některému z těchto následků:

a) smrt určité osoby nebo závažné poškození zdraví určité osoby, majetku nebo životního prostředí;

b) závažné a nevratné narušení správy a provozu kritické infrastruktury.

Článek 4
Změny přílohy I

Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 73 za účelem změny seznamu technik a přístupů uvedených v příloze I s cílem tento seznam aktualizovat podle tržního a technologického vývoje na základě vlastností, které jsou podobné technikám a přístupům, jež jsou v něm uvedeny.

HLAVA II

ZAKÁZANÉ POSTUPY V OBLASTI UMĚLÉ INTELIGENCE

Článek 5

1. Zakazují se následující postupy v oblasti umělé inteligence:

a) uvádění na trh, uvádění do provozu nebo používání systémů UI, které využívají podprahových technik mimo vědomí osob s cílem podstatně ovlivnit chování těchto osob tak, že to dotčené osobě nebo jiné osobě způsobuje nebo by mohlo způsobit fyzickou nebo psychickou újmu;

b) uvádění na trh, uvádění do provozu nebo používání systémů UI, které využívají zranitelnosti určité skupiny osob v důsledku jejich věku nebo tělesného nebo mentálního postižení, s cílem podstatně ovlivnit chování osoby náležející k této skupině tak, že to dotčené osobě nebo jiné osobě způsobuje nebo by mohlo způsobit fyzickou nebo psychickou újmu;

c) uvádění na trh, uvádění do provozu nebo používání systémů UI orgány veřejné moci nebo jejich jménem pro účely hodnocení nebo klasifikace důvěryhodnosti fyzických osob v určitém časovém úseku na základě jejich sociálního chování nebo známých nebo předvídaných osobních či osobnostních vlastností, přičemž výsledný sociální kredit vede k jednomu nebo oběma následujícím důsledkům:

i) ke znevýhodňujícímu nebo nepříznivému zacházení s některými fyzickými osobami nebo celými skupinami těchto osob v sociálních kontextech nesouvisejících s kontextem, ve kterém byly dané údaje původně vytvořeny nebo shromážděny;

ii) ke znevýhodňujícímu nebo nepříznivému zacházení s některými fyzickými osobami nebo celými skupinami těchto osob, které je neodůvodněné nebo nepřiměřené jejich sociálnímu chování nebo jeho závažnosti;

d) používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva, pokud to není nezbytně nutné pro jeden z následujících cílů a jen do té míry, do níž je to nezbytně nutné:

i) cílené vyhledávání určitých potenciálních obětí trestných činů, včetně pohřešovaných dětí;

ii) prevenci konkrétního, závažného a bezprostředního ohrožení života nebo fyzické bezpečnosti fyzických osob nebo teroristického útoku;

iii) odhalování, lokalizaci, identifikaci nebo stíhání pachatelů nebo osob podezřelých z trestného činu uvedeného v čl. 2 odst. 2 rámcového rozhodnutí Rady 2002/584/SVV[62], pokud lze tento trestný čin v dotčeném členském státě potrestat trestem odnětí svobody nebo ochranným opatřením spojeným s odnětím osobní svobody s horní hranicí sazby v délce nejméně tři roky, jak je stanoveno v právních předpisech tohoto členského státu.

2. Při používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva pro dosažení kteréhokoli z cílů uvedených v odst. 1 písm. d) je nutno zohlednit následující prvky:

a) povahu situace, která vede k jejich potenciálnímu použití, zejména závažnost, pravděpodobnost a rozsah újmy způsobené v případě, že by systém použit nebyl;

b) důsledky používání systému pro práva a svobody všech dotčených osob, zejména závažnost, pravděpodobnost a rozsah těchto důsledků.

Použití systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva pro dosažení kteréhokoli z cílů uvedených v odst. 1 písm. d) musí být navíc v souladu s nezbytnými a přiměřenými zárukami a podmínkami ve vztahu k tomuto použití, zejména pokud jde o časová, zeměpisná a osobní omezení.

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

3. Pokud jde o odst. 1 písm. d) a odstavec 2, každé jednotlivé použití systému biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva podléhá předchozímu povolení ze strany justičního orgánu nebo nezávislého správního orgánu členského státu, ve kterém má k tomuto použití dojít, vydanému na základě odůvodněné žádosti a v souladu s podrobnými pravidly vnitrostátního práva uvedenými v odstavci 4. V řádně odůvodněné naléhavé situaci však může být používání systému zahájeno bez povolení a o povolení lze požádat až v průběhu používání nebo po něm.

   Příslušný justiční nebo správní orgán udělí povolení pouze v případě, že je na základě objektivních důkazů nebo jednoznačných údajů, které mu byly předloženy, přesvědčen, že použití dotčeného systému biometrické identifikace na dálku „v reálném čase“ je nezbytné a přiměřené k dosažení jednoho z cílů specifikovaných v odst. 1 písm. d), který je uveden v žádosti. Při rozhodování o žádosti zohlední příslušný justiční nebo správní orgán skutečnosti uvedené v odstavci 2.

4. Členský stát se může rozhodnout, že umožní plně nebo částečně povolit používání systémů biometrické identifikace na dálku „v reálném čase“ na veřejně přístupných místech pro účely prosazování práva v mezích a za podmínek uvedených v odst. 1 písm. d) a v odstavcích 2 a 3. Daný členský stát stanoví ve svých vnitrostátních právních předpisech nezbytná podrobná pravidla upravující žádosti o povolení uvedená v odstavci 3, vydávání a výkon těchto povolení a dohled nad nimi. Tato pravidla rovněž stanoví, ve vztahu ke kterému cíli uvedenému v odst. 1 písm. d) a ke kterému trestnému činu uvedenému v písmenu iii) tohoto odstavce lze příslušným orgánům povolit používání těchto systémů pro účely prosazování práva.

HLAVA III

VYSOCE RIZIKOVÉ SYSTÉMY UI

KAPITOLA 1

KLASIFIKACE SYSTÉMŮ UI JAKO VYSOCE RIZIKOVÝCH

Článek 6

Klasifikační pravidla pro vysoce rizikové systémy UI

1. Bez ohledu na to, zda je určitý systém UI uváděn na trh nebo do provozu nezávisle na produktech uvedených v písmenech a) a b), je tento systém UI považován za vysoce rizikový, jsou-li splněny obě následující podmínky:

   a) systém UI je určen k použití jako bezpečnostní součást výrobku nebo je sám výrobkem, na který se vztahují harmonizační právní předpisy Unie uvedené v příloze II;

   b) na produkt, jehož je daný systém UI bezpečnostní součástí, případně na samotný tento systém UI jako produkt se vztahuje povinnost posouzení shody třetí stranou za účelem uvedení tohoto produktu na trh nebo do provozu podle harmonizačních právních předpisů Unie uvedených v příloze II.

2. Kromě vysoce rizikových systémů UI uvedených v odstavci 1 jsou za vysoce rizikové považovány také systémy UI uvedené v příloze III.

Článek 7
Změny přílohy III

1. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 73 za účelem aktualizace seznamu v příloze III přidáním vysoce rizikových systémů UI, pokud jsou splněny obě tyto podmínky:

   a) systémy UI jsou určeny pro použití v kterékoli z oblastí uvedených v bodech 1 až 8 přílohy III;

   b) systémy UI představují riziko újmy na zdraví a bezpečnosti nebo riziko nepříznivého dopadu na základní práva, které je z hlediska závažnosti a pravděpodobnosti výskytu stejné nebo větší než riziko újmy nebo nepříznivého dopadu, které představují vysoce rizikové systémy UI, jež jsou již uvedeny v příloze III.

2. Při posuzování toho, zda systém UI představuje riziko újmy na zdraví a bezpečnosti nebo riziko nepříznivého dopadu na základní práva stejné nebo větší než riziko újmy nebo nepříznivého dopadu, které představují vysoce rizikové systémy UI, jež jsou již uvedeny v příloze III, pro účely odstavce 1, zohlední Komise tato kritéria:

   a) určený účel daného systému UI;

   b) do jaké míry je daný systém UI již využíván nebo bude pravděpodobně využíván;

   c) do jaké míry již používání systému UI způsobilo újmu na zdraví a bezpečnosti nebo nepříznivý dopad na základní práva nebo vzbudilo významné obavy ohledně toho, že by k této újmě nebo nepříznivému dopadu mohlo dojít, jak vyplývá ze zpráv nebo zdokumentovaných obvinění předložených příslušným vnitrostátním orgánům;

   d) potenciální rozsah této újmy nebo nepříznivého dopadu, zejména pokud jde o jejich intenzitu a schopnost ovlivnit více osob;

   e) do jaké míry jsou osoby, které potenciálně utrpěly újmu nebo nepříznivý dopad, závislé na výsledku vytvořeném pomocí systému UI zejména proto, že z praktických nebo právních důvodů není přiměřeně možné odmítnout účast na tomto výsledku;

   f) do jaké míry se osoby, které potenciálně utrpěly újmu nebo nepříznivý dopad, nacházejí ve zranitelném postavení ve vztahu k danému uživateli systému UI, zejména v důsledku nerovnováhy sil, znalostí, ekonomických nebo sociálních podmínek nebo věku;

   g) do jaké míry je výsledek vytvořený systémem UI snadno zvrátitelný, přičemž výsledky, které mají dopad na zdraví nebo bezpečnost osob, se za snadno zvrátitelné nepovažují;

   h) do jaké míry stávající právní předpisy Unie stanoví:

      i) účinná nápravná opatření ve vztahu k rizikům, která daný systém UI představuje, s výjimkou nároků na náhradu škody;

      ii) účinná opatření vedoucí k prevenci nebo podstatné minimalizaci těchto rizik.

KAPITOLA 2

POŽADAVKY NA VYSOCE RIZIKOVÉ SYSTÉMY UI

Článek 8
Soulad s požadavky

1. Vysoce rizikové systémy UI musí být v souladu s požadavky stanovenými v této kapitole.

2. Při zajišťování souladu s těmito požadavky se zohlední určený účel daného vysoce rizikového systému UI a systém řízení rizik uvedený v článku 9.

Článek 9
Systém řízení rizik

1. Ve vztahu k vysoce rizikovým systémům UI bude zaveden, uplatňován, zdokumentován a udržován systém řízení rizik.

2. Systém řízení rizik spočívá v nepřetržitém opakujícím se procesu prováděném v rámci celého životního cyklu vysoce rizikového systému UI, který vyžaduje pravidelnou systematickou aktualizaci. Zahrnuje následující kroky:

   a) identifikaci a analýzu známých a předvídatelných rizik souvisejících s jednotlivými vysoce rizikovými systémy UI;

   b) odhad a vyhodnocení rizik, která mohou vzniknout, když je vysoce rizikový systém UI používán v souladu s určeným účelem a za podmínek důvodně předvídatelného nesprávného použití;

   c) hodnocení dalších rizik, která mohou potenciálně vzniknout, na základě analýzy shromážděných údajů ze systému monitorování po uvedení na trh uvedeného v článku 61;

   d) přijetí vhodných opatření k řízení rizik v souladu s ustanoveními následujících odstavců.

3. Opatření k řízení rizik uvedená v odst. 2 písm. d) věnují náležitou pozornost účinkům a možným interakcím vyplývajícím z kombinovaného uplatňování požadavků stanovených v této kapitole 2. Zohledňují obecně uznávaný nejnovější vývoj, včetně toho, jak se odráží v příslušných harmonizovaných normách nebo společných specifikacích.

4. Opatření k řízení rizik uvedená v odst. 2 písm. d) musí být taková, aby bylo jakékoli zbytkové riziko spojené s každým nebezpečím a rovněž celkové zbytkové riziko vysoce rizikových systémů UI považováno za přijatelné za předpokladu, že je daný vysoce rizikový systém UI používán v souladu s určeným zamýšleným účelem nebo za podmínek důvodně předvídatelného nesprávného použití. Uživatel je o těchto zbytkových rizicích informován.

   Při určování nejvhodnějších opatření k řízení rizik je třeba zajistit:

   a) vyloučení rizik nebo jejich snížení na nejnižší možnou míru prostřednictvím bezpečného návrhu a vývoje;

   b) ve vhodných případech zavedení odpovídajících zmírňujících a kontrolních opatření, pokud jde o rizika, která nelze vyloučit;

c) poskytování odpovídajících informací podle článku 13, zejména pokud jde o rizika uvedená v odst. 2 písm. b) tohoto článku, a v případě potřeby zajistit pro uživatele školení.

Při vylučování nebo snižování rizik souvisejících s používáním daného vysoce rizikového systému UI by měly být náležitě zváženy technické znalosti, zkušenosti, vzdělání, školení, které může uživatel očekávat, a případně prostředí, ve kterém má být systém používán.

5. Vysoce rizikové systémy UI jsou testovány za účelem identifikace nejvhodnějších opatření k řízení rizik. Testování zajistí, aby vysoce rizikové systémy UI podávaly výkony konzistentní s jejich určeným účelem a aby byly v souladu s požadavky stanovenými v této kapitole.

6. Zkušební postupy musí být vhodné k dosažení určeného účelu systému UI a nemusí překračovat rámec toho, co je pro dosažení tohoto účelu nezbytné.

7. Testování vysoce rizikových systémů UI se provádí podle potřeby kdykoli v průběhu celého procesu vývoje a v každém případě před uvedením na trh nebo do provozu. Testování musí být provedeno na základě předem definovaných měřítek a pravděpodobnostních prahových hodnot, které jsou vhodné pro určený účel vysoce rizikového systému UI.

8. Při zavádění systému řízení rizik popsaného v odstavcích 1 až 7 je třeba věnovat zvláštní pozornost tomu, zda je pravděpodobné, že k danému vysoce rizikovému systému UI budou mít přístup děti nebo zda bude mít na ně dopad.

9. U úvěrových institucí podléhajících směrnici 2013/36/EU jsou aspekty popsané v odstavcích 1 až 8 součástí postupů pro řízení rizik stanovených těmito institucemi podle článku 74 uvedené směrnice.

Článek 10
Data a správa dat

1. Vysoce rizikové systémy UI, které využívají techniky zahrnující trénování modelů obsahujících data, jsou vyvíjeny na základě souborů tréninkových dat, dat pro ověřování platnosti a testovacích dat, které splňují kritéria kvality uvedená v odstavcích 2 až 5.

2. Soubory tréninkových dat, dat pro ověřování platnosti a testovacích dat podléhají příslušným postupům v oblasti správy a řízení dat. Tyto postupy se týkají zejména:

a) příslušných možností návrhu;

b) sběru dat;

c) příslušných operací zpracování přípravy dat, jako jsou anotace, označování, čištění, obohacování a agregace;

d) formulace příslušných předpokladů, zejména s ohledem na informace, které mají daná data měřit a představovat;

e) předchozího posouzení dostupnosti, množství a vhodnosti potřebných souborů dat;

f) zkoumání s ohledem na potenciální zkreslení;

g) identifikace případných nedostatků nebo chyb v datech a způsob, jak tyto nedostatky a chyby vyřešit.

3. Soubory tréninkových dat, dat pro ověřování platnosti a testovacích dat musí být relevantní, reprezentativní, bez chyb a úplné. Musí mít příslušné statistické vlastnosti a tam, kde je to relevantní, rovněž s ohledem na osoby nebo skupiny osob, pro které má být daný vysoce rizikový systém UI používán. Tyto vlastnosti souborů dat lze splnit na úrovni jednotlivých souborů dat nebo jejich kombinací.

4. Soubory tréninkových dat, dat pro ověřování platnosti a testovacích dat zohledňují v rozsahu nezbytném pro jejich určený účel vlastnosti nebo prvky, které jsou specifické pro konkrétní zeměpisné, behaviorální nebo funkční prostředí ve kterém má být daný vysoce rizikový systém UI používán.

5. Pokud je to nezbytně nutné pro zajištění monitorování, detekce a oprav zkreslení ve vztahu k vysoce rizikovým systémům UI, mohou poskytovatelé těchto systémů zpracovávat zvláštní kategorie osobních údajů uvedené v čl. 9 odst. 1 nařízení (EU) 2016/679, v článku 10 směrnice (EU) 2016/680 a v čl. 10 odst. 1 nařízení (EU) 2018/1725 s výhradou vhodných záruk týkajících se základních práv a svobod fyzických osob, včetně technických omezení opakovaného používání a používání nejmodernějších opatření v oblasti bezpečnosti a ochrany soukromí, jako je pseudonymizace nebo šifrování v případech, kdy anonymizace může významně ovlivnit sledovaný účel.

6. Pro vývoj vysoce rizikových systémů UI s výjimkou těch, které využívají techniky zahrnující trénink modelů, se použijí vhodné postupy správy a řízení dat s cílem zajistit, aby byly tyto vysoce rizikové systémy UI v souladu s odstavcem 2.

Článek 11
Technická dokumentace

1. Technická dokumentace vysoce rizikového systému UI musí být vypracována před uvedením tohoto systému na trh nebo do provozu a musí být průběžně aktualizována.

   Technická dokumentace musí být vypracována tak, aby prokazovala, že daný vysoce rizikový systém UI splňuje požadavky stanovené v této kapitole, a aby poskytovala příslušným vnitrostátním orgánům a oznámeným subjektům veškeré informace nezbytné k posouzení souladu systému UI s těmito požadavky. Obsahuje přinejmenším prvky uvedené v příloze IV.

2. Pokud je uváděn na trh nebo do provozu vysoce rizikový systém UI související s produktem, na který se vztahují právní akty uvedené v příloze II oddíle A, musí být vypracována jediná technická dokumentace obsahující všechny informace uvedené v příloze IV, jakož i informace požadované podle těchto právních aktů.

3. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 73 za účelem změny přílohy IV, je-li to nezbytné k zajištění toho, aby technická dokumentace s ohledem na technický pokrok poskytovala veškeré informace nezbytné k posouzení souladu systému s požadavky stanovenými v této kapitole.

Článek 12
Vedení záznamů

1. Vysoce rizikové systémy UI musí být navrženy a vyvinuty tak, aby v průběhu své činnosti umožňovaly automatické zaznamenávání událostí („protokoly“). Tyto

možnosti vedení protokolů musí být v souladu s uznávanými normami nebo společnými specifikacemi.

2. Schopnosti vedení protokolů zajistí úroveň sledovatelnosti fungování systému UI v průběhu jeho životního cyklu, která odpovídá určenému účelu tohoto systému.

3. Schopnosti vedení protokolů umožňují zejména monitorování činnosti vysoce rizikového systému UI ve vztahu k výskytu situací, které mohou vést k tomu, že daný systém UI bude představovat riziko ve smyslu čl. 65 odst. 1, nebo které mohou vést k podstatné změně, a usnadňují monitorování po uvedení na trh uvedené v článku 61.

4. U vysoce rizikových systémů UI uvedených v odst. 1 písm. a) přílohy III musí schopnosti vedení protokolů zajišťovat minimálně:

   a) záznam trvání každého použití systému (datum a čas zahájení a datum a čas ukončení každého použití);

   b) referenční databázi, s níž systém porovnává vstupní data;

   c) vstupní data, u nichž vyhledávání vedlo ke shodě;

   d) identifikaci fyzických osob podílejících se na ověřování výsledků, jak je uvedeno v čl. 14 odst. 5.

Článek 13
Transparentnost a poskytování informací uživatelům

1. Vysoce rizikové systémy UI musí být navrženy a vyvinuty tak, aby bylo jejich fungování dostatečně transparentní a uživatelům umožňovalo interpretovat výstup systému a vhodně jej používat. Je zajištěn vhodný typ a stupeň transparentnosti s cílem dosáhnout souladu s příslušnými povinnostmi uživatele a poskytovatele stanovenými v kapitole 3 této hlavy.

2. Vysoce rizikové systémy UI musí být opatřeny návodem k použití ve vhodném digitálním nebo jiném formátu, který obsahuje stručné, úplné, správné a jasné informace, které jsou pro uživatele relevantní, přístupné a srozumitelné.

3. Informace podle odstavce 2 uvádějí:

   a) totožnost a kontaktní údaje poskytovatele a tam, kde je to relevantní, jeho zplnomocněného zástupce;

   b) vlastnosti, schopnosti a omezení výkonnosti vysoce rizikového systému UI, včetně:

      i) jeho zamýšleného účelu;

      ii) úrovně přesnosti, spolehlivosti a kybernetické bezpečnosti uvedené v článku 15, ve vztahu k níž byl daný vysoce rizikový systém UI testován a ověřen a kterou lze očekávat, a jakékoli známé a předvídatelné okolnosti, které mohou mít na tuto očekávanou úroveň přesnosti, spolehlivost a kybernetické bezpečnosti dopad;

      iii) jakýchkoli známých nebo předvídatelných okolností souvisejících s používáním daného vysoce rizikového systému UI v souladu s jeho určeným účelem nebo za podmínek důvodně předvídatelného nesprávného použití, které mohou vést k rizikům pro zdraví a bezpečnost nebo pro základní práva;

iv) jeho výkonnosti ve vztahu k osobám nebo skupinám osob, na něž má být systém používán;

v) případně specifikací vstupních údajů nebo jakýchkoli dalších informací příslušných z hlediska použitých souborů tréninkových dat, dat pro ověřování platnosti a testovacích dat při zohlednění určeného účelu systému UI;

c) změny vysoce rizikového systému UI a jeho výkonnosti, které poskytovatel stanovil předem v okamžiku počátečního posouzení shody;

d) opatření v oblasti lidského dohledu uvedená v článku 14, včetně technických opatření zavedených za účelem usnadnění interpretace výstupů systémů UI ze strany uživatelů;

e) očekávanou životnost vysoce rizikového systému UI a veškerá nezbytná opatření v oblasti údržby a péče umožňující zajistit řádné fungování tohoto systému UI, včetně aktualizací softwaru.

Článek 14
Lidský dohled

1. Vysoce rizikové systémy UI musí být navrženy a vyvinuty takovým způsobem, a to i pomocí vhodných nástrojů rozhraní člověk-stroj, aby na ně mohly během období, kdy je daný systém UI používán, účinně dohlížet fyzické osoby.

2. Lidský dohled je zaměřen na prevenci nebo minimalizaci rizik pro zdraví, bezpečnost nebo základní práva, která mohou vzniknout při používání vysoce rizikového systému UI v souladu s jeho určeným účelem nebo za podmínek důvodně předvídatelného nesprávného použití, zejména pokud tato rizika přetrvávají bez ohledu na uplatňování dalších požadavků stanovených v této kapitole.

3. Lidský dohled je zajištěn prostřednictvím jednoho nebo všech následujících opatření:

a) opatření, která identifikuje poskytovatel, a pokud je to technicky proveditelné, zabuduje je do daného vysoce rizikového systému UI před jeho uvedením na trh nebo do provozu;

b) opatření, která identifikuje poskytovatel před uvedením daného vysoce rizikového systému UI na trh nebo do provozu a u nichž je vhodné, aby je provedl uživatel.

4. Opatření uvedená v odstavci 3 umožňují jednotlivcům, kteří jsou pověřeni lidským dohledem, aby v závislosti na okolnostech:

a) plně porozuměli kapacitám a omezením daného vysoce rizikového systému UI a byli schopni náležitě monitorovat jeho fungování tak, aby bylo možné co nejdříve objevit a řešit příznaky anomálií, dysfunkcí a neočekávaného výkonu;

b) si nadále uvědomovali možnou tendenci automatického nebo nadměrného spoléhání na výstup vysoce rizikového systému UI (dále jen „automatizační zkreslení“), zejména u vysoce rizikových systémů UI užívaných pro poskytování informací nebo doporučení pro rozhodování fyzických osob;

c) byli schopni správně interpretovat výstup vysoce rizikového systému UI, zejména s ohledem na vlastnosti tohoto systému a na dostupné interpretační nástroje a metody;

d) byli schopni se v jakékoli konkrétní situaci rozhodnout, že vysoce rizikový systém UI nepoužijí nebo výstup z vysoce rizikového systému UI jiným způsobem nezohlední, zruší nebo zvrátí;

e) byli schopni zasáhnout do fungování vysoce rizikového systému UI nebo jej přerušit tlačítkem „stop“ nebo podobným postupem.

5. U vysoce rizikových systémů UI uvedených v bodě 1 písm. a) přílohy III musí být opatření uvedená v odstavci 3 taková, aby navíc zajišťovala, že uživatel neprovede žádné kroky ani rozhodnutí na základě identifikace vyplývající z tohoto systému, pokud tato identifikace nebude ověřena a potvrzena alespoň dvěma fyzickými osobami.

Článek 15
Přesnost, spolehlivost a kybernetická bezpečnost

1. Vysoce rizikové systémy UI jsou navrženy a vyvinuty tak, aby s ohledem na svůj určený účel dosahovaly odpovídající úrovně přesnosti, spolehlivosti a kybernetické bezpečnosti a aby v tomto ohledu dosahovaly konzistentních výsledků v průběhu celého svého životního cyklu.

2. Úrovně přesnosti a příslušná měřítka přesnosti vysoce rizikových systémů UI jsou oznámeny v přiloženém návodu k použití.

3. Vysoce rizikové systémy UI musí být odolné vůči chybám, poruchám nebo nesrovnalostem, které se mohou vyskytnout v daném systému nebo v prostředí, ve kterém tento systém funguje, zejména v důsledku jejich interakce s fyzickými osobami nebo jinými systémy.

4. Spolehlivosti vysoce rizikových systémů UI lze dosáhnout pomocí technicky redundantních řešení, která mohou zahrnovat plány zálohování nebo zajištění proti selhání.

5. Vysoce rizikové systémy UI, které se po uvedení na trh nebo do provozu dále učí, musí být vyvíjeny způsobem zajišťujícím, že výstupy, které budou případně zkresleny v důsledku výstupů použitých jako vstup pro budoucí operace („smyčky zpětné vazby“) budou řádně řešeny formou vhodných zmírňujících opatření.

6. Vysoce rizikové systémy UI musí být odolné proti pokusům neoprávněných třetích stran změnit jejich použití nebo výkonnost zneužitím zranitelných míst těchto systémů.

Technická řešení zaměřená na zajištění kybernetické bezpečnosti vysoce rizikových systémů UI musí odpovídat příslušným okolnostem a rizikům.

Technická řešení umožňující řešení zranitelných míst specifických pro UI zahrnují tam, kde je to vhodné, opatření pro prevenci a kontrolu útoků, které se pokoušejí manipulovat soubory tréninkových dat (tzv. data poisoning), vstupů, jejichž cílem je přimět daný model k tomu, aby udělal chybu (tzv. matoucí vzory), nebo chyb v modelech.

KAPITOLA 3

POVINNOSTI POSKYTOVATELŮ A UŽIVATELŮ VYSOCE RIZIKOVÝCH SYSTÉMŮ UI A DALŠÍCH STRAN

Článek 16
Povinnosti poskytovatelů vysoce rizikových systémů UI

Poskytovatelé vysoce rizikových systémů UI:

a) zajišťují, aby jejich vysoce rizikové systémy UI splňovaly požadavky stanovené v kapitole 2 této hlavy;

b) mají zaveden systém řízení kvality, který je v souladu s článkem 17;

c) vypracovávají technickou dokumentaci daného vysoce rizikového systému UI;

d) pokud jsou vysoce rizikové systémy UI pod jejich kontrolou, zajišťují automatické generování protokolů těmito systémy;

e) zajišťují, aby byl u daného vysoce rizikového systému UI před jeho uvedením na trh nebo do provozu proveden příslušný postup posuzování shody;

f) dodržují povinnosti registrace uvedené v článku 51;

g) přijímají nezbytná nápravná opatření v případě, že daný vysoce rizikový systém UI není v souladu s požadavky stanovenými v kapitole 2 této hlavy;

h) informují příslušné vnitrostátní orgány členských států, do kterých daný systém UI dodali nebo jej uvedli do provozu, případně oznámený subjekt o nesouladu a o případných přijatých nápravných opatřeních;

i) umisťují na své vysoce rizikové systémy UI označení CE, aby vyjádřili jejich soulad s tímto nařízením podle článku 49;

j) na žádost příslušného vnitrostátního orgánu prokazují soulad daného vysoce rizikového systému UI s požadavky stanovenými v kapitole 2 této hlavy.

Článek 17
Systém řízení kvality

1. Poskytovatelé vysoce rizikových systémů UI zavádějí systém řízení kvality, který zajišťuje soulad s tímto nařízením. Tento systém je systematicky a řádně dokumentován formou písemných politik, postupů a pokynů a obsahuje alespoň tyto aspekty:

   a) strategii pro zajištění souladu s právními předpisy, včetně souladu s postupy posuzování shody a postupy pro řízení úprav daného vysoce rizikového systému UI;

   b) techniky, postupy a systematická opatření využívaná při vytváření, kontrole a ověřování návrhu vysoce rizikového systému UI;

   c) techniky, postupy a systematická opatření využívaná při vývoji, kontrole a zajišťování kvality daného vysoce rizikového systému UI;

d) vyšetřovací, testovací a ověřovací postupy prováděné před vývojem vysoce rizikového systému UI, během něho a po něm, a četnost, s níž musí být prováděny;

e) technické specifikace, včetně norem, které mají být uplatňovány, a pokud nejsou příslušné harmonizované normy uplatňovány v plném rozsahu, prostředky, které mají být použity k zajištění toho, aby vysoce rizikový systém UI splňoval požadavky stanovené v kapitole 2 této hlavy;

f) systémy a postupy pro správu dat, včetně shromažďování, analýzy, označování, ukládání, filtrace, vytěžování, agregace a uchovávání dat a jakékoli další operace týkající se dat, které se provádějí před uvedením vysoce rizikových systémů UI na trh nebo do provozu a pro účely tohoto uvedení;

g) systém řízení rizik podle článku 9.

h) vytvoření, uplatňování a udržování systému monitorování po uvedení na trh v souladu s článkem 61;

i) postupy týkající se ohlašování závažných incidentů a chybného fungování v souladu s článkem 62;

j) řešení komunikace s příslušnými vnitrostátními orgány a příslušnými orgány, včetně odvětvových, a zajišťování nebo podpora přístupu k datům, k oznámeným subjektům, k jiným provozovatelům, zákazníkům nebo k jiným zúčastněným stranám;

k) systémy a postupy pro uchovávání záznamů o veškeré příslušné dokumentaci a informacích;

l) řízení zdrojů, včetně opatření souvisejících s bezpečností dodávek;

m) rámec odpovědnosti stanovující odpovědnost vedení a ostatních zaměstnanců ve vztahu ke všem aspektům uvedeným v tomto odstavci.

2. Provádění aspektů uvedených v odstavci 1 musí být přiměřené velikosti organizace poskytovatele.

3. U poskytovatelů, kteří jsou úvěrovými institucemi podléhajícími směrnici 2013/36/EU, se povinnost zavést systém řízení kvality považuje za splněnou, jsou-li dodržena pravidla týkající se systémů, postupů a mechanismů vnitřní správy podle článku 74 uvedené směrnice. V této souvislosti se zohlední veškeré harmonizované normy uvedené v článku 40 tohoto nařízení.

Článek 18

Povinnost vypracovat technickou dokumentaci

1. Poskytovatelé vysoce rizikových systémů UI vypracují technickou dokumentaci uvedenou v článku 11 v souladu s přílohou IV.

2. Poskytovatelé, kteří jsou úvěrovými institucemi podléhajícími směrnici 2013/36/EU, vedou technickou dokumentaci jako součást dokumentace týkající se vnitřní správy, systémů, postupů a mechanismů podle článku 74 uvedené směrnice.

Článek 19
Posuzování shody

1. Poskytovatelé vysoce rizikových systémů UI zajišťují, že bude u jejich vysoce rizikových systémů UI před uvedením na trh nebo do provozu proveden příslušný postup posuzování shody v souladu s článkem 43. Pokud je po tomto posouzení shody prokázán soulad daných systémů UI s požadavky stanovenými v kapitole 2 této hlavy, vypracují poskytovatelé EU prohlášení o shodě v souladu s článkem 48 a umístí označení shody CE v souladu s článkem 49.

2. U vysoce rizikových systémů UI uvedených v bodě 5 písm. b) přílohy III, uváděných na trh nebo do provozu poskytovateli, kteří jsou úvěrovými institucemi podléhajícími směrnici 2013/36/EU, se posuzování shody provádí jako součást postupu uvedeného v článcích 97 až 101 uvedené směrnice.

Článek 20
Automaticky generované protokoly

1. Poskytovatelé vysoce rizikových systémů UI uchovávají protokoly automaticky generované jejich vysoce rizikovými systémy UI v rozsahu, v jakém jsou tyto protokoly pod jejich kontrolou na základě smluvního ujednání s uživatelem nebo jinak na základě právních předpisů. Tyto protokoly jsou uchovávány po dobu, která je přiměřená z hlediska určeného účelu vysoce rizikového systému UI a příslušných právních povinností podle práva Unie nebo vnitrostátního práva.

2. Poskytovatelé, kteří jsou úvěrovými institucemi podléhajícími směrnici 2013/36/EU, uchovávají protokoly automaticky generované jejich vysoce rizikovými systémy UI jako součást dokumentace podle článku 74 uvedené směrnice.

Článek 21
Nápravná opatření

Poskytovatelé vysoce rizikových systémů UI, kteří se domnívají nebo mají důvod se domnívat, že vysoce rizikový systém UI, který uvedli na trh nebo do provozu, není ve shodě s tímto nařízením, přijmou okamžitě nezbytná nápravná opatření k uvedení daného systému ve shodu nebo k jeho případnému stažení z trhu či z oběhu. Náležitě informují distributory dotčeného vysoce rizikového systému UI a tam, kde je to relevantní, zplnomocněného zástupce a dovozce.

Článek 22
Informační povinnost

Pokud vysoce rizikový systém UI představuje riziko ve smyslu čl. 65 odst. 1 a toto riziko je poskytovateli systému známo, informuje tento poskytovatel okamžitě příslušné vnitrostátní orgány členských států, do kterých tento systém dodal, a tam, kde je to relevantní, oznámený subjekt, který vydal pro daný vysoce rizikový systém UI certifikát, a uvede při tom zejména informace o nesouladu a o veškerých přijatých nápravných opatřeních.

Článek 23
Spolupráce s příslušnými orgány

Poskytovatelé vysoce rizikových systémů UI předloží příslušnému vnitrostátnímu orgánu na požádání všechny informace a dokumentaci nezbytné k prokázání shody vysoce rizikového

systému UI s požadavky stanovenými v kapitole 2 této hlavy, a to v úředním jazyce Unie, který dotčený členský stát stanoví. Na základě odůvodněné žádosti příslušného vnitrostátního orgánu mu poskytovatelé poskytnou také přístup k protokolům automaticky generovaným jejich vysoce rizikovým systémem UI v rozsahu, v jakém jsou tyto protokoly pod jejich kontrolou na základě smluvního ujednání s uživatelem nebo jinak na základě právních předpisů.

Článek 24
Povinnosti výrobců produktů

Pokud je vysoce rizikový systém UI týkající se produktů, na které se vztahují právní akty uvedené v příloze II oddíle A, uveden na trh nebo do provozu společně s produktem vyrobeným v souladu s těmito právními akty a pod názvem výrobce tohoto produktu, přebírá výrobce tohoto produktu odpovědnost za soulad tohoto systému UI s tímto nařízením a má ve vztahu k tomuto systému UI stejné povinnosti, které toto nařízení ukládá poskytovateli.

Článek 25
Zplnomocnění zástupci

1. V případě, že poskytovatelé usazení mimo Unii dodávají do Unie systémy umělé inteligence, u nichž nelze identifikovat dovozce, jmenují předem zplnomocněného zástupce usazeného v Unii formou písemného pověření.

2. Zplnomocněný zástupce provádí úkoly vymezené v pověření, které obdržel od poskytovatele. Pověření zmocňuje zplnomocněného zástupce k provádění alespoň těchto úkolů:

   a) uchovávat kopii EU prohlášení o shodě a technickou dokumentaci k dispozici pro příslušné vnitrostátní orgány a vnitrostátní orgány uvedené v čl. 63 odst. 7;

   b) poskytnout příslušnému vnitrostátnímu orgánu na odůvodněnou žádost veškeré informace a dokumentaci nezbytné k prokázání shody vysoce rizikového systému UI s požadavky stanovenými v kapitole 2 této hlavy, včetně přístupu k protokolům, které daný vysoce rizikový systém UI automaticky generuje, v rozsahu, v jakém jsou tyto protokoly pod kontrolou poskytovatele na základě smluvního ujednání s uživatelem nebo jinak na základě zákona;

   c) spolupracovat s příslušnými vnitrostátními orgány na základě odůvodněné žádosti na veškerých opatřeních, která takový orgán v souvislosti s daným vysoce rizikovým systémem UI přijme.

Článek 26
Povinnosti dovozců

1. Před uvedením vysoce rizikového systému UI na trh dovozci tohoto systému zajistí, aby:

   a) poskytovatel daného systému UI provedl příslušný postup posuzování shody;

   b) poskytovatel vypracoval technickou dokumentaci v souladu s přílohou IV;

   c) systém nesl požadované označení CE a aby k němu byla přiložena požadovaná dokumentace a návod k použití.

2. Domnívá-li se dovozce nebo má-li důvod se domnívat, že vysoce rizikový systém UI není ve shodě s tímto nařízením, neuvede tento systém UI na trh, dokud nebude

uveden ve shodu. Pokud vysoce rizikový systém UI představuje riziko ve smyslu čl. 65 odst. 1, informuje o tom dovozce poskytovatele systému UI a orgány dozoru nad trhem.

3. Dovozci uvedou na vysoce rizikovém systému UI, případně není-li to možné, podle potřeby na obalu nebo v dokumentaci, která je k vysoce rizikovému systému UI přiložena, svoje jméno, zapsaný obchodní název nebo zapsanou ochrannou známku a adresu, na které je lze kontaktovat.

4. Dovozci zajistí, aby v době, kdy nesou za vysoce rizikový systém UI odpovědnost, tam, kde je to relevantní, skladovací a přepravní podmínky neohrožovaly jeho soulad s požadavky stanovenými v kapitole 2 této hlavy.

5. Dovozci poskytnou příslušným vnitrostátním orgánům na odůvodněnou žádost veškeré informace a dokumentaci nezbytné k prokázání shody vysoce rizikového systému UI s požadavky stanovenými v kapitole 2 této hlavy v jazyce, který je příslušnému vnitrostátnímu orgánu snadno srozumitelný, včetně přístupu k protokolům automaticky generovaným vysoce rizikovým systémem UI, v rozsahu, v jakém jsou tyto protokoly pod kontrolou poskytovatele na základě smluvního ujednání s uživatelem nebo jinak na základě právních předpisů. S těmito orgány rovněž spolupracují na veškerých opatřeních, která vnitrostátní příslušný orgán v souvislosti s tímto systémem přijme.

Článek 27
Povinnosti distributorů

1. Před dodáním vysoce rizikového systému UI na trh distributoři ověří, zda je na daném vysoce rizikovém systému UI umístěno požadované označení CE, zda je k němu přiložena požadovaná dokumentace a návod k použití a zda poskytovatel a dovozce systému případně splnili povinnosti stanovené v tomto nařízení.

2. Domnívá-li se distributor nebo má-li důvod se domnívat, že vysoce rizikový systém UI není ve shodě s požadavky stanovenými v kapitole 2 této hlavy, neuvede tento vysoce rizikový systém UI na trh, dokud nebude uveden ve shodu s těmito požadavky. Pokud navíc tento systém představuje riziko ve smyslu čl. 65 odst. 1, informuje o tom distributor poskytovatele, případně dovozce tohoto systému.

3. Distributoři zajistí, aby v době, kdy nesou za vysoce rizikový systém UI odpovědnost, tam, kde je to relevantní, skladovací a přepravní podmínky neohrožovaly soulad tohoto systému s požadavky stanovenými v kapitole 2 této hlavy.

4. Distributor, který se domnívá nebo má důvod se domnívat, že vysoce rizikový systém UI, který dodal na trh, není ve shodě s požadavky stanovenými v kapitole 2 této hlavy, přijme nápravná opatření nezbytná k uvedení tohoto systému ve shodu s těmito požadavky nebo k jeho stažení z trhu či z oběhu, případně zajistí, aby tato nápravná opatření přijal poskytovatel, dovozce nebo jakýkoli příslušný provozovatel. Představuje-li vysoce rizikový systém UI riziko ve smyslu čl. 65 odst. 1, distributor okamžitě informuje příslušné vnitrostátní orgány členských států, v nichž tento produkt za tímto účelem dodal na trh, a uvede přitom zejména podrobnosti o nesouladu a o veškerých přijatých nápravných opatřeních.

5. Na odůvodněnou žádost příslušného vnitrostátního orgánu poskytnou distributoři vysoce rizikových systémů UI tomuto orgánu všechny informace a dokumentaci nezbytné k prokázání shody vysoce rizikového systému s požadavky stanovenými

v kapitole 2 této hlavy. Distributoři rovněž spolupracují s příslušným vnitrostátním orgánem na veškerých opatřeních, které tento orgán přijme.

Článek 28

Povinnosti distributorů, dovozců, uživatelů nebo jakékoli jiné třetí strany

1. Jakýkoli distributor, dovozce, uživatel nebo jiná třetí strana se pro účely tohoto nařízení považuje za poskytovatele a vztahují se na něj povinnosti poskytovatele podle článku 16, pokud nastane kterákoli z následujících okolností:

   a) uvádějí vysoce rizikový systém UI na trh nebo do provozu pod svým jménem nebo ochrannou známkou;

   b) mění určený účel vysoce rizikového systému UI již uvedeného na trh nebo do provozu;

   c) provedou podstatnou změnu daného vysoce rizikového systému UI.

2. Pokud nastanou okolnosti uvedené v odst. 1 písm. b) nebo c), není poskytovatel, který původně uvedl vysoce rizikový systém UI na trh nebo do provozu, již nadále považován za poskytovatele pro účely tohoto nařízení.

Článek 29

Povinnosti uživatelů vysoce rizikových systémů UI

1. Uživatelé vysoce rizikových systémů UI tyto systémy používají v souladu s návodem k použití přiloženým k těmto systémům na základě odstavců 2 a 5.

2. Povinnostmi uvedenými v odstavci 1 nejsou dotčeny ostatní povinnosti uživatelů podle právních předpisů Unie nebo vnitrostátních právních předpisů ani volnost uživatelů při organizaci vlastních zdrojů a činností za účelem provádění opatření v oblasti lidského dohledu uvedených poskytovatelem.

3. Aniž je dotčen odstavec 1, zajistí uživatel, aby byla vstupní data relevantní s ohledem na určený účel vysoce rizikového systému UI v rozsahu, v jakém uživatel vykonává kontrolu nad vstupními údaji.

4. Uživatelé monitorují provoz vysoce rizikového systému UI na základě návodu k použití. Pokud mají důvody se domnívat, že použití v souladu s návodem k použití může vést k tomu, že systém UI bude představovat riziko ve smyslu čl. 65 odst. 1, uvědomí o tom poskytovatele nebo distributora a používání systému pozastaví. V případě, že zjistí jakýkoliv závažný incident nebo chybné fungování ve smyslu článku 62, rovněž informují poskytovatele nebo distributora a používání daného systému UI přeruší. V případě, že se uživateli nepodaří poskytovatele kontaktovat, použije se obdobně článek 62.

5. V případě uživatelů, kteří jsou úvěrovými institucemi podléhajícími směrnici 2013/36/EU, se povinnost monitorování stanovená v prvním pododstavci považuje za splněnou, jsou-li dodržena pravidla týkající se systémů, postupů a mechanismů vnitřní správy podle článku 74 uvedené směrnice.

6. Uživatelé vysoce rizikových systémů UI uchovávají protokoly automaticky generované jejich vysoce rizikovým systémem UI v rozsahu, v jakém jsou tyto protokoly pod jejich kontrolou. Tyto protokoly jsou uchovávány po dobu, která je přiměřená z hlediska určeného účelu vysoce rizikového systému UI a příslušných právních povinností podle práva Unie nebo vnitrostátního práva.

Uživatelé, kteří jsou úvěrovými institucemi podléhajícími směrnici 2013/36/EU udržují tyto protokoly jako součást dokumentace týkající se vnitřní správy, systémů, postupů a mechanismů podle článku 74 uvedené směrnice.

7. Uživatelé vysoce rizikových systémů UI použijí informace poskytnuté podle článku 13 ke splnění své povinnosti provést posouzení vlivu na ochranu osobních údajů podle článku 35 nařízení (EU) 2016/679 a tam, kde je to relevantní, podle článku 27 směrnice (EU) 2016/680.

KAPITOLA 4

OZNAMUJÍCÍ ORGÁNY A OZNÁMENÉ SUBJEKTY

Článek 30
Oznamující orgány

1. Každý členský stát jmenuje nebo určí oznamující orgán odpovědný za stanovení a provádění postupů nezbytných pro posuzování, jmenování a oznamování subjektů posuzování shody a za jejich monitorování.

2. Členské státy mohou jako oznamující orgán jmenovat vnitrostátní akreditační orgán uvedený v nařízení (ES) č. 765/2008.

3. Oznamující orgány musí být zřízeny, organizovány a fungovat tak, aby nedocházelo k žádným střetům zájmů se subjekty posuzování shody a aby byla chráněna objektivita a nestrannost jejich činností.

4. Oznamující orgány jsou organizovány tímto způsobem, aby bylo rozhodnutí týkající se oznámení subjektů posuzování shody přijímáno příslušnými osobami, které jsou jinými osobami než osoby, které posuzování těchto subjektů prováděly.

5. Oznamující orgány nenabízejí ani neposkytují žádné činnosti, které provádějí subjekty posuzování shody, ani žádné poradenské služby na komerčním nebo konkurenčním základě.

6. Oznamující orgány zachovají důvěrnost získaných informací.

7. Oznamující orgány mají k dispozici dostatečný počet kvalifikovaných pracovníků, aby mohly řádně vykonávat své povinnosti.

8. Oznamující orgány zajistí, aby bylo posuzování shody prováděno přiměřeným způsobem s cílem zabránit přílišnému zatížení poskytovatelů a aby oznámené subjekty při výkonu své činnosti řádně zohlednily velikost a strukturu dotčeného podniku, odvětví, v němž působí, a míru složitosti technologie daného systému UI.

Článek 31
Žádost subjektu posuzování shody o oznámení

1. Subjekty posuzování shody podávají žádost o oznámení oznamujícímu orgánu členského státu, v němž jsou usazeny.

2. Součástí žádosti o oznámení je popis činností posuzování shody, modulu nebo modulů posuzování shody a technologií umělé inteligence, pro něž se subjekt posuzování shody prohlašuje za způsobilý, jakož i osvědčení o akreditaci, pokud existuje, vydané vnitrostátním akreditačním orgánem, které potvrzuje, že subjekt posuzování shody splňuje požadavky stanovené v článku 33. Přikládá se rovněž

jakýkoli platný dokument týkající se stávajících jmenování žádajícího oznámeného subjektu podle jiných harmonizačních právních předpisů Unie.

3. Nemůže-li dotčený subjekt posuzování shody předložit osvědčení o akreditaci, poskytne oznamujícímu orgánu veškeré doklady nezbytné k ověření, uznání a pravidelné kontrole svého souladu s požadavky stanovenými v článku 33. U oznámených subjektů, které jsou jmenovány podle jiných harmonizačních právních předpisů Unie, lze případně pro doložení postupů jmenování podle tohoto nařízení použít veškeré dokumenty a certifikáty související s tímto jmenováním.

Článek 32
Postup oznamování

1. Oznamující orgány mohou oznámit pouze subjekty posuzování shody, které splňují požadavky stanovené v článku 33.

2. K oznámení Komisi a ostatním členským státům využijí oznamující orgány elektronický nástroj pro oznamování vyvinutý a spravovaný Komisí.

3. Oznámení musí obsahovat veškeré podrobnosti o dotčených činnostech posuzování shody, modulu nebo modulech posuzování shody a o dotčených technologiích umělé inteligence.

4. Dotčený subjekt posuzování shody může vykonávat činnosti oznámeného subjektu, pouze pokud proti tomu Komise nebo ostatní členské státy nevznesly námitky do jednoho měsíce po oznámení.

5. Oznamující orgány oznámí Komisi a členským státům jakékoli následné významné změny týkající se oznámení.

Článek 33
Oznámené subjekty

1. Oznámené subjekty ověřují shodu daného vysoce rizikového systému UI v souladu s postupy posuzování shody uvedenými v článku 43.

2. Oznámené subjekty splňují organizační požadavky a požadavky na řízení kvality, zdroje a postupy, které jsou k plnění uvedených úkolů nezbytné.

3. Organizační struktura, rozdělení povinností, hierarchické vztahy a fungování oznámených subjektů musí být takové, aby zajišťovaly důvěru ve výkon oznámených subjektů a ve výsledky činností posuzování shody, které oznámené subjekty provádějí.

4. Oznámené subjekty jsou nezávislé na poskytovateli vysoce rizikového systému UI, u něhož provádějí činnosti posuzování shody. Oznámené subjekty jsou rovněž nezávislé na jakémkoliv jiném provozovateli, který má na posuzovaném vysoce rizikovém systému UI zájem, i na jakýchkoliv konkurentech poskytovatele.

5. Oznamující subjekty jsou organizovány a provozovány tak, aby byla zaručena nezávislost, objektivita a nestrannost jejich činností. Oznámené subjekty musí zdokumentovat a zavést strukturu a postupy pro zajištění nestrannosti a pro prosazování a uplatňování zásad nestrannosti v rámci celé své organizace, všech činností posuzování a u všech pracovníků.

6. Oznámené subjekty musí mít zavedeny zdokumentované postupy zajišťující, aby jejich pracovníci, výbory, pobočky, subdodavatelé a jakýkoliv přidružený subjekt

nebo pracovníci externích subjektů zachovávali důvěrnost informací získaných při provádění činností posuzování shody, s výjimkou případů, kdy je zveřejnění těchto informací ze zákona povinné. Zaměstnanci subjektů posuzování shody jsou povinni zachovávat služební tajemství, pokud jde o veškeré informace, které obdrželi při plnění svých úkolů podle tohoto nařízení, nikoli však ve vztahu k oznamujícím orgánům členského státu, v němž vykonávají svou činnost.

7. Oznámené subjekty mají k dispozici postupy pro provádění činností, jež řádně zohledňují velikost podniků, odvětví, v němž působí, jejich strukturu a míru složitosti daného systému UI.

8. Oznámené subjekty uzavřou pojištění odpovědnosti za škodu s ohledem na své činnosti v oblasti posuzování shody, pokud tuto odpovědnost nepřevzal dotčený členský stát v souladu s vnitrostátními právními předpisy nebo pokud není tento členský stát za posuzování shody přímo odpovědný.

9. Oznámené subjekty musí být schopny provádět všechny úkoly, které se na ně podle tohoto nařízení vztahují, při nejvyšší úrovni profesní bezúhonnosti a náležité způsobilosti v této konkrétní oblasti bez ohledu na to, zda jsou uvedené úkoly prováděny samotnými oznámenými subjekty, nebo jejich jménem a na jejich odpovědnost.

10. Oznámené subjekty mají dostatečnou interní způsobilost, aby byly schopny účinně hodnotit úkoly, které jejich jménem provádějí externí strany. Za tímto účelem má oznámený subjekt vždy a pro každý postup posuzování shody a každý typ vysoce rizikového systému UI, pro něž byl jmenován, neustále k dispozici dostatek administrativních, technických a vědeckých pracovníků se zkušenostmi a znalostmi ohledně příslušných technologií umělé inteligence, dat a datových výpočtů, jakož i požadavků uvedených v kapitole 2 této hlavy.

11. Oznámené subjekty se podílejí na koordinačních činnostech uvedených v článku 38. Rovněž se přímo účastní činnosti evropských normalizačních organizací nebo jsou v nich zastoupeny, případně zajistí, aby měly povědomí a aktuální informace o příslušných normách.

12. Oznámené subjekty na požádání zpřístupní a předloží veškerou příslušnou dokumentaci, včetně dokumentace poskytovatelů oznamujícímu orgánu uvedenému v článku 30 s cílem umožnit mu provádět činnosti související s posuzováním, jmenováním, oznamováním, monitorováním a dozorem a usnadnit posuzování uvedené v této kapitole.

Článek 34

Dceřiné společnosti oznámených subjektů a zadávání subdodávek

1. Pokud oznámený subjekt zadá konkrétní úkoly týkající se posuzování shody subdodavateli nebo dceřiné společnosti, zajistí, že subdodavatel nebo dceřiná společnost splňuje požadavky stanovené v článku 33, a informuje o tom oznamující orgán.

2. Oznámené subjekty nesou plnou odpovědnost za úkoly provedené subdodavateli nebo dceřinými společnostmi bez ohledu na to, kde jsou tito subdodavatelé nebo dceřiné společnosti usazeni.

3. Činnosti lze zadat subdodavateli nebo dceřiné společnosti pouze se souhlasem poskytovatele.

4. Oznámený subjekt uchovává pro potřebu oznamujícího orgánu příslušné doklady týkající se posouzení kvalifikací subdodavatele nebo dceřiné společnosti a práce provedené subdodavatelem nebo dceřinou společností podle tohoto nařízení.

Článek 35

Identifikační čísla a seznamy oznámených subjektů jmenovaných podle tohoto nařízení

1. Komise oznámeným subjektům přiděluje identifikační číslo. Přidělí jim jediné číslo i v případě, že je daný subjekt oznámen podle několika aktů Unie.

2. Komise zveřejní seznam subjektů oznámených podle tohoto nařízení, včetně identifikačních čísel, která jim byla přidělena, a činností, pro něž byly oznámeny. Komise zajistí, aby byl tento seznam průběžně aktualizován.

Článek 36

Změny v oznámeních

1. Pokud má oznamující orgán podezření nebo je upozorněn na to, že oznámený subjekt již nesplňuje požadavky stanovené v článku 33 nebo neplní své povinnosti, prošetří tuto záležitost s největší péčí. V této souvislosti informuje dotčený oznámený subjekt o vznesených námitkách a poskytne mu možnost, aby vyjádřil svá stanoviska. Pokud oznamující orgán dospěje k závěru, že šetření oznámeného subjektu již nesplňuje požadavky stanovené v článku 33 nebo že tento subjekt neplní své povinnosti, omezí, pozastaví nebo případně zruší oznámení podle toho, jak je toto neplnění závažné. Informuje o tom rovněž neprodleně Komisi a ostatní členské státy.

2. V případě omezení, pozastavení nebo zrušení oznámení nebo v případě, že oznámený subjekt ukončil svou činnost, zajistí oznamující orgán, aby byly spisy tohoto oznámeného subjektu buď převzaty jiným oznámeným subjektem, nebo aby byly na vyžádání k dispozici příslušným oznamujícím orgánům.

Článek 37

Zpochybnění způsobilosti oznámených subjektů

1. Komise v případě potřeby vyšetří všechny případy, u nichž jsou důvody pochybovat o tom, zda oznámený subjekt splňuje požadavky uvedené v článku 33.

2. Oznamující orgán předloží Komisi na vyžádání všechny informace týkající se oznámení dotčeného oznámeného subjektu.

3. Komise zajistí, aby se se všemi důvěrnými informacemi získanými v průběhu jejího šetření podle tohoto článku nakládalo jako s důvěrnými.

4. Pokud Komise zjistí, že oznámený subjekt nesplňuje nebo přestal splňovat požadavky uvedené v článku 33, přijme odůvodněné rozhodnutí a vyzve oznamující členský stát, aby přijal nezbytná nápravná opatření, včetně případného zrušení oznámení. Tento prováděcí akt se přijme přezkumným postupem uvedeným v čl. 74 odst. 2.

Článek 38

Koordinace oznámených subjektů

1. Komise zajistí, aby byla mezi oznámenými subjekty zabývajícími se postupy posuzování shody systémů UI podle tohoto nařízení zavedena a řádně prováděna

náležitá koordinace a spolupráce ve vztahu k oblastem upraveným tímto nařízením, která se provádí formou odvětvové skupiny oznámených subjektů.

2. Členské státy zajistí, aby se jimi oznámené subjekty účastnily práce této skupiny, a to přímo nebo prostřednictvím určených zástupců.

Článek 39
Subjekty posuzování shody třetích zemí

K provádění činnosti oznámených subjektů podle tohoto nařízení mohou být oprávněny subjekty posuzování shody zřízené podle práva třetí země, se kterou Unie uzavřela dohodu.

KAPITOLA 5

NORMY, POSUZOVÁNÍ SHODY, CERTIFIKÁTY, REGISTRACE

Článek 40
Harmonizované normy

Předpokládá se, že vysoce rizikové systémy UI, které jsou ve shodě s harmonizovanými normami nebo jejich částmi, na něž byly zveřejněny odkazy v *Úředním věstníku Evropské unie*, jsou ve shodě s požadavky stanovenými v kapitole 2 této hlavy v rozsahu, v jakém se tyto normy vztahují na tyto požadavky.

Článek 41
Společné specifikace

1. Pokud neexistují harmonizované normy uvedené v článku 40 nebo pokud má Komise za to, že příslušné harmonizované normy nejsou dostatečné nebo že je třeba reagovat na konkrétní obavy týkající se bezpečnosti nebo základních práv, může Komise prostřednictvím prováděcích aktů přijímat společné specifikace, pokud jde o požadavky stanovené v kapitole 2 této hlavy. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 74 odst. 2.

2. Při přípravě společných specifikací uvedených v odstavci 1 shromáždí Komise názory příslušných subjektů nebo skupin odborníků zřízených podle příslušných odvětvových právních předpisů Unie.

3. Předpokládá se, že vysoce rizikové systémy UI, které jsou ve shodě s obecnými specifikacemi uvedenými v odstavci 1, jsou ve shodě s požadavky stanovenými v kapitole 2 této hlavy v rozsahu, v jakém se tyto obecné specifikace vztahují na uvedené požadavky.

4. Pokud poskytovatelé nejsou ve shodě se společnými specifikacemi uvedenými v odstavci 1, řádně zdůvodní, že přijali technická řešení, která jsou s nimi přinejmenším rovnocenná.

Článek 42
Předpoklad shody s určitými požadavky

1. U vysoce rizikových systémů UI, které byly trénovány a testovány na údajích týkajících se konkrétního zeměpisného, behaviorálního a funkčního prostředí, ve kterém mají být používány, se s ohledem na jejich zamýšlený účel předpokládá, že jsou v souladu s požadavkem stanoveným v čl. 10 odst. 4.

2. Má se za to, že vysoce rizikové systémy UI, které byly certifikovány nebo pro které bylo vydáno prohlášení o shodě v rámci systému kybernetické bezpečnosti podle nařízení Evropského parlamentu a Rady (EU) 2019/881[63] a odkaz na něž byl zveřejněn v *Úředním věstníku Evropské unie*, jsou v souladu s požadavky na kybernetickou bezpečnost stanovenými v článku 15 tohoto nařízení, pokud se tento certifikát o kybernetické bezpečnosti nebo prohlášení o shodě, případně jejich části, na tyto požadavky vztahují.

Článek 43
Posuzování shody

1. V případě vysoce rizikových systémů UI uvedených v bodě 1 přílohy III, u nichž poskytovatel při prokazování souladu vysoce rizikového systému UI s požadavky stanovenými v kapitole 2 této hlavy použil harmonizované normy uvedené v článku 40, nebo tam, kde je to relevantní, společné specifikace uvedené v článku 41, uplatňuje poskytovatel jeden z následujících postupů:

   a) postup posuzování shody založený na vnitřní kontrole podle přílohy VI;

   b) postup posuzování shody založený na posouzení systému řízení kvality a posouzení technické dokumentace za účasti oznámeného subjektu podle přílohy VII.

   Pokud poskytovatel při prokazování souladu vysoce rizikového systému UI s požadavky stanovenými v kapitole 2 této hlavy nepoužil harmonizované normy uvedené v článku 40 nebo je použil pouze částečně, případně pokud tyto harmonizované normy neexistují a společné specifikace uvedené v článku 41 nejsou k dispozici, uplatňuje poskytovatel postup posuzování shody podle přílohy VII.

   Pro účely postupu posuzování shody uvedeného v příloze VII si poskytovatel může zvolit kterýkoli z oznámených subjektů. Je-li však systém určen k uvedení do provozu donucovacími, imigračními nebo azylovými orgány, jakož i institucemi, orgány nebo agenturami EU, jedná jako oznámený subjekt orgán dozoru nad trhem uvedený v čl. 63 odst. 5, případně 6.

2. U vysoce rizikových systémů UI uvedených v bodech 2 až 8 přílohy III uplatňují poskytovatelé postup posuzování shody založený na vnitřní kontrole uvedené v příloze VI, který nestanoví zapojení oznámeného subjektu. U vysoce rizikových systémů UI uvedených v bodě 5 písm. b) přílohy III, které jsou uváděny na trh nebo do provozu úvěrovými institucemi podléhajícími směrnici 2013/36/EU, se posuzování shody provádí jako součást postupu uvedeného v článcích 97 až 101 uvedené směrnice.

3. U vysoce rizikových systémů UI, na které se vztahují právní akty uvedené v příloze II oddílu A, uplatňuje poskytovatel příslušné posouzení shody, které stanoví uvedené právní akty. Na tyto vysoce rizikové systémy UI se vztahují požadavky stanovené v kapitole 2 této hlavy, které jsou součástí uvedeného posouzení. Použijí se rovněž body 4.3, 4.4, 4.5 a pátý odstavec bodu 4.6 přílohy VII.

[63] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 1).

Pro účely tohoto posouzení jsou oznámené subjekty, které byly oznámeny podle těchto právních aktů, oprávněny kontrolovat shodu vysoce rizikových systémů UI s požadavky stanovenými v kapitole 2 této hlavy, pokud byl posouzen soulad těchto oznámených subjektů s požadavky stanovenými v čl. 33 odst. 4, 9 a 10 v rámci postupu pro oznamování podle těchto právních aktů.

Pokud právní akty uvedené v příloze II oddíle A umožňují výrobci produktu neúčastnit se posuzování shody třetí stranou za předpokladu, že tento výrobce uplatnil všechny harmonizované normy pokrývající všechny příslušné požadavky, může tento výrobce tuto možnost využít pouze v případě, že uplatnil rovněž harmonizované normy, nebo tam, kde je to relevantní, společné specifikace uvedené v článku 41, které pokrývají požadavky stanovené v kapitole 2 této hlavy.

4. U vysoce rizikových systémů UI musí být proveden nový postup posuzování shody pokaždé, když jsou podstatně změněny, bez ohledu na to, zda má být změněný systém dále distribuován nebo zda jej i nadále používá jeho současný uživatel.

   U vysoce rizikových systémů UI, které se po uvedení na trh nebo do provozu dále učí, nepředstavují změny takového vysoce rizikového systému UI a jeho výkonnosti podstatnou změnu, pokud byly poskytovatelem stanoveny předem v okamžiku počátečního posouzení shody a jsou součástí informací obsažených v technické dokumentaci uvedené v bodě 2 písm. f) přílohy IV.

5. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 73 za účelem aktualizace příloh VI a VII s cílem zavést prvky postupů posuzování shody, které mohou být nutné s ohledem na technický pokrok.

6. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci za účelem změny odstavců 1 a 2 s cílem podrobit vysoce rizikové systémy UI uvedené v bodech 2 až 8 přílohy III postupu posuzování shody uvedenému v příloze VII nebo jejích částech. Komise přijímá tyto akty v přenesené pravomoci s přihlédnutím k účinnosti postupu posuzování shody založeného na vnitřní kontrole podle přílohy VI v oblasti prevence nebo minimalizace rizik pro zdraví, bezpečnost a ochranu základních práv, která tyto systémy představují, jakož i k dostupnosti přiměřených kapacit a zdrojů mezi oznámenými subjekty.

Článek 44
Certifikáty

1. Certifikáty vydané oznámenými subjekty v souladu s přílohou VII se vyhotovují v úředním jazyce Unie, který stanoví členský stát, v němž je oznámený subjekt usazen, nebo v úředním jazyce Unie, který je pro oznámený subjekt případně jinak přijatelný.

2. Certifikáty jsou platné po dobu v nich uvedenou, která nesmí překročit délku pěti let. Na základě žádosti poskytovatele může být platnost certifikátu prodlužována o další období, z nichž žádné nepřekročí délku pěti let, a to na základě nového posouzení v souladu s příslušnými postupy posuzování shody.

3. Pokud oznámený subjekt zjistí, že systém UI již nesplňuje požadavky uvedené v kapitole 2 této hlavy, pozastaví s ohledem na zásadu proporcionality platnost certifikátu nebo ho zruší či jinak omezí, dokud není vhodnými nápravnými opatřeními přijatými poskytovatelem tohoto systému v rámci příslušné lhůty stanovené oznámeným subjektem zajištěno dosažení souladu s těmito požadavky. Oznámený subjekt své rozhodnutí zdůvodní.

Článek 45
Odvolání proti rozhodnutím oznámených subjektů

Členské státy zajistí, aby byl stranám, které mají na uvedeném rozhodnutí oprávněný zájem, k dispozici postup pro podání opravného prostředku proti rozhodnutím oznámených subjektů.

Článek 46
Informační povinnosti oznámených subjektů

1. Oznámené subjekty informují oznamující orgán:

   a) o veškerých certifikátech Unie o posouzení technické dokumentace, o veškerých dodatcích k těmto certifikátům a o schváleních systému řízení kvality vydaných v souladu s požadavky přílohy VII;

   b) o veškerých zamítnutích, omezeních, pozastaveních a odnětích certifikátu Unie o posouzení technické dokumentace nebo o schváleních systému řízení kvality vydaných v souladu s požadavky přílohy VII;

   c) o všech okolnostech majících vliv na působnost nebo podmínky oznámení;

   d) o každé žádosti o informace týkající se činností posuzování shody, kterou obdržely od orgánů dozoru nad trhem;

   e) na vyžádání o činnostech posuzování shody vykonaných v rámci působnosti jejich oznámení a o jakékoli jiné vykonané činnosti, včetně přeshraničních činností a zadávání subdodávek.

2. Každý oznámený subjekt informuje ostatní oznámené subjekty:

   a) o schváleních systému kvality, která zamítl, pozastavil či odňal, a na požádání o schváleních systému kvality, která vydal;

   b) o EU certifikátech posouzení technické dokumentace nebo jakýchkoli jejich dodatcích, které zamítl, odňal, pozastavil či jinak omezil, a na požádání o certifikátech a/nebo dodatcích k nim, které vydal.

3. Každý oznámený subjekt poskytne ostatním oznámeným subjektům, které vykonávají obdobné činnosti posuzování shody a zabývají se stejnými technologiemi umělé inteligence, příslušné informace o otázkách týkajících se negativních a na vyžádání pozitivních výsledků posuzování shody.

Článek 47
Odchylka od postupu posuzování shody

1. Odchylně od článku 43 může kterýkoli orgán dozoru nad trhem povolit uvedení konkrétních vysoce rizikových systémů UI na trh nebo do provozu na území dotčeného členského státu z výjimečných důvodů veřejné bezpečnosti nebo ochrany života a zdraví osob, ochrany životního prostředí a ochrany klíčových průmyslových a infrastrukturních aktiv. Toto povolení se uděluje na omezenou dobu, dokud jsou prováděny nezbytné postupy posuzování shody, a končí, jakmile jsou tyto postupy dokončeny. Dokončení těchto postupů bude provedeno bez zbytečného odkladu.

2. Povolení uvedené v odstavci 1 bude vydáno jen tehdy, pokud orgán dozoru nad trhem dospěje k závěru, že daný vysoce rizikový systém UI splňuje požadavky kapitoly 2 této hlavy. Orgán dozoru nad trhem informuje Komisi a ostatní členské státy o každém povolení vydaném podle odstavce 1.

3. Pokud do patnácti kalendářních dnů od obdržení informací uvedených v odstavci 2 žádný členský stát ani Komise nevznese námitku proti povolení vydanému orgánem dozoru nad trhem členského státu v souladu s odstavcem 1, považuje se povolení za oprávněné.

4. Pokud členský stát do patnácti kalendářních dnů od přijetí oznámení uvedeného v odstavci 2 vznese námitky proti povolení vydanému orgánem dozoru nad trhem jiného členského státu nebo pokud se Komise domnívá, že toto povolení je v rozporu s právními předpisy Unie nebo se závěrem členských států ohledně souladu systému podle odstavce 2 neopodstatněné, zahájí Komise neprodleně konzultace s příslušným členským státem; dotčený provozovatel či provozovatelé jsou konzultováni a mají možnost předložit svá stanoviska. S ohledem na to Komise rozhodne, zda je povolení oprávněné či nikoli. Rozhodnutí Komise je určeno dotčenému členskému státu a příslušnému provozovateli nebo provozovatelům.

5. Pokud je povolení považováno za neodůvodněné, orgán dozoru nad trhem dotčeného členského státu jej zruší.

6. Odchylně od odstavců 1 až 5 se na vysoce rizikové systémy UI, které mají být použity jako bezpečnostní součásti zařízení nebo které jsou samy o sobě zařízeními a na něž se vztahují nařízení (EU) 2017/745 a nařízení (EU) 2017/746, použije článek 59 nařízení (EU) 2017/745 a článek 54 nařízení (EU) 2017/746 také ve vztahu k odchylce od posuzování shody týkající se souladu s požadavky stanovenými v kapitole 2 této hlavy.

Článek 48
EU prohlášení o shodě

1. Poskytovatel vypracuje pro každý systém UI písemné EU prohlášení o shodě a po dobu deseti let od uvedení systému UI na trh nebo do provozu je uchovává pro potřebu příslušných vnitrostátních orgánů. V EU prohlášení o shodě je uveden systém UI, pro nějž bylo vypracováno. Kopie EU prohlášení o shodě bude na vyžádání poskytnuta dotčeným příslušným vnitrostátním orgánům.

2. EU prohlášení o shodě stanoví, že dotyčný vysoce rizikový systém UI splňuje požadavky stanovené v kapitole 2 této hlavy. EU prohlášení o shodě obsahuje informace stanovené v příloze V a je přeloženo do úředního jazyka nebo jazyků Unie požadovaných členským státem nebo členskými státy, v nichž je vysoce rizikový systém UI dodáván na trh.

3. Pokud se na vysoce rizikové systémy AI vztahují jiné harmonizační právní předpisy Unie, které také vyžadují EU prohlášení o shodě, vypracuje se jediné EU prohlášení o shodě s ohledem na všechny právní předpisy Unie, které se vztahují na daný vysoce rizikový systém UI. Toto prohlášení musí obsahovat veškeré informace požadované pro identifikaci harmonizačních právních předpisů Unie, k nimž se prohlášení vztahuje.

4. Vypracováním EU prohlášení o shodě přebírá poskytovatel odpovědnost za soulad s požadavky stanovenými v kapitole 2 této hlavy. Poskytovatel toto EU prohlášení o shodě podle potřeby průběžně aktualizuje.

5. Komisi je svěřena pravomoc přijímat akty v přenesené pravomoci v souladu s článkem 73 za účelem aktualizace obsahu EU prohlášení o shodě uvedeného v příloze V s cílem zavést prvky, které mohou být nutné s ohledem na technický pokrok.

Článek 49
Označení shody CE

1. Označení CE se viditelně, čitelně a nesmazatelně umístí na daný vysoce rizikový systém UI. Pokud to není možné nebo to nelze s ohledem na charakter vysoce rizikového systému UI zaručit, umístí se podle potřeby na obal nebo na průvodní doklady.

2. Označení CE uvedené v odstavci 1 tohoto článku podléhá obecným zásadám uvedeným v článku 30 nařízení (ES) č. 765/2008.

3. Tam, kde je to relevantní, následuje za označením CE identifikační číslo oznámeného subjektu odpovědného za postupy posuzování shody stanovené v článku 43. Identifikační číslo je rovněž uvedeno ve všech propagačních materiálech, které uvádí, že daný vysoce rizikový systém UI splňuje požadavky na označení CE.

Článek 50
Uchovávání dokumentů

Poskytovatel uchovává po dobu deseti let od uvedení systému UI na trh nebo do provozu pro potřebu příslušných vnitrostátních orgánů následující dokumenty:

a) technickou dokumentaci uvedenou v článku 11;

b) dokumentaci týkající se systému řízení kvality podle článku 17;

c) tam, kde je to relevantní, dokumentaci týkající se změn schválených oznámenými subjekty;

d) tam, kde je to relevantní, rozhodnutí a další dokumenty vydané oznámenými subjekty;

e) EU prohlášení o shodě podle článku 48.

Článek 51
Registrace

Před uvedením vysoce rizikového systému UI podle čl. 6 odst. 2 na trh nebo do provozu jej poskytovatel nebo tam, kde je to relevantní, zplnomocněný zástupce zaregistruje do databáze EU uvedené v článku 60.

HLAVA IV

POVINNOSTI TRANSPARENTNOSTI URČITÝCH SYSTÉMŮ UI

Článek 52
Povinnosti transparentnosti určitých systémů UI

1. Poskytovatelé zajistí, že systémy UI určené k interakci s fyzickými osobami budou navrhovány a vyvíjeny tak, aby byly fyzické osoby informovány o tom, že komunikují se systémem UI, pokud to není zřejmé z okolností a kontextu použití. Tato povinnost se nevztahuje na systémy UI, které jsou ze zákona oprávněny odhalovat trestné činy, předcházet jim, vyšetřovat je a stíhat, s výjimkou případů, kdy jsou tyto systémy k dispozici veřejnosti za účelem hlášení trestných činů.

2. Uživatelé systému rozpoznávání emocí nebo systému biometrické kategorizace musí o fungování tohoto systému informovat fyzické osoby, které jsou mu vystaveny. Tato povinnost se nevztahuje na systémy UI používané pro biometrickou kategorizaci, u nichž zákon povoluje odhalování, prevenci a vyšetřování trestných činů.

3. Uživatelé systému UI vytvářejícího obrazový, zvukový nebo video obsah, který se znatelně podobá existujícím osobám, objektům, místům nebo jiným subjektům nebo událostem a který by se určité osobě mohl nepravdivě jevit jako autentický nebo pravdivý (tzv. deep fake), případně manipulujícího s takovým obsahem, zveřejní, že tento obsah byl uměle vytvořen nebo s ním bylo manipulováno.

   První pododstavec se však nepoužije, pokud toto použití povoluje zákon pro účely odhalování, prevence, vyšetřování a stíhání trestných činů nebo pokud je to nezbytné pro výkon práva na svobodu projevu a práva na svobodu umění a věd zaručených Listinou základních práv EU a s výhradou příslušných záruk práv a svobod třetích stran.

4. Odstavci 1, 2 a 3 nejsou dotčeny požadavky a povinnosti stanovené v hlavě III tohoto nařízení.

HLAVA V

OPATŘENÍ NA PODPORU INOVACÍ

Článek 53
Regulační pískoviště UI

1. Regulační pískoviště UI vytvořená jedním nebo více příslušnými orgány členských států nebo evropským inspektorem ochrany údajů poskytují kontrolované prostředí, které usnadňuje vývoj, testování a ověřování inovativních systémů UI po omezenou dobu před jejich uvedením na trh nebo do provozu podle konkrétního plánu. K tomu dochází pod přímým dohledem a vedením příslušných orgánů s cílem zajistit soulad s požadavky tohoto nařízení a případně dalších právních předpisů Unie a členských států, nad nimiž je prováděn dohled v rámci tohoto pískoviště.

2. Členské státy zajistí, aby v rozsahu, v němž dané inovativní systémy UI zahrnují zpracování osobních údajů nebo jinak spadají do oblasti dohledu jiných vnitrostátních orgánů nebo příslušných orgánů poskytujících nebo podporujících přístup k údajům, byly vnitrostátní orgány pro ochranu údajů a tyto další vnitrostátní orgány spojovány s fungováním daného regulačního pískoviště UI.

3. Regulační pískoviště UI nebudou mít vliv na pravomoci příslušných orgánů v oblasti dohledu a nápravy. Veškerá významná rizika pro zdraví, bezpečnost a základní práva, která budou zjištěna během vývoje a testování těchto systémů, budou mít za následek okamžité zmírnění, a pokud se to nezdaří, pozastavení procesu vývoje a testování, dokud k tomuto zmírnění nedojde.

4. Účastníci regulačního pískoviště UI nesou podle platných právních předpisů Unie a členských států o odpovědnosti nadále odpovědnost za jakoukoli škodu způsobenou třetím stranám v důsledku experimentů prováděných v daném pískovišti.

5. Příslušné orgány členských států, které zřídily regulační pískoviště UI, koordinují své činnosti a spolupracují v rámci Evropské rady pro umělou inteligenci. Předkládají této radě a Komisi výroční zprávy o výsledcích provádění uvedených systémů, včetně osvědčených postupů, získaných zkušeností a doporučení o jejich

uspořádání a případně o uplatňování tohoto nařízení a dalších právních předpisů Unie, nad nimiž je prováděn dohled v rámci daného pískoviště.

6. Způsob a podmínky fungování regulačních pískovišť UI, včetně kritérií způsobilosti a postupu pro podávání žádostí o účast na tomto pískovišti, výběr, účast a ukončení této účasti, jakož i práva a povinnosti účastníků, jsou stanoveny v prováděcích aktech. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 74 odst. 2.

Článek 54

Další zpracování osobních údajů pro účely vývoje určitých systémů UI ve veřejném zájmu v rámci regulačního pískoviště UI

1. V regulačním pískovišti UI budou zpracovávány osobní údaje zákonně shromážděné pro jiné účely za účelem vývoje a testování určitých inovativních systémů UI v daném pískovišti za následujících podmínek:

   a) inovativní systémy UI budou vyvinuty za účelem ochrany podstatného veřejného zájmu v jedné nebo více z následujících oblastí:

      i) prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkon trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení pod dozorem a v pravomoci příslušných orgánů. Zpracování je založeno na právu členských států nebo na právu Unie;

      ii) veřejná bezpečnost a veřejné zdraví, včetně prevence, tlumení a léčby nemocí;

      iii) vysoká úroveň ochrany a zlepšování kvality životního prostředí;

   b) zpracovávané údaje jsou nezbytné pro splnění jednoho nebo více požadavků uvedených v hlavě III kapitole 2, pokud tyto požadavky nelze účinně splnit zpracováním anonymizovaných, syntetických nebo jiných neosobních údajů;

   c) existují účinné monitorovací mechanismy umožňující identifikovat, zda mohou během experimentování v pískovišti vzniknout vysoká rizika pro základní práva subjektů údajů, jakož i mechanismus reakce umožňující okamžité zmírnění těchto rizik a v případě potřeby i zastavení zpracování;

   d) veškeré osobní údaje, které mají být zpracovány v rámci pískoviště, se nacházejí ve funkčně odděleném, izolovaném a chráněném prostředí pro zpracování údajů pod kontrolou účastníků a mají k nim přístup pouze oprávněné osoby;

   e) žádné zpracovávané osobní údaje nejsou přenášeny ani převáděny třetím stranám, ani k nim tyto strany nemají přístup;

   f) žádné zpracování osobních údajů v rámci pískoviště nevede k opatřením nebo rozhodnutím ovlivňujícím subjekty údajů;

   g) veškeré osobní údaje zpracovávané v rámci pískoviště jsou vymazány, jakmile skončí účast v pískovišti nebo skončí doba uchovávání osobních údajů;

   h) protokoly o zpracování osobních údajů v rámci pískoviště jsou uchovávány po dobu účasti na pískovišti a jeden rok po jejím ukončení pouze za účelem splnění povinností odpovědnosti a dokumentace podle tohoto článku nebo jiného uplatňování právních předpisů Unie nebo členských států a pouze po dobu k tomu nezbytnou;

i) úplný a podrobný popis postupu a zdůvodnění trénování, testování a validace systému UI je uchováván společně s výsledky testování jako součást technické dokumentace v příloze IV;

j) zveřejnění stručného shrnutí projektu UI vyvinutého v pískovišti, jeho cílů a očekávaných výsledků na internetových stránkách příslušných orgánů.

2. Odstavcem 1 nejsou dotčeny právní předpisy Unie nebo členských států vylučující zpracování pro jiné účely, než které jsou výslovně uvedeny v těchto právních předpisech.

Článek 55
Opatření pro malé poskytovatele a uživatele

1. Členské státy přijmou tato opatření:

a) poskytovat malým poskytovatelům a začínajícím podnikům přednostní přístup k regulačním pískovištím UI v rozsahu, v jakém splňují podmínky způsobilosti;

b) organizovat konkrétní činnosti zaměřené na zvyšování povědomí o uplatňování tohoto nařízení přizpůsobené potřebám malých poskytovatelů a uživatelů;

c) případně zřídit vyhrazený kanál pro komunikaci s malými poskytovateli a uživateli a dalšími inovátory, který bude poskytovat pokyny a reagovat na dotazy týkající se provádění tohoto nařízení.

2. Při stanovování poplatků za posuzování shody podle článku 43 jsou zohledňovány zvláštní zájmy a potřeby malých poskytovatelů, přičemž se tyto poplatky snižují úměrně jejich velikosti a velikosti trhu.

HLAVA VI

SPRÁVA

KAPITOLA 1

EVROPSKÁ RADA PRO UMĚLOU INTELIGENCI

Článek 56
Zřízení Evropské rady pro umělou inteligenci

1. Zřizuje se „Evropská rada pro umělou inteligenci“ (dále jen „rada“).

2. Rada poskytuje Komisi poradenství a pomoc Komisi s cílem:

a) přispívat k účinné spolupráci vnitrostátních dozorových úřadů a Komise s ohledem na záležitosti, na které se vztahuje toto nařízení;

b) koordinovat pokyny a analýzu Komise a vnitrostátních dozorových úřadů a jiných příslušných orgánů, pokud jde o nově se objevující otázky na vnitřním trhu s ohledem na záležitosti, na něž se vztahuje toto nařízení, a přispívat k nim;

c) pomáhat vnitrostátním dozorovým úřadům a Komisi při zajišťování jednotného uplatňování tohoto nařízení.

Článek 57
Struktura rady

1. Rada se skládá z vnitrostátních dozorových úřadů, které jsou zastoupeny vedoucím nebo odpovídajícím vysokým úředníkem daného úřadu a evropským inspektorem ochrany údajů. Na zasedání mohou být přizvány další vnitrostátní orgány v případě, že jsou pro ně projednávané otázky relevantní.

2. Rada přijímá svůj jednací řád prostou většinou svých členů na základě souhlasu Komise. Jednací řád obsahuje rovněž provozní aspekty související s plněním úkolů rady uvedených v článku 58. Rada může podle potřeby zřizovat podskupiny pro účely zkoumání konkrétních otázek.

3. Radě předsedá Komise. Komise svolává zasedání a připravuje pořad jednání v souladu s úkoly rady podle tohoto nařízení a s jejím jednacím řádem. Komise poskytuje administrativní a analytickou podporu činnostem rady podle tohoto nařízení.

4. Rada může přizvat k účasti na svých zasedáních externí odborníky a pozorovatele a může provádět výměny se zúčastněnými třetími stranami s cílem získávat v přiměřeném rozsahu informace pro účely svých činností. Za tímto účelem může Komise umožňovat výměny mezi radou a jinými subjekty, úřady, agenturami a poradními skupinami Unie.

Článek 58
Úkoly rady

Při poskytování poradenství a pomoci Komisi v souvislosti s čl. 56 odst. 2 rada zejména:

a) shromažďuje a sdílí odborné znalosti a osvědčené postupy mezi členskými státy;

b) přispívá k jednotné správní praxi v členských státech, včetně fungování regulačních pískovišť uvedených v článku 53;

c) vydává stanoviska, doporučení nebo písemné příspěvky k záležitostem souvisejícím s prováděním tohoto nařízení, zejména

   i) k technickým specifikacím nebo stávajícím normám týkajícím se požadavků stanovených v hlavě III kapitole 2;

   ii) k používání harmonizovaných norem nebo společných specifikací uvedených v článcích 40 a 41;

   iii) k přípravě pokynů, včetně pokynů pro stanovení správních pokut uvedených v článku 71.

KAPITOLA 2

PŘÍSLUŠNÉ VNITROSTÁTNÍ ORGÁNY

Článek 59
Určení příslušných vnitrostátních orgánů

1. Každý členský stát zřizuje nebo určuje příslušné vnitrostátní orgány s cílem zajistit uplatňování a provádění tohoto nařízení. Příslušný vnitrostátní orgán je organizován tak, aby chránil objektivitu a nestrannost svých činností a úkolů.

2. Každý členský stát určí z řad příslušných vnitrostátních orgánů vnitrostátní dozorový orgán. Vnitrostátní dozorový orgán jedná jako oznamující orgán a orgán dozoru nad trhem, pokud daný členský stát nemá organizační a správní důvody k určení více než jednoho orgánu.

3. Členské státy informují Komisi o tom, který orgán nebo orgány určily a tam, kde je to relevantní, o důvodech určení více než jednoho orgánu.

4. Členské státy zajistí, aby příslušným vnitrostátním orgánům byly poskytnuty odpovídající finanční a lidské zdroje, které jim umožní plnit úkoly podle tohoto nařízení. Příslušné vnitrostátní orgány mají zejména trvale k dispozici dostatečný počet pracovníků, jejichž způsobilost a odborné znalosti zahrnují důkladné porozumění technologiím umělé inteligence, údajům a výpočtu údajů, základním právům a zdravotním a bezpečnostním rizikům, jakož i znalost platných norem a právních předpisů.

5. Členské státy podávají Komisi každoročně zprávy o stavu finančních a lidských zdrojů příslušných vnitrostátních orgánů s hodnocením jejich přiměřenosti. Komise předá tyto informace radě k projednání a případným doporučením.

6. Komise usnadňuje výměnu zkušeností mezi příslušnými vnitrostátními orgány.

7. Příslušné vnitrostátní orgány mohou poskytovat pokyny a rady ohledně provádění tohoto nařízení, a to i malým poskytovatelům. Kdykoli mají příslušné vnitrostátní orgány v úmyslu poskytnout pokyny a rady týkající se systému UI v oblastech, na které se vztahují jiné právní předpisy Unie, provedou podle potřeby konzultaci s vnitrostátními orgány příslušnými podle těchto právních předpisů Unie. Členské státy mohou rovněž zřídit jedno ústřední kontaktní místo pro komunikaci s provozovateli.

8. Pokud orgány, instituce a subjekty Unie spadají do oblasti působnosti tohoto nařízení, jedná jako orgán příslušný pro dohled nad nimi evropský inspektor ochrany údajů.

HLAVA VII

DATABÁZE EU OBSAHUJÍCÍ SAMOSTATNÉ VYSOCE RIZIKOVÉ SYSTÉMY UI

Článek 60

Databáze EU obsahující samostatné vysoce rizikové systémy UI

1. Komise ve spolupráci s členskými státy zřizuje a udržuje databázi EU obsahující informace uvedené v odstavci 2 ohledně vysoce rizikových systémů UI podle čl. 6 odst. 2, které jsou registrovány v souladu s článkem 51.

2. Údaje uvedené v příloze VIII zadávají do databáze EU poskytovatelé. Komise jim poskytuje technickou a administrativní podporu.

3. Informace obsažené v databázi EU jsou přístupné veřejnosti.

4. Databáze EU obsahuje osobní údaje pouze do té míry, která je nezbytná pro shromažďování a zpracovávání informací v souladu s tímto nařízením. Tyto informace zahrnují jména a kontaktní údaje fyzických osob, které odpovídají za registraci systému a mají zákonnou pravomoc zastupovat poskytovatele.

5. Správcem databáze EU je Komise. Ta rovněž zajišťuje poskytovatelům přiměřenou technickou a administrativní podporu.

HLAVA VIII

MONITOROVÁNÍ PO UVEDENÍ NA TRH, SDÍLENÍ INFORMACÍ, DOZOR NAD TRHEM

KAPITOLA 1

MONITOROVÁNÍ PO UVEDENÍ NA TRH

Článek 61
Monitorování po uvedení na trh prováděné poskytovateli a plán monitorování po uvedení vysoce rizikových systémů UI na trh

1. Poskytovatelé zavádějí a dokumentují systém monitorování po uvedení na trh způsobem, který je přiměřený povaze technologií umělé inteligence a rizikům daného vysoce rizikového systému UI.

2. Systém monitorování po uvedení na trh aktivně a systematicky shromažďuje, dokumentuje a analyzuje příslušné údaje získané od uživatelů nebo shromážděné z jiných zdrojů, které se týkají výkonnosti vysoce rizikových systémů UI po celou dobu jejich životnosti, a umožňuje poskytovateli vyhodnocovat nepřetržitý soulad systémů UI s požadavky stanovenými v hlavě III kapitole 2.

3. Systém monitorování po uvedení na trh je založen na plánu monitorování po uvedení na trh. Plán monitorování po uvedení na trh je součástí technické dokumentace uvedené v příloze IV. Komise přijme prováděcí akt, kterým se stanoví podrobná ustanovení zavádějící vzor plánu monitorování po uvedení na trh a seznam prvků, které mají být do tohoto plánu zahrnuty.

4. U vysoce rizikových systémů UI, na které se vztahují právní akty uvedené v příloze II, u nichž je systém a plán monitorování po uvedení na trh podle daných právních předpisů již stanoven, jsou prvky popsané v odstavcích 1, 2 a 3 do tohoto systému a plánu začleněny podle potřeby.

   První pododstavec se vztahuje také na vysoce rizikové systémy UI uvedené v bodě 5 písm. b) přílohy III, které jsou uvedeny na trh nebo do provozu úvěrovými institucemi upravenými směrnicí 2013/36/EU.

KAPITOLA 2

SDÍLENÍ INFORMACÍ O NEŽÁDOUCÍCH PŘÍHODÁCH A O CHYBNÉM FUNGOVÁNÍ

Článek 62
Ohlašování závažných incidentů a chybného fungování

1. Poskytovatelé vysoce rizikových systémů UI uváděných na trh Unie ohlašují každý závažný incident nebo chybné fungování těchto systémů představující porušení povinností podle práva Unie, jehož cílem je ochrana základních práv, orgánům

dozoru nad trhem v členských státech, v nichž k této nežádoucí příhodě nebo porušení došlo.

Toto oznámení musí být učiněno neprodleně poté, co poskytovatel zjistí příčinnou souvislost mezi daným systémem UI a daným závažným incidentem nebo chybným fungováním nebo přiměřenou pravděpodobnost této souvislosti, v každém případě však nejpozději do patnácti dnů poté, co se poskytovatelé o daném závažném incidentu nebo chybném fungování dozvěděli.

2. Po obdržení oznámení týkajícího se porušení povinností podle právních předpisů Unie, jejichž cílem je ochrana základních práv, informuje orgán dozoru nad trhem vnitrostátní orgány veřejné správy nebo veřejnoprávní subjekty uvedené v čl. 64 odst. 3. Komise vypracuje zvláštní pokyny s cílem usnadnit plnění povinností stanovených v odstavci 1. Tyto pokyny jsou vydány nejpozději dvanáct měsíců po vstupu tohoto nařízení v platnost.

3. U vysoce rizikových systémů UI podle bodu 5 písm. b) přílohy III uváděných na trh nebo do provozu poskytovateli, kteří jsou úvěrovými institucemi podléhajícími směrnici 2013/36/EU, a u vysoce rizikových systémů UI, které jsou bezpečnostními součástmi zařízení nebo jsou samy zařízeními a na něž se vztahuje nařízení (EU) 2017/745 a nařízení (EU) 2017/746, se oznamování závažných incidentů nebo chybného fungování omezuje na ty, které představují porušení povinností podle právních předpisů Unie, jejichž cílem je ochrana základních práv.

KAPITOLA 3

PROSAZOVÁNÍ PRÁVA

Článek 63
Dozor nad trhem a kontrola systémů UI na trhu Unie

1. Na systémy UI upravené tímto nařízením se vztahuje nařízení (EU) 2019/1020. Pro účely účinného prosazování tohoto nařízení však platí, že:

   a) jakýkoli odkaz na hospodářský subjekt podle nařízení (EU) 2019/1020 je třeba chápat tak, že zahrnuje všechny provozovatele uvedené v hlavě III kapitole 3 tohoto nařízení;

   b) jakýkoli odkaz na výrobek podle nařízení (EU) 2019/1020 je třeba chápat tak, že zahrnuje všechny systémy UI spadající do oblasti působnosti tohoto nařízení.

2. Vnitrostátní dozorový orgán podává Komisi pravidelné zprávy o výsledcích příslušných činností v oblasti dozoru nad trhem. Vnitrostátní dozorový orgán neprodleně ohlásí Komisi a příslušným vnitrostátním orgánům pro hospodářskou soutěž veškeré informace zjištěné v průběhu činností v oblasti dozoru nad trhem, které by mohly mít potenciální význam pro uplatňování právních předpisů Unie na pravidla hospodářské soutěže.

3. U vysoce rizikových systémů UI souvisejících s výrobky, na které se vztahují právní akty uvedené v příloze II oddíle A, je orgánem dozoru nad trhem pro účely tohoto nařízení orgán odpovědný za činnosti v oblasti dozoru nad trhem určený podle uvedených právních aktů.

4. U systémů UI uváděných na trh, do provozu nebo využívaných finančními institucemi, na něž se vztahují právní předpisy Unie o finančních službách, je orgánem dozoru nad trhem pro účely tohoto nařízení příslušný orgán odpovědný za finanční dohled nad těmito institucemi podle uvedených právních předpisů.

5. Pokud jde o systémy UI uvedené v bodě 1 písm. a), pokud se tyto systémy používají pro účely prosazování práva dle bodů 6 a 7 přílohy III, určí členské státy jako orgány dozoru nad trhem pro účely tohoto nařízení buď příslušné dozorové úřady pro ochranu údajů podle směrnice (EU) 2016/680 či nařízení 2016/679, nebo příslušné vnitrostátní orgány vykonávající dohled nad činností donucovacích, imigračních nebo azylových orgánů, které uvádějí tyto systémy do provozu nebo je využívají.

6. Pokud orgány, instituce a subjekty Unie spadají do oblasti působnosti tohoto nařízení, jedná jako jejich orgán dozoru nad trhem evropský inspektor ochrany údajů.

7. Členské státy usnadňují koordinaci mezi orgány dozoru nad trhem určenými podle tohoto nařízení a dalšími příslušnými vnitrostátními orgány nebo subjekty, které dohlížejí na uplatňování harmonizačních právních předpisů Unie uvedených v příloze II nebo jiných právních předpisů Unie, které by mohly být relevantní pro vysoce rizikové systémy UI uvedené v příloze III.

Článek 64
Přístup k údajům a dokumentaci

1. Orgány dozoru nad trhem mají přístup k údajům a dokumentaci v rámci svých činností a je jim poskytnut neomezený přístup k souborům tréninkových dat, dat pro ověřování platnosti a testovacích dat využívaných poskytovatelem, a to i prostřednictvím aplikačních programovacích rozhraní (API) nebo jiných vhodných technických prostředků a nástrojů umožňujících vzdálený přístup.

2. Je-li to nezbytné k posouzení shody vysoce rizikového systému UI s požadavky uvedenými v hlavě III kapitole 2 a na odůvodněnou žádost bude orgánům dozoru nad trhem poskytnut přístup ke zdrojovému kódu daného systému UI.

3. Vnitrostátní veřejné orgány nebo subjekty, které dohlížejí na dodržování povinností stanovených v právních předpisech Unie na ochranu základních práv v souvislosti s používáním vysoce rizikových systémů UI uvedených v příloze III, případně je vymáhají, jsou oprávněny vyžádat si jakoukoli dokumentaci vytvořenou nebo vedenou podle tohoto nařízení a mít k ní přístup, pokud je přístup k této dokumentaci nezbytný k plnění pravomocí vyplývajících z jejich pověření v rámci jejich příslušnosti. Příslušný veřejný orgán nebo subjekt o každé této žádosti informuje orgán dozoru nad trhem dotčeného členského státu.

4. Každý členský stát určí do tří měsíců po vstupu tohoto nařízení v platnost orgány veřejné moci nebo subjekty uvedené v odstavci 3 a jejich seznam zveřejní na internetových stránkách vnitrostátního dozorového orgánu. Členské státy oznámí tento seznam Komisi a všem ostatním členským státům a průběžně jej aktualizují.

5. Pokud dokumentace uvedená v odstavci 3 není dostatečná k tomu, aby bylo možné zjistit, zda došlo k porušení povinností podle právních předpisů Unie, jejichž cílem je ochrana základních práv, může orgán veřejné moci nebo subjekt uvedený v odstavci 3 podat orgánu dozoru nad trhem odůvodněnou žádost o uspořádání testů vysoce rizikového systému UI technickými prostředky. Orgán dozoru nad trhem uspořádá tyto testy, do nichž bude dožadující orgán veřejné moci nebo subjekt významně zapojen, v přiměřené lhůtě po podání žádosti.

6. S veškerými informacemi a dokumentací získanými vnitrostátními orgány veřejné správy nebo veřejnoprávními subjekty uvedenými v odstavci 3 podle ustanovení tohoto článku se nakládá v souladu s povinnostmi zachování důvěrnosti stanovenými v článku 70.

Článek 65

Postup nakládání se systémy UI, které představují riziko, na vnitrostátní úrovni

1. Systémy UI, které představují riziko, jsou považovány za výrobek představující riziko podle čl. 3 bodu 19 nařízení (EU) 2019/1020, pokud jde o rizika pro zdraví, bezpečnost nebo ochranu základních práv osob.

2. Pokud má orgán dozoru nad trhem členského státu dostatečné důvody domnívat se, že systém UI představuje riziko podle odstavce 1, provede hodnocení dotčeného systému UI z hlediska jeho souladu se všemi požadavky a povinnostmi stanovenými v tomto nařízení. Pokud existují rizika z hlediska ochrany základních práv, informuje orgán dozoru nad trhem rovněž příslušné vnitrostátní orgány veřejné správy nebo veřejnoprávní subjekty uvedené v čl. 64 odst. 3. Příslušní provozovatelé podle potřeby spolupracují s orgány dozoru nad trhem a s dalšími vnitrostátními orgány veřejné správy nebo veřejnoprávními subjekty uvedenými v čl. 64 odst. 3.

   Pokud v průběhu tohoto hodnocení orgán dozoru nad trhem zjistí, že systém UI nesplňuje požadavky a povinnosti stanovené tímto nařízením, neprodleně vyzve příslušného provozovatele, aby přijal veškerá vhodná nápravná opatření k uvedení systému UI do souladu nebo k jeho stažení z trhu nebo z oběhu ve lhůtě, kterou může orgán dozor nad trhem stanovit a která je přiměřená povaze rizika.

   Orgán dozoru nad trhem o tom informuje příslušný oznámený subjekt. Na opatření uvedená v druhém pododstavci se použije článek 18 nařízení (EU) 2019/1020.

3. Domnívá-li se orgán dozoru nad trhem, že se nesoulad netýká pouze území jeho členského státu, informuje Komisi a ostatní členské státy o výsledcích hodnocení a o opatřeních, která má provozovatel na jeho žádost přijmout.

4. Provozovatel zajistí, aby byla přijata všechna vhodná nápravná opatření ohledně všech dotčených systémů UI, které dodal na trh v celé Unii.

5. Pokud provozovatel systému UI ve lhůtě uvedené v odstavci 2 nepřijme přiměřená nápravná opatření, přijme orgán dozoru nad trhem všechna vhodná dočasná opatření k omezení nebo zákazu dodávání systému UI na trh svého členského státu nebo k zajištění toho, že je tento produkt stažen z trhu nebo z oběhu. O takových opatřeních tento orgán neprodleně informuje Komisi a ostatní členské státy.

6. Součástí informací uvedených v odstavci 5 jsou všechny dostupné podrobnosti, zejména údaje nezbytné pro identifikaci nevyhovujícího systému UI, údaje o původu systému UI, povaze nesouladu a souvisejícího rizika, povaze a době trvání opatření přijatých na vnitrostátní úrovni a stanoviska příslušného poskytovatele. Orgány dozoru nad trhem zejména uvedou, zda je důvodem nesouladu jeden nebo více těchto nedostatků:

   a) systém UI nesplňuje požadavky uvedené v hlavě III kapitole 2;

   b) nedostatky v harmonizovaných normách nebo ve společných specifikacích uvedených v článcích 40 a 41, na nichž je založen předpoklad shody.

7. Orgány dozoru nad trhem členských států jiné než orgán dozoru nad trhem členského státu, který zahájil tento postup, neprodleně informují Komisi a ostatní členské státy o veškerých opatřeních, která přijaly, a o všech doplňujících údajích týkajících se nesouladu dotčeného systému UI, které mají k dispozici, a v případě nesouhlasu s oznámeným vnitrostátním opatřením o svých námitkách.

8. Jestliže do tří měsíců od přijetí informací uvedených v odstavci 5 nevznese žádný členský stát ani Komise námitku proti předběžnému opatření přijatému členským státem, považuje se uvedené opatření za odůvodněné. Tím nejsou dotčena procesní práva dotčeného provozovatele v souladu s článkem 18 nařízení (EU) 2019/1020.

9. Orgány dozoru nad trhem všech členských států zajistí, aby byla v souvislosti s dotčeným produktem bezodkladně přijata náležitá restriktivní opatření, například stažení daného produktu z jejich trhů.

Článek 66
Ochranný postup Unie

1. Pokud do tří měsíců od obdržení oznámení uvedeného v čl. 65 odst. 5 vznese některý členský stát námitky proti opatření přijatému jiným členským státem nebo pokud se Komise domnívá, že je dané opatření v rozporu s právem Unie, zahájí Komise neprodleně konzultaci s dotčeným členským státem a provozovatelem nebo provozovateli a provede hodnocení tohoto vnitrostátního opatření. Na základě výsledků tohoto hodnocení Komise do devíti měsíců od oznámení uvedeného v čl. 65 odst. 5 rozhodne, zda je dané vnitrostátní opatření odůvodněné či nikoli, a toto rozhodnutí oznámí dotčenému členskému státu.

2. Pokud je dané vnitrostátní opatření považováno za odůvodněné, přijmou všechny členské státy opatření nezbytná k zajištění toho, aby byl nevyhovující systém UI stažen z jejich trhu, a informují o tom Komisi. Je-li vnitrostátní opatření považováno za neodůvodněné, dotčený členský stát toto opatření zruší.

3. Pokud je vnitrostátní opatření považováno za odůvodněné a je-li nesoulad systému UI přisuzován nedostatkům v harmonizovaných normách nebo společných specifikacích, jak je uvedeno v článcích 40 a 41 tohoto nařízení, použije Komise postup stanovený v článku 11 nařízení (EU) č. 1025/2012.

Článek 67
Vyhovující systémy UI, které představují riziko

1. Pokud orgán dozoru nad trhem členského státu po provedení hodnocení podle článku 65 zjistí, že ačkoli je systém UI v souladu s tímto nařízením, představuje riziko pro zdraví nebo bezpečnost osob, pro plnění povinností podle právních předpisů Unie nebo vnitrostátních právních předpisů, jejichž záměrem je chránit základní práva, nebo pro jiné aspekty ochrany veřejného zájmu, vyzve dotčeného provozovatele, aby přijal veškerá vhodná opatření k zajištění toho, aby dotčený systém UI, pokud bude uveden na trh nebo do provozu, dále nepředstavoval toto riziko, nebo aby byl tento systém UI stažen z trhu nebo z oběhu ve lhůtě, kterou může členský stát stanovit a která je přiměřená povaze rizika.

2. Poskytovatel nebo jiní příslušní provozovatelé zajistí, aby byla přijata nápravná opatření ve vztahu ke všem dotčeným systémům UI, které dodali na trh v rámci celé Unie, ve lhůtě stanovené orgánem dozoru nad trhem členského státu uvedeného v odstavci 1.

3. Tento členský stát o tom neprodleně informuje Komisi a ostatní členské státy. Tato informace musí obsahovat všechny dostupné podrobnosti, zejména údaje nezbytné pro identifikaci dotčeného systému UI, údaje o jeho původu a dodavatelském řetězci, údaje o povaze souvisejícího rizika a údaje o povaze a době trvání opatření přijatých na vnitrostátní úrovni.

4. Komise neprodleně zahájí konzultaci s členskými státy a s příslušným provozovatelem a vyhodnotí přijatá vnitrostátní opatření. Na základě výsledků tohoto hodnocení Komise rozhodne, zda jsou opatření odůvodněná či nikoli, a pokud je to nutné, navrhne vhodná opatření.

5. Rozhodnutí Komise je určeno všem členským státům.

Článek 68
Formální nesoulad

1. Orgán dozoru nad trhem daného členského státu požádá příslušného provozovatele, aby odstranil dotčený nesoulad, pokud zjistí jeden z těchto nedostatků:

   a) označení CE bylo umístěno v rozporu s článkem 49;

   b) označení CE nebylo umístěno;

   c) nebylo vypracováno EU prohlášení o shodě;

   d) EU prohlášení o shodě nebylo vypracováno správně;

   e) identifikační číslo oznámeného subjektu, který je tam, kde je to relevantní, zapojen do postupu posuzování shody, nebylo umístěno.

2. Pokud nesoulad uvedený v odstavci 1 nadále trvá, přijme dotčený členský stát všechna vhodná opatření a omezí nebo zakáže dodávání vysoce rizikového systému UI na trh, nebo zajistí, aby byl tento systém stažen z oběhu nebo z trhu.

HLAVA IX

KODEXY CHOVÁNÍ

Článek 69
Kodexy chování

1. Komise a členské státy podporují a usnadňují vypracovávání kodexů chování, které mají podpořit dobrovolné uplatňování požadavků stanovených v hlavě III kapitole 2 na systémy UI jiných než vysoce rizikové systémy UI na základě technických specifikací a řešení představujících vhodné prostředky k zajištění souladu s těmito požadavky s ohledem na určený účel uvedených systémů.

2. Komise a rada podporují a usnadňují vypracovávání kodexů chování, které mají podpořit dobrovolné uplatňování požadavků týkajících se například udržitelnosti z hlediska životního prostředí, přístupnosti pro osoby se zdravotním postižením, účasti zúčastněných stran na návrhu a vývoji systémů UI a rozmanitosti vývojových týmů na systémy UI na základě jasných cílů a klíčových ukazatelů výkonnosti umožňujících měřit dosahování těchto cílů.

3. Kodexy chování mohou vypracovat jednotliví poskytovatelé systémů UI nebo organizace, které je zastupují, případně obojí, a to i za účasti uživatelů a veškerých zúčastněných stran a jejich zastupujících organizací. Kodexy chování se mohou

vztahovat na jeden nebo více systémů UI s přihlédnutím k podobnosti určeného účelu daných systémů.

4. Při podpoře a usnadňování vypracovávání kodexů chování zohlední Komise a rada konkrétní zájmy a potřeby malých poskytovatelů a začínajících podniků.

HLAVA X

DŮVĚRNOST A SANKCE

Článek 70
Důvěrnost

1. Příslušné vnitrostátní orgány a oznámené subjekty zapojené do používání tohoto nařízení zachovávají důvěrnost informací a údajů, které získají při provádění svých úkolů a činností, takovým způsobem, aby chránily zejména:

   a) práva duševního vlastnictví a důvěrné obchodní informace nebo obchodní tajemství fyzických nebo právnických osob, včetně zdrojového kódu s výjimkou případů, na které se vztahuje článek 5 směrnice 2016/943 o ochraně nezveřejněného know-how a obchodních informací (obchodního tajemství) před jejich neoprávněným získáním, využitím a zpřístupněním;

   b) účinné provádění tohoto nařízení, zejména za účelem inspekcí, šetření nebo auditů; c) veřejný zájem a zájem národní bezpečnosti;

   c) integritu trestního nebo správního řízení.

2. Aniž je dotčen odstavec 1, informace vyměňované důvěrně mezi příslušnými vnitrostátními orgány a mezi příslušnými vnitrostátními orgány a Komisí se nezpřístupní bez předchozí dohody s příslušným vnitrostátním orgánem, který informace poskytl, a uživatelem, pokud jsou vysoce rizikové systémy UI uvedené v bodech 1, 6 a 7 přílohy III používány donucovacími, imigračními nebo azylovými orgány a jejich zveřejnění by ohrozilo zájmy veřejné a vnitrostátní bezpečnosti.

   Pokud jsou uvedené donucovací, imigrační nebo azylové orgány poskytovateli vysoce rizikových systémů UI uvedených v bodech 1, 6 a 7 přílohy III, technická dokumentace uvedená v příloze IV zůstává v prostorách těchto orgánů. Tyto orgány zajistí, aby orgány dozoru nad trhem uvedené v čl. 63 odst. 5 a 6 mohly případně na požádání okamžitě získat přístup k této dokumentaci nebo obdržet její kopii. K této dokumentaci nebo k jakékoli její kopii mají přístup pouze pracovníci orgánu dozoru nad trhem, kteří mají bezpečnostní prověrku na odpovídající úrovni.

3. Ustanoveními odstavců 1 a 2 nejsou dotčena práva a povinnosti Komise, členských států a oznámených subjektů ohledně vzájemného informování a šíření výstrah, ani povinnosti dotčených stran poskytovat informace podle trestního práva členských států.

4. Komise a členské státy si mohou v případě potřeby vyměňovat důvěrné informace s regulačními orgány třetích zemí, s nimiž uzavřely dvoustranná nebo vícestranná ujednání o ochraně důvěrnosti zaručující přiměřenou úroveň důvěrnosti.

Článek 71
Sankce

1. Členské státy stanoví v souladu s podmínkami uvedenými v tomto nařízení pravidla pro ukládání sankcí, včetně správních pokut za porušení tohoto nařízení, a přijmou veškerá opatření nezbytná k zajištění jejich řádného a účinného uplatňování. Stanovené sankce musí být účinné, přiměřené a odrazující. Zohledňují zejména zájmy malých poskytovatelů a začínajících podniků a jejich ekonomickou životaschopnost.

2. Členské státy oznámí tato pravidla a opatření Komisi a neprodleně jí oznámí všechny jejich následné změny.

3. Za následující porušení předpisů lze uložit správní pokuty až do výše 30 000 000 EUR nebo, dopustí-li se porušení společnost, až do výše 6 % jejího celkového ročního obratu celosvětově za předchozí finanční rok podle toho, která hodnota je vyšší:

   a) nedodržení zákazu postupů v oblasti umělé inteligence uvedených v článku 5;

   b) nesoulad systému UI s požadavky stanovenými v článku 10.

4. Za nesoulad systému UI s jakýmikoli požadavky nebo povinnostmi podle tohoto nařízení s výjimkou těch, které jsou stanoveny v článcích 5 a 10, se uloží správní pokuty až do výše 20 000 000 EUR, nebo, dopustí-li se porušení společnost, až do výše 4 % jejího celkového ročního obratu celosvětově za předchozí finanční rok podle toho, která hodnota je vyšší.

5. Za poskytnutí nesprávných, neúplných nebo zavádějících informací oznámeným subjektům a příslušným vnitrostátním orgánům v reakci na žádost se uloží správní pokuty až do výše 10 000 000 EUR, nebo, dopustí-li se porušení společnost, až do výše 2 % jejího celkového ročního obratu celosvětově za předchozí finanční rok podle toho, která hodnota je vyšší.

6. Při rozhodování o výši správní pokuty v jednotlivých případech se zohlední všechny příslušné okolnosti konkrétní situace s náležitým přihlédnutím k následujícím okolnostem:

   a) povaha, závažnost a doba trvání porušení těchto ustanovení a jeho následky;

   b) zda již byly stejnému provozovateli za stejné protiprávní jednání uloženy správní pokuty jinými orgány dozoru nad trhem;

   c) velikost provozovatele, který se porušení dopustil, a jeho podíl na trhu.

7. Každý členský stát stanovuje pravidla týkající se toho, zda a do jaké míry je možno ukládat správní pokuty orgánům veřejné moci a veřejným subjektům usazeným v daném členském státě.

8. V závislosti na právním systému členských států lze pravidla pro správní pokuty použít tak, aby pokuty byly ukládány příslušnými vnitrostátními soudy jiných orgánů dle úpravy platné v těchto členských státech. Uplatňování těchto pravidel v uvedených členských státech má rovnocenný účinek.

Článek 72

Správní pokuty ukládané orgánům, institucím a subjektům Unie

1. Evropský inspektor ochrany údajů může ukládat správní pokuty orgánům, institucím a subjektům Unie, které spadají do oblasti působnosti tohoto nařízení. Při rozhodování o tom, zda uložit správní pokutu, a rozhodování o výši správní pokuty v jednotlivých případech se zohlední všechny příslušné okolnosti konkrétní situace s náležitým přihlédnutím k následujícím okolnostem:

   a) povaha, závažnost a doba trvání porušení těchto ustanovení a jeho následky;

   b) spolupráce s evropským inspektorem ochrany údajů za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků, včetně splnění případných opatření, která dříve nařídil evropský inspektor ochrany údajů dotčené instituci, orgánu nebo subjektu Unie v souvislosti s touž záležitostí;

   c) všechna podobná předchozí porušení ze strany orgánu, instituce nebo subjektu Unie.

2. Za porušení následujících ustanovení lze uložit správní pokuty až do výše 500 000 EUR:

   a) nedodržení zákazu postupů v oblasti umělé inteligence uvedených v článku 5;

   b) nesoulad systému UI s požadavky stanovenými v článku 10.

3. Za nesoulad systému UI s jakýmikoli požadavky nebo povinnostmi podle tohoto nařízení s výjimkou těch, které jsou stanoveny v článcích 5 a 10, se uloží správní pokuty až do výše 250 000 EUR.

4. Před přijetím rozhodnutí podle tohoto článku poskytne evropský inspektor ochrany údajů orgánu, instituci nebo subjektu Unie, se kterým vede řízení, příležitost vyjádřit své stanovisko k záležitosti týkající se daného možného porušení. Evropský inspektor ochrany údajů zakládá své rozhodnutí pouze na prvcích a okolnostech, ke kterým se dotčené osoby mohly vyjádřit. Případní stěžovatelé jsou do řízení úzce zapojeni.

5. Při řízení se plně dodrží právo dotčených stran na obhajobu. Musí mít přístup do spisu evropského inspektora ochrany údajů, s výhradou oprávněného zájmu jednotlivců nebo podniků na ochraně jejich osobních údajů nebo obchodního tajemství.

6. Prostředky vybrané ukládáním pokut podle tohoto článku jsou příjmem souhrnného rozpočtu Unie.

HLAVA XI

PŘENESENÍ PRAVOMOCI A POSTUP PROJEDNÁVÁNÍ VE VÝBORU

Článek 73

Výkon přenesené pravomoci

1. Pravomoc přijímat akty v přenesené pravomoci je svěřena Komisi za podmínek stanovených v tomto článku.

2. Pravomoc přijímat akty v přenesené pravomoci uvedená v článku 4, v čl. 7 odst. 1, čl. 11 odst. 3, čl. 43 odst. 5 a 6 a v čl. 48 odst. 5 je svěřena Komisi na dobu neurčitou od [*vstupu tohoto nařízení v platnost*].

3. Evropský parlament nebo Rada mohou přenesení pravomocí uvedené v článku 4, v čl. 7 odst. 1, čl. 11 odst. 3, čl. 43 odst. 5 a 6 a v čl. 48 odst. 5 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomoci v něm blíže určené. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v *Úředním věstníku Evropské unie* nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.

4. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.

5. Akt v přenesené pravomoci přijatý podle článku 4, čl. 7 odst. 1, čl. 11 odst. 3, čl. 43 odst. 5 a 6 a čl. 48 odst. 5 vstoupí v platnost, pouze pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě tří měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o tři měsíce.

Článek 74
Postup projednávání ve výboru

1. Komisi je nápomocen výbor. Tento výbor je výborem ve smyslu nařízení (EU) č. 182/2011.

2. Odkazuje-li se na tento odstavec, použije se článek 5 nařízení (EU) č. 182/2011.

HLAVA XII

ZÁVĚREČNÁ USTANOVENÍ

Článek 75
Změna nařízení (ES) č. 300/2008

V čl. 4 odst. 3 nařízení (ES) č. 300/2008 se doplňuje nový pododstavec, který zní:

„Při přijímání podrobných prováděcích opatření týkajících se technických specifikací a postupů pro schvalování a používání bezpečnostního vybavení ve vztahu k systémům umělé inteligence ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [o umělé inteligenci]*, se zohledňují požadavky uvedené v kapitole 2 hlavě III uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

Článek 76
Změna nařízení (EU) č. 167/2013

V čl. 17 odst. 5 nařízení (EU) č. 167/2013 se doplňuje nový pododstavec, který zní:

„Při přijímání aktů v přenesené pravomoci podle prvního pododstavce týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [o umělé inteligenci]*, se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

Článek 77
Změna nařízení (EU) č. 168/2013

V čl. 22 odst. 5 nařízení (EU) č. 168/2013 se doplňuje nový pododstavec, který zní:

„Při přijímání aktů v přenesené pravomoci podle prvního pododstavce týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [o umělé inteligenci]*, se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

Článek 78
Změna směrnice 2014/90/EU

V článku 8 směrnice 2014/90/EU se doplňuje nový odstavec, který zní:

„4. Pro systémy umělé inteligence, které představují součásti ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [o umělé inteligenci]* zohlední Komise při provádění svých činností podle odstavce 1 a při přijímání technických specifikací a zkušebních norem v souladu s odstavci 2 a 3 požadavky stanovené v hlavě III kapitole 2 uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

Článek 79
Změna směrnice (EU) 2016/797

V článku 5 směrnice (EU) 2016/797 se doplňuje nový odstavec, který zní:

„12. Při přijímání aktů v přenesené pravomoci podle odstavce 1 a prováděcích aktů podle odstavce 11 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [o umělé inteligenci]* se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

Článek 80
Změny nařízení (EU) 2018/858

V článku 5 nařízení (EU) 2018/858 se doplňuje nový odstavec, který zní:

„4. Při přijímání aktů v přenesené pravomoci podle odstavce 3 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [o umělé inteligenci] *, se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

Článek 81
Změny nařízení (EU) 2018/1139

Nařízení (EU) 2018/1139 se mění takto:

1) V článku 17 se doplňuje nový odstavec, který zní:

„3. Aniž je dotčen odstavec 2, zohledňují se při přijímání prováděcích aktů podle odstavce 1 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [*o umělé inteligenci*]*, požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

2) V článku 19 se doplňuje nový odstavec, který zní:

„4. Při přijímání aktů v přenesené pravomoci podle odstavců 1 a 2 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení (EU) YYY/XX [o umělé inteligenci], se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.“

3) V článku 43 se doplňuje nový odstavec, který zní:

„4. Při přijímání prováděcích aktů podle odstavce 1 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení (EU) YYY/XX [o umělé inteligenci], se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.“

4) V článku 47 se doplňuje nový odstavec, který zní:

„3. Při přijímání aktů v přenesené pravomoci podle odstavců 1 a 2 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení (EU) YYY/XX [o umělé inteligenci], se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.“

5) V článku 57 se doplňuje nový odstavec, který zní:

„Při přijímání těchto prováděcích aktů týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení (EU) YYY/XX [o umělé inteligenci], se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.“

6) V článku 58 se doplňuje nový odstavec, který zní:

„3. Při přijímání aktů v přenesené pravomoci podle odstavců 1 a 2 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení (EU) YYY/XX [o umělé inteligenci], se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.“

Článek 82
Změny nařízení (EU) 2019/2144

V článku 11 nařízení (EU) 2019/2144 se doplňuje nový odstavec, který zní:

„3. Při přijímání prováděcích aktů podle odstavce 2 týkajících se systémů umělé inteligence, které představují bezpečnostní součásti ve smyslu nařízení Evropského parlamentu a Rady (EU) YYY/XX [o umělé inteligenci]*, se zohledňují požadavky uvedené v hlavě III kapitole 2 uvedeného nařízení.

_____

* nařízení (EU) YYY/XX [o umělé inteligenci] (Úř. věst. …).“

Článek 83
Systémy UI, které již byly uvedeny na trh nebo do provozu

1. Toto nařízení se nevztahuje na systémy UI, které jsou součástmi rozsáhlých informačních systémů zřízených právními akty uvedenými v příloze IX a které byly uvedeny na trh nebo do provozu před *[12 měsíci od data použitelnosti tohoto nařízení uvedeného v čl. 85 odst. 2)]*, pokud nahrazení nebo změna těchto právních aktů nevede k významné změně návrhu nebo určeného účelu dotčeného systému UI nebo dotčených systémů UI.

   Požadavky stanovené v tomto nařízení se tam, kde je to relevantní, zohlední při hodnocení všech rozsáhlých informačních systémů zřízených právními akty uvedenými v příloze IX, které se má provádět v souladu s těmito příslušnými akty.

2. Toto nařízení se vztahuje na vysoce rizikové systémy UI jiné než ty, jež upravuje odstavec 1, které byly uvedeny na trh nebo do provozu před [*datem použitelnosti tohoto nařízení uvedeným v čl. 85 odst. 2*], pouze pokud po uvedeném datu dojde k významným změnám návrhu nebo určeného účelu těchto systémů.

Článek 84
Hodnocení a přezkum

1. Komise posuzuje potřebu změny seznamu uvedeného v příloze III jednou ročně po vstupu tohoto nařízení v platnost.

2. Do [*tří let od data použitelnosti tohoto nařízení uvedeného v čl. 85 odst. 2*] a poté každé čtyři roky předloží Komise Evropskému parlamentu a Radě zprávu o hodnocení a přezkumu tohoto nařízení. Tyto zprávy se zveřejní.

3. Zprávy uvedené v odstavci 2 věnují obzvláštní pozornost následujícím skutečnostem:

   a) stavu finančních a lidských zdrojů příslušných vnitrostátních orgánů určených na účinné plnění úkolů, kterými byly tyto orgány pověřeny podle tohoto nařízení;

   b) stavu sankcí, a zejména správních pokut uvedených v čl. 71 odst. 1, které členské státy uplatňují v případě porušení ustanovení tohoto nařízení.

4. Do [*tří let od data použitelnosti tohoto nařízení uvedeného v čl. 85 odst. 2*] a poté každé čtyři roky zhodnotí Komise dopad a účinnost kodexů chování, které mají podpořit uplatňování požadavků stanovených v hlavě III kapitole 2, a případně dalších požadavků na systémy UI, které nejsou vysoce rizikové.

5. Pro účely odstavců 1 až 4 poskytuje rada, členské státy a příslušné vnitrostátní orgány Komisi na její žádost příslušné informace.

6. Při provádění hodnocení a přezkumů podle odstavců 1 až 4 zohlední Komise postoje a zjištění rady, Evropského parlamentu, Rady a dalších příslušných subjektů nebo zdrojů.

7. Komise v případě potřeby předloží vhodné návrhy na změnu tohoto nařízení, zejména s přihlédnutím k vývoji technologií a dosaženému pokroku v informační společnosti.

Článek 85
Vstup v platnost a použitelnost

1. Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

2. Toto nařízení se použije [24 měsíců od vstupu tohoto nařízení v platnost].

3. Odchylně od odstavce 2:

   a) hlava III kapitola 4 a hlava VI se použijí ode dne [*tři měsíce od vstupu tohoto nařízení v platnost*];

   b) článek 71 se použije ode dne [dvanáct měsíců od vstupu tohoto nařízení v platnost].

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne

Za Evropský parlament	*Za Radu*
předseda	*předseda/předsedkyně*

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

1.2. Příslušné oblasti politik

1.3. Povaha návrhu/podnětu

1.4. Cíle

1.4.1. Obecné cíle

1.4.2. Specifické cíle

1.4.3. Očekávané výsledky a dopady

1.4.4. Ukazatele výkonnosti

1.5. Odůvodnění návrhu/podnětu

1.5.1. Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu, včetně podrobného harmonogramu pro zahajovací fázi provádění podnětu

1.5.2. Přidaná hodnota ze zapojení Unie (může být důsledkem různých faktorů, např. přínosů z koordinace, právní jistoty, vyšší účinnosti nebo doplňkovosti). Pro účely tohoto bodu se „přidanou hodnotou ze zapojení Unie“ rozumí hodnota plynoucí ze zásahu Unie, jež doplňuje hodnotu, která by jinak vznikla činností samotných členských států.

1.5.3. Závěry vyvozené z podobných zkušeností v minulosti

1.5.4. Slučitelnost s víceletým finančním rámcem a možné synergie s dalšími vhodnými nástroji

1.5.5 Posouzení různých dostupných možností financování, včetně prostoru pro přerozdělení prostředků

1.6. Doba trvání a finanční dopad návrhu/podnětu

1.7. Předpokládaný způsob řízení

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

2.2. Systém řízení a kontroly

2.2.1. Odůvodnění navrhovaných způsobů řízení, mechanismů provádění financování, způsobů plateb a kontrolní strategie

2.2.2. Informace o zjištěných rizicích a systémech vnitřní kontroly zřízených k jejich zmírnění

2.2.3. Odhad a odůvodnění nákladové efektivnosti kontrol (poměr „náklady na kontroly ÷ hodnota souvisejících spravovaných finančních prostředků“) a posouzení očekávané míry rizika výskytu chyb (při platbě a při uzávěrce)

2.3. Opatření k zamezení podvodů a nesrovnalostí

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

3.2. Odhadovaný finanční dopad návrhu na prostředky

3.2.1. Odhadovaný souhrnný dopad na operační prostředky

3.2.2. Odhadovaný výstup financovaný z operačních prostředků

3.2.3. Odhadovaný souhrnný dopad na správní prostředky

3.2.4. Slučitelnost se stávajícím víceletým finančním rámcem

3.2.5. Příspěvky třetích stran

3.3. Odhadovaný dopad na příjmy

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

Nařízení Evropského parlamentu a Rady, kterým se stanoví harmonizovaná pravidla týkající se umělé inteligence (akt o umělé inteligenci) a mění určité legislativní akty Unie

1.2. Příslušné oblasti politik

Komunikační sítě, obsah a technologie;

vnitřní trh, průmysl, podnikání a malé a střední podniky.

Dopad na rozpočet se týká nových úkolů svěřených Komisi, včetně podpory rady EU pro UI.

Aktivita: formování digitální budoucnosti Evropy.

1.3. Povaha návrhu/podnětu

X **nové akce**

☐ **nové akce následující po pilotním projektu / přípravné akci**[64]

☐ **prodloužení stávající akce**

☐ **akce přesměrované na jinou akci**

1.4. Cíle

1.4.1. Obecné cíle

Obecným cílem zásahu je zajistit řádné fungování jednotného trhu vytvořením podmínek pro rozvoj a využívání důvěryhodné umělé inteligence v Unii.

1.4.2. Specifické cíle

Specifický cíl č. 1

Stanovit požadavky specifické pro systémy UI a povinnosti všech účastníků hodnotového řetězce s cílem zajistit, aby systémy UI, které jsou uváděny na trh a používány, byly bezpečné a aby dodržovaly stávající právní předpisy o základních právech a hodnotách Unie.

Specifický cíl č. 2

Zajistit právní jistotu s cílem usnadnit investice a inovace v oblasti UI na základě vyjasnění, jaké základní požadavky, povinnosti a postupy pro zajištění shody a souladu je třeba dodržovat při uvádění systému UI na trh Unie nebo jeho používání na tomto trhu.

Specifický cíl č. 3

Zlepšit správu a účinné vymáhání stávajících právních předpisů upravujících základní práva a bezpečnostní požadavky na systémy UI tím, že příslušným orgánům budou poskytnuty nové pravomoci, zdroje a jasná pravidla ohledně postupů

[64] Uvedené v čl. 54 odst. 2 písm. a) nebo b) finančního nařízení.

posuzování shody a monitorování *ex post*, a rozdělením úkolů správy a dohledu mezi vnitrostátní úroveň a úroveň EU.

Specifický cíl č. 4

Usnadnit rozvoj jednotného trhu pro zákonné, bezpečné a důvěryhodné aplikace UI a zabránit roztříštění trhu tím, že bude přijato opatření EU s cílem stanovit minimální požadavek na uvádění systémů UI na trh Unie a jejich používání na tomto trhu v souladu se stávajícími právními předpisy o základních právech a bezpečnosti.

1.4.3. Očekávané výsledky a dopady

Upřesněte účinky, které by návrh/podnět měl mít na příjemce / cílové skupiny.

Přínosem pro dodavatele UI by měl být minimální, ale jasný soubor požadavků, který vytvoří právní jistotu a zajistí přístup na celý jednotný trh.

Přínosem pro uživatele UI by měla být právní jistota, že vysoce rizikové systémy UI, které kupují, jsou v souladu s evropskými právními předpisy a hodnotami.

Přínosem pro spotřebitele by mělo být snížení rizika porušování jejich bezpečnosti nebo základních práv.

1.4.4. Ukazatele výkonnosti

Upřesněte ukazatele, podle kterých je možno uskutečňování návrhu/podnětu sledovat.

Ukazatel 1

Počet závažných incidentů nebo případů činnosti UI, které představují závažný incident nebo porušení povinností v oblasti základních práv (pololetně), podle oblastí aplikace a vypočtený a) v absolutních číslech, b) jako podíl nasazených aplikací a c) jako podíl zúčastněných občanů.

Ukazatel 2

a) Investice do UI v EU celkem (ročně);

b) investice do UI celkem podle členských států (ročně);

c) podíl společností využívajících UI (ročně);

d) podíl malých a středních podniků využívajících UI (ročně).

a) a b) se vypočtou na základě oficiálních zdrojů a porovnají se se soukromými odhady

c) a d) budou shromážděny na základě pravidelných průzkumů společností

1.5. Odůvodnění návrhu/podnětu

1.5.1. Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu, včetně podrobného harmonogramu pro zahajovací fázi provádění podnětu

Nařízení by mělo být v plném rozsahu použitelné jeden a půl roku po přijetí. Některé prvky struktury řízení by však měly být zavedeny ještě dříve. Členské státy mají již jmenovány stávající orgány a/nebo zřízeny nové orgány, které plní úkoly stanovené již dříve v právních předpisech, a měla by být zřízena a měla by fungovat rada EU pro UI. Evropská databáze systémů UI by měla být k datu použitelnosti již plně funkční. Souběžně s procesem přijímání je proto nezbytné vytvořit databázi tak, aby při vstupu nařízení v platnost byl její vývoj již dokončen.

1.5.2. Přidaná hodnota ze zapojení Unie (může být důsledkem různých faktorů, např. přínosů z koordinace, právní jistoty, vyšší účinnosti nebo doplňkovosti). Pro účely tohoto bodu se „přidanou hodnotou ze zapojení Unie“ rozumí hodnota plynoucí ze zásahu Unie, jež doplňuje hodnotu, která by jinak vznikla činností samotných členských států.

Vznikající nejednotný rámec potenciálně rozdílných vnitrostátních pravidel bude brzdit bezproblémové poskytování systémů UI v celé EU a je neúčinný při zajišťování bezpečnosti a ochrany základních práv a hodnot Unie v jednotlivých

členských státech. Společné legislativní opatření EU v oblasti UI by mohlo posílit vnitřní trh a má velký potenciál poskytnout evropskému průmyslu konkurenční výhodu v celosvětovém měřítku a úspory z rozsahu, kterých nelze dosáhnout pouze na úrovni jednotlivých členských států.

1.5.3. Závěry vyvozené z podobných zkušeností v minulosti

Směrnice 2000/31/ES o elektronickém obchodu poskytuje hlavní rámec pro fungování jednotného trhu a dohled nad digitálními službami a stanoví základní strukturu pro obecný mechanismus spolupráce mezi členskými státy zahrnující v zásadě všechny požadavky, které se na digitální služby vztahují. Hodnocení směrnice poukázalo na nedostatky v několika aspektech tohoto mechanismu spolupráce, včetně důležitých procesních aspektů, jako je nedostatek jasných časových rámců pro reakci ze strany členských států a obecná nedostatečná schopnost reagovat na žádosti jejich protějšků. To v průběhu let vyústilo v nedostatek důvěry mezi členskými státy ohledně řešení obav týkajících se poskytovatelů, kteří nabízejí přeshraniční digitální služby. Hodnocení směrnice poukázalo na potřebu vytvořit diferencovaný soubor pravidel a požadavků na evropské úrovni. Z tohoto důvodu by provádění konkrétních povinností stanovených v tomto nařízení vyžadovalo zvláštní mechanismus spolupráce na úrovni EU se strukturou řízení, která by zajišťovala koordinaci konkrétních odpovědných orgánů na úrovni EU.

1.5.4. Slučitelnost s víceletým finančním rámcem a možné synergie s dalšími vhodnými nástroji

Nařízení, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění určité legislativní akty Unie, vymezuje nový společný rámec požadavků vztahujících se na systémy UI, jenž značně přesahuje rámec stanovený stávajícími právními předpisy. Z tohoto důvodu je nutné tímto návrhem zavést novou vnitrostátní a evropskou funkci v oblasti regulace a koordinace.

S ohledem na možné synergie s jinými vhodnými nástroji mohou úlohu oznamujících orgánů na vnitrostátní úrovni plnit vnitrostátní orgány, které již podobné funkce plní podle jiných nařízení EU.

Toto nařízení navíc tím, že zvyšuje důvěru v UI a tak podporuje investice do rozvoje a přijímání UI, doplňuje program Digitální Evropa, který má podporu šíření UI jako jednu ze svých pěti priorit.

1.5.5. Posouzení různých dostupných možností financování, včetně prostoru pro přerozdělení prostředků

Zaměstnanci budou přeloženi z jiných oddělení; ostatní náklady budou podporovány z rámce na program Digitální Evropa vzhledem k tomu, že cíl tohoto nařízení – zajištění důvěryhodné UI – přímo přispívá k jednomu z klíčových cílů digitální Evropy – zrychlení vývoje UI a její zavedení v Evropě.

1.6. Doba trvání a finanční dopad návrhu/podnětu

☐ **Časově omezená doba trvání**

– ☐ s platností od [DD.MM.]RRRR do [DD.MM.]RRRR,

– ☐ finanční dopad od RRRR do RRRR u prostředků na závazky a od RRRR do RRRR u prostředků na platby.

X **Časově neomezená doba trvání**

– Provádění s obdobím rozběhu od roku jedna/dva (potřeba doplnit),

– poté plné fungování.

1.7. Předpokládaný způsob řízení[65]

X **Přímé řízení** Komisí

– ☐ prostřednictvím jejích útvarů, včetně jejích zaměstnanců v delegacích Unie,

– ☐ prostřednictvím výkonných agentur.

☐ **Sdílené řízení** s členskými státy

☐ **Nepřímé řízení**, při kterém jsou úkoly souvisejícími s plněním rozpočtu pověřeny:

– ☐ třetí země nebo subjekty určené těmito zeměmi,

– ☐ mezinárodní organizace a jejich agentury (upřesněte),

– ☐ EIB a Evropský investiční fond,

– ☐ subjekty uvedené v článcích 70 a 71 finančního nařízení,

– ☐ veřejnoprávní subjekty,

– ☐ soukromoprávní subjekty pověřené výkonem veřejné služby v rozsahu, v jakém poskytují dostatečné finanční záruky,

– ☐ soukromoprávní subjekty členského státu pověřené uskutečňováním partnerství soukromého a veřejného sektoru a poskytující dostatečné finanční záruky,

– ☐ osoby pověřené prováděním specifických akcí v rámci společné zahraniční a bezpečnostní politiky podle hlavy V Smlouvy o EU a určené v příslušném základním právním aktu.

– *Pokud vyberete více způsobů řízení, upřesněte je v části „Poznámky“.*

Poznámky

[65] Vysvětlení způsobů řízení spolu s odkazem na finanční nařízení jsou k dispozici na stránkách BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

Upřesněte četnost a podmínky.

Nařízení bude přezkoumáno a hodnoceno pět let od svého vstupu v platnost. Komise předloží zprávu o zjištěních při tomto hodnocení Evropskému parlamentu, Radě a Evropskému hospodářskému a sociálnímu výboru.

2.2. Systémy řízení a kontroly

2.2.1. Odůvodnění navrhovaných způsobů řízení, mechanismů provádění financování, způsobů plateb a kontrolní strategie

Nařízení zavádí novou politiku s ohledem na harmonizovaná pravidla pro poskytování systémů umělé inteligence na vnitřním trhu, přičemž současně zajišťuje dodržování bezpečnosti a základních práv. Tato nová pravidla vyžadují mechanismus jednotnosti pro přeshraniční uplatňování povinností podle tohoto nařízení v podobě nové poradní skupiny koordinující činnosti vnitrostátních orgánů. K plnění těchto nových úkolů je nutné poskytnout útvarům Komise náležité zdroje. Vymáhání nového nařízení bude podle odhadu vyžadovat deset ekvivalentů plného pracovního úvazku (FTE) na režim (pět FTE na podporu činností rady a pět FTE pro evropského inspektora ochrany údajů, který funguje jako oznámený subjekt pro systémy UI zavedené orgánem Evropské unie).

2.2.2. Informace o zjištěných rizicích a systémech vnitřní kontroly zřízených k jejich zmírnění

Aby bylo zajištěno, že členové rady mohou provádět informovanou analýzu na základě faktických důkazů, předpokládá se, že by radu měla podporovat správní struktura Komise a že by měla být vytvořena odborná skupina, která v případě potřeby poskytne další odborné znalosti.

2.2.3. Odhad a odůvodnění nákladové efektivnosti kontrol (poměr „náklady na kontroly ÷ hodnota souvisejících spravovaných finančních prostředků“) a posouzení očekávané míry rizika výskytu chyb (při platbě a při uzávěrce)

Pokud jde o výdaje na zasedání, vzhledem k nízké hodnotě na transakci (například úhrada cestovních nákladů delegátovi vyslanému na zasedání) se jeví jako dostatečné standardní kontrolní postupy. Pokud jde o vytváření databáze, má GŘ CNECT zaveden silný systém vnitřních kontrol přidělování zakázek prostřednictvím centralizovaného zadávání zakázek.

2.3. Opatření k zamezení podvodů a nesrovnalostí

Upřesněte stávající či předpokládaná preventivní a ochranná opatření, např. opatření uvedená ve strategii pro boj proti podvodům.

Stávající opatření k předcházení podvodům vztahující se na Komisi budou zahrnovat dodatečné prostředky potřebné pro toto nařízení.

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

- Stávající rozpočtové položky

V pořadí okruhů víceletého finančního rámce a rozpočtových položek.

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdaje	Příspěvek			
	Číslo	RP/NRP[66].	zemí ESVO[67]	kandidátských zemí[68]	třetích zemí	ve smyslu čl. 21 odst. 2 písm. b) finančního nařízení
7	20 02 06 Správní výdaje	NRP	NE	NE	NE	NE
1	02 04 03 Program Digitální Evropa – umělá inteligence	RP	ANO	NE	NE	NE
1	02 01 30 01 Výdaje na podporu programu Digitální Evropa	NRP	ANO	NE	NE	NE

3.2. Odhadovaný finanční dopad návrhu na prostředky

3.2.1. Odhadovaný finanční dopad návrhu na výdaje z operačních prostředků

– ☐ Návrh/podnět nevyžaduje využití operačních prostředků.

– X Návrh/podnět vyžaduje využití operačních prostředků, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

66 RP = rozlišené prostředky / NRP = nerozlišené prostředky.

67 ESVO: Evropské sdružení volného obchodu.

68 Kandidátské země a tam, kde je to relevantní, potenciální kandidátské země západního Balkánu.

Okruh víceletého finančního rámce	1	

GŘ: CNECT				Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**[69]	**CELKEM**	
• Operační prostředky											
Rozpočtová položka[70] 02 04 03		Závazky	(1a)		1,000						**1,000**
		Platby	(2a)		0,600	0,100	0,100	0,100	0,100		**1,000**
Rozpočtová položka		Závazky	(1b)								
		Platby	(2b)								
Prostředky správní povahy financované z rámce na zvláštní programy[71]											
Rozpočtová linie 02 01 30 01			(3)		0,240	0,240	0,240	0,240	0,240		**1,200**
Prostředky na GŘ <…….> CELKEM GŘ CNECT		Závazky	=1a+1b +3		**1,240**		**0,240**	**0,240**	**0,240**		**2,200**
		Platby	=2a+2b +3		**0,840**	**0,340**	**0,340**	**0,340**	**0,340**		**2,200**

• Operační prostředky CELKEM	Závazky	(4)		1,000						**1,000**
	Platby	(5)		0,600	0,100	0,100	0,100	0,100		**1,000**

69 Orientační a závislé na dostupnosti rozpočtu.

70 Podle oficiální rozpočtové nomenklatury.

71 Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

• Prostředky správní povahy financované z rámce na zvláštní programy CELKEM		(6)		**0,240**	**0,240**	**0,240**	**0,240**	**0,240**		**1,200**
CELKEM prostředky z OKRUHU 1 víceletého finančního rámce	Závazky	=4+6		1,240	0,240	0,240	.0.240	0,240		**2,200**
	Platby	=5+6		0,840	0,340	0,340	0,340	0,340		**2,200**

Pokud je návrhem/podnětem dotčen více než jeden okruh, zopakuje se výše uvedený oddíl:

• Operační prostředky CELKEM (všechny operační okruhy)	Závazky	(4)								
	Platby	(5)								
• Prostředky správní povahy financované z rámce na zvláštní programy (všechny operační okruhy) CELKEM		(6)								
Prostředky z OKRUHŮ 1 až 6 víceletého finančního rámce **CELKEM** (referenční částka)	Závazky	=4+6								
	Platby	=5+6								

Okruh víceletého finančního rámce	7	Správní výdaje

Tento oddíl se vyplní pomocí „rozpočtových údajů správní povahy“, jež se nejprve uvedou v příloze legislativního finančního výkazu (příloha V interních pravidel), která se pro účely konzultace mezi útvary vloží do aplikace DECIDE.

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**Po roce 2027**[72]	**CELKEM**
GŘ: CNECT								
• Lidské zdroje		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Ostatní správní výdaje		**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,050**
CELKEM GŘ CNECT	**Prostředky**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,850**
Evropský inspektor ochrany údajů								
• Lidské zdroje		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Ostatní správní výdaje								
EIOÚ CELKEM	**Prostředky**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,800**
Prostředky z OKRUHU 7 víceletého finančního rámce **CELKEM**	(Závazky celkem = platby celkem)	1,530	1,530	1,530	1,530	1,530	1,530	**7,650**

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**		**CELKEM**
Prostředky z OKRUHŮ 1 až 7	Závazky		2,770	1,770	1,770	1,770	1,770		**9,850**

[72] Všechny údaje v tomto sloupci jsou orientační a jsou podmíněny pokračováním programů a dostupností prostředků.

víceletého finančního rámce **CELKEM**	Platby		2,370	1,870	1,870	1,870	1,870	**9,850**

3.2.2. Odhadovaný výstup financovaný z operačních prostředků

Prostředky na závazky v milionech EUR (zaokrouhleno na tři desetinná místa)

Uveďte cíle a výstupy ⇩			Rok **2022**		Rok **2023**		Rok **2024**		Rok **2025**		Rok **2026**		Rok **2027**		Po roce **2027**[73]		**CELKEM**	
	VÝSTUPY																	
	Druh	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL č. 1[74]…																		
Databáze					1	1,000	1		1		1		1		1	0,100	1	1,000
Zasedání – výstup					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Komunikační činnosti					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Mezisoučet za specifický cíl č. 1																		
SPECIFICKÝ CÍL č. 2 …																		
– Výstup																		
Mezisoučet za specifický cíl č. 2																		
CELKEM					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

[73] Všechny údaje v tomto sloupci jsou orientační a jsou podmíněny pokračováním programů a dostupností prostředků.

[74] Popsaný v bodě 1.4.2. „Specifické cíle…“.

3.2.3. Odhadovaný souhrnný dopad na správní prostředky

– ☐ Návrh/podnět nevyžaduje využití prostředků správní povahy.

– X Návrh/podnět vyžaduje využití prostředků správní povahy, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **2022**	Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**Ročně po roce 2027**[75]	**CELKEM**
OKRUH 7 víceletého finančního rámce								
Lidské zdroje		1,520	1,520	1,520	1,520	1,520	**1,520**	**7,600**
Ostatní správní výdaje		0,010	0,010	0,010	0,010	0,010	**0,010**	**0,050**
Mezisoučet za OKRUH 7 víceletého finančního rámce		1,530	1,530	1,530	1,530	1,530	**1,530**	**7,650**
Mimo OKRUH 7[76] **of the multiannual financial framework**								
Lidské zdroje								
Ostatní výdaje správní povahy		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
Mezisoučet mimo OKRUH 7 víceletého finančního rámce		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
CELKEM		**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**8,850**

Potřebné prostředky na oblast lidských zdrojů a na ostatní výdaje správní povahy budou pokryty z prostředků GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přerozděleny v rámci GŘ a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

75 Všechny údaje v tomto sloupci jsou orientační a jsou podmíněny pokračováním programů a dostupností prostředků.

76 Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

3.2.3.1. Odhadované potřeby v oblasti lidských zdrojů

– ☐ Návrh/podnět nevyžaduje využití lidských zdrojů.

– X Návrh/podnět vyžaduje využití lidských zdrojů, jak je vysvětleno dále:

Odhad vyjádřete v přepočtu na plné pracovní úvazky

.		Rok **2023**	Rok **2024**	Rok **2025**	**2026**	**2027**	**Po roce 2027**[77]	
• Pracovní místa podle plánu pracovních míst (místa úředníků a dočasných zaměstnanců)								
20 01 02 01 (v ústředí a v zastoupeních Komise)		10	10	10	10	10	10	
20 01 02 03 (při delegacích)								
01 01 01 01 (v nepřímém výzkumu)								
01 01 01 11 (v přímém výzkumu)								
Jiné rozpočtové položky (upřesněte)								
• Externí zaměstnanci (v přepočtu na plné pracovní úvazky: FTE)[78]								
20 02 01 (SZ, VNO, ZAP z celkového rámce)								
20 02 03 (SZ, MZ, VNO, ZAP a MOD při delegacích)								
XX 01 xx **yy zz**[79]	– v ústředí							
	– při delegacích							
01 01 01 02 (SZ, VNO, ZAP v nepřímém výzkumu)								
01 01 01 12 (SZ, VNO, ZAP v přímém výzkumu)								
Jiné rozpočtové položky (upřesněte)								
CELKEM		**10**	**10**	**10**	**10**	**10**	**10**	

XX je oblast politiky nebo dotčená hlava rozpočtu.

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ, které jsou již vyčleněny na řízení akce a/nebo byly vnitřně přeobsazeny v rámci GŘ, a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Předpokládá se, že polovinu požadovaných zdrojů poskytne EIOÚ.

Popis úkolů:

Úředníci a dočasní zaměstnanci	Příprava celkem 13–16 zasedání, vypracování zpráv, pokračování v práci na politice, například pokud jde o budoucí změny na seznamu vysoce rizikových aplikací UI a udržování vztahů s orgány členských států, bude vyžadovat čtyři pracovní místa AD FTE a jedno pracovní místo AST FTE. Za systémy UI vyvinuté institucemi EU odpovídá evropský inspektor ochrany údajů. Na základě minulých zkušeností lze odhadnout, že ke splnění povinností EIOÚ podle legislativního návrhu bude zapotřebí 5 pracovních míst AD FTE.
Externí zaměstnanci	

[77] Všechny údaje v tomto sloupci jsou orientační a jsou podmíněny pokračováním programů a dostupností prostředků.

[78] SZ = smluvní zaměstnanec; MZ = místní zaměstnanec; VNO = vyslaný národní odborník; ZAP = zaměstnanec agentury práce; MOD = mladý odborník při delegaci.

[79] Dílčí strop na externí zaměstnance financované z operačních prostředků (bývalé položky „BA“).

3.2.4. Slučitelnost se stávajícím víceletým finančním rámcem

Návrh/podnět:

– X může být v plném rozsahu financován přerozdělením prostředků v rámci příslušného okruhu víceletého finančního rámce (VFR).

Není nutno provést žádné přeprogramování.

– ☐ vyžaduje použití nepřiděleného rozpětí v rámci příslušného okruhu VFR a/nebo použití zvláštních nástrojů definovaných v nařízení o VFR.

Upřesněte, co se požaduje, příslušné okruhy a rozpočtové položky, odpovídající částky a navrhované nástroje, které mají být použity.

– ☐ vyžaduje revizi VFR.

Upřesněte, co se požaduje, příslušné okruhy a rozpočtové položky a odpovídající částky.

3.2.5. Příspěvky třetích stran

Návrh/podnět:

– X nepočítá se spolufinancováním od třetích stran.

– ☐ počítá se spolufinancováním od třetích stran podle následujícího odhadu:

prostředky v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **N**[80]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)			Celkem
Upřesněte spolufinancující subjekt								
Spolufinancované prostředky CELKEM								

[80] Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět. Výraz „N“ nahraďte předpokládaným prvním rokem provádění (například 2021). Totéž proveďte u let následujících.

3.3. Odhadovaný dopad na příjmy

– ☐ Návrh/podnět má tento finanční dopad:

– ☐ Návrh/podnět má tento finanční dopad:

  – ☐ na jiné příjmy

  – ☐ na jiné příjmy

  – Uveďte, zda je příjem účelově vázán na výdajové položky ☐

v milionech EUR (zaokrouhleno na tři desetinná místa)

Příjmová rozpočtová položka:	Prostředky dostupné v běžném rozpočtovém roce	Dopad návrhu/podnětu[81]						
		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Vložit počet let podle trvání finančního dopadu (viz bod 1.6)		
Článek …….								

U účelově vázaných příjmů upřesněte dotčené výdajové rozpočtové položky.

Jiné poznámky (např. způsob/vzorec výpočtu dopadu na příjmy nebo jiné údaje).

[81] Pokud jde o tradiční vlastní zdroje (cla, dávky z cukru), je třeba uvést čisté částky, tj. hrubé částky po odečtení 20 % nákladů na výběr.