EVROPSKÁ
KOMISE

V Bruselu dne 24.6.2025
COM(2025) 349 final

SDĚLENÍ KOMISE EVROPSKÉMU PARLAMENTU, RADĚ, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ

Plán pro zákonný a účinný přístup k údajům pro účely prosazování práva

Úvod

Jak je uvedeno v Evropské strategii vnitřní bezpečnosti („ProtectEU“)[1], **bezpečnost je základním kamenem, na němž stojí všechny naše svobody**. Demokracie, právní stát, základní práva, dobré životní podmínky Evropanů, konkurenceschopnost a prosperita – to vše závisí na naší schopnosti zajistit základní bezpečnostní záruky.

EU a členské státy mají povinnost zajistit občanům **vysokou úroveň bezpečnosti v jejich každodenním životě**. Za tímto účelem musí mít donucovací a justiční orgány k dispozici nástroje nezbytné ke sledování nezákonné činnosti, k identifikaci pachatelů, k rozbíjení zločineckých sítí a k ochraně obětí, což v konečném důsledku zajistí trestní spravedlnost při plném dodržování základních práv.

Terorismus, organizovaná trestná činnost, podvody na internetu, obchod s drogami, pohlavní zneužívání dětí, sexuální vydírání na internetu, ransomware a mnohé další trestné činy mají něco společného: zanechávají **digitální stopy**. Jak uvádí Europol ve svém posouzení hrozeb závažné a organizované trestné činnosti (SOCTA) pro rok 2025, téměř všechny formy závažné a organizované trestné činnosti mají digitální stopu[2]. **Při přibližně 85 % vyšetřování trestné činnosti se dnes využívají elektronické důkazy**[3]. Počet žádostí o poskytnutí údajů adresovaných poskytovatelům služeb se mezi lety 2017 a 2022 ztrojnásobil a potřeba těchto údajů se jen zvyšuje[4].

Ačkoli jsme v poslední době svědky mimořádných příkladů úspěšných zásahů donucovacích a justičních orgánů proti sítím využívaným ke komunikaci pachatelů trestné činnosti[5], mnohem více vyšetřování se **zpožďuje nebo končí neúspěchem kvůli absenci včasného přístupu k digitálním důkazům**[6]. Donucovací a justiční orgány v posledním desetiletí za pachateli trestné činnosti zaostávají, protože ti využívají nástroje a produkty poskytovatelů služeb, kteří zavedli opatření znemožňující spolupráci při zákonných žádostech[7].

Zásadní důkazy pro trestní řízení zůstávají nedostupné, protože[8]:

- je poskytovatelé služeb během několika dnů **mažou** v souladu s jejich povinnostmi v oblasti ochrany osobních údajů a soukromí nebo v souladu s jejich obchodními potřebami,

---

[1] EUR-Lex - 52025DC0148 – CS – EUR-Lex.

[2] Posouzení hrozeb závažné a organizované trestné činnosti v Evropské unii 2025 EU-SOCTA-2025.pdf.

[3] Posouzení dopadů návrhů nařízení o elektronických důkazech a směrnice o elektronických důkazech, které provedla Komise (17. dubna 2018) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2018:0119:FIN:CS:PDF.

[4] Zpráva projektu SIRIUS za rok 2023, https://www.eurojust.europa.eu/sites/default/files/assets/sirius-eueesr-2023.pdf, s. 69.

[5] Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized (Prolomení šifrované komunikace pachatelů trestné činnosti přes síť EncroChat vedlo k více než 6 500 zatčením a k zabavení téměř 900 milionů EUR) | Europol
joint_ep_ej_third_report_of_the_observatory_function_on_encryption_en.pdf / Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe (Prolomení šifrované sítě způsobilo otřesy v organizovaných zločineckých skupinách po celé Evropě) | Europol.

[6] Zpráva: Skupina na vysoké úrovni pro přístup k údajům pro účely účinného prosazování práva – Evropská komise.

[7] Závěrečná zpráva Skupiny na vysoké úrovni pro přístup k údajům pro účely účinného prosazování práva (15. listopadu 2024).

[8] Common Challenges in Cybercrime, 2024 Review by Europol and Eurojust (Společné výzvy v oblasti kyberkriminality, přezkum provedený Eurojustem a Europolem, 2024).

- je **nelze získat** z důvodu kolize právních řádů mezi jurisdikcemi, protože různé země mají různé zákony a předpisy týkající se přístupu k údajům, což ztěžuje získání údajů uložených v zahraničí,
- je **nelze získat ze zařízení zabavených při vyšetřování trestných činů**, neboť **digitální forenzní analýza** je obtížná, ne-li zcela neproveditelná,
- je **nelze přečíst**, neboť data jsou zašifrovaná,
- je **nelze účinně a zákonným způsobem analyzovat**, neboť chybí vhodné technologie nebo dostatečné lidské zdroje, které by umožnily účinně filtrovat a analyzovat velké množství zabavených dat, aniž by se to dotklo právních rámců EU a členských států.

V reakci na tyto výzvy byla v roce 2023 zřízena **Skupina na vysoké úrovni pro přístup k údajům pro účely prosazování práva** (skupina na vysoké úrovni), která v květnu a listopadu 2024 předložila soubor 42 doporučení. **Rada EU pro spravedlnost a vnitřní věci** doporučení skupiny na vysoké úrovni schválila[9] dne 13. června 2024 a později v prosinci 2024 přijala závěry, v nichž vyzvala Komisi k vypracování plánu postupu. Plán měl vycházet z práce skupiny na vysoké úrovni a jejích doporučení pro zavedení opatření k zajištění zákonného a účinného přístupu k údajům pro účely prosazování práva[10]. Toto sdělení je odpovědí na tuto výzvu.

Vzhledem k tomu, že digitalizace je stále rozšířenější a poskytuje pachatelům trestné činnosti stále více nových nástrojů, je nezbytný rámec pro **zákonný přístup k údajům**, aby bylo zajištěno, že pachatelé trestné činnosti budou postaveni před soud. „Zákonný přístup“, na nějž tento plán odkazuje, je přístup k digitálním informacím, který je v souladu s právními předpisy, pokud donucovací orgány tyto informace potřebují za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, včetně ochrany před hrozbami pro veřejnou bezpečnost a jejich předcházení.

Aby byl přístup k údajům zákonný, musí být **nezbytný a přiměřený a musí dodržovat základní práva** a zajišťovat odpovídající ochranu soukromí a osobních údajů; musí být založen na **jasných, přesných a srozumitelných pravidlech stanovených právními předpisy**, podléhat nezávislým **mechanismům dohledu** a mít k dispozici **účinnou právní ochranu pro** osoby, které mohou být přístupem ke svým údajům dotčeny. Stejně důležité pro ochranu před kybernetickými bezpečnostními hrozbami je zajistit, aby digitální systémy zůstaly **kyberneticky zabezpečené** proti neoprávněnému přístupu.

I. Zajištění dostupnosti digitálních důkazů: uchovávání údajů[11]

Ve Španělsku se v roce 2019 podařilo vyřešit vyšetřování ohledně zmizení mladé ženy díky lokalizačním údajům, které v souladu s vnitrostátními právními povinnostmi uchovával poskytovatel komunikačních služeb. Tyto údaje umožnily vyšetřovatelům lokalizovat pohřešovanou ženu, zjistit, že podezřelý z únosu se v této oblasti také nachází, a vyloučit další

[9] Recommendations of the High-Level Group on access to data for effective law enforcement (Doporučení Skupiny na vysoké úrovni pro přístup k údajům pro účely účinného prosazování práva).

[10] Závěry Rady o přístupu k údajům pro účely účinného prosazování práva (12. prosince 2024) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/cs/pdf; Závěry Rady o budoucích prioritách na podporu společného úsilí Evropské unie a jejích členských států v boji proti terorismu (12. prosince 2024) https://data.consilium.europa.eu/doc/document/ST-16820-2024-INIT/cs/pdf.

[11] Uchovávání údajů se týká poskytovatelů služeb, kteří po danou dobu uchovávají určité neobsahové údaje zpracovávané v souvislosti s komunikačními službami, které poskytují, aby k nim mohly mít za splnění vhodných bezpečnostních záruk přístup příslušné orgány za účelem vyšetřování trestných činů a pro zajištění výkonu trestní spravedlnosti.

podezřelé[12]. Neobsahové údaje o komunikaci (například informace o zákazníkovi, lokalizační údaje a datum, čas, doba trvání, odesílatel a příjemce a velikost komunikace) mají zásadní význam pro většinu vyšetřování a stíhání trestných činů. Tyto údaje mohou být rozhodující při identifikaci a lokalizaci obětí, podezřelých a obviněných osob, mohou objasnit spáchaný trestný čin a pomoci vyloučit podezřelé osoby.

V souladu s právními předpisy EU v oblasti ochrany soukromí a osobních údajů mohou poskytovatelé služeb elektronických komunikací uchovávat neobsahové údaje o komunikaci, které procházejí jejich systémy, pouze po dobu nezbytnou pro konkrétní, výslovně vyjádřené a legitimní obchodní účely. Na základě právních povinností lze však od nich vyžadovat, aby tyto údaje měli k dispozici (nebo „uchovávali“) pro jiné účely, například pokud jsou potřebné pro prevenci, vyšetřování, odhalování a stíhání trestných činů.

Platnost směrnice EU o uchovávání údajů[13] byla zrušena v roce 2014[14] a od té doby je legislativní prostředí EU týkající se povinnosti poskytovatelů služeb uchovávat údaje roztříštěné a nejednotné. Rámce členských států pro uchovávání údajů se liší z hlediska typu elektronických komunikací, které musí poskytovatelé služeb uchovávat, kategorií údajů, jichž se týkají, a požadovaných lhůt pro uchovávání[15]. Některé členské státy navíc žádné právní předpisy o uchovávání údajů nemají. Donucovací a justiční orgány se při výkonu své práce potýkají s právními a provozními překážkami. Poskytovatelé elektronických komunikací, zejména menší společnosti, čelí při poskytování svých služeb v celé EU také dalším nákladům a překážkám, protože musí splňovat různé právní požadavky v různých členských státech.

Skupina na vysoké úrovni proto doporučila zřídit **harmonizovaný rámec EU pro uchovávání údajů** s cílem zajistit dostupnost digitálních důkazů potřebných k vyšetřování a stíhání trestných činů. Cílem harmonizovaného režimu EU by bylo omezit roztříštěnost mezi členskými státy, pokud jde o pravidla uchovávání a záruky týkající se základních práv, zejména soukromí a ochrany údajů a práva na obhajobu, včetně práva na spravedlivý proces. Takový právní rámec by také zajistil právní jistotu příslušným orgánům na jedné straně a poskytovatelům služeb na straně druhé.[16]

Klíčové opatření

- **Komise v roce 2025 připraví posouzení dopadů s cílem případně aktualizovat pravidla EU týkající se uchovávání údajů.**

[12] La cobertura del móvil de Diana Quer desmonta la versión del Chicle: no la abordó donde él dijo que estaba robando gasolina | Španělsko.
[13] https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32006L0024j.
[14] Rozsudek Soudního dvora (velkého senátu) ze dne 8. dubna 2014. Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources a další.
[15] Pro přehled viz The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU (Dopad judikatury Soudního dvora Evropské unie na vnitrostátní režimy uchovávání údajů a justiční spolupráci v EU) | Eurojust | Agentura Evropské unie pro justiční spolupráci v trestních věcech a European Commission Study on the retention of electronic communications non-content data for law enforcement purposes (Studie Evropské komise o uchovávání neobsahových údajů z elektronických komunikací pro účely prosazování práva).
[16] Doporučení blok 6, závěrečná zpráva skupiny na vysoké úrovni.

Skupina na vysoké úrovni zjistila, že je třeba **posílit součinnost mezi pracovníky donucovacích orgánů a poskytovateli služeb**[17].

Za tímto účelem se **Agentura Evropské unie pro spolupráci v oblasti prosazování práva (Europol) a Agentura Evropské unie pro justiční spolupráci v trestních věcech (Eurojust)** vyzývají, aby s trvalou podporou Komise pokračovaly v úsilí o **usnadnění spolupráce a výměny informací a osvědčených postupů mezi odborníky z praxe a poskytovateli služeb** prostřednictvím **projektu SIRIUS**[18], a dále toto úsilí zintenzivňovaly. Projekt SIRIUS se stal nejdůležitějším zdrojem informací na **podporu pracovníků donucovacích orgánů a justičních orgánů v EU i mimo ni při přístupu k elektronickým důkazům uloženým poskytovateli online služeb** se sídlem ve třetích zemích. Platforma SIRIUS má více než 8 000 členů z řad donucovacích a justičních orgánů ze 47 zemí světa a přímo podpořila téměř 70 policejních operací.

Ze stejného důvodu by Europol a Eurojust měly využít projekt SIRIUS k tomu, aby ve spolupráci se **soukromým sektorem** vytvořily **katalog údajů, které služby elektronických komunikací oprávněně zpracovávají pro své obchodní účely**. To pomůže příslušným orgánům zjistit, jaké údaje mohou být k dispozici pro jejich žádosti o zákonný přístup, identifikovat příslušné poskytovatele služeb a lépe zacílit žádosti o zákonný přístup, což ušetří čas a náklady jak orgánům veřejné správy, tak poskytovatelům služeb.

Klíčová opatření

- **Europol a Eurojust se vyzývají, aby s trvalou podporou Komise navázaly na projekt SIRIUS a zefektivnily spolupráci s poskytovateli elektronických komunikačních služeb.**

- **Europol a Eurojust se vyzývají, aby ve spolupráci se soukromým sektorem vypracovaly katalog údajů, které poskytovatelé elektronických komunikací zpracovávají pro své obchodní účely (zahájení ve 4. čtvrtletí 2025).**

II. Získávání důkazů napříč systémy a jurisdikcemi: zákonný odposlech

Zákonný přístup ke komunikačním údajům v reálném čase je nezbytný pro boj proti pachatelům trestné činnosti online i offline. V roce 2020 rozbil společný francouzsko-nizozemský vyšetřovací tým šifrovanou telefonní síť EncroChat, kterou hojně využívaly skupiny organizovaného zločinu. Toto společné vyšetřování zahrnovalo zachycení milionů zpráv v reálném čase, které si vyměňovali pachatelé trestné činnosti plánující spáchat závažné trestné činy, sdílení těchto zpráv s dalšími orgány a jejich analýzu. Díky získaným informacím se donucovacím orgánům v celé Evropě a dalších částech světa podařilo překazit trestnou činnost, včetně násilných útoků, korupce, pokusů o vraždu a rozsáhlého obchodování s drogami. Některé zprávy naznačovaly plány na spáchání bezprostředně hrozících násilných

[17] Doporučení blok 5, závěrečná zpráva skupiny na vysoké úrovni.
[18] Projekt SIRIUS | Europol.

trestných činů a umožnily donucovacím orgánům jim zabránit[19]. Evropský vyšetřovací příkaz usnadnil účinné sdílení těchto důkazů.[20]

Případ EncroChat ukazuje, že přístup k údajům o obsahu komunikace v reálném čase je zásadním nástrojem pro účinné vyšetřování a stíhání skupin organizovaného zločinu. Tento případ však zůstává jedním z mála úspěšných: skupina na vysoké úrovni konstatovala, že účinnost zákonného odposlechu[21] se drasticky snížila, protože komunikace se přesunula od tradičních telefonních hovorů a SMS ke službám pro zasílání zpráv „over the top" (OTT) prostřednictvím aplikací. V současné době se přibližně 97 % všech mobilních zpráv posílá prostřednictvím aplikací pro zasílání zpráv, zatímco tradiční zprávy SMS a MMS tvoří pouze asi 3 % zpráv[22]. Skupina na vysoké úrovni rovněž uvedla, že od roku 2020 se po narušení některých hlavních sítí, které používali pachatelé trestné činnosti ke komunikaci, mnoho zločineckých skupin rozhodlo vrátit k běžným službám OTT pro zasílání zpráv šifrovaných mezi koncovými body.[23]

Vnitrostátní pravidla ukládající povinnosti ve věci zákonného odposlechu jsou v EU roztříštěná[24]. Skupina na vysoké úrovni konstatovala, že ačkoli některé členské státy ukládají podobné povinnosti pro všechny typy služeb elektronické komunikace, včetně služeb OTT, jiné je vylučují. Poskytovatelé služeb navíc často nejsou usazeni v členském státě dožadujícího orgánu, což může vést ke složitým problémům ohledně soudní příslušnosti, kolizím právních předpisů a problémům s vymáháním[25]. V důsledku toho je obsah těchto služeb pro zasílání zpráv prakticky nedostupný.

Evropský vyšetřovací příkaz a další nástroje spolupráce mohou v některých částech EU pomoci překonat problém týkající se přeshraničního odposlechu. Orgány členských států se však při jejich používání stále potýkají s obtížemi: tyto nástroje nemohou podporovat odposlech, pokud je služba poskytována buď z členských států, které se daného nástroje neúčastní, nebo ze třetí země. Skupina na vysoké úrovni proto doporučila řadu opatření, která mají zajistit, aby široká škála poskytovatelů, včetně poskytovatelů služeb OTT, reagovala na zákonné žádosti o odposlech.[26]

V reakci na to **Komise navrhne, jak zlepšit opatření pro posílení přeshraniční spolupráce v oblasti odposlechu** jak mezi orgány navzájem, tak mezi orgány a poskytovateli služeb. V návaznosti na doporučení skupiny na vysoké úrovni bude Komise pracovat především na zdokonalení stávajících nástrojů, zejména evropského vyšetřovacího příkazu, a na dobrovolné spolupráci (v případech, kdy nedochází ke střetu právních předpisů se třetími zeměmi nebo

[19] Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe (Prolomení šifrované sítě způsobilo otřesy v organizovaných zločineckých skupinách po celé Evropě) | Europol; Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hackké la messagerie chiffrée utilisée par la criminalité organisée.

[20] Evropský vyšetřovací příkaz| Eurojust | Agentura Evropské unie pro justiční spolupráci v trestních věcech.

[21] V kontextu tohoto sdělení se jedná o technologie zákonného odposlechu, které operátor komunikačních služeb použije při soudním vyšetřování za účelem získání přístupu ke komunikačním údajům v reálném čase, a také o technologie, které mohou samostatně použít donucovací orgány.

[22] Závěrečná zpráva skupiny na vysoké úrovni, s. 38.

[23] Internet Organised Crime Threat Assessment IOCTA 2024 (Posouzení hrozeb organizované trestné činnosti na internetu, 2024).

[24] Viz Bílá kniha EU o digitální infrastruktuře, s. 14; Lettova zpráva o vnitřním trhu, s. 59, a Draghiho zpráva o konkurenceschopnosti EU, s. 70, 74 a 76.

[25] Závěrečná zpráva skupiny na vysoké úrovni, s. 41.

[26] Doporučení blok 8, závěrečná zpráva skupiny na vysoké úrovni.

byly tyto střety odstraněny). V konečném důsledku by členské státy měly mít možnost vymáhat povinnosti zákonného odposlechu od všech poskytovatelů komunikačních služeb, kteří nabízejí služby na domácím trhu, jak je stanoveno ve vnitrostátních právních předpisech, bez ohledu na to, zda se jedná o tradiční telekomunikační služby nebo služby poskytované přes internet, a bez ohledu na jejich lokalizaci.

Některé členské státy navíc nemají potřebné síťové kapacity pro sdílení údajů v rámci přeshraniční spolupráce. **Komise** proto **zjistí potřeby členských států** a podpoří zavedení zabezpečených sítí s dostatečnou šířkou pásma mezi příslušnými členskými státy, které umožní přenos velkého množství dat v reálném čase. Tato iniciativa by mohla být financována z programů EU.

Klíčová opatření

Komise:

- **navrhne opatření ke zlepšení účinnosti přeshraničních žádostí o zákonný odposlech prostřednictvím stávajících nástrojů, včetně posouzení potřeby dalšího posílení evropského vyšetřovacího příkazu (do roku 2027),**
- **prozkoumá opatření k vytvoření rovných podmínek pro všechny typy poskytovatelů komunikačních služeb při prosazování povinností zákonného odposlechu,**
- **určí nejúčinnější přístup k řešení problému ohledně nespolupracujících poskytovatelů komunikačních služeb,**
- **podpoří zavedení kapacit pro bezpečné sdílení informací mezi členskými státy, Europolem a dalšími bezpečnostními agenturami (od roku 2026 do roku 2028).**

Členské státy se vybízejí, aby prováděly opatření týkající se přeshraničního zákonného odposlechu, a to na základě stávajících mechanismů, jako je evropský vyšetřovací příkaz a dvoustranné a mnohostranné dohody.

III. Získávání důkazů ze zařízení zabavených při vyšetřování: digitální forenzní analýza

Aby mohly donucovací a justiční orgány provádět vyšetřování trestných činů, musí mít možnost přístupu k digitálním důkazům uloženým v elektronických zařízeních a musí mít možnost je shromažďovat, analyzovat a uchovávat. Tyto digitální důkazy mohou například pomoci identifikovat členy organizovaných zločineckých skupin nebo vyloučit osoby z podezření[27].

Skupina na vysoké úrovni diskutovala o řadě problémů, které brání přístupu k těmto digitálním důkazům. Vnitrostátním orgánům výrazným způsobem chybí zdroje a schopnosti pro provádění digitální forenzní analýzy. Snaží se držet tempo s potřebou neustále rozvíjet nové dovednosti a nástroje, aby udržely krok s novými technologiemi (například nové typy zařízení a operačních systémů, internet věcí a cloud computing). Přeshraniční spolupráci mezi členskými státy ohrožuje nedostatek srovnatelných kapacit a neexistence mechanismů pro

[27] Případ projednávaný ve skupině na vysoké úrovni se týkal analýzy zařízení, které pomohlo prokázat, že podezřelý nebyl zapojen do vraždy. Závěrečná zpráva skupiny na vysoké úrovni, s. 12.

uznávání dovedností a znalostí odborníků na digitální forenzní analýzu. Stávající komerční řešení rychle zastarávají, jsou cenově nedostupná a často jsou vyvinuta v zemích mimo EU. Mohou být také nedostatečně přizpůsobena potřebám orgánů členských států nebo nemusí být v souladu s normami v oblasti odpovědnosti a forenzní analýzy v rámci Unie nebo jinými právními požadavky.

Skupina na vysoké úrovni proto doporučila, aby byly v zájmu posílení schopnosti evropských donucovacích orgánů provádět digitální forenzní analýzu zabavených zařízení poskytnuty prostředky určené na financování projektů, a to jak na výzkum a vývoj nástrojů pro digitální forenzní analýzu, tak na jejich zavádění. Skupina na vysoké úrovni uvítala pokračující úsilí Komise o jejich podporu prostřednictvím financování v rámci některých nástrojů EU (Horizont Evropa, program Digitální Evropa a Fond pro vnitřní bezpečnost) a odpovídajících nástrojů v rámci příštího dlouhodobého rozpočtu EU (víceletý finanční rámec).

V reakci na tato doporučení[28] **bude Komise s podporou Europolu koordinovat analýzu nedostatků a potřeb v oblasti výzkumu, vývoje, zavádění, údržby a využívání společných technických řešení pro digitální forenzní analýzu.**

Využití zdrojů musí být maximalizováno vytvářením synergií mezi projekty digitální forenzní analýzy, včetně začlenění projektů financovaných v rámci programů členských států do stávajících mechanismů nebo sítí. To by mělo zahrnovat financování partnerství veřejného a soukromého sektoru, které by poskytovalo plně otestované a k použití připravené softwarové nástroje bez licenčních poplatků[29].

V rámci svého mandátu k provádění správních vyšetřování získal úřad OLAF značné zkušenosti s postupy a nástroji digitální forenzní analýzy a prostřednictvím Programu Unie pro boj proti podvodům může pomáhat orgánům členských států při posilování jejich kapacit.

Úložiště nástrojů Europolu je bezpečná online platforma, která je k dispozici výhradně donucovacím orgánům a slouží ke sdílení bezplatného nekomerčního softwaru vyvinutého Europolem, evropskými donucovacími orgány a akademickou obcí. Vnitrostátní vyšetřovací orgány hojně využívají nástroje z úložiště k podpoře související s oblastmi závažné a organizované trestné činnosti, včetně obchodování s lidmi, kyberkriminality a pohlavního zneužívání dětí on-line. Toto úložiště by mělo zůstat privilegovaným distribučním kanálem pro digitální vyšetřovací nástroje vyvinuté v rámci projektů EU a pro členské státy, které budou vybízeny ke sdílení nástrojů digitální forenzní analýzy s otevřeným zdrojovým kódem vyvinutých na vnitrostátní úrovni v rámci stávajících mechanismů nebo sítí. **Europol může své úložiště nástrojů dále rozvíjet a propagovat**, aby donucovacím orgánům EU zpřístupnil důvěryhodné, bezpečné, bezplatné, snadno instalovatelné a škálovatelné vyšetřovací nástroje.

[28] Doporučení blok 1, závěrečná zpráva skupiny na vysoké úrovni.

[29] Například Evropské sdružení pro rozvoj technologií proti kyberkriminalitě (EACTDA) (www.eactda.eu) poskytuje donucovacím orgánům EU plně otestované a funkčně připravené softwarové nástroje bez licenčních poplatků a s přístupem ke zdrojovému kódu. Kromě osmi dosud dokončených nástrojů vyvíjí sdružení EACTDA dalších 16 nástrojů pro digitální vyšetřování, které mají být dodány do poloviny roku 2025.

Komise bude rovněž **podporovat zavádění inovativních řešení donucovacími orgány členských států prostřednictvím stávajících mechanismů, jako je platforma EMPACT[30], a prostřednictvím specializovaných výzev Fondu pro vnitřní bezpečnost**.

Skupina na vysoké úrovni zdůraznila, že **licence na nástroje pro digitální forenzní analýzu** jsou nákladné a pro některé donucovací orgány někdy nedostupné. Nástroje pro digitální forenzní analýzu mohou poskytovat data ve formátech, které nejsou kompatibilní se systémy používanými pro další zpracování. Vzhledem k tomu, že pro činnosti digitální forenzní analýzy má navíc zásadní význam důvěra, neměly by se spoléhat na nástroje typu „černá skříňka" (tj. nástroje, které zpracovávají data, aniž by důvěryhodné orgány mohly ověřit, jak fungují). Sdílení nástrojů digitální forenzní analýzy by mělo být podpořeno schématy hodnocení a případně certifikací komerčních nástrojů na úrovni EU, aby se zajistilo, že splňují normy důvěryhodnosti a forenzní normy, aniž by to znamenalo nadměrnou zátěž. Podpora by měla být poskytována také prostřednictvím společných systémů zadávání veřejných zakázek, které zajistí spolupráci mezi operativními jednotkami a kontaktními místy orgánů pro zadávání veřejných zakázek.[31]

Komise proto **podpoří operativní útvary členských států a jejich orgány pro zadávání veřejných zakázek při zavádění společných nákupů licencí na nástroje pro digitální forenzní analýzu, a to od pilotní fáze.**

Klíčová opatření

Komise bude s podporou Europolu:

- **do 2. čtvrtletí 2026 koordinovat analýzu nedostatků a potřeb v oblasti výzkumu, vývoje, zavádění, údržby a využívání společných technických řešení pro digitální forenzní analýzu,**

- **pokračovat v podpoře vývoje technických řešení pro digitální forenzní analýzu prostřednictvím vhodných mechanismů financování a koordinace,**

- **podporovat členské státy a orgány pro zadávání veřejných zakázek při zavádění společných nákupů licencí na nástroje pro digitální forenzní analýzu (do 2. čtvrtletí 2027), a to od pilotní fáze.**

Europol se vyzývá, aby dále rozvíjel a propagoval své úložiště nástrojů a umožnil tak donucovacím orgánům přístup k nekomerčním digitálním nástrojům (od 3. čtvrtletí 2025).

Členské státy se vyzývají, aby se podílely na vývoji, validaci a zavádění nástrojů pro digitální forenzní analýzu a tyto činnosti podpořily a řídily.

Agentura EU pro vzdělávání a výcvik v oblasti prosazování práva (CEPOL) poskytuje odbornou přípravu pro vyšetřovatele v oblasti forenzní digitální analýzy, včetně forenzní analýzy mobilních zařízení a forenzní analýzy živých dat. V návaznosti na doporučení skupiny

[30] EMPACT (evropská multidisciplinární platforma pro boj proti hrozbám vyplývajícím z trestné činnosti) je bezpečnostní iniciativa vedená členskými státy EU, jež má identifikovat a řešit hrozby představované organizovanou a závažnou mezinárodní trestnou činností a stanovovat v této oblasti priority.

[31] V návaznosti na projekt iProcureNet (www.iprocurenet.eu/), který byl financován v rámci programu EU pro výzkum a inovace Horizont Evropa a vytvořil metodiku pro společné zadávání veřejných zakázek v oblasti bezpečnosti a rovněž síť orgánů pro zadávání veřejných zakázek v členských státech.

na vysoké úrovni[32] **by Komise měla nadále podporovat vytváření vzdělávacích materiálů a zdrojů** prostřednictvím stávajících mechanismů se zapojením odborníků z praxe a akademické obce.[33] Kromě toho by CEPOL a členské státy měly **přednostně poskytovat odbornou přípravu v oblasti digitální forenzní vědy.**

Skupina na vysoké úrovni rovněž zdůraznila, že by na úrovni EU mohl být vytvořen systém certifikace pro odborníky v oblasti digitální forenzní vědy. Takový systém by zajistil kvalitu digitální forenzní práce, přispěl by k transparentnějšímu soudnímu řízení a zvýšil důvěru mezi donucovacími orgány napříč hranicemi.

V souladu s doporučeními skupiny na vysoké úrovni[34] **by** agentura CEPOL **mohla podpořit odborníky z praxe a akademickou obec při vytváření systému certifikace na úrovni EU pro odborníky v oblasti digitální kriminalistiky, přičemž by plně využila stávající sítě a mechanismy.**[35]

Klíčová opatření

<u>Komise</u>:

- **bude pokračovat v podpoře tvorby vzdělávacích materiálů a zdrojů.**

Agentura <u>CEPOL a členské státy</u> se vyzývají, aby:

- **přednostně poskytovaly odbornou přípravu v oblasti digitální forenzní vědy (od 3. čtvrtletí 2025),**
- **podpořily vývoj a zavedení systému certifikace na úrovni EU pro odborníky v oblasti digitální forenzní vědy (měl by být připraven v období od 1. čtvrtletí 2026 do 4. čtvrtletí 2028).**

Skupina na vysoké úrovni vydala doporučení, jak v prostředí důvěry usnadnit sdílení řešení a nástrojů pro digitální forenzní analýzu mezi členskými státy.[36] V reakci na to **<u>by Europol měl dále rozvíjet svou úlohu střediska excelence EU pro donucovací orgány v oblasti digitálních operativních odborných znalostí na poli digitální forenzní analýzy</u>**. To by mohlo zahrnovat vytvoření projektu podobného projektu SIRIUS[37], který by usnadnil v prostředí důvěry sdílení vědomostí, odborných znalostí, technických řešení, nástrojů pro digitální forenzní analýzu a osvědčených postupů. Europol by měl rovněž posílit svou koordinační úlohu při vytváření znalostí v oblasti digitální forenzní vědy na úrovni EU, a to v návaznosti na mechanismy vytvořené v posledních letech[38]. Některé z těchto opatření může

[32] Doporučení blok 3, závěrečná zpráva skupiny na vysoké úrovni.

[33] Například Evropská skupina pro odbornou přípravu a vzdělání v oblasti kyberkriminality ECTEG (www.ecteg.eu) je sdružení, které úzce spolupracuje s Europolem a agenturou CEPOL s cílem poskytovat donucovacím orgánům bezplatné vzdělávací zdroje v oblasti digitálního vyšetřování. V současné době je financována z Fondu pro vnitřní bezpečnost EU.

[34] Doporučení blok 3, závěrečná zpráva skupiny na vysoké úrovni.

[35] Zejména ECTEG.

[36] Doporučení blok 1, závěrečná zpráva skupiny na vysoké úrovni.

[37] Projekt SIRIUS, který vedou Europol a Eurojust, podporuje donucovací a justiční orgány EU tím, že usnadňuje účinný přeshraniční přístup k elektronickým důkazům uchovávaným poskytovateli online služeb. Poskytuje praktické nástroje, odbornou přípravu a zdroje pro více než 9 000 odborníků z praxe, podporuje spolupráci mezi poskytovateli online služeb a sdílení znalostí prostřednictvím mezinárodních akcí a partnerství.

[38] Specializované skupiny odborníků na platformě Europolu pro odborníky (https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts); Fórum forenzních znalců (https://www.europol.europa.eu/publications-

Europol zahájit v rámci svého stávajícího mandátu. Europol však bude potřebovat posílený mandát a další zdroje, aby mohl tato opatření plně rozvinout a účinně plnit operativní potřeby členských států.

V návaznosti na závazek stanovený v politických směrech pro Evropskou komisi na období 2024–2029 a oznámený v Evropské strategii vnitřní bezpečnosti **navrhne Komise ambiciózní revizi mandátu Europolu**. V rámci přípravy na tento krok Komise v úzké spolupráci s členskými státy posoudí, jak posílit technologické odborné znalosti a kapacitu Europolu na podporu vnitrostátních donucovacích orgánů v digitálním prostoru. Zásadní význam v tomto úsilí bude mít posílení kapacit Europolu v oblasti digitální forenzní vědy na základě posíleného mandátu a s využitím dalších zdrojů.

Skupina na vysoké úrovni doporučila, aby se zlepšil přístup odborníků ke znalostem prostřednictvím specializovaných mechanismů a aby odborníci spolupracovali s výrobci a vývojáři nástrojů pro digitální forenzní analýzu[39]. Od roku 2026 **by měl Europol s využitím svých vlastních zdrojů podporovat spolupráci mezi příslušnými vnitrostátními orgány a odborníky s cílem usnadnit spolupráci veřejného a soukromého sektoru v oblasti digitální forenzní analýzy**. Měl by podporovat členské státy při vývoji digitálních nástrojů a společných postupů, včetně stanovení společných datových formátů pro účely digitální forenzní analýzy[40].

Klíčová opatření

Europol se vyzývá, aby:

- **se postupně stal centrem excelence pro operativní odborné znalosti v oblasti digitální forenzní vědy a posílil svou úlohu při koordinaci vytváření znalostí v této oblasti na úrovni EU (od roku 2026),**

- **usnadnil spolupráci mezi donucovacími orgány a soukromými subjekty, včetně poskytovatelů služeb, v oblasti digitální forenzní analýzy a pomohl stanovit společné formáty dat pro účely digitální forenzní analýzy (od roku 2026).**

IV. Zajištění čitelnosti důkazů: dešifrování dat

Šifrování a další opatření kybernetické bezpečnosti hrají důležitou roli při ochraně informačních systémů před špionáží a narušením a při zabezpečení komunikace, soukromí a osobních údajů. Celkem 60 % až 80 % aplikací pro zasílání zpráv je šifrováno mezi koncovými body, a to i u hlavních poskytovatelů, jako jsou WhatsApp, Messenger, Signal a iMessage, zatímco používání SMS a tradičních telefonních hovorů celosvětově drasticky klesá[41].

Skupina na vysoké úrovni zdůraznila, že tento vývoj má dopad na schopnost donucovacích a justičních orgánů shromažďovat důkazy při vyšetřování a stíhání trestných činů, neboť většina zákonně odposlouchávaných komunikací se stává nepoužitelnou. Dále pak skupina na vysoké úrovni podtrhla, že členské státy mají omezené odborné znalosti a kapacity pro dešifrování

events/events/forensic-experts-forum-2024-conference); Dny průmyslu a výzkumu Europolu (https://www.europol.europa.eu/publications-events/events/europol-industry-and-research-days-2025).

[39] Doporučení blok 1, závěrečná zpráva skupiny na vysoké úrovni.

[40] Tyto snahy by měly být podpořeny vhodným zdrojem financování EU (programy pro výzkum nebo vývoj, v závislosti na úrovni vyspělosti plánovaných systémů).

[41] Uvedené procento se vztahuje na šifrování mezi koncovými body během přenosu.

neaktivních údajů, přičemž existují značné rozdíly v míře úspěšnosti, která se pohybuje od 15–20 % v některých členských státech po více než 66 % v jiných.

Dešifrovací zařízení jsou drahá a vysoce specializovaná a hardware spotřebovává mnoho zdrojů. Většina oddělení donucovacích orgánů, která se věnují digitální forenzní analýze, se při přístupu údajům na zařízeních spoléhá na komerční řešení. Tato řešení mají problém držet krok s technologickým vývojem a rychle zastarávají; vysoké náklady na licence výrazně snižují počet oprávněných uživatelů; navíc jsou řešení jsou často vyvíjena mimo EU, a proto nemusí splňovat potřeby orgánů EU nebo normy digitální forenzní analýzy. V důsledku toho se úspěšně používají jen ve velmi malém počtu vyšetřování.

Spoléhání se na tyto nástroje přináší navíc další nevýhody. Orgány při vyšetřování často zneužívají zranitelná místa, aby získaly přístup k dešifrovacím klíčům v zařízeních, což by v některých případech mohlo vytvořit napětí ve vztahu k politickému cíli zajistit standardně kybernetickou bezpečnost. Přístup k zašifrovaným údajům je navíc stále složitější. Skupina na vysoké úrovni konstatovala, že k údajům uloženým na určitých typech moderních zařízení, která jsou chráněna kryptografickými čipy nebo silnými šifrovacími algoritmy a složitými hesly, nemají úřady přístup ani pomocí nejvýkonnějších dešifrovacích platforem.

Vývoj a zavádění **kvantově bezpečné kryptografie** je nutností pro ochranu údajů před budoucími útoky kvantových počítačů, po nichž by citlivé komunikace, finanční transakce a státní tajemství byly zranitelné vůči dešifrování a zneužití. Jak je uvedeno v doporučení Komise o plánu pro koordinovanou implementaci přechodu na **postkvantovou kryptografii**[42] a v Evropské strategii vnitřní bezpečnosti (ProtectEU), bude pro ochranu dat v nové kvantové éře zásadní zavádění řešení postkvantové kryptografie a vývoj kvantové distribuce klíčů. Jak však zdůraznil Europol, v nadcházejících letech to ztíží zákonný přístup k digitálním důkazům a donucovací orgány musí investovat, aby udržely krok s rychlým technologickým vývojem[43].

Skupina na vysoké úrovni[44] doporučila vypracovat technologický plán, který v příslušných případech zavede cílený zákonný přístup již od fáze návrhu, při současném zajištění silné bezpečnosti a kybernetické bezpečnosti a plném dodržování právních povinností týkajících se zákonného přístupu. V reakci na to **Komise pověřuje skupinu odborníků, aby poskytla podporu při přípravě technologického plánu pro šifrování.** Skupina určí a posoudí technologická řešení, která by donucovacím orgánům umožnila zákonný přístup k zašifrovaným údajům a zároveň zaručila kybernetickou bezpečnost a základní práva. Skupina bude zahrnovat odborníky na vymáhání práva, kybernetickou bezpečnost, šifrování, komunikační technologie, normalizaci a základní práva. Tuto práci podpoří technologické studie a ověřování koncepcí. Cílem této práce je určit:

- **nástroje, které donucovací orgány v současnosti potřebují a v budoucnu budou potřebovat** k zákonnému vyhledávání, získávání a analýze zašifrovaných údajů; tyto nástroje musí usnadňovat digitální forenzní analýzu, dešifrování, sběr údajů na dálku a analýzu trestné činnosti,

[42] Doporučení o plánu pro koordinovanou implementaci přechodu na postkvantovou kryptografii.
[43] The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement (Druhá kvantová revoluce: dopad kvantové výpočetní techniky a kvantových technologií na prosazování práva) | Europol.
[44] Doporučení blok 10, závěrečná zpráva skupiny na vysoké úrovni.

- **technologie, které zajistí, aby budoucí informační a komunikační technologie**, jako je šestá generace mobilních sítí (6G) a kvantově odolné šifrování, nepoškozovaly schopnost donucovacích orgánů získávat přístup k údajům v souladu se zákonem, a zároveň zajistily dodržování základních práv a kybernetickou bezpečnost.

Pokud v současné době žádné nástroje neexistují, očekává se, že technologický plán poskytne doporučení ohledně jejich vývoje a způsobů, jak zajistit slučitelnost s právním rámcem EU a zaručit kybernetickou bezpečnost. Výsledek technologického plánu může být také podkladem pro konkrétní opatření na podporu koordinovaného přístupu k normalizaci.

Dešifrovací platforma Europolu se ukázala jako nápomocná při podpoře významných trestních případů, včetně těch, které souvisejí s případy Sky ECC[45] a EncroChat. K zajištění schopnosti donucovacích orgánů dešifrovat stále složitější algoritmy je zapotřebí posílených dešifrovacích kapacit, k nimž rovněž přispějí další investice do umělé inteligence a vysoce výkonné výpočetní techniky.

Skupina na vysoké úrovni vydala doporučení[46] zvýšit financování na podporu inovací v oblasti přístupu k údajům. V reakci na to **Komise podpoří výzkum a vývoj nových dešifrovacích kapacit** s cílem zajistit, aby byl Europol po roce 2030 dobře vybaven pro podporu členských států, a to s ohledem na nový technologický vývoj a nejpokročilejší výzkum v této oblasti. Tato iniciativa by mohla zahrnovat navýšení finančních prostředků na podporu výzkumu v oblasti dešifrování, jakož i vývoj a zavádění nástrojů členskými státy. Členské státy se budou úzce podílet na sdílení svých specifických požadavků s cílem zvýšit své kapacity, dovednosti a technické zdroje, přičemž budou vycházet z technologií navržených na úrovni EU a případně posoudí možnost společného zadávání veřejných zakázek.

Klíčová opatření

Komise:

- **předloží technologický plán pro šifrování (ve 2. čtvrtletí 2026),**
- **podpoří výzkum a vývoj nových dešifrovacích kapacit, které Europol vybaví dešifrovacími kapacitami nové generace (od roku 2030).**

V. Sladění technologie a zákonného přístupu: normalizace

Normy jsou v digitální komunikaci zásadní. Vyvinula je široká škála subjektů, většinou z daného odvětví, a zajišťují interoperabilitu mezi systémy a zařízeními vyvinutými poskytovateli technologií a usnadňují soulad technologií s právními povinnostmi, včetně zákonného přístupu pro účely prosazování práva. Evropský ústav pro telekomunikační normy (ETSI) vypracoval několik norem v oblasti zákonného odposlechu a zákonného zpřístupnění. Existují však mezery, jako například v případě páté generace mobilních sítí (5G), kde nedostatečné zohlednění zákonného přístupu při jejím vývoji zabránilo donucovacím a

[45] New major interventions to block encrypted communications of criminal networks (Nové významné zásahy za účelem zablokování šifrované komunikace zločineckých sítí) | Europol.
[46] Doporučení blok 10, závěrečná zpráva skupiny na vysoké úrovni.

justičním orgánům získat přístup k důkazům nezbytným k identifikaci pachatelů trestné činnosti a zahájení soudního řízení proti nim[47].

Skupina na vysoké úrovni doporučila zaujmout obezřetný přístup k navrhování řešení pro zákonný přístup k systémům, neboť od průmyslových subjektů by nemělo být požadováno, aby integrovaly jakýkoli systém, který by mohl oslabit šifrování obecným nebo systémovým způsobem pro všechny uživatele služby Zákonný přístup k údajům musí být i nadále cílený a omezený na konkrétní komunikace pro jednotlivé případy zvlášť.

Obecně platí, že veškerá řešení by měla být prováděna na základě jasných norem vypracovaných za přispění všech zúčastněných stran, včetně zástupců odvětví, odborníků na ochranu údajů, soukromí a kybernetickou bezpečnost a pracovníků donucovacích orgánů. Jak však zdůraznila skupina na vysoké úrovni, je třeba ohledně šifrování postupovat obezřetně. Na základě řešení uvedených v technologickém plánu se připraví konkrétní opatření na podporu koordinovaného přístupu k normalizaci.

Jakákoli normalizace by měla odrážet platné právní požadavky a měla by vycházet z vyhodnocených řešení. Musí zajistit, aby zákonný přístup nebyl v rozporu s platnými normami kybernetické bezpečnosti, jako jsou normy vypracované na základě aktu o kybernetické odolnosti, nebo normami podporujícími provádění směrnice NIS2, ani jinak nenarušoval bezpečnost produktů a služeb.

Pokud jde o doporučení skupiny na vysoké úrovni[48], **Komise vypracuje a zefektivní přístup EU k normalizaci v oblasti vnitřní bezpečnosti se zaměřením na digitální forenzní analýzu, zákonné zpřístupnění a zákonný odposlech.** Tento přístup bude založen na průběžné analýze prostředí prováděné pracovníky donucovacích orgánů, zejména prostřednictvím Evropské pracovní skupiny pro normalizaci v oblasti vnitřní bezpečnosti vedené Europolem. Tento krok rovněž rozšíří zdroje a oblast působnosti pracovní skupiny a bude zahrnovat další spolupráci s ostatními iniciativami v oblasti normalizace, zejména pokud jde o umělou inteligenci a digitální forenzní analýzu. Cílem je zajistit, aby byly do politiky normalizace začleněny otázky bezpečnosti. Kromě toho bude tato iniciativa zahrnovat rozvoj a organizaci odborného vzdělávání v oblasti normalizace zaměřeného na bezpečnost a její součástí bude i poskytování finanční podpory prostřednictvím Fondu pro vnitřní bezpečnost odborníkům, kteří se účastní příslušných fór pro normalizaci. Budou v ní začleněny také příslušné mechanismy řízení.

Klíčová opatření

- **Komise v úzké spolupráci s Europolem vypracuje a zefektivní normalizační činnosti zaměřené na zákonný přístup a podporované vhodnými mechanismy řízení (od 2. čtvrtletí 2025 do 2. čtvrtletí 2027).**

- **Členské státy se vyzývají, aby věnovaly dostatečné zdroje na zajištění účasti bezpečnostních pracovníků na příslušných fórech pro normalizaci v oblasti zákonného přístupu.**

[47] Viz First report on Encryption from the EU Innovation Hub on Internal Security (První zpráva inovačního centra EU pro vnitřní bezpečnost o šifrování), 11. června 2024.
[48] Doporučení blok 10, závěrečná zpráva skupiny na vysoké úrovni.

VI. Účinná a zákonná analýza důkazů: umělá inteligence

Europol a Eurojust nedávno konstatovaly, že stále větší počet vyšetřování obsahuje velmi velké množství údajů[49]. V případech pohlavního zneužívání dětí je běžné, že vyšetřování často vyžaduje analýzu 1 až 3 terabytů dat, což může zahrnovat 1 až 10 milionů snímků a tisíce hodin videozáznamů[50]. V roce 2023 bylo prostřednictvím nástroje pro výměnu velkých souborů (large file exchange – LFE) Europolu vyměněno 1 553 822 velkých souborů[51]. V případu EncroChat bylo odposlechnuto více než 115 milionů konverzací mezi osobami podezřelými z organizovaného zločinu. V následujících měsících se Europolu a donucovacím orgánům podařilo díky pokročilým analytickým technikám a prostředkům, jako je strojové učení, identifikovat vzorce, spojení a hotspoty, což vedlo k zatčení 6 558 podezřelých osob. Nizozemské a francouzské orgány sdílely tyto informace se svými protějšky v členských státech EU a třetích zemích, což vedlo k tomu, že jen ve Spojeném království bylo zmařeno více než 200 plánovaných vražd[52].

Neustálý nárůst objemu dat zpracovávaných v průběhu vyšetřování ztěžuje jejich ukládání, správu a efektivní analýzu, aniž by musely být využity značné odborné znalosti, výpočetní zdroje a specializované nástroje. Europol a Eurojust potvrdily, že objem dat může vyšetřovatele zahltit a vést k delší době zpracování a k problémům s kapacitou úložiště. Členské státy také často nemají mechanismy a infrastrukturu potřebnou k tomu, aby zvládly předávání velkého množství údajů jiným členským státům a Europolu.

Využívání umělé inteligence je proto pro donucovací orgány zásadní, aby mohly předcházet trestné činnosti, odhalovat ji a vyšetřovat, a tudíž chránit naše společnosti v digitálním věku. Řešení založená na umělé inteligenci mohou provádět jednoduché úkoly, jako je strojový překlad nebo převod řeči na text, nebo složitější úkoly, jako je filtrování údajů, hledání vzájemných vztahů mezi důkazy z obrovského množství dat nebo boj proti zneužívání umělé inteligence. Nástroje pro donucovací orgány využívající umělou inteligenci musí být přesné, transparentní a plně v souladu s právním rámcem EU pro umělou inteligenci, ochranu údajů a soukromí, aby bylo zajištěno důvěryhodné a etické vyšetřování založené na datech. Umělá inteligence a vysoce výkonná výpočetní technika mají zásadní význam pro získání přístupu k zašifrovaným údajům a pro podporu vyšetřování a forenzní analýzy.

Komise v návaznosti na doporučení skupiny na vysoké úrovni na zvýšení financování výzkumu a vývoje nástrojů pro analýzu dat na bázi umělé inteligence a stanovení jasných výstupů[53], **podpoří vývoj a zavádění řešení založených na umělé inteligenci.** To zahrnuje cílené investice do vývoje klíčových schopností, jako jsou řešení pro vyhledávání informací důležitých pro vyšetřování z velmi velkého množství dat při plném dodržování zásad ochrany údajů a soukromí nebo zlepšení sledování transakcí v kryptoměnách. Rovněž by bylo možné využít příležitosti pro vytváření, testování a hodnocení nástrojů umělé inteligence v regulačním

[49] Common Challenges in Cybercrime, 2024 Review by Europol and Eurojust (Společné výzvy v oblasti kyberkriminality, přezkum provedený Eurojustem a Europolem, 2024).
[50] Posouzení hrozeb organizované trestné činnosti na internetu provedené Europolem.
[51] Konsolidovaná výroční zpráva o činnosti Europolu za rok 2023.
[52] Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hackké la messagerie chiffrée utilisée par la criminalité organisée; Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized (Prolomení šifrované komunikace zločinců EncroChat vedlo k více než 6 500 zatčením a k zabavení téměř 900 milionů EUR) | Europol. EncroChat.
[53] Doporučení 4, Doporučení skupiny na vysoké úrovni.

sandboxu pro umělou inteligenci, jak je stanoveno v aktu o umělé inteligenci[54], s podporou a vedením příslušných dozorových orgánů. Kromě toho by továrny na umělou inteligenci a budoucí gigatovárny mohly podporovat vývoj nástrojů a služeb založených na umělé inteligenci pro prosazování práva. Komise by měla toto úsilí usnadnit na základě analýzy potřeb se zúčastněnými stranami, včetně inovační laboratoře Europolu a inovačního centra pro vnitřní bezpečnost agentur EU pro spravedlnost a vnitřní věci.

Členské státy mohou mít s nízkými nebo nulovými náklady přístup k příslušným kapacitám, čímž zajistí slučitelnost s požadavky aktu o umělé inteligenci. Zásadní význam má komplexní přístup k umělé inteligenci, včetně vytváření standardizovaných datových formátů pro výměny dat a vypracování pokynů pro používání těchto systémů v souladu s aktem o umělé inteligenci a platnými právními předpisy EU o ochraně údajů. Toto opatření by mohlo být podpořeno finančními prostředky z Fondu pro vnitřní bezpečnost, programu Digitální Evropa a programu Horizont Evropa. To bude zahrnovat podporu Europolu a platformy EMPACT s cílem zajistit řádný soulad s operativními potřebami a prosadit přijetí a začlenění do praxe.

Klíčová opatření

<u>Komise</u>:

- **podpoří vytváření a zavádění nových řešení umělé inteligence a bude zlepšovat stávající řešení pro filtrování a analýzu digitálních důkazů, a to i prostřednictvím plného využívání regulačních sandboxů pro umělou inteligenci pro účely jejich vývoje, testování a hodnocení v souladu s aktem o umělé inteligenci (od roku 2025 do roku 2028),**

- **naváže dialog s donucovacími orgány a dalšími zúčastněnými stranami s cílem zjistit jejich potřeby v návaznosti na práci inovační laboratoře Europolu a inovačního centra agentur EU pro spravedlnost a vnitřní věci,**

- **podpoří vytvoření jasných pokynů pro využívání umělé inteligence při prosazování práva,**

- **podpoří pilotní projekty zaměřené na vývoj a učení právně a technicky správných řešení umělé inteligence pro digitální forenzní analýzu, analýzu dat a další vyšetřovací nástroje pro použití v oblasti prosazování práva.**

[54] Viz článek 57 aktu o umělé inteligenci.