

Devátá státní smlouva, kterou se mění státní smlouvy o sdělovacích prostředcích

Věc: Použití technických prostředků při dohledu nad sdělovacími prostředky
Návrh na zakotvení normy ve státní smlouvě o sdělovacích prostředcích

§ 109a Použití technických prostředků při dohledu	Poznámky
(1) Orgány veřejné moci v oblasti sdělovacích prostředků mohou při zjišťování porušení zákona ve smyslu § 109 této státní smlouvy o sdělovacích prostředcích a § 20 JMStV používat technické prostředky, které automaticky porovnávají textový, obrazový, zvukový a pohyblivý obrazový obsah vysílání a telekomunikačních médií z hlediska možného porušení zákona. Věta 1 zahrnuje také obsah vysílání a telekomunikačních médií, který podléhá omezením přístupu.	Odstavec 1 stanoví základní přípustnost automatického vyhledávání a kontroly obsahu z hlediska možného porušení právních předpisů. Automatizované porovnávání zahrnuje také používání systémů založených na umělé inteligenci, na které se kromě požadavků na ochranu údajů podle odstavce 2 a násl. vztahují požadavky nařízení o umělé inteligenci. Možnost využití technických prostředků slouží k zajištění účinného a efektivního nezávislého dohledu nad médii a může rovněž přispět ke zvýšení ochrany zaměstnanců při práci s inkriminovanými materiály. V rámci oprávnění používat tyto technické prostředky jsou porušení zákona omezena na ta, která jsou zároveň předmětem dozorových opatření státních orgánů veřejné moci v oblasti sdělovacích prostředků podle § 109 MStV nebo § 20 JMStV. Automatizované porovnávání je rovněž omezeno na obsah rozhlasového vysílání a telekomunikační obsah. Pouze tyto nabídky spadají do oblasti působnosti mezistátní smlouvy o sdělovacích prostředcích a mezistátní smlouvy o ochraně nezletilých ve sdělovacích prostředcích, a podléhají proto doзору orgánů veřejné moci v oblasti sdělovacích prostředků. To zároveň omezuje srovnání s obsahem, který poskytovatel „zveřejňuje“, neboť jak vysílání, tak telekomunikační média jsou publicistickými nabídkami, které jsou na rozdíl od individuální komunikace určeny neurčitému počtu uživatelů. V tomto ohledu jsou omezeními přístupu ve smyslu věty 2 nabídky, které je třeba posuzovat jako vysílání nebo telekomunikační média, ale jsou přístupné například pouze po registraci nebo vytvoření uživatelského účtu, za systémem ověřování věku nebo paywall.
2) Údaje obsažené v textovém, obrazovém, zvukovém a pohyblivém obrazovém obsahu, včetně zvláštních kategorií osobních údajů ve smyslu čl. 9 odst. 1 nařízení (EU) 2016/679, mohou být zpracovávány v rámci automatizovaného porovnávání podle odstavce 1, pokud a v rozsahu nezbytném pro přesvědčivé posouzení obsahu. Automatizované porovnání na základě konkrétních osobních údajů není přípustné.	Porušení ve smyslu odstavce 1 je zaměřeno na obecné skutečnosti, nikoli na konkrétní osoby, takže shromažďování osobních údajů není a nesmí být středem pozornosti. Nicméně porovnávaný obsah může nevyhnutelně a nutně obsahovat osobní údaje. Za určitých okolností mohou tyto osobní údaje představovat i zvláštní kategorie osobních údajů. Zejména obrazový materiál může například obsahovat odkazy na rasový a etnický původ, politické názory, náboženské či filozofické přesvědčení nebo členství v odborech, případně může obsahovat údaje o zdravotním stavu nebo údaje týkající se sexuálního života či sexuální orientace fyzické osoby.

	Zpracování těchto údajů je proto povoleno pouze v úzkých mezích. V souladu s tím je povoleno zpracování, zejména shromažďování, pouze takových údajů, které vyplývají ze samotného odpovídajícího obsahu a jsou nezbytné k tomu, aby bylo možné obsah podle práva dozoru vůbec posoudit. Toto zpracování údajů je povoleno na základě čl. 9 odst. 2 písm. e) GDPR, pokud byly údaje subjektem údajů „zjevně zveřejněny“. Pokud však jde o zveřejněné údaje třetích stran, je vyvažování požadované podle čl. 9 odst. 2 písm. g) GDPR („podstatný veřejný zájem“) do značné míry určeno úzkou neoddělitelnou vazbou s posuzovaným obsahem a dotčenými vysokými zájmy ochrany. Obsah tedy není možné posoudit bez celkového kontextu, a proto nelze konstatovat porušení. Rovněž a zejména ve zvláště citlivých případech, např. sexuálních aktů, slouží opatření, zejména příkazy k zákazu, vymazání a zablokování ze strany orgánů veřejné moci v oblasti sdělovacích prostředků, jakož i zájmům těchto třetích osob. Pokud je možné osobní údaje oddělit, a není tedy nutné je shromažďovat, nesmí být zvláště citlivé údaje uchovávány. „Profilování“ není součástí porovnání stanoveného v odstavci 1 a nebylo by přípustné. Kromě toho je výslovně vyloučeno srovnání založené na konkrétních osobních údajích, tj. údajích týkajících se konkrétní osoby.
(3) Pokud je potenciální porušení ve smyslu odstavce 1 zjištěno pomocí technických prostředků, mohou být pomocí technických prostředků zpracovávány i následující osobní údaje související s potenciálně porušujícím obsahem, pokud je to nezbytné pro účely odstavce 4: Údaje o poskytovateli, včetně informací podle § 18, webová adresa obsahu, datum zveřejnění a čas shromáždění údajů, zeměpisné zařazení, odkazy a interakce s obsahem.	Pokud nástroj zjistí potenciální porušení zákona, které je předmětem dozorových opatření podle § 109 MStV nebo § 20 JMStV, mohou být kromě samotného obsahu shromažďovány a zpracovávány další osobní údaje, pokud je to nezbytné pro následná dozorová opatření.
(4) Zjistí-li technické prostředky možné porušení zákona ve smyslu odstavce 1, musí fyzická osoba neprodleně zkontrolovat, zda lze tuto skutečnost potvrdit; pokud tomu tak není, musí zpracovávané osobní údaje neprodleně vymazat. K výmazu podle věty 1 musí dojít nejpozději do 30 dnů, a to i v případě, že do té doby nebylo možné provést ověření.	Shromážděné údaje musí být neprodleně podrobeny lidskému přezkumu. Neexistuje-li konkrétní podezření na právní delikt, musí být údaje vymazány okamžitě. Pokud k přezkoumání nedojde, musí být údaje vymazány nejdéle po 30 dnech.
(5) Osoby podílející se na zpracování zvláštních kategorií osobních údajů musí být upozorněny na zvláštní potřebu ochrany těchto údajů. Musí být přijata vhodná technická a organizační opatření, která zajistí, aby bylo možné zpětně zkontrolovat, zda a kým byly osobní údaje ve smyslu odstavců 2 a 3 vloženy, změněny nebo odstraněny. Obecná ustanovení právních předpisů o ochraně údajů, zejména o zabezpečení osobních údajů, zůstávají jinak nedotčena.	Jsou definovány pokyny pro zabezpečení údajů. Ostatní právní předpisy o ochraně údajů (např. problematika předávání do třetích zemí, zabezpečení osobních údajů atd. zůstávají nedotčeny.

(6) Existuje-li po přezkumu podle odstavce 4 konkrétní podezření na porušení zákona, mohou být osobní údaje zpracovávány pro účely provádění opatření v oblasti dozoru podle § 109 této státní smlouvy a § 20 JMStV, jakož i pro účely trestání správních deliktů podle § 115 odst. 1 této státní smlouvy a § 24 odst. 1 a 2 JMStV. Pokud existuje podezření na trestný čin v souvislosti se znaky § 4 odst. 1 nebo odst. 2 č. 1 JMStV nebo trestný čin podle § 23 JMStV, mohou být osobní údaje předány také jiným příslušným orgánům, pokud je to nezbytné pro vyšetřování a stíhání těchto trestných činů. Použití pro jiné účely není přípustné. Osobní údaje musí být neprodleně vymazány, pokud již nejsou potřebné pro provádění dozorových opatření nebo trestání správních deliktů, a to nejpozději po 6 měsících, pokud do té doby neprobíhá žádné dozorové řízení.	Pokud existuje konkrétní podezření na porušení zákona, mohou být osobní údaje použity pro dozorová opatření a stíhání správních deliktů. Promlčecí lhůta správních deliktů tvoří hranici přípustného uchovávání. Kromě toho jsou povinnosti týkající výmazu uložených údajů, u nichž nebylo zahájeno řízení. Pokud existuje podezření ze spáchání trestného činu na základě skutkové podstaty podle § 4 odst. 1 nebo 2 odst. 1 nebo § 23 JMStV, mohou být potřebné údaje předány orgánům činným v trestním řízení.
(7) Technické prostředky ve smyslu odstavce 1 musí být založeny na vhodných algoritmech, modelech a zaučovacích údajích. Technické prostředky musí být před jejich použitím a následně pravidelně ověřovány. Školení s anonymizovanými údaji je povoleno. Použití osobních údajů pro účely zaučení technických prostředků pro použití podle odstavce 1 není přípustné; výjimky se vztahují na nezbytné osobní údaje podle odstavce 2 bodu 1 a na osoby s novodobou historií, pokud pseudonymizace není účelná nebo nepřiměřená. Anonymizace nebo pseudonymizace osobních údajů před jejich výmazem v souladu s odst. 4 první větou druhou polovinou je pro účely zaučení technického prostředku přípustná, pokud jsou údaje nezbytné pro vyšetřování porušení právních předpisů ve smyslu odstavce 1. Před použitím technických prostředků musí být provedeno posouzení vlivu na ochranu osobních údajů ve smyslu článku 35 nařízení (EU) 2016/679.	Jsou stanoveny požadavky na technické nástroje a jejich ověřování. Zejména je předepsáno pravidelné ověřování a jsou stanoveny požadavky na údaje o školení. V souladu s tím není školení s osobními údaji obecně povoleno. Aby však byla zajištěna funkčnost a přesnost takového nástroje z hlediska minimalizace údajů, musí být možné použít osobní údaje i pro školení, pokud je to nezbytné. Věta 3 stanoví odpovídající výjimku. Ta se vztahuje rovněž na nezbytné údaje o osobách současnosti, které mohou být relevantními referenčními body pro vyhledávání, zejména z důvodu historických souvislostí. Před vymazáním osobních údajů podle odstavce 4 věty 1 druhé poloviny je přípustná anonymizace osobních údajů za účelem zaučení technických nástrojů. To však za podmínky, že údaje jsou nezbytné pro použití nástroje, tj. pro zjišťování porušení práv podle odstavce 1. Procesy anonymizace musí odpovídat aktuálním standardům.
(8) Podrobnosti o typu, účelu a použití technických prostředků podle odstavce 1 upravují zemské orgány pro sdělovací prostředky společným předpisem. Použití technických prostředků musí být zdokumentováno; podstatné výsledky použití musí být každoročně zveřejněny ve zprávě. V rámci kontrolních opatření musí být dotčenému poskytovateli sděleno použití technických prostředků.	Na základě zmocnění ve stanovách jsou orgány veřejné moci zapojeny do základů koncepce a použití technických prostředků; stanovy mohou zejména blíže určit oblasti použití, dobu nebo cykly použití, způsob fungování a kategorie kritérií vyhledávání. Společný soubor předpisů zajišťuje, že zemské orgány pro sdělovací prostředky jednají podle jednotných standardů.
(9) Poskytovatelé on-line platforem ve smyslu nařízení (EU) 2022/2065 jsou povinni na žádost příslušného zemského mediálního úřadu, pokud je to technicky a ekonomicky přijatelné, poskytnout vhodné rozhraní pro použití technických prostředků podle odstavce 1. Prostřednictvím rozhraní musí být zpřístupněny výhradně údaje ve smyslu odstavců 2 a 3. Ustanovení § 109 odst. 4 a § 21 odst. 3 státní smlouvy o ochraně mládeže ve sdělovacích prostředcích se použijí	Vedle stávající povinnosti poskytovatelů povolit dohled nad jejich službami dle § 109 odst. 4 MStV a § 21 odst. 3 JMStV se zavádí zvláštní povinnost rozhraní pro použití technických prostředků. Tato povinnost se týká on-line platforem, a tedy i telekomunikačních médií, které na rozdíl od poskytovatelů obsahu a mediálních platforem nenabízejí obsah nebo celkovou nabídku, za kterou nesou výhradní odpovědnost. Jedná se v podstatě o mediální zprostředkovatele.

odpovídajícím způsobem.	Tyto telekomunikační služby podléhají režimu odpovědnosti podle nařízení (EU) 2022/2065, a jsou proto obecně vyňata z odpovědnosti za informace poskytnuté jejich uživateli. Tyto pokyny zůstávají nedotčeny. Povinnost poskytnout regulačním orgánům pro sdělovací prostředky potřebné rozhraní zajišťuje přístup k obsahu, za který jsou odpovědné třetí strany, a tím i dohled nad tímto obsahem nebo poskytovateli obsahu. Prostřednictvím rozhraní se zpřístupňují pouze příslušné, veřejně přístupné údaje uvedené v odstavcích 2 a 3, nikoli však smluvní údaje nebo údaje uložené za účty. Přístup musí být udělen bezplatně, jako v případech ustanovení § 109 odst. 4 MStV a § 21 odst. 3 JMStV.