

**VÝZVA K PŘEDLOŽENÍ FAKTICKÝCH PODKLADŮ
PRO POSOUZENÍ DOPADŮ**

NÁZEV INICIATIVY	Posouzení dopadů týkající se uchovávání údajů poskytovateli služeb pro účely trestního řízení
PŘÍSLUŠNÉ GŘ (ODPOVĚDNÉ ODDĚLENÍ)	HOME.D4
PRAVDĚPODOBNÝ DRUH INICIATIVY	
PŘEDBĚŽNÝ HARMONOGRAM	1. čtvrtletí roku 2026
DALŠÍ INFORMACE	Kyberkriminalita – Evropská komise ; Skupina na vysoké úrovni pro přístup k údajům pro účely účinného prosazování práva – Evropská komise

A. Politické souvislosti, vymezení problému a kontrola subsidiarity**Politické souvislosti**

Aby mohly policejní a soudní orgány účinně bojovat proti trestným činům a stíhat je, mohou potřebovat přístup k určitým neobsahovým údajům zpracovávaným poskytovateli služeb elektronické komunikace. Pokud neexistují zvláštní povinnosti ukládající těmto poskytovatelům, aby uchovávali údaje po přiměřenou a omezenou dobu, mohou být údaje vymazány před tím, než si je orgány vyžádají pro účely trestního řízení. V současné době neexistuje celounijní rámec v této oblasti. Zatímco většina členských států EU se spoléhá na vnitrostátní právní předpisy, které se v rámci EU liší, jiné členské státy žádná pravidla nemají. Policie, státní zastupitelství a justiční orgány označily nedostatek harmonizovaných pravidel pro uchovávání klíčových kategorií údajů za značnou komplikaci pro vnitrostátní trestní řízení u trestných činů, k nimž dochází online i offline, což brání přeshraniční spolupráci v celé EU. Toto téma mělo zásadní význam ve [skupině na vysoké úrovni pro přístup k údajům](#), kde odborníci doporučili přijetí rámce EU pro uchovávání údajů pro účely prosazování práva, který by zahrnoval rovněž záruky přístupu. Předsedkyně Komise von der Leyenová (1) (2) a členské státy EU v závěrech Rady [o přístupu k údajům pro účinné prosazování práva](#) a [o podpoře společného úsilí v boji proti terorismu](#) nedávno zdůraznily potřebu opatření k zajištění zákonného a účinného přístupu k údajům pro účely prosazování práva. Ve sdělení [ProtectEU: Evropská strategie vnitřní bezpečnosti](#), se Komise zavázala předložit v roce 2025 plán, který stanoví další postup v oblasti zákonného a účinného přístupu k údajům pro donucovací orgány, a stanovit jako prioritu posouzení dopadu pravidel pro uchovávání údajů na úrovni EU.

Problém, který má iniciativa řešit

V digitální společnosti mají elektronické důkazy zásadní význam pro většinu vyšetřování a stíhání trestných činů. Neobsahové údaje (např. informace o účastníkovi, zdroj a cíl zprávy, umístění zařízení, datum, čas, trvání, velikost nebo jiný druh interakce, který nezahrnuje obsah komunikace) by mohly být rozhodující pro identifikaci nebo lokalizaci podezřelých a/nebo obviněných osob, obětí a obecně pro objasnění trestného činu. Poskytovatelé služeb elektronických komunikací uchovávají neobsahové údaje komunikace procházející jejich systémy. Vzhledem k tomu, že tyto neobsahové údaje mohou být osobní povahy a mohou poskytovat informace o soukromém životě osob, jichž se týkají, musí je poskytovatelé služeb v souladu se základními právy (zejména články 7, 8 a 11 Listiny) a [právními předpisy EU o ochraně soukromí a údajů](#) vymazat, pokud již nejsou nezbytné pro legitimní obchodní účely. Uchovávání údajů po delší dobu je možné pouze tehdy, pokud to vyžadují zvláštní právní povinnosti. V návaznosti na rozhodnutí Soudního dvora Evropské unie [prohlašující za neplatnou](#)

směrnici EU o uchovávání údajů z důvodu závažného zásahu do základních práv a nedostatku zvláštních záruk přístupu od roku 2014 již právo EU neukládá žádné povinnosti poskytovatelům služeb uchovávat údaje pro účely vymáhání (prosazování) práva. Ačkoli tyto povinnosti existují v mnoha členských státech EU, panují značné rozdíly mezi jejich právními předpisy, pokud jde o požadavky na uchovávání. V důsledku toho se policie a státní zástupci potýkají s překážkami při výkonu své práce, neboť při vyšetřování často nejsou vůbec nebo již nejsou k dispozici potřebné údaje. Podle současného scénáře nemohou být některé trestné činy – zejména ty, k nimž dochází výhradně na internetu – účinně vyšetřovány a stíhány.

Poskytovatelé služeb elektronické komunikace se rovněž potýkají s vyššími náklady a překážkami při nabízení svých služeb v celé EU, a to kvůli tomu, že musí splňovat odlišné právní požadavky v různých členských státech, a v důsledku častých změn vnitrostátních právních předpisů kvůli rozsudkům na vnitrostátní úrovni a/nebo na úrovni EU¹. Kromě toho se většina vnitrostátních právních předpisů o uchovávání údajů vztahuje pouze na tradiční telekomunikační platformy a nevztahuje se na poskytovatele komunikací, kteří nabízejí své služby přes internet, tj. na dnes nejpoužívanější komunikační služby. Rozdílné vnitrostátní právní předpisy mají rovněž dopad na občany, neboť v době, kde je vedeno trestní vyšetřování, byly nezbytné neobsahové údaje již vymazány. Orgány by pak nemusely být schopny odpovídajícím způsobem chránit a zajišťovat spravedlnost pro občany. Tyto rozdíly mezi vnitrostátními právními předpisy se budou s nástupem nových digitálních komunikačních technologií a služeb, které budou vyvinuty v budoucnu, pravděpodobně dále zvětšovat.

Příčiny současné situace lze nalézt v nedostatku harmonizovaných požadavků a záruk pro poskytovatele služeb elektronických komunikací, a to jak služeb závislých na číslech, tak nezávislých na číslech, pokud jde o uchovávání údajů po uplynutí doby potřebné pro jejich specifické obchodní potřeby, aby tyto údaje mohly být pro účely vymáhání práva k dispozici déle.

Základ pro opatření na úrovni EU (právní základ a kontrola subsidiarity)

Právní základ

O právním základu je třeba rozhodnout a závisí na výsledku posouzení dopadů.

Praktická potřeba opatření na úrovni EU

Zjištěné problémy nemohou uspokojivě řešit jednotlivé členské státy samy. Bez opatření na úrovni EU lze očekávat, že členské státy budou pokračovat v novelizaci svých vnitrostátních právních předpisů s cílem provést požadavky vyplývající z judikatury Soudního dvora EU, Evropského soudu pro lidská práva a vnitrostátních soudů. Budou rovněž muset reagovat na nové a vznikající technologie, což s sebou nese riziko, že se pravidla budou ještě více odchylovat. To znásobí negativní dopady na občany EU, trestní vyšetřování, poskytovatele služeb elektronické komunikace a další příslušné zúčastněné strany. Zároveň je třeba zajistit, aby zásah do základních práv uživatelů vyplývající z povinnosti uchovávat údaje a umožňovat přístup k nim byl přiměřený, jak stanoví judikatura Soudního dvora Evropské unie. Právní předpisy o uchovávání údajů se týkají různých oblastí politiky, včetně bezpečnosti, spravedlnosti, základních práv a hospodářství, a mají dopad na různé zúčastněné strany (např. orgány, podniky a občany). Vzhledem k dopadu na vnitřní trh EU a prostor svobody, bezpečnosti

¹ Nedávná analýza Eurojustu a Evropské justiční sítě pro boj proti kyberkriminalitě – EJCEN „[Dopad judikatury Soudního dvora Evropské unie na vnitrostátní režimy uchovávání údajů a justiční spolupráci v EU](#)“ uvádí, že dvanáct členských států (BE, DK, EE, IE, FR, HR, IT, LV, LT, PT, SK, SE) provedlo v letech 2018 až 2022 klíčové změny svých právních předpisů v přímém důsledku věci C-746/18, Prokuratuur, a spojených věcí C-511/18, C-512/18 a C-520/18, La Quadrature du Net a další; čtyři členské státy již nemají zavedena pravidla pro povinné uchovávání údajů pro účely trestního vyšetřování (DE, NL, RO, SI), s. 6.

a práva EU by za nejvhodnější cestu vpřed mohla být považována opatření na úrovni EU zaměřená na řešení zjištěných problémů. Hlavním cílem opatření EU by mohlo být zajistit harmonizované uplatňování povinností poskytovatelů služeb týkajících se uchovávání údajů, včetně záruk pro přístup policejních a soudních orgánů, a zajistit tak právní jistotu pro příslušné zúčastněné strany a rovné podmínky pro poskytovatele služeb, kteří nabízejí své služby v rámci EU.

B. Cíle a zvažovaná opatření

Celkovým cílem iniciativy je zajistit dostupnost určitých kategorií neobsahových údajů pro účely úspěšného trestního vyšetřování a stíhání při současném dodržování a zachování norem EU na ochranu základních práv a zachování kybernetické bezpečnosti a integrity trhu EU.

Za tímto účelem Komise zváží a posoudí různé možnosti. Jedná se například o:

— právně nevynutitelná opatření k posílení spolupráce mezi veřejnými orgány a poskytovateli služeb elektronické komunikace, a to jak služeb závislých na číslech, tak i nezávislých na číslech, jako jsou společné normy na úrovni EU pro kategorizaci údajů, formuláře pro vyžádání a poskytování údajů, pokyny týkající se minimální doby uchovávání adres účastníků a IP adres/w časového razítka, dobrovolná spolupráce,

— legislativní opatření stanovující povinné požadavky na uchovávání neobsahových údajů a přístup k nim pro všechny poskytovatele služeb, na něž se vztahuje evropský kodex pro elektronické komunikace², v souladu se stávající judikaturou Soudního dvora Evropské unie. V závislosti na neobsahových údajích, které mají být uchovávány v souvislosti s trestným činem, jenž má být stíhán, by mohla být navržena různá legislativní řešení.

Nejvhodnější možnost bude určena během posouzení dopadů, a to na základě shromážděných důkazů, konzultací se zúčastněnými stranami a po porovnání různých možností.

C. Pravděpodobné dopady

Očekává se, že tato iniciativa bude mít dopady v řadě odvětví:

Společenské dopady: dostupnost neobsahových údajů by veřejným orgánům pomohla účinněji odhalovat, vyšetřovat a stíhat trestnou činnost, čímž by se občanům EU zajistila bezpečnější společnost, a to jak v prostředí online, tak offline. Očekává se, že pozitivní dopady se projeví jak ve vnitrostátních trestních řízeních, tak v přeshraniční spolupráci v boji proti trestné činnosti.

Hospodářské dopady: poskytovatelé služeb elektronické komunikace se vyhnou dodatečným nákladům na dodržování předpisů a právní nejistotě vyplývající z rozdílných právních a technických požadavků v závislosti na členském státě nebo členských státech EU, v nichž jsou usazeni či působí. Iniciativa bude posuzovat způsoby, jak omezit překážky poskytování služeb na vnitřním trhu EU. Zároveň se tím zvýší náklady na uchovávání údajů v členských státech, v nichž neexistuje povinnost uchovávat údaje pro účely vymáhání práva.

Dopady na základní práva: uchovávané a zpřístupněné neobsahové údaje by mohly orgánům poskytovat informace o soukromém životě osob, jichž se tyto údaje týkají, a zasahovat tak do základních práv na ochranu jejich soukromí (článek 7 Listiny základních práv Evropské unie), jejich osobních údajů (článek 8) a svobody projevu (článek 11). Posílení schopnosti veřejných orgánů získávat neobsahové údaje a získávat důkazy v trestním řízení by sloužilo veřejnému zájmu na účinnějším odhalování a stíhání trestných činů, volnému pohybu služeb v rámci vnitřního trhu EU a mohlo by přinést více spravedlnosti pro oběti, podezřelé a obviněné osoby. Pokud by možnosti

² Ustanovení čl. 2 odst. 4 směrnice (EU) 2018/1972: „službou elektronických komunikací“ [se rozumí] služba obvykle poskytovaná za úplatu prostřednictvím sítí elektronických komunikací, která s výjimkou služeb poskytujících obsah přenášený prostřednictvím sítí a služeb elektronických komunikací nebo vykonávajících redakční dohled nad tímto obsahem zahrnuje tyto druhy služeb:

- „službu přístupu k internetu“ ve smyslu čl. 2 druhého pododstavce bodu 2 nařízení (EU) 2015/2120;
- interpersonální komunikační službu ;
- služby spočívající zcela nebo převážně v přenosu signálů, například přenosové služby používané pro poskytování služby komunikace mezi stroji a pro vysílání;“

zvažované v posouzení dopadů měly omezovat základní práva, budou tyto možnosti zváženy oproti zásahu do těchto práv a bude plně zváženo poskytnutí odpovídajících záruk, které zajistí jejich nezbytnost a přiměřenost pro dosažení zamýšleného cíle.

D. Nástroje zlepšování právní úpravy

Posouzení dopadů

Komise provede posouzení dopadů s cílem podle potřeby aktualizovat pravidla pro uchovávání údajů na úrovni EU. V souladu s politikou Komise v oblasti zlepšování právní úpravy bude ve druhém a třetím čtvrtletí 2025 zveřejněna veřejná konzultace. Komise provede důkladný sběr důkazů z různých zdrojů, včetně široké veřejnosti, různými prostředky, jako je tato veřejná výzva k předložení faktických podkladů a průzkumy zaměřené na příslušné zúčastněné strany.

Konzultační strategie

Na podporu této iniciativy plánuje Komise několik konzultačních činností. Cílem je shromáždit důkazy a názory široké škály zúčastněných stran. Hlavní konzultační činnosti budou zahrnovat:

- zpětnou vazbu k této výzvě k předložení faktických podkladů,
- zpětnou vazbu k veřejné konzultaci, která bude po dobu 12 týdnů zveřejněna ve všech úředních jazycích EU na internetových stránkách Komise „[Podělte se o svůj názor](#)“,
- cílené konzultace s příslušnými zúčastněnými stranami v podobě rozhovorů a průzkumů s cílem shromáždit rovněž kvantitativní a kvalitativní důkazy o nezbytnosti a přiměřenosti těchto opatření.

V souladu s cílem politiky Komise v oblasti zlepšování právní úpravy, kterým je rozvíjet iniciativy na základě nejlepších dostupných znalostí, vyzýváme rovněž výzkumné pracovníky, akademické organizace, odborné společnosti a vědecká sdružení s odbornými znalostmi v technických a politických oblastech souvisejících s iniciativou, aby předložili relevantní zveřejněné i dosud nezveřejněné vědecké analýzy, údaje a další materiály. Komise zejména přivítá materiály, které shrnují současné poznatky v příslušné oblasti / příslušných oblastech.

Komise zveřejní věcnou souhrnnou zprávu s příspěvkem k veřejné konzultaci. Rovněž bude analyzovat zpětnou vazbu k této výzvě k předložení faktických podkladů a výsledky následných konzultací v souhrnné zprávě připojené k posouzení dopadů (pracovní dokument útvarů Komise).

Proč se konzultace koná?

Cílem konzultace je zajistit, aby se posouzení dopadů opíralo o rozsáhlé kvantitativní a kvalitativní důkazy a odborné znalosti, a umožnit zúčastněným stranám (včetně občanů a těch, kterých by se tato iniciativa přímo týkala) vyjádřit své názory a příspěvky k možným variantám dalšího postupu.

Cílová skupina

Mezi hlavní kategorie zúčastněných stran, které Komise plánuje konzultovat, patří: široká veřejnost; odborníci působící v oblasti veřejné bezpečnosti (spravedlnost, vnitřní věci a digitální politika); policejní a soudní orgány; odborníci na kybernetickou bezpečnost, orgány pro ochranu údajů a soukromí; profesní sdružení právníků, akademická obec, výzkumní pracovníci a think tanky; organizace občanské společnosti, které se zabývají právy obětí v oblasti digitálních práv nebo obecněji základními právy; průmyslové odvětví.