Rada
Európskej únie

V Bruseli 24. marca 2025
(OR. en)

15941/4/24
REV 4 (sk)

COSI 214
ENFOPOL 463
IXIM 234
CATS 109
COPEN 500
CYBER 342
DATAPROTECT 332

POZNÁMKA

Od:	Predsedníctvo
Komu:	Delegácie
Č. predch. dok.:	11281/24
Predmet:	Záverečná správa skupiny na vysokej úrovni pre prístup k údajom na účely účinného presadzovania práva

Predsedníctvo v mene spolupredsedov skupiny na vysokej úrovni pre prístup k údajom na účely účinného presadzovania práva predkladá delegáciám v prílohe záverečnú správu uvedenej skupiny.

Táto revidovaná verzia odráža redakčné zmeny vykonané počas jazykového preskúmania.

PRÍLOHA

Záverečná správa skupiny na vysokej úrovni pre prístup k údajom na účely účinného presadzovania práva

15. novembra 2024

Vyjadrené názory sú len názormi expertov pôsobiacich v skupine na vysokej úrovni a nemali by sa považovať za názory reprezentujúce oficiálne stanoviská Európskej komisie ani Rady.

Odporúčania, ktoré predložila skupina na vysokej úrovni pre prístup k údajom na účely účinného presadzovania práva, sa vykonávajú pri plnom rešpektovaní právomocí členských štátov. Uplatňujú sa len na činnosti v oblasti presadzovania práva a na komerčné nástroje používané na justičné účely a nie je nimi dotknutá výlučná zodpovednosť členských štátov za národnú bezpečnosť. Z rozsahu pôsobnosti týchto odporúčaní sú preto vylúčené suverénne nástroje a nástroje používané a/alebo vyvinuté výlučne na účely národnej bezpečnosti.

Obsah

Zhrnutie

Európska únia predstavuje priestor slobody, bezpečnosti a spravodlivosti, v ktorom sa rešpektujú základné práva a rozličné právne systémy a tradície členských štátov. Usiluje sa zabezpečiť vysokú úroveň bezpečnosti[1] prostredníctvom opatrení na predchádzanie trestnej činnosti a boj proti nej a uľahčiť koordináciu a spoluprácu medzi orgánmi presadzovania práva, justičnými a inými príslušnými orgánmi.

Technologický vývoj a digitalizácia našich spoločností priniesli významné zmeny v každodennom živote občanov a zároveň nové výzvy pre orgány presadzovania práva a justičné orgány pri zabezpečovaní vysokej úrovne bezpečnosti na vnútroštátnej úrovni aj na úrovni EÚ. V digitálnom veku, v ktorom žijeme, obsahuje takmer každé vyšetrovanie trestného činu digitálnu zložku. Táto otázka sa riešila v apríli 2023 v orientačnom dokumente pre expertnú skupinu na vysokej úrovni pre prístup k údajom na účely účinného presadzovania práva:

> Technológie a nástroje [...] sa zneužívajú aj na účely trestnej činnosti. V dôsledku tohto vývoja je čoraz náročnejšie pokračovať v účinnom presadzovaní práva v celej EÚ, zachovávať verejnú bezpečnosť a predchádzať, odhaľovať, vyšetrovať a stíhať trestnú činnosť, ako aj napĺňať oprávnené očakávania obetí v oblasti spravodlivosti a odškodnenia. Ak sa tejto problematike nebudeme náležite venovať, existuje skutočné riziko, že páchatelia trestnej činnosti sa stratia z dohľadu orgánov […]“. To predstavuje vážnu hrozbu pre bezpečnosť jednotlivcov a spoločnosti a môže v konečnom dôsledku brániť štátu pri vykonávaní jeho pozitívnej povinnosti naďalej zabezpečovať dodržiavanie zásad právneho štátu a fungovanie demokratickej spoločnosti[2].

[1] Na účely tohto dokumentu pojem „bezpečnosť“ znamená boj proti trestnej činnosti alebo predchádzanie ohrozeniu verejnej bezpečnosti.

[2] Dokument 8281/23 z 13. apríla 2023.

Právo na rešpektovanie súkromného a rodinného života, obydlia a komunikácie a právo na ochranu osobných údajov sú zaručené Chartou základných práv EÚ. Dôvernosť komunikácie, či už písomnej alebo telefonickej, je významným výdobytkom demokratických spoločností, zabezpečuje, že štátne ani súkromné subjekty nemôžu zasahovať do slobody prejavu ľudí a umožňuje vytvoriť prosperujúcu občiansku spoločnosť. Uplatňovanie týchto práv môže podliehať určitým zákonným obmedzeniam, najmä pokiaľ ide o opatrenia zamerané na ochranu národnej bezpečnosti, obranu alebo verejnú bezpečnosť a predchádzanie trestným činom alebo neoprávnenému používaniu elektronických komunikačných systémov, ich vyšetrovanie, odhaľovanie a stíhanie za predpokladu, že tieto opatrenia sú v rámci demokratickej spoločnosti nevyhnutné, vhodné a primerané. Orgány presadzovania práva a justičné orgány preto môžu otvárať a čítať písomnú komunikáciu, odpočúvať telefonické hovory a načúvať konverzáciám vtedy, ak sa to považuje za potrebné, primerané a odôvodnené, ak sú takéto opatrenia v súlade s uplatniteľnými právnymi ustanoveniami a ak sa vykonávajú pri náležitom dodržiavaní základných práv. Túto možnosť by mali mať k dispozícii všetky príslušné orgány bez ohľadu na technologický vývoj. V posledných rokoch sa rozšírili nové formy medziľudskej komunikácie, a preto sa celá spoločnosť musí prispôsobiť novej realite. Musíme dosiahnuť, aby komunikácia medzi občanmi zostala chránená a aby orgány presadzovania práva a justičné orgány naďalej dokázali predchádzať závažnej a organizovanej trestnej činnosti a terorizmu a bojovať proti nim a naďalej si tak plnili povinnosť chrániť občanov. Je potrebné adaptovať sa naliehavo na novú situáciu, pričom odborníci vyzývajú tvorcov politík, aby konali rýchlo, keďže orgány presadzovania práva už zaostávajú za tempom technologického vývoja, čo priamo ovplyvňuje ich schopnosť presadzovať práva občanov.

Ministri vnútra na neformálnom zasadnutí ministrov spravodlivosti a vnútorných vecí 26. januára 2023 diskutovali o výzvach, ktoré prináša technologický vývoj v oblasti presadzovania práva v digitálnom veku. Okrem iného vyjadrili obavy, že v dôsledku uplatniteľných pravidiel a ich výkladu prostredníctvom judikatúry, ako aj pre praktické a prevádzkové prekážky je pre orgány presadzovania práva čoraz náročnejšie vykonávať si prácu, najmä pokiaľ ide o uchovávanie údajov potrebných na vyšetrovanie a stíhanie trestných činov a prístup k nim[3].

[3] Pozri súhrn pripomienok členských štátov uvedený v dokumente 7184/1/23 REV 1 z 23. marca 2023.

Rada po uvedenom rokovaní schválila zriadenie **skupiny na vysokej úrovni pre prístup k údajom na účely účinného presadzovania práva (skupina na vysokej úrovni)**[4], s úlohou vypracovať strategickú výhľadovú víziu v oblasti účinného a zákonného prístupu justičných orgánov a orgánov presadzovanie práva k údajom, elektronickým dôkazom a informáciám v digitálnom veku.

Skupina na vysokej úrovni mala za cieľ vyriešiť otázku, ako umožniť zákonný prístup k údajom tak, aby sa prostredníctvom efektívnych a nadčasových riešení zachovala vysoká úroveň bezpečnosti všetkých ľudí žijúcich v EÚ a zároveň bolo zabezpečené dodržiavanie základných práv vrátane práva na súkromie a ochranu údajov, ako aj vysoká úroveň kybernetickej bezpečnosti.

Hlavným výsledkom práce skupiny na vysokej úrovni je **42 odporúčaní**[5], ktoré prichádzajú v čase, keď čoraz častejšie zaznieva volanie po vyvodzovaní zodpovednosti za online obsah. Odporúčania sa zaoberajú súčasnými a očakávanými výzvami vzhľadom na technologický vývoj a majú za cieľ pripraviť komplexný prístup EÚ k zabezpečeniu účinného vyšetrovania a stíhania trestných činov. Sú zoskupené do troch blokov: **budovanie kapacít; spolupráca s príslušným odvetvím a normalizácia; legislatívne opatrenia.** Zdôrazňujú sa v nich výzvy, pred ktorými stoja orgány presadzovania práva pri prístupe k údajom v čitateľnom formáte na účely vyšetrovania trestných činov, keďže neexistujú harmonizované povinnosti v oblasti uchovávania údajov ani prísne požiadavky judikatúry EÚ, častejšie sa využíva šifrovanie medzi koncovými zariadeniami a niektoré netradičné telekomunikačné služby nespolupracujú dostatočne. Hoci sa v odporúčaniach vítajú pravidlá týkajúce sa elektronických dôkazov, poukazuje sa v nich na to, že pri riešení výziev, ktoré predstavuje šifrovanie, majú určité obmedzenia; tiež sa v nich vyzýva na intenzívnejšiu spoluprácu medzi orgánmi presadzovania práva a justičnými orgánmi a poskytovateľmi služieb, ktorou by sa mal podporiť trvalý dialóg a vzájomné porozumenie týkajúce sa operačných, technických a obchodných potrieb a ktorou by sa mali prekonať ťažkosti pri prístupe k šifrovaným údajom. Podľa expertov sa situácia do určitej miery zlepší intenzívnejšou spoluprácou medzi orgánmi presadzovania práva a poskytovateľmi služieb, avšak nadčasové riešenie si vyžaduje aj to, aby sa povinnosť poskytovateľov služieb spolupracovať presadzovala právnymi predpismi bez toho, aby sa všeobecne alebo systematicky oslabilo šifrovanie pre používateľov služieb.

---

4 Skupina na vysokej úrovni pre prístup k údajom na účely účinného presadzovania práva – Európska komisia (europa.eu).

5 Odporúčania skupiny na vysokej úrovni.

V Rade prebehla 13. júna 2024 **výmena názorov** na odporúčania skupiny na vysokej úrovni, v ktorej sa vo všeobecnosti uvítala práca expertov tejto skupiny a zdôraznilo sa, že je potrebné urýchlene sa ďalej venovať prístupu k údajom na účely účinného presadzovania práva[6]. Ministri vnútra určili tieto priority: 1. vytvorenie harmonizovaného právneho rámca EÚ pre uchovávanie údajov na účely presadzovania práva; 2. stanovenie pravidiel účinného prístupu k údajom týkajúcim sa interpersonálnej elektronickej komunikácie a 3. zavedenie právne a technicky spoľahlivých riešení prístupu k šifrovanej elektronickej komunikácii v jednotlivých prípadoch podmieneného súdnym príkazom na účely predchádzania, vyšetrovania a stíhania závažnej a organizovanej trestnej činnosti a terorizmu.

Ministri sa okrem toho vyjadrili za posilnenie vplyvu EÚ na normalizáciu protokolov a technológií a za koordinovaný prístup k certifikácii digitálnych forenzných nástrojov a postupov. Napokon zdôraznili, že je nutné vypracovať plán vykonávania odporúčaní, ktorý bude obsahovať aj stručný harmonogram, posúdenie uskutočniteľnosti a primerané finančné zdroje. Uznali tiež, že je dôležité koordinovať vykonávanie jednotlivých odporúčaní.

Cieľom tejto záverečnej správy je podrobne opísať výzvy, ktoré určili experti, a uviesť, ako by bolo možné pokračovať v práci a **zaviesť odporúčania do praxe**. V správe sa načrtáva niekoľko kľúčových otázok identifikovaných expertmi, ktoré viedli tri pracovné okruhy v súlade s mandátom skupiny na vysokej úrovni.

Po prvé, prístup k údajom má zásadný význam pre **digitálnu forenznú analýzu**, aby orgány presadzovania práva mohli získavať a analyzovať dôkazy z elektronických zariadení. Tieto údaje poskytujú spoľahlivé informácie o trestnej činnosti a identifikácii osôb zodpovedných za trestné činy. Rýchly pokrok a rozsiahle využívanie určitých technológií, ako je šifrovanie, si vyžadujú lepšie zdroje, zručnosti a technické riešenia orgánov presadzovania práva, pokiaľ ide o prístup k šifrovaným údajom. V tejto súvislosti a so zreteľom na využívanie komerčných riešení môže účinná cezhraničná spolupráca pomôcť prostredníctvom výmeny odborných znalostí, vývoja štandardizovaných nástrojov a postupov a združovania zdrojov. Experti sa však zhodli, že samotným budovaním kapacít sa spôsobilosti v oblasti presadzovania práva nezlepšia. Ako udržateľnejšie dlhodobé riešenie uvádzali niektorí odborníci umožnenie prístupu k údajom v čitateľnom formáte za jasne regulovaných okolností.

[6] Dokument 11281/24 z 21. júna 2024.

Po druhé, na to, aby orgány presadzovania práva mohli účinne vyšetrovať a stíhať trestné činy, sú potrebné harmonizované a konzistentné právne predpisy o **uchovávaní údajov**, ktoré sú úplne v súlade so základnými právami. Z dôvodu rýchleho pokroku v oblasti technológií je čoraz cennejší včasný prístup orgánov presadzovania práva k relevantným údajom uchovávaným poskytovateľmi. Na identifikáciu podozrivých a pochopenie ich konania je nevyhnutné mať najmä prístup k metaúdajom o komunikácii uchovávaných poskytovateľmi služieb, ktorého význam pre pokrok vyšetrovaní už bol preukázaný.

Po tretie, na účinné vyšetrovanie a stíhanie organizovanej trestnej činnosti a teroristických skupín je nevyhnutné **zákonné odpočúvanie**. To orgánom umožňuje na základe súdnych príkazov a v plnom súlade so základnými právami požiadať poskytovateľov služieb, aby predložili obsah komunikácie, pričom tento obsah poskytuje neoceniteľný vhľad do trestnej činnosti. Vzhľadom na prechod od poskytovateľov tradičných komunikačných služieb k službám OTT (over-the-top) v zmysle vymedzenia v európskom kódexe elektronických komunikácií (EECC)[7], a na skutočnosť, že páchatelia trestnej činnosti čoraz viac využívajú platformy šifrované medzi koncovými zariadeniami[8], sa v záujme zákonného prístupu ku komunikácii v reálnom čase musí posúdiť, či sú potrebné jasné pravidlá spolupráce medzi orgánmi presadzovania práva a technologickými spoločnosťami a posilnená spolupráca na úrovni EÚ na uľahčenie cezhraničných žiadostí.

Odporúčania a obsah tejto záverečnej správy odrážajú len **očakávania a požiadavky expertov skupiny na vysokej úrovni**.

Touto správou **skupina na vysokej úrovni ukončila svoju prácu** a vyzýva Komisiu, členské štáty, Európsky parlament a všetky príslušné zainteresované strany, aby sa odporúčaniami a správou inšpirovali pri vypracúvaní opatrení v oblasti prístupu k údajom na účely účinného presadzovania práva. Pri opatreniach by sa mal uvádzať presvedčivý naratív, v ktorom sa preukáže, že je naliehavo potrebné prijať významné opatrenia na zabezpečenie účinného zákonného prístupu k údajom. Experti nabádajú všetky inštitúcie a orgány EÚ, aby v tejto práci bezodkladne pokračovali vykonávaním konkrétnych iniciatív prostredníctvom osobitného plánu.

---

[7] Smernicou (EÚ) 2018/1972 z 11. decembra 2018, ktorou sa stanovuje európsky kódex elektronických komunikácií, sa pôsobnosť časti právneho rámca, ktorá sa vzťahuje na tradičné telekomunikácie, rozširuje na spoločnosti, ktoré ponúkajú internetové služby prostredníctvom telekomunikačnej infraštruktúry, ktorú nevlastnia ani nespravujú, vrátane interpersonálnych komunikačných služieb nezávislých od číslovania (NI-ICS).

[8] Hodnotenie hrozieb internetovej organizovanej trestnej činnosti (IOCTA), 2024.

Zákonný prístup: hlavné výzvy

Naša schopnosť bojovať proti trestnej činnosti a zachovávať bezpečnosť EÚ sa v posledných rokoch v mnohých oblastiach zlepšila. Presadzovanie práva a justičná spolupráca sa stali účinnejšími, zaviedli sa nové právne predpisy a nástroje na boj proti závažnej a organizovanej trestnej činnosti a posilnilo sa spoločné úsilie v boji proti prevádzačstvu, obchodovaniu s ľuďmi, strelnými zbraňami a drogami, korupcii a iným závažným trestným činom.

Orgány presadzovania práva však každý deň čelia novým výzvam, pokiaľ ide o bezpečnosť našich občanov, a to najmä hrozbám, ktoré prináša digitalizácia našej spoločnosti.

Digitálne technológie menia náš život – od spôsobu, akým komunikujeme, až po to, ako žijeme a pracujeme – a spoločenské aspekty tejto zmeny sú zásadné. Digitalizácia má potenciál vyriešiť mnohé výzvy, ktorým Európa a Európania čelia, a ponúka veľké množstvo príležitostí – príležitosti na vytváranie pracovných miest, pokrok vo vzdelávaní, podporu konkurencieschopnosti a inovácie, boj proti zmene klímy, uľahčenie zelenej transformácie a ďalšie príležitosti.

Digitalizácia však vytvára aj podmienky pre páchateľov trestnej činnosti na využívanie technologického pokroku na páchanie trestných činov online aj offline. Šifrované zariadenia a aplikácie, noví operátori, virtuálne súkromné siete (VPN) atď. sú navrhnuté tak, aby chránili súkromie legitímnych používateľov. Zároveň však zločincom poskytujú účinné prostriedky na to, aby zatajovali svoju totožnosť, uvádzali na trh svoje nezákonné výrobky a služby, presmerovávali platby a zakrývali svoje činnosti a komunikáciu, čím sa účinne vyhýbajú svojmu odhaleniu, vyšetrovaniu a stíhaniu. Hoci existujú účelovo vytvorené nástroje a služby, ktoré sa primárne využívajú na protiprávne konanie, existujú dôkazy o tom, že páchatelia trestnej činnosti čoraz viac využívajú opatrenia na ochranu súkromia sprístupnené legitímnymi elektronickými komunikačnými službami (ECS). ***Orgány presadzovania práva v tejto súvislosti za páchateľmi trestnej činnosti často zaostávajú, pretože im chýba vhodný personál, nástroje a prostriedky na účinné riešenie tejto výzvy.*** V dôsledku tohto vývoja sa v posledných rokoch stal kľúčovou výzvou pre vyšetrovanie a stíhanie trestných činov prístup k údajom na účely presadzovania práva. Napriek tomu sa dosiahli pozoruhodné úspechy: orgánom presadzovania práva sa napríklad podarilo rozložiť šifrované komunikačné siete trestnej povahy, ako sú EncroChat a Sky ECC, a naďalej vykonávajú operácie ako „Desert Light“, počas ktorej bol v novembri 2022 rozložený „superkartel“ obchodníkov s kokaínom. Dešifrovacia platforma Europolu v posledných rokoch podporila niekoľko vyšetrovaní na vysokej úrovni, čím prispela k úspešným opatreniam presadzovania práva proti terorizmu a závažnej a organizovanej trestnej činnosti.

Za týmito úspešnými príbehmi sa však skrýva mnoho oneskorených a neúspešných vyšetrovaní, keďže odborníci z praxe hlásia pretrvávajúce výzvy pri včasnom plnení operačných potrieb.

Zákonný prístup sťažuje používanie technológie na účely trestnej činnosti tým, že sa orgánom umožní cielene monitorovať a odpočúvať kriminálnu komunikáciu a narúšať konanie páchateľov trestnej činnosti. Naopak, bez spoľahlivého právneho rámca a primeraných zdrojov budú orgány presadzovania práva naďalej zápasiť s neprekonateľnými ťažkosťami a existuje riziko, že kritické dôkazy zostanú z rôznych dôvodov mimo ich dosahu.

- **Údaje nie sú k dispozícii vždy**, najmä po vymazaní, z dôvodu nekonzistentných a neprimeraných pravidiel uchovávania údajov na účely presadzovania práva. Tento nedostatok vážne bráni vyšetrovaniu závažnej a organizovanej trestnej činnosti. V prieskume vykonanom v rámci projektu SIRIUS v roku 2023[9] takmer polovica oslovených vyšetrovateľov uviedla ako hlavnú prekážku absenciu harmonizovanej úpravy uchovávania údajov. Bez harmonizovaných pravidiel existuje riziko, že kľúčové údaje zostanú mimo ich dosahu, čo oslabuje úsilie o účinný boj proti trestnej činnosti.

- **Údaje nemožno získať**, najmä ak zlyhá extrakcia zo zariadenia. Nedostatok potrebných zručností, vhodných nástrojov a dostatočnej spolupráce s výrobcami zariadení a zo strany výrobcov zariadení spôsobuje, že digitálna forenzná analýza a je zložitá, nákladná a časovo náročná, ak nie úplne neuskutočniteľná. Tento významný nedostatok bráni účinnému vyšetrovaniu. Bez pokročilých forenzných spôsobilostí a zručností a lepšej spolupráce s priemyslom a medzi vnútroštátnymi orgánmi ostávajú kľúčové digitálne dôkazy nedostupné, čo má vážny vplyv na úsilie v oblasti presadzovania práva.

- **Údaje nemožno vždy prečítať**, lebo sú zašifrované. Mnohé služby v súčasnosti používajú šifrovanie medzi koncovými zariadeniami na ochranu dôvernosti komunikácie, súkromia a kybernetickej bezpečnosti, čo však môže orgánom presadzovania práva mimoriadne sťažovať prístup ku komunikačným údajom. To znamená, že aj keď sú údaje získané zákonným odpočúvaním, často nie je možné ich dekódovať. Bez schopnosti prečítať tieto údaje zostávajú dôležité dôkazy skryté, čo sťažuje vyšetrovanie trestných činov.

[9] SIRIUS – cezhraničný prístup k elektronickým dôkazom (projekt SIRIUS), https://www.europol.europa.eu/operations-services-innovation/sirius-project.

- **Údaje nemožno vždy analyzovať**, napr. nie vždy sú k dispozícii technológie a/alebo ľudské zdroje na preverovanie veľkého množstva údajov alebo na filtrovanie a analýzu zaistených údajov účinným spôsobom, ktorý je zlučiteľný so základnými hodnotami EÚ a právnymi rámcami EÚ a členských štátov.

- **Údaje nemožno získať** z dôvodu kolízie právnych poriadkov medzi jurisdikciami. Údaje často prekračujú medzinárodné hranice, čo vedie k zložitým výzvam súvisiacim s jurisdikciou. Rôzne krajiny majú rôzne zákony a iné právne predpisy týkajúce sa prístupu k údajom, čo sťažuje získavanie údajov uchovávaných v zahraničí. Nové nariadenie a smernica EÚ o elektronických dôkazoch sú dôležitými krokmi k zjednodušeniu tejto situácie, ale na úplné vykonanie týchto opatrení je ešte potrebné vykonať veľa práce – a bez úplného vykonania zostáva prístup ku kľúčovým údajom z iných krajín pre orgány presadzovanie práva veľkou výzvou.

Toto sú niektoré z každodenných výziev, ktorým v súčasnosti orgány presadzovania práva čelia.

Zločinci neustále prispôsobujú svoje správanie tak, aby unikli odhaleniu. Z dostupných štatistík[10] vyplýva, že páchatelia trestnej činnosti čoraz viac prechádzajú na legitímne platformy šifrované medzi koncovými zariadeniami. Je však pravdepodobné, že keď sa nájdu účinné protiopatrenia, opäť sa presunú na iné komunikačné kanály. Z tohto dôvodu je mimoriadne dôležité, aby orgány presadzovania práva s pomocou odborníkov zo všetkých príslušných komunít boli schopné monitorovať technologický vývoj a predvídať zmeny v správaní páchateľov, ako sú napríklad tie, ktoré súvisia so 6G, internetom vecí a satelitnou komunikáciou. Okrem toho je potrebné uchovať si kapacity, ktoré umožnili úspešné operácie proti špecializovaným komunikačným službám používaným na trestnú činnosť (napr. EncroChat, Ghost ECC), a prispôsobovať ich tak, aby mohli čeliť podobným výzvam v budúcnosti.

[10] Europol IOCTA 2024.

Orgány presadzovania práva čoraz naliehavejšie potrebujú zákonný prístup k digitálnym informáciám. Keďže páchatelia trestnej činnosti čoraz viac využívajú online služby, počet žiadostí o údaje adresovaných poskytovateľom online služieb sa zvyšuje: v rokoch 2017 až 2022 sa strojnásobil.[11] Komunikačné údaje (metaúdaje aj obsahové údaje) sú pre mnohé vyšetrovania trestných činov kľúčové. Usudzuje sa, že prístup k digitálnym dôkazom zohráva kľúčovú úlohu v 85 % vyšetrovaní[12]. Nový súbor pravidiel o cezhraničnom prístupe k elektronickým dôkazom zvýši schopnosť príslušných orgánov získať prístup k takýmto údajom. Tieto pravidlá však môžu fungovať len vtedy, keď sú údaje dostupné v čitateľnom formáte. Podobne prístup k údajom uloženým v zaistených zariadeniach a zákonné odpočúvanie komunikačnej prevádzky sú naďalej pozoruhodne náročné, a to z právneho aj praktického hľadiska. Pokiaľ ide o účinné odpočúvanie prenášaných údajov v cezhraničných prípadoch, členské štáty môžu požiadať o justičnú spoluprácu prostredníctvom dohovoru o vzájomnej právnej pomoci[13] a európskeho vyšetrovacieho príkazu[14]; tieto nástroje však boli navrhnuté zväčša so zreteľom na výmenu fyzických dôkazov a ich účinnosť môže byť v kontexte technologického vývoja obmedzená.

Zákonný prístup musí podliehať prísnym podmienkam zakotveným vo vnútroštátnom práve, v práve EÚ a medzinárodnom práve a musia byť zavedené transparentné postupy, ktorých súčasťou je zodpovednosť za ne, na reguláciu takéhoto prístupu, a to aj tým, že sa zabráni akémukoľvek nezákonnému sprístupneniu obchodného tajomstva a v prípade jeho zákonného sprístupnenia sa zabezpečí prijatie primeraných opatrení na zachovanie jeho dôvernosti.

Zákonný prístup musí v plnej miere rešpektovať zásady nevyhnutnosti a proporcionality a v prípade potreby podliehať schváleniu súdom alebo nezávislým orgánom. Prístup k údajom musí byť vyvážený spoľahlivými opatreniami na ochranu súkromia a kybernetickobezpečnostnými opatreniami (napr. šifrovanie, firewall a antivírusový a antimalvérový softvér). Zabezpečenie toho, aby bol prístup k údajom obmedzený na to, čo je nevyhnutné na účely vyšetrovania, pomáha chrániť súkromie jednotlivých používateľov.

---

11 Projekt SIRIUS.

12 Posúdenie vplyvu, ktoré vypracovala Komisia, týkajúce sa návrhov nariadenia o elektronických dôkazoch a smernice o elektronických dôkazoch (17. apríla 2018).

13 Vzájomná právna pomoc – normy Rady Európy – výbor odborníkov na uplatňovanie európskych dohovorov Rady Európy v oblasti spolupráce v trestných veciach (coe.int).

14 https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex:32014L0041

Hoci zákonný prístup k údajom na účely presadzovania práva je základom toho, aby sa našim občanom poskytla najvyššia možná úroveň bezpečnosti, nesmie to byť na úkor základných práv ani kybernetickej bezpečnosti systémov a produktov. Nesmie existovať žiadny kompromis medzi ochranou osobnej integrity a bezpečnosti ľudí na jednej strane a ich právami na strane druhej; je potrebné nájsť rovnováhu, ktorá zabezpečí, aby jeden cieľ nezasahoval do druhého. EÚ aj členské štáty majú povinnosť zabezpečiť, aby občania mohli požívať vysokú úroveň ochrany svojich základných práv a aby sa cítili bezpečne vo svojom každodennom živote. Technologický vývoj nesmie vytvárať bezpečné útočiská pre zločincov: ak existuje dôvodné podozrenie, že bol spáchaný alebo má byť spáchaný trestný čin, orgány presadzovania práva musia mať prístup k nástrojom, ktoré im umožnia prístup k príslušným údajom.

Európsky dohovor o ľudských právach, štátne ústavy a Charta základných práv EÚ uznávajú, že každý má právo na súkromný život a že to zahŕňa komunikáciu osoby. V Charte základných práv EÚ sa stanovuje aj právo na ochranu údajov. Právo na súkromie a právo na ochranu osobných údajov nie sú absolútnymi právami, ale musia sa posudzovať vo vzťahu k ich funkcii v spoločnosti[15]. Orgány verejnej moci nesmú zasahovať do výkonu týchto práv ***okrem prípadov, keď je takýto zásah v súlade so zákonom, rešpektuje podstatu práv a je nevyhnutný a primeraný v demokratickej spoločnosti.*** Za týchto podmienok môžu byť práva na súkromie a na ochranu osobných údajov obmedzené, a to aj v záujme národnej a verejnej bezpečnosti a na účely predchádzania trestnej činnosti, jej vyšetrovania, odhaľovania a stíhania.

Zásadný význam má dôsledné vyvodzovanie zodpovednosti. V našich demokratických spoločnostiach je zodpovednosťou zákonodarcov vytvoriť podmienky pre takéto vyvodzovanie zodpovednosti, čím sa zabezpečí vysoká úroveň súkromia a bezpečnosti. ***Súkromie a bezpečnosť sa navzájom nevylučujú***.

Riešenia na zabezpečenie zákonného prístupu v odôvodnených prípadoch je potrebné navrhnúť v spolupráci so všetkými príslušnými zainteresovanými stranami vrátane priemyslu s cieľom podporovať inovácie a vysokú kybernetickú bezpečnosť. ***Tieto riešenia musia byť navrhnuté tak, aby náležite zohľadňovali všetky relevantné potreby a požiadavky, a nemožno ich ponechať výlučne na uvážení technologických spoločností.***

[15] Rozsudok z 30. apríla 2024, *La Quadrature du Net a i.*, vec C-470/21, EU:C:2024:370, bod 70.

Pred prijatím ďalších krokov sa musia vykonať technické posúdenia s cieľom riešiť obavy niektorých odborníkov na kybernetickú bezpečnosť, pokiaľ ide o zložitosť zabezpečenia zákonného prístupu pri zachovaní vysokej kybernetickej bezpečnosti. ***Kybernetická bezpečnosť produktov a služieb aj zákonný prístup k údajom vyplývajú zo zákonných povinností a musia byť schopné koexistovať.*** Zákonné požiadavky na prístup sa musia vykonávať na základe jasných noriem vypracovaných všetkými príslušnými zainteresovanými stranami (vrátane zástupcov priemyslu, odborníkov na ochranu údajov a kybernetickú bezpečnosť a odborníkov z praxe v oblasti presadzovania práva), pričom sa zohľadnia príslušné právne požiadavky, a na základe riadne posúdených potenciálnych riešení, čím sa zabezpečí, aby zákonný prístup nenarúšal bezpečnosť produktov a služieb.

Mnohé spoločnosti a poskytovatelia služieb váhajú, či spolupracovať s orgánmi presadzovania práva vzhľadom na právnu neistotu spojenú s dobrovoľnými opatreniami a riziko potenciálnej negatívnej reakcie ich používateľov. Táto neochota bráni vyšetrovaniu. Okrem toho vnímanie, že používatelia uprednostňujú súkromie pred verejnou bezpečnosťou, môže spôsobovať, že subjekty v tomto odvetví sa zdráhajú sprístupniť komunikačné kanály orgánom presadzovania práva a tvoriť prispôsobené mechanizmy zaručujúce zákonný prístup. Na riešenie tohto problému je potrebný jasný právny rámec pre zákonný prístup k údajom. Platné právne predpisy obsahujú značné prekážky, ktoré komplikujú poskytovanie takéhoto prístupu, najmä na dobrovoľnom základe.

Spolupráca medzi spoločnosťami a orgánmi presadzovania práva je neprimeraná a nedostatočná a je potrebné ju doplniť jasnými pravidlami. ***Bez jasných a vymáhateľných právnych povinností spoločnosti často nie sú schopné pomáhať orgánom presadzovania práva pri prístupe k údajom***.

Keď neexistujú účinné riešenia na zabezpečenie zákonného prístupu, ***často sa za jedinú možnosť považujú riešenia založené na využívaní zraniteľností.***

Keď sa údaje získané odpočúvaním (a potenciálne iné údaje extrahované zo zariadenia) spracúvajú pomocou nástrojov navrhnutých súkromnými spoločnosťami, bez ohľadu na akékoľvek záruky, ktoré tieto spoločnosti poskytnú, vnútroštátne orgány v skutočnosti nevedia, ktoré údaje sa kontrolujú a ako, a musia sa spoliehať sa výlučne na osvedčenia poskytnuté vládou krajiny, v ktorej majú spoločnosti poskytujúce služby odpočúvania údajov sídlo. Tento problém ešte zhoršuje potreba zachovať využitú zraniteľnosť v tajnosti, aby sa zachovala účinnosť nástrojov/služieb. Táto otázka je obzvlášť pálčivá v prípadoch, keď má poskytovateľ sídlo mimo EÚ.

V neposlednom rade majú súkromné spoločnosti poskytujúce služby rušivých vyšetrovacích techník motiváciu maximalizovať svoje zisky, a preto sa môžu rozhodnúť predávať svoje nástroje režimom, ktoré nie sú demokratické (ako to bolo v prípade škandálu Hacking Team[16]).

Alternatívne môžu výzvy v oblasti prístupu k údajom ***viesť orgány presadzovania práva k vykonávaniu rušivejších vyšetrovacích úkonov***. V takýchto prípadoch sú orgány presadzovania práva nútené uchýliť sa k opatreniam, ktoré viac zasahujú do súkromia, ako je fyzické sledovanie namiesto prístupu ku geolokalizačným údajom a domové prehliadky namiesto zákonného odpočúvania.

Neschopnosť orgánov presadzovania práva získať prístup k údajom môže viesť k značnej strate dôvery verejnosti v justičný systém. Ak sa vyšetrovania oneskorujú alebo maria, občania môžu systém vnímať ako neúčinný. Takéto narušenie dôvery môže oslabiť verejný poriadok a ochotu verejnosti prispievať k úsiliu v oblasti presadzovania práva.

Zákonný prístup napokon ***umožňuje orgánom presadzovania práva zabezpečovať dôkazy s cieľom zabezpečiť spravodlivosť pre obete a chrániť ich pred ďalšou ujmou.*** Údaje môžu predstavovať dôležité indície na odhaľovanie a stíhanie rôznych druhov trestných činov, a to offline aj online. Jednotlivci môžu byť v dôsledku trestného zneužívania digitálnych technológií, služieb a komunikácií vystavení závažným formám kybernetického šikanovania, krádeže totožnosti, podvodov atď. Tieto skúsenosti môžu na obetiach zanechať vážne emocionálne a duševné dôsledky, čím sa prehlbujú existujúce nerovnosti a zraniteľnosti.

[16] Pozri https://www.cbsnews.com/news/italy-hacking-team-breach-suggest-spy-software-sold-fbi-russia-vatican/.

Pri každom vyšetrovaní trestného činu sú potrebné dôkazy na identifikáciu páchateľa alebo na preukázanie jeho zodpovednosti pred sudcom. Môžu tiež pomôcť vyviniť občana, ak bol mylne obvinený. Ak vyšetrovatelia a prokurátori nemajú prístup k potrebným informáciám, nemusia byť schopní pokročiť vo vyšetrovaní a identifikovať páchateľa, čo obeti spôsobí ďalšie ťažkosti a finančné straty a naruší dôveru v justičný systém. Samotné tradičné fyzické dôkazy nie sú vždy dostatočné na vytvorenie prepojení a nájdenie indícií. ***Orgány presadzovania práva a súdny systém musia byť pripravené na digitálny vek. Až potom budú môcť plne chrániť naše spoločnosti a hospodárstva*** pred rastúcimi hrozbami vyplývajúcimi z kybernetických útokov a hybridných hrozieb, ako aj z organizovanej trestnej činnosti.

Na záver, ak orgány presadzovania práva nemajú účinný prístup k údajom, ich schopnosť zaistiť bezpečnosť a zadržať páchateľov najzávažnejších trestných činov je výrazne oslabená. ***Orgánom presadzovania práva by sa mal poskytnúť zákonný a prísne kontrolovaný účinný prístup k údajom so spoľahlivými zárukami ochrany súkromia a kybernetickej bezpečnosti s cieľom predchádzať trestným činom, odhaľovať ich, vyšetrovať a stíhať, čo im umožní zaistiť bezpečnosť; občanom EÚ to umožní bezpečne žiť svoj život a domôcť sa spravodlivosti za trestné činy, ktoré boli na nich spáchané***.

Kapitola I: Digitálna forenzná analýza

O ČO IDE?

Digitálna forenzná analýza je získavanie, analýza a uchovávanie digitálnych dôkazov (komunikačných metaúdajov aj obsahových údajov) uložených v akejkoľvek digitálnej forme na elektronickom zariadení vrátane informácií z pevných diskov počítača, mobilných telefónov, inteligentných zariadení, navigačných systémov vozidiel, elektronických zámkov dverí, údajov uložených v cloude a iných digitálnych zariadeniach.

S narastajúcimi ťažkosťami pri prístupe ku komunikačným údajom nadobúda získavanie informácií zo zaistených zariadení (alebo zo sietí pripojených zariadení) čoraz väčší význam pre vyšetrovanie trestných činov. Prístup k údajom v zaistených zariadeniach môže orgánom presadzovania práva poskytnúť kvalitnejšie informácie týkajúce sa napríklad totožnosti členov organizovaných zločineckých skupín než iné techniky, ako je zákonné odpočúvanie. Niektorí odborníci tvrdia, že nie je možné vopred vedieť, ktoré údaje sú dôležité pre konkrétne vyšetrovanie: aj informácie, ktoré sa môžu spočiatku zdať irelevantné, sa môžu ukázať ako nevyhnutné pri napredovaní vyšetrovania. Prístup ku všetkým údajom v zariadení môže byť dôležitý aj na potvrdenie neviny podozrivého a ochranu práv odporcu[17]. Okrem toho musia byť vyšetrovacie metódy vždy primerané.

Chronický **nedostatok zdrojov** a spôsobilostí, ktorým čelia orgány presadzovania práva v tejto oblasti, zhoršuje zavádzanie nových technológií (napr. nových typov zariadení, internetu vecí a cloud computingu), ktoré si vyžadujú nové zručnosti a nástroje. Aj keď orgány a inštitúcie členských štátov už majú k dispozícii rozsiahle odborné znalosti v oblasti digitálnej forenznej analýzy, tieto poznatky sú rozptýlené a neexistujú jasné mechanizmy na výmenu a šírenie spôsobilostí, čo znamená, že zostávajú izolovanými subjektmi.

[17] Expert uviedol prípad, v ktorom analýza činnosti prístroja pomohla preukázať, že podozrivý nemohol byť zapojený do vraždy.

Hrozí, že cezhraničnú spoluprácu bude brzdiť **nedostatok porovnateľných kapacít digitálnych forenzných laboratórií** a všeobecný nedostatok normalizovaných forenzných postupov a mechanizmov umožňujúcich **uznávanie zručností a odborných znalostí expertov** v oblasti digitálnej forenznej analýzy.

Experti skupiny na vysokej úrovni sa vyjadrili jasne: štandardné **šifrovanie** údajov na zariadeniach je hlavnou výzvou, s ktorou sa orgány presadzovania práva stretávajú. Orgány presadzovania práva nemajú prístup k údajom uloženým na určitých typoch moderných zariadení, ktoré sú chránené šifrovacími čipmi[18] alebo silnými šifrovacími algoritmami a komplexnými heslami, a to ani prostredníctvom najsilnejších dešifrovacích platforiem. Šifrovanie a iné opatrenia v oblasti kybernetickej bezpečnosti a ochrany súkromia sú potrebné na ochranu informačných systémov a komunikácie a osobných údajov, ale tieto opatrenia – a najmä čoraz častejšie používanie štandardného šifrovania – znižujú schopnosť orgánov presadzovania práva zabezpečovať dôkazy.

Členské štáty majú v tejto oblasti obmedzené **odborné znalosti a spôsobilosti**: takmer všetky z nich uvádzajú, že im chýbajú technické riešenia na uspokojenie potrieb odborníkov z praxe a prevažná väčšina považuje svoje zručnosti a finančné prostriedky za nedostatočné. Schopnosť orgánov presadzovania práva dešifrovať informácie uložené na zaistených zariadeniach sa v jednotlivých členských štátoch značne líši, pričom sa pohybuje od miery úspešnosti 15 – 20 % v niektorých prípadoch až po viac ako dve tretiny v iných. Ak aj spôsobilosti existujú, zvyčajne sú neúčinné, pokiaľ ide o dešifrovanie údajov, ktoré boli zabezpečené silnými heslami, a súbory uchovávané v špeciálnych zašifrovaných schránkach. Dokonca aj v prípadoch, keď je dešifrovanie úspešné, často sa ho nepodarí vykonať včas. Dešifrovacie zariadenia sú nákladné a vysoko špecializované a hardvér je náročný na kapacitu.

Väčšina útvarov pre digitálnu forenznú analýzu orgánov presadzovania práva sa pri prístupe k údajom na zariadeniach spolieha na komerčné riešenia, čo vytvára ďalšie výzvy: tieto riešenia majú problém držať krok s technologickým vývojom a rýchlo zastarávajú; vysoké náklady na licencie výrazne znižujú počet oprávnených používateľov; a takéto riešenia sa často vyvíjajú mimo Európy a môžu byť nedostatočne prispôsobené potrebám orgánov presadzovania práva EÚ alebo nemusia spĺňať normy EÚ v oblasti digitálnej forenznej analýzy týkajúce sa vyvodzovania zodpovednosti.

[18] Napríklad bezpečnostný čip T2 na novších laptopoch Apple.

Orgány presadzovania práva často nemajú inú možnosť ako využívať na získanie prístupu k dešifrovacím kľúčom na zariadeniach **zraniteľnosti**. Vyšetrovacie techniky založené na tomto prístupe však treba zosúladiť s cieľom zabezpečiť bezpečnejší hardvér a softvér, ako je zakotvené v akte o kybernetickej odolnosti; systémami riadenia zraniteľnosti a sprístupňovania informácií by sa nezamýšľané dôsledky takýchto techník zmiernili. Experti zvážili alternatívne riešenia, ako napríklad povinnosť podozrivých odovzdať vyšetrovacím orgánom prvky potrebné na prístup k príslušným zariadeniam (napr. heslá). Vnútroštátne právne rámce uplatniteľné v takýchto prípadoch sa výrazne líšia a len tri členské štáty uviedli, že majú osobitné legislatívne ustanovenia, ktorými sa podozrivej osobe ukladá povinnosť poskytnúť prístup k šifrovacím kľúčom alebo dešifrovaným údajom[19]. Niektoré členské štáty ukladajú podozrivým povinnosť sprístupniť určité biometrické údaje (napr. odtlačky prstov), čím sa umožní prístup k zariadeniu; v ostatných prípadoch musia podozrivé osoby zverejniť svoje heslo. Vo všeobecnosti ide stále o oblasť, ktorá si vyžaduje ďalšie hodnotenie.

Niektoré z uvedených problémov možno zmierniť **spoločným využívaním kapacít členských** štátov, pričom sa bude rešpektovať ich výlučná právomoc v otázkach národnej bezpečnosti. Toto riešenie sa však stále zanedbáva, niekedy z dôvodu právnych obmedzení (v siedmich členských štátoch existujú obmedzenia týkajúce sa zdieľania nástrojov, zatiaľ čo päť z nich identifikovalo obmedzenia pri využívaní nástrojov, ktoré zdieľajú iné členské štáty), ale všeobecnejšie z dôvodu nedostatku zavedených mechanizmov na zdieľanie nástrojov alebo spoločné nákupy licencií.

V minulosti mali orgány presadzovania práva **jasné komunikačné kanály s výrobcami, poskytovateľmi a dodávateľmi.** To im umožnilo vypracúvať protokoly o spolupráci, čo im zase umožnilo lepšie chápať technologické novinky a v dôsledku toho uľahčilo presadzovanie práva a zároveň zabezpečilo kybernetickú bezpečnosť. Vzhľadom na tempo zavádzania nových technológií a vstupu nových spoločností na trh sa podmienky zmenili a spolupráca s priemyslom už neexistuje.

Prijatím vhodných noriem by sa mohlo umožniť formovanie protokolov produktov a technickej architektúry spôsobom, ktorým by sa zabezpečilo, že obavy orgánov presadzovania práva a technické požiadavky sa zohľadnia v počiatočnom štádiu. **Účasť orgánov presadzovania práva v príslušných normalizačných orgánoch** však nie je dostatočná, čo ovplyvňuje ich schopnosť účinne sa zúčastňovať na vývoji budúcich technologických noriem.

---

[19] Eurojust Cybercrime Judicial Monitor (Justičný monitor počítačovej kriminality), číslo 4, december 2018, s. 34, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_cybercime_judicial_monitor_4_2018.pdf.

MOŽNÉ RIEŠENIA

I. Zvýšiť a racionalizovať úsilie o posilnenie kapacity v oblasti digitálnych forenzných nástrojov

Členské štáty už majú odborné znalosti a kapacity na vykonávanie digitálnej forenznej analýzy; zdieľaním a spoločným využívaním svojich technických riešení však príslušné vnútroštátne inštitúcie a orgány môžu ťažiť zo skúseností iných orgánov a dosiahnuť významné úspory z rozsahu, čím sa znížia potrebné finančné zdroje. Členské štáty môžu ďalej skúmať príslušné riešenia, a to tak v oblasti digitálnych forenzných nástrojov, ako aj v oblasti odbornej prípravy a rozvoja zručností.

Blok odporúčaní 1

S cieľom posilniť spoluprácu a vybudovať silnejšiu kolektívnu kapacitu v oblasti digitálnej forenznej analýzy experti odporúčajú:

1. *mapovanie a prepájanie existujúcich digitálnych forenzných sietí a zriadenie sekretariátu [odporúčanie 1];*
2. *zlepšenie dostupnosti poznatkov a ich šírenie medzi expertmi [odporúčanie 1];*
3. *úvahy o mechanizmoch na združovanie poznatkov [odporúčanie 2];*
4. *zvýšenie financovania výskumu a vývoja s jasnými požadovanými výsledkami [odporúčanie 4];*
5. *podpora registra nástrojov Europolu ako centrálneho uzla pre zdieľanie nástrojov [odporúčanie 4];*
6. *uľahčenie zdieľania riešení a digitálnych forenzných nástrojov medzi členskými štátmi v prostredí dôvery (pri zohľadnení vnútroštátnych pravidiel) [odporúčanie 2];*
7. *vytvorenie mechanizmu na úrovni EÚ na spoločný nákup licencií na digitálne forenzné nástroje s cieľom zdieľať ich medzi členskými štátmi [odporúčanie 3];*
8. *podpora spolupráce s výrobcami a vývojármi digitálnych forenzných nástrojov s cieľom zefektívniť štruktúru a formát údajov získaných orgánmi presadzovania práva pomocou týchto nástrojov, v ideálnom prípade podľa dohodnutých noriem [odporúčanie 12];*
9. *vytvorenie mechanizmu/schémy hodnotenia a v relevantných prípadoch certifikácie komerčných digitálnych forenzných nástrojov na úrovni EÚ so zreteľom na akýkoľvek potenciálny negatívny vplyv na vyšetrovanie a stíhanie, ako je napríklad zvýšenie zbytočnej záťaže [odporúčanie 5].*

Viaceré organizácie, siete, združenia a projekty spájajú odborníkov z praxe a rôzne kategórie partnerov s cieľom posilniť kapacity presadzovania práva EÚ v oblasti digitálneho vyšetrovania:

- *Európska sieť ústavov forenzných vied* (ENFSI)[20] je hlavnou európskou sieťou, ktorá sa zaoberá (okrem iných tém) digitálnou forenznou analýzou; má 73 členov z 39 krajín a títo členovia sa zúčastňujú na pracovných skupinách zameraných napríklad na forenzné informačné technológie a digitálne zobrazovanie;

- *Európske združenie pre vývoj technológií na boj proti počítačovej kriminalite* (EACTDA)[21] spája orgány presadzovania práva, výskumno-technologické organizácie, partnerov z priemyslu a akademickú obec z mnohých členských štátov s cieľom uľahčiť využívanie výsledkov výskumných projektov v oblasti bezpečnosti a poskytnúť plne otestované softvérové nástroje pripravené na prevádzku bez licenčných nákladov, ako aj prístup k zdrojovému kódu pre organizácie verejnej bezpečnosti EÚ;

- Európsky úrad pre boj proti podvodom (OLAF) ponúka od roku 2007 vnútroštátnym orgánom presadzovania práva špecializovanú odbornú prípravu forenzných expertov a analytikov v digitálnej oblasti (*Digital Forensics and Analysts Training* – DFAT) s osobitným zameraním na podvody, korupciu a iné protiprávne konanie poškodzujúce finančné záujmy Únie; ročne sa vyškolí približne 175 expertov v oblasti digitálnej forenznej analýzy, čím sa buduje solídna komunita v tejto oblasti trestnej činnosti;

- iné projekty, ako sú *CYCLOPES*[22] a *I-LEAD*[23], nie sú stálymi štruktúrami, ale spájajú expertov a poskytujú relevantné analýzy nedostatkov.

Existujúce stále siete však nespájajú digitálne forenzné útvary orgánov presadzovania práva EÚ, ani organizácie, ktoré s nimi úzko spolupracujú (napríklad Centrum pre kybernetickú bezpečnosť a vyšetrovanie počítačovej kriminality Univerzity v Dubline (University College Dublin – UCD) alebo litovské Centrum excelentnosti pre odbornú prípravu, výskum a vzdelávanie v oblasti počítačovej kriminality).

---

20 https://enfsi.eu/
21 https://www.eactda.eu/index.html
22 https://www.cyclopes-project.eu/
23 https://cordis.europa.eu/project/id/740685/sk

Europol (najmä inovačné laboratórium Europolu spolu s Európskym centrom boja proti počítačovej kriminalite) už do určitej miery spolupracuje so všetkými uvedenými sieťami a preukázal schopnosť spájať značný počet odborníkov z praxe, napríklad vo forme základných skupín Európskej kliringovej rady pre inovácie (EuCB), organizovania *fóra expertov v oblasti forenzných vied*[24] a spájania expertov s príslušnými partnermi, napríklad prostredníctvom *fóra pre kybernetické inovácie*[25].

Europol ponúka aj už pripravenú infraštruktúru – platformu Europolu pre expertov (EPE), ktorá umožňuje spoluprácu a výmenu poznatkov medzi expertmi o konkrétnych témach.

Kľúčové opatrenia: Experti skupiny na vysokej úrovni vyzývajú na posilnenie spôsobilostí Europolu v oblasti digitálnej forenznej analýzy

Aktéri: Europol, Európska komisia, členské štáty)	*Harmonogram: 2028*	*Rozpočet: prerokuje sa neskôr v závislosti od výsledku prebiehajúcich rokovaní o budúcom VFR.*

- V rámci výrazného posilnenia Europolu ohláseného v politických usmerneniach pre Európsku komisiu na roky 2024 – 2029 experti skupiny na vysokej úrovni vyzývajú na posilnenie kapacity Europolu s cieľom pomôcť členským štátom **združovať zdroje, poznatky a odborné znalosti a zdieľať riešenia a digitálne forenzné nástroje** v prostredí dôvery. Suverénne nástroje a nástroje používané a/alebo vyvinuté výlučne na účely národnej bezpečnosti by sa mali vylúčiť.
- Experti skupiny na vysokej úrovni vyzývajú Europol, aby zohrával **úlohu centra** pre prístup k relevantným operačným odborným znalostiam v tejto oblasti a prípadne **vytvoril projekt podobný projektu SIRIUS v oblasti digitálnej forenznej analýzy s** cieľom uľahčiť zdieľanie poznatkov a odborných znalostí a výmenu najlepších postupov.
- Experti skupiny na vysokej úrovni vyzývajú Europol, aby zintenzívnil svoju úlohu pri **koordinácii organizácií a projektov**, ktoré prispievajú k vytváraniu znalostí v oblasti digitálnej forenznej analýzy na úrovni EÚ, a to pod vedením EuCB a s prihliadnutím na vstupy ostatných príslušných agentúr.

[24] https://www.europol.europa.eu/publications-events/events/forensic-experts-forum-2024-conference
[25] https://www.europol.europa.eu/publications-events/events/ec3-cyber-innovation-forum-2024

Existuje niekoľko finančných nástrojov na podporu výskumu a vývoja nástrojov v oblasti digitálnej forenznej analýzy.

- V rámci *Fondu pre vnútornú bezpečnosť (ISF)* Európska komisia pravidelne uverejňuje otvorené výzvy na predkladanie návrhov v oblasti počítačovej kriminality a digitálneho vyšetrovania. Napriek pomerne obmedzenému rozpočtu (v rámci súčasného VFR bolo na tieto akcie vyčlenených približne 15 miliónov EUR) sa projekty vybrané v rámci týchto výziev ukázali ako cielené a úspešné.

  Približne dve tretiny rozpočtu ISF sa prideľujú prostredníctvom zdieľaného riadenia, pričom členské štáty si vyberajú, ktoré projekty budú financovať, a preberajú zodpovednosť za ich každodenné riadenie. Členské štáty tak majú možnosť podporovať projekty v oblasti digitálnej forenznej analýzy v rámci svojich príslušných národných programov.

- Účelom osobitného cieľa *klastra Civilná bezpečnosť pre spoločnosť v rámci programu Horizont Európa* s celkovým rozpočtom 1,596 miliardy EUR na sedem rokov je podporovať bezpečné európske spoločnosti v kontexte bezprecedentných transformácií a rastúcej globálnej vzájomnej závislosti a hrozieb a zároveň posilňovať európsku kultúru slobody a spravodlivosti. V posledných rokoch sa v rámci neho podporilo niekoľko relevantných výskumných projektov, ako sú FORMOBILE[26] a EXFILES[27], ktoré podporujú odborníkov z praxe v ich každodenných činnostiach.

- *Program Digitálna Európa* je hlavným nástrojom financovania EÚ zameraným na posilnenie digitálnej infraštruktúry EÚ prostredníctvom rôznych iniciatív. Z programu s celkovým rozpočtom 7,5 miliardy EUR na obdobie 2021 až 2027 sa vyčleňujú značné zdroje osobitne na kybernetickú bezpečnosť a financuje sa z neho aj digitálna forenzná analýza.

[26] FORMOBILE – Z mobilných telefónov pred súd – Úplný FORenzný vyšetrovací reťazec zameraný na MOBILnÉ zariadenia: https://cordis.europa.eu/project/id/832800.

[27] EXFILES – Európa bojuje proti trestnej činnosti a terorizmu: https://exfiles.eu/.

Dešifrovacia platforma Europolu je jedným z hlavných projektov ISF. Táto platforma, ktorú zriadil Europol v roku 2020 v úzkej spolupráci so Spoločným výskumným centrom Európskej komisie (ďalej len „JRC“), podporuje vnútroštátne orgány presadzovania práva dešifrovaním ich digitálnych dôkazov. Jej cieľom je poskytnúť orgánom presadzovania práva udržateľné riešenie, pokiaľ ide o prístup k technickým a IT zdrojom, ktoré potrebujú. V posledných rokoch sa platforma využívala v mnohých významných prípadoch a v takmer polovici z nich priniesla zásadné výsledky, čo viedlo k niekoľkým úspechom. V roku 2023 platforma úspešne podporila 37 vyšetrovaní (v súvislosti so sexuálnym vykorisťovaním detí, s terorizmom, počítačovou kriminalitou, organizovanou trestnou činnosťou, pašovaním drog a podvodmi, ako aj dôležitými finančnými vyšetrovaniami) vrátane vyšetrovaní s vysokou prioritou, ako sú vyšetrovania vo veciach Sky ECC a Encrochat. Platforma sa stala základným nástrojom pre orgány presadzovania práva, ale nestačí na riešenie všetkých problémov súvisiacich s dešifrovaním, s ktorými sa orgány EÚ stretávajú.

Kľúčové opatrenia: Experti skupiny na vysokej úrovni vyzývajú na ďalší rozvoj a podporu využívania dešifrovacích spôsobilostí EÚ

Aktéri: Európska komisia, Eurostat	*Harmonogram: 2028*	*Rozpočet: určia členské štáty (napr. v národných programoch ISF)*

- Experti skupiny na vysokej úrovni vyzývajú Európsku komisiu, aby podporovala schopnosť vnútroštátnych orgánov získavať vysokokvalitné kontextové informácie a zároveň rešpektovať výlučnú právomoc členských štátov v otázkach národnej bezpečnosti prostredníctvom osobitného financovania (napríklad v rámci národných programov ISF) a výmeny najlepších postupov, aby mohli prispievať k zvyšovaniu efektívnosti dešifrovacej platformy Europolu.
- Experti skupiny na vysokej úrovni vyzývajú Európsku komisiu, aby podporila investície Europolu do udržiavania technických spôsobilostí a zvyšovania dešifrovacích spôsobilostí, aby sa udržiaval krok s technologickým vývojom a zohľadňoval výskum kvantovej kryptografie.
- Experti skupiny na vysokej úrovni vyzývajú Európsku komisiu, aby finančne podporovala členské štáty pri rozvoji **vnútroštátnych a regionálnych dešifrovacích spôsobilostí** s cieľom doplniť úsilie Europolu.

Existujúce programy financovania z prostriedkov EÚ ponúkajú orgánom presadzovania práva významnú podporu. Ďalším zefektívňovaním týchto príležitostí by sa zvýšil ich príspevok k zlepšeniu kapacít digitálnych forenzných oddelení/útvarov pre digitálnu forenznú analýzu a k zníženiu odkázanosti na určitých dodávateľov a toho, aby sa orgány presadzovania práva museli spoliehať na tzv. čierne skrinky, čiže nástroje, ktoré spracúvajú údaje bez toho, aby dôveryhodné orgány boli schopné overiť, ako fungujú, vyvinuté mimo EÚ.

Kroky v cykle činností (výskum, vývoj, využívanie), ktoré by sa mali prijať na dosiahnutie hmatateľnej pridanej hodnoty pre orgány presadzovania práva, sa podporujú rôznymi systémami. Aby sa v plnej miere využili príležitosti dostupné na úrovni EÚ, vnútroštátne správne orgány, orgány presadzovania práva a odborníci z praxe by si mali uvedomovať funkcie a ciele každého konkrétneho programu a mechanizmu.

Z programu Horizont Európa sa podporili rôzne úspešné projekty s aktívnou účasťou odborníkov z praxe v oblasti presadzovania práva. Horizont Európa je však výskumný program a očakávania týkajúce sa toho, ako blízko sú vyvíjané nástroje k tomu, aby boli pripravené na operačné nasadenie, by sa mali upraviť.

Cieľom projektu *Tools4LEAs* („nástroje pre orgány presadzovania práva“), financovaného z ISF a realizovaného združením EACTDA, je uľahčiť využívanie výsledkov výskumných projektov v oblasti bezpečnosti a poskytnúť plne otestované softvérové nástroje pripravené na prevádzku bez licenčných nákladov a s prístupom k zdrojovému kódu pre organizácie verejnej bezpečnosti EÚ. Projekt *Tools4LEAs* má najlepšie predpoklady na to, aby staval na výsledkoch výskumných projektov s cieľom pomôcť pri poskytovaní operačných nástrojov. Europol je zapojený do projektu *Tools4LEAs* a spolu so všetkými koncovými používateľmi, ktorí sú členmi združenia EACTDA, riadi prácu na ňom.

Rada EuCB vytvorila viac ako 15 základných skupín členských štátov s cieľom využívať nové technológie a spoločne vytvárať inovačné nástroje. Členské štáty využívajú základné skupiny EuCB na koordináciu časti vývoja inovačných nástrojov financovaných z grantov ISF, ako sú Marit-D, ProfID a webové vyhľadávacie roboty. Základné skupiny sú ideálnym rámcom, prostredníctvom ktorého môžu členské štáty koordinovať spoluvytváranie digitálnych vyšetrovacích nástrojov.

Európska komisia prostredníctvom cielených *výziev na predkladanie návrhov v rámci ISF* naďalej financuje projekty, ktoré významne prispievajú k úspechu operačných opatrení. Napríklad v rámci projektu CERBERUS sa zistili zraniteľnosti systému EncroChat, ktoré francúzskym žandárskym silám s podporou holandského národného forenzného inštitútu a UCD umožnili rozložiť ho. Projekt FREETOOL[28], ktorý vedie centrum univerzity UCD pre kybernetickú bezpečnosť a vyšetrovanie počítačovej kriminality, medzitým umožnil vývoj celého radu bezplatných nástrojov na vyšetrovanie počítačovej kriminality[29] prispôsobených osobitným požiadavkám orgánov presadzovania práva pri digitálnom vyšetrovaní a analýze. Tieto nástroje boli vyvinuté v partnerstve s orgánmi presadzovania práva a sú voľne dostupné pre komunitu takýchto orgánov. K prístupu k týmto nástrojom, ktoré na organizačnej úrovni prijali aj viaceré orgány presadzovania práva a ktoré sa používajú pri vyšetrovaniach významných prípadov, sa prihlásilo 3 000 používateľov z viac ako 100 orgánov presadzovania práva z desiatok jurisdikcií. *Program Spravodlivosť* sa vzťahuje aj na justičnú spoluprácu v trestných veciach a mohol by sa ním potenciálne podporovať cezhraničnú spoluprácu pri využívaní digitálnych vyšetrovacích nástrojov.

[28] https://www.ucd.ie/cci/projects/freetool/

[29] Nástroje sa vzťahujú na rôzne fázy vyšetrovania: získavanie spravodajských informácií z otvorených zdrojov (OSINT) pred vyhľadávaním; forenzná analýza údajov live; analýza pamäte; OSINT po vyhľadávaní a uchovávanie online zdrojov; automatizované vyhľadávanie súborov/artefaktov; forenzné správy; analýza médií; a geolokalizáciu artefaktov.

Register nástrojov Europolu (ETR) sa od svojho vytvorenia vyvinul tak, že zahŕňa viac ako 40 pokročilých nástrojov, ktoré poskytujú priamy prístup k najmodernejším technológiám pre presadzovanie práva v Európe. Každý mesiac sa pridávajú nové nástroje a register sa stal primárnym zdrojom pre odborníkov z praxe z EÚ, ktorí hľadajú softvér, ktorý by im pomohol ich vyšetrovaniach. ETR má v súčasnosti viac ako 2 700 používateľov, ktorí si viac ako 7 800 krát stiahli niektorý z rôznych nástrojov. Vnútroštátne vyšetrovacie jednotky tieto nástroje vo veľkej miere využívajú na podporu viacerých operácií, a to aj v rôznych oblastiach trestnej činnosti, ako je obchodovanie s ľuďmi, závažná a organizovaná trestná činnosť, počítačová kriminalita a sexuálne zneužívanie detí online. ETR ponúka možnosť priameho využitia pre projekty financované z prostriedkov EÚ, ktoré ponúkajú konkrétne a vyspelé výsledky a ktorých tvorcovia sú ochotní udeliť na ne licenciu Europolu na účely ich šírenia všetkým európskym orgánom presadzovania práva. Vybraní partneri z projektov INSPECTr, Tools4LEAs a FORMOBILE už zdieľali svoje nástroje cez ETR. Europol koordinuje svoju činnosť s Agentúrou EÚ pre odbornú prípravu v oblasti presadzovania práva (CEPOL) s cieľom ponúknuť používateľom školenia o nástrojoch ETR.

Okrem toho by mal program Digitálna Európa čoraz viac podporovať synergie a komplementárnosť medzi kybernetickou bezpečnosťou a bojom proti počítačovej kriminalite, ktoré sa často opierajú o rovnaké digitálne forenzné nástroje a techniky.

V súčasnosti neexistuje mechanizmus na zabezpečenie toho, aby boli digitálne forenzné nástroje v súlade s normami vyvodzovania zodpovednosti a forenznými normami v EÚ. Takýmto mechanizmom by sa malo zaistiť technické hodnotenie, ktorým sa zabezpečí, aby sa v plnej miere dodržiavala proporcionalita (t. j. poskytnutie dôkazu o tom, že nástroj umožňuje prístup k cieleným informáciám, čím sa analýza obmedzí len na to, čo je potrebné), transparentnosť a právo na obhajobu (t. j. preukázanie toho, že nástroj získava informácie, ktoré sú pravé a správne, čím sa poskytuje záruka obhajcom a nezávislým forenzným expertom, ktorí vypovedajú na súde) a iné právne požiadavky (napr. súlad s aktom o umelej inteligencii). Zvýšila by sa tým dôveryhodnosť dôkazov na súdoch, na vnútroštátnej, ako aj cezhraničnej úrovni, čím by sa posilnila cezhraničná spolupráca.

Kľúčové opatrenia: Experti skupiny na vysokej úrovni vyzývajú na cielené financovanie projektov v oblasti výskumu, vývoja a využívania digitálnych forenzných nástrojov

Aktéri: Európska komisia, Europol, členské štáty, združenie EACTDA, sieť ENFSI | *Harmonogram: od roku 2024* | *Rozpočet:*

- Experti skupiny na vysokej úrovni vyzývajú členské štáty, aby **začlenili projekty digitálnej forenznej analýzy financované v rámci ich príslušných národných programov ISF do existujúcich mechanizmov** (napr. platforma EMPACT) alebo sietí (napr. skupina ECTEG, združenie EACTDA) s cieľom využiť skúsenosti odborníkov z praxe z iných členských štátov a zároveň podporovať šírenie a využívanie výsledkov inými orgánmi presadzovania práva.

- Experti skupiny na vysokej úrovni vítajú pokračujúce úsilie Európskej komisie o podporu výskumu, vývoja a zavádzania digitálnych forenzných nástrojov prostredníctvom financovania v rámci príslušných finančných programov: **Horizont Európa, Digitálna Európa a ISF.** V závislosti od dostupných zdrojov uverejní Európska komisia každé dva roky **otvorené výzvy na predkladanie návrhov** v oblasti počítačovej kriminality a digitálneho vyšetrovania v rámci ISF.

- Experti skupiny na vysokej úrovni vítajú pokračujúce úsilie Európskej komisie o financovanie združenia **EACTDA** v rámci ISF, aby mohlo poskytovať plne otestované softvérové nástroje pripravené na prevádzku bez licenčných nákladov a s prístupom k zdrojovému kódu pre organizácie verejnej bezpečnosti EÚ.

- Experti skupiny na vysokej úrovni vítajú pokračujúce úsilie Európskej komisie o podporu, v rámci možností financovania, využívania **archívu nástrojov Europolu** ako centrálneho uzla na šírenie nástrojov; nabádajú **inovačné laboratórium Europolu**, aby pokračovalo vo svojom úsilí o zabezpečenie dôveryhodných, bezpečných, bezplatných, ľahko inštalovateľných a škálovateľných vyšetrovacích nástrojov, ktoré budú k dispozícii orgánom presadzovania práva EÚ.

- Experti skupiny na vysokej úrovni vyzývajú, aby sa ďalej zvážilo **vytvorenie systémov hodnotenia a v relevantných prípadoch certifikácie** komerčných digitálnych forenzných nástrojov na úrovni EÚ. To sa môže uskutočniť napríklad v **rámci Európskej siete ústavov forenzných vied**.

Licencie na digitálne forenzné nástroje sú pre niektoré orgány presadzovania práva nákladné a niekedy až nedostupné. Spoločným obstarávaním licencií, ktoré sa potom môžu zdieľať medzi orgánmi v rôznych členských štátoch, sa môžu vyrokovať nižšie ceny.

V rámci projektu *iProcureNet*[30] financovaného z programu Horizont Európa sa vytvorila metodika spoločného obstarávania v oblasti bezpečnosti, ako aj sieť orgánov verejného obstarávania v členských štátoch. *Európske inovačné centrum pre vnútornú bezpečnosť* by vzhľadom na svoje zloženie a organizáciu svojej práce malo dobré predpoklady na to, aby sprevádzalo vymedzenie spoločných potrieb členskými štátmi a určilo, ktoré nástroje by boli najužitočnejšie za predpokladu, že sa vytvorí špecializovaný pracovný okruh pre oblasť digitálnej forenznej analýzy.

Digitálne forenzné nástroje často prinášajú okrem nákladov aj ďalšie problémy. Napríklad údaje získané týmito nástrojmi môžu byť štruktúrované alebo prezentované vo formáte, ktorý nie je v súlade s existujúcimi vnútroštátnymi informačnými systémami používanými na ďalšie spracúvanie (napr. analýza alebo zdieľanie údajov). Preto je potrebné sformulovať súbor spoločných požiadaviek členských štátov, pokiaľ ide o štruktúru a formát údajov získaných prostredníctvom digitálnych forenzných nástrojov. Na tomto základe by orgány členských štátov mohli viesť diskusie s poskytovateľmi digitálnych forenzných nástrojov, aby sa ich požiadavky mohli náležite zohľadniť, napríklad v rámci postupov spoločného obstarávania, ako sa uvádza vyššie.

Kľúčové opatrenia: Experti skupiny na vysokej úrovni zdôrazňujú potrebu lepšieho pomeru medzi hodnotou a cenou pri obstarávaní digitálnych forenzných nástrojov

Aktéri: členské štáty, Európska komisia, Európske inovačné centrum pre vnútornú bezpečnosť, Europol	*Harmonogram: od roku 2025 (spoločné obstarávanie)*	*Rozpočet: neuvádza sa*

- Experti skupiny na vysokej úrovni vyzývajú Európsku komisiu, aby:
  - podporovala členské štáty pri **identifikovaní digitálnych forenzných nástrojov**, ktoré sú najviac potrebné na účinné vyšetrovanie (možno aj v rámci Európskeho inovačného centra pre vnútornú bezpečnosť);
  - podporovala **spoluprácu medzi operatívnymi útvarmi a kontaktnými miestami v orgánoch verejného obstarávania**, ktoré sú spojené v projekte iProcureNet;
  - zrealizovala **pilotné spoločné nákupy licencií na digitálne forenzné nástroje**.
- Experti skupiny na vysokej úrovni sa domnievajú, že **Europol** je schopný pomáhať členským štátom pri vymedzovaní **spoločných požiadaviek týkajúcich sa štruktúry a formátu údajov získaných** pomocou digitálnych forenzných nástrojov a na tomto základe podporovať spoluprácu medzi príslušnými vnútroštátnymi orgánmi a expertmi s cieľom umožniť im angažovať sa s výrobcami a vývojármi týchto nástrojov, aby sa mohli dohodnúť na normách a aby sa mohli požiadavky členských štátov náležite zohľadniť.

[30] https://www.iprocurenet.eu/

II. Výmena kapacít a zdieľanie citlivých nástrojov

Využívanie zraniteľností na prístup k dešifrovacím kľúčom na zariadeniach zostáva v súčasnosti hlavnou možnosťou, ktorú majú orgány presadzovania práva, pokiaľ ide o prístup k šifrovanému obsahu, vzhľadom na obmedzenú dostupnosť dešifrovacích spôsobilostí (napr. platformy Europolu pre dešifrovanie) a chýbajúcu účinnú spoluprácu s priemyslom alebo osobitný právny rámec na zabezpečenie zákonného prístupu k informáciám o digitálnych zariadeniach.

Aj keď sú uvedené podmienky (alebo niektoré z nich) možno do určitej miery splnené, páchatelia trestnej činnosti sa pravdepodobne spoliehajú na špecializované šifrovacie zariadenia na skrytie informácií alebo nezákonného obsahu. Preto bude v dohľadnej budúcnosti aj naďalej potrebné, aby orgány presadzovania práva využívali citlivé nástroje[31] a kapacity využívať a prípadne ich zdieľali.

Blok odporúčaní 2

Na zdieľanie citlivých nástrojov a zodpovedné riadenie súvisiacich kapacít experti odporúčajú:

1. *úvahy o vytvorení mechanizmov na zabezpečenie toho, aby sa citlivé nástroje mohli zdieľať spôsobom, ktorý plne rešpektuje vnútroštátne pravidlá [odporúčanie 1];*

2. *vytvorenie procesu zameraného na výmenu kapacít, ktoré potenciálne zahŕňajú využívanie zraniteľností, čo by umožnilo združovať poznatky a zdroje a zároveň zabezpečiť, aby sa rešpektovala dôvernosť a citlivosť informácií [odporúčanie 6];*

3. *prípadne preskúmať európsky prístup k riadeniu zraniteľností a informovaniu o nich, ktorými sa zaoberajú orgány presadzovania práva, na základe existujúcich osvedčených postupov [odporúčanie 2].*

Prostredníctvom programov Horizont Európa a ISF podporuje Európska komisia projekty (*EXFILES* a *ForRES*[32]) zamerané na zraniteľnosti a exploity softvéru, ktoré odborníkom v oblasti presadzovania práva v praxi poskytujú nástroje a protokoly na rýchlu a konzistentnú extrakciu údajov, ktoré sú však v súlade so všetkými príslušnými právnymi ustanoveniami.

---

31 „Citlivé nástroje“ sú digitálne forenzné nástroje aj nástroje taktického odpočúvania.

32 https://forres.eu

Zdieľanie citlivých nástrojov a súvisiacich kapacít medzi dôveryhodnými európskymi partnermi uľahčuje operačnú spoluprácu, umožňuje vzájomné využívanie poznatkov a vytvára úspory z rozsahu, čím sa znižujú potrebné zdroje.

Hoci stále platí, že využívanie zraniteľností je niekedy pre vyšetrovanie kľúčové, musí sa vykonávať mimoriadne citlivo a v súlade s príslušným vnútroštátnym právnym rámcom, pretože má vplyv na stav bezpečnosti hardvéru a softvéru.

Kľúčové opatrenia: Experti skupiny na vysokej úrovni vyzývajú na podporu pri zdieľaní citlivých nástrojov a zodpovednom riadení súvisiacich kapacít

Aktéri: členské štáty, Európska komisia *Harmonogram: od roku 2024* *Rozpočet: neuvádza sa*

- Experti skupiny na vysokej úrovni vyzývajú Európsku komisiu, aby naďalej podporovala projekty zamerané na zdieľanie citlivých nástrojov (digitálne forenzné nástroje aj nástroje taktického odpočúvania) a združovanie zdrojov prostredníctvom príslušných programov financovania; Komisia by tiež mohla podporiť **vytvorenie nadnárodnej platformy na štruktúrovanie a zdieľanie poznatkov**.
- Experti skupiny na vysokej úrovni vyzývajú JRC Európskej komisie, aby preskúmalo uskutočniteľnosť stanovenia **európskeho prístupu k riadeniu zraniteľností a informovaniu o nich**, ktorými sa zaoberajú orgány presadzovania práva, na základe existujúcich osvedčených postupov.

III. Kolektívne investície na rozvoj zručností a zlepšenie odborných znalostí v oblasti digitálnej forenznej analýzy

Príslušní pracovníci orgánov presadzovania práva by mali byť vyškolení na používanie vyšetrovacích nástrojov a techník obvyklých pre vyšetrovanie, pre ktoré sú príslušní, a ich odborné znalosti by sa mali certifikovať. Ich požadované a zdokumentované spôsobilosti by mali odrážať ich úlohu a mali by zahŕňať aspoň forenznú analýzu mobilných zariadení na všeobecnej úrovni (bez ohľadu na konkrétne zariadenie), témy týkajúce sa reťazca starostlivosti/dôkazov a základné informácie o druhoch získavania dôkazov, ich analýze, podávaní správ o nich a o účasti na súdnom pojednávaní. V dokumentácii by sa malo odzrkadľovať, či sa tieto spôsobilosti získali prostredníctvom odbornej prípravy alebo v praxi.

Blok odporúčaní 3

Na podporu rozvoja zručností a odborných znalostí v oblasti digitálnej forenznej analýzy vrátane dešifrovania a normalizácie experti odporúčajú:

1. *zvýšenie počtu príležitostí odbornej prípravy pre odborníkov [odporúčanie 7];*
2. *vytvorenie systému na úrovni EÚ na certifikáciu expertov v oblasti digitálnej forenznej analýzy s cieľom zaručiť kvalitu a jednotnosť poskytovanej technickej odbornej prípravy [odporúčanie 7];*
3. *investície do odstránenia nedostatkov, pokiaľ ide o technické zručnosti v oblasti normalizácie, a zvyšovanie informovanosti uzatváraním dohôd s akademickou obcou a inými relevantnými inštitúciami [odporúčanie 8].*

CEPOL poskytuje kurzy odbornej prípravy týkajúce sa niekoľkých relevantných tém[33]. Európska skupina pre vzdelávanie a odbornú prípravu v oblasti boja proti počítačovej kriminalite (ECTEG)[34] pripravuje kurzy o počítačovej kriminalite a digitálnej forenznej analýze a bezplatne ich sprístupňuje agentúre CEPOL a vnútroštátnym orgánom presadzovania práva.

Skupina ECTEG vyvinula *Decrypt*, zdroj odbornej prípravy na posilnenie zákonných dešifrovacích spôsobilostí orgánov presadzovania práva členských štátov EÚ prostredníctvom sofistikovaných stratégií zákonného zaobchádzania so zašifrovanými dôkazmi. Decrypt môže používať CEPOL, ako aj národné útvary, pričom sa využije infraštruktúra, ktorú sprístupní JRC.

---

[33] Odborná príprava vyšetrovateľa v oblasti digitálnej forenznej analýzy, forenznej analýzy mobilných zariadení, forenznej analýzy údajov live a forenznej analýzy zariadení s operačným systémom macOS.

[34] Skupina ECTEG je nezisková organizácia, ktorá združuje 30 organizácií presadzovania práva z 20 európskych krajín, medzinárodných orgánov a akademickej obce. Skupina ECTEG s podporou ISF vyvíja, propaguje a zdieľa zdroje, riešenia a materiály súvisiace s odbornou prípravou. Pozri https://www.ecteg.eu/.

Rovnako dôležité je poskytnúť základné zručnosti týkajúce sa digitálnej forenznej analýzy špecialistom prvého zásahu. Okrem iných projektov vytvorila skupina ECTEG *eFirst* („Vzdelávanie špecialistov prvého zásahu v oblasti presadzovania práva, pokiaľ ide o základné kybernetické znalosti“). eFirst je online modul odbornej prípravy zameraný na príslušníkov polície v teréne (hliadky, miesto činu, domová prehliadka) alebo príslušníkov poverených vybavením prvého oznámenia zo strany obete, pričom tempo prípravy si určujú samotní používatelia. Ponúka základné znalosti o počítačovej kriminalite a digitálnej forenznej analýze. Môže sa použiť aj ako základ pre prezenčné kurzy na policajných akadémiách.

Certifikáciou profilov expertov sa zabezpečuje, aby každá osoba mala potrebné vedomosti a zručnosti. Motivuje odborníkov, aby rozvíjali svoje zručnosti a boli informovaní o vývoji vo svojej oblasti, a podporuje aj kariérny postup a osobné uznanie. To vedie ku kvalitnejšej a presnejšej práci. Okrem toho osobná certifikácia môže:

- poskytnúť jasný a transparentný opis zručností a kompetencií expertov v oblasti digitálnej forenznej analýzy, ktorý odborníkom z praxe, ako aj vedúcim útvarov umožní určiť, koho potrebujú na splnenie potrebných požiadaviek na efektívne plnenie príslušných úloh;

- uľahčovať rozvoj a riadenie organizovania kurzov odbornej prípravy na vnútroštátnej a regionálnej úrovni a na úrovni EÚ; porovnateľná odborná príprava polície vo všetkých členských štátoch EÚ zabezpečuje, aby všetci príslušníci polície mali prístup ku konzistentnej úrovni znalostí a zručností bez ohľadu na krajinu, z ktorej pochádzajú;

- prispievať k transparentnejším súdnym konaniam;

- zvýšiť dôveru medzi vyšetrovateľmi a inými aktérmi, a tým posilniť medzinárodnú spoluprácu medzi vnútroštátnymi orgánmi presadzovania práva.

Agentúra CEPOL začala vyvíjať *sektorový kvalifikačný rámec* pre policajnú prácu so zameraním na cezhraničnú spoluprácu. Tento model sa môže uviesť do praxe na základe práce, ktorú vykonala skupina ECTEG, pokiaľ ide o certifikáciu expertov v oblasti digitálnej forenznej analýzy v rámci svojho *projektu globálnej certifikácie v oblasti počítačovej kriminality*[35].

Skupina ECTEG aj združenie EACTDA investujú časť svojich zdrojov do podpory účinnej *účasti príslušných odborníkov v oblasti presadzovania práva z praxe na normalizačných procesoch*, napríklad uľahčením získavania potrebných zručností.

Kľúčové opatrenia: Experti skupiny na vysokej úrovni vyzývajú na zlepšenie technických zručností a certifikáciu profilov

Aktéri: CEPOL, ECTEG	*Harmonogram: opatrenia práve prebiehajú; systém certifikácie expertov v oblasti digitálnej forenznej analýzy do roku 2026*	*Rozpočet:*

- Experti skupiny na vysokej úrovni vyzývajú agentúru CEPOL, aby pokračovala v **poskytovaní** kurzov odbornej prípravy (najmä kurzov odbornej prípravy školiteľov).
- Experti skupiny na vysokej úrovni vyzývajú skupinu ECTEG, aby naďalej **vyvíjala a aktualizovala** kurzy odbornej prípravy v oblasti digitálnej forenznej analýzy pre expertov a špecialistov prvého zásahu s osobitným zameraním na dešifrovanie a **aby organizovala ich skúšobné verzie**.
- Experti skupiny na vysokej úrovni vítajú pokračujúce úsilie Komisie (prostredníctvom otvorených výziev na predkladanie návrhov v rámci ISF) o podporu skupiny ECTEG, ako aj **organizáciu** kurzov odbornej prípravy na regionálnej úrovni.
- Skupina na vysokej úrovni vyzýva skupinu ECTEG, aby naďalej skúmala možnosť zavedenia systému na úrovni EÚ na certifikáciu expertov v oblasti digitálnej forenznej analýzy, a vyzýva agentúru CEPOL, aby k tomuto úsiliu čo najviac prispela na základe svojej práce na **sektorovom rámci kvalifikácií pre policajnú činnosť** a na **globálnej certifikácii v oblasti počítačovej kriminality**.
- Skupina na vysokej úrovni vyzýva skupinu ECTEG, aby naďalej uľahčovala získavanie **kompetencií a odborných znalostí v oblasti normalizačných procesov** príslušnými odborníkmi z praxe.

[35] https://www.ecteg.eu/running/gcc/

IV. Uľahčenie zákonného prístupu

Bez noriem upravujúcich zákonný prístup už v štádiu návrhu musia orgány presadzovania práva na získanie prístupu k zaisteným zariadeniam, na ktorých sú informácie chránené šifrovaním, čoraz častejšie využívať zraniteľnosti. Napriek tomu, že táto metóda môže pomôcť pokročiť vo vyšetrovaní, je spojená s vysokými finančnými nákladmi. Preto je potrebné zvážiť možné alternatívy.

Blok odporúčaní 4

S cieľom vytvoriť mechanizmy spolupráce s príslušnými partnermi z odvetvia a preskúmať možnosť zavedenia záväzných noriem a aproximácie právnych predpisov v oblasti zákonného prístupu v súlade s judikatúrou Súdneho dvora Európskej únie (SDEÚ) a Európskeho súdu pre ľudské práva odborníci odporúčajú:

1. *vytvorenie platformy (SIRIUS alebo rovnocennej platformy) na zdieľanie nástrojov, najlepších postupov a poznatkov o tom, ako získať prístup k údajom od vlastníkov a výrobcov produktov a výrobcov hardvéru [odporúčanie 11];*

2. *mapovanie kontaktných miest pre orgány presadzovania práva medzi výrobcami digitálneho hardvéru a softvéru [odporúčanie 11];*

3. *komplexné zmapovanie platných právnych predpisov v členských štátoch a vypracovanie súvisiacej príručky EÚ s cieľom podrobne opísať zákonné povinnosti výrobcov digitálneho hardvéru a softvéru, pokiaľ ide o to, vyhovieť žiadostiam orgánov presadzovania práva o údaje, pričom sa zohľadnia osobitné scenáre a požiadavky, ktoré nútia spoločnosti získať prístup k zariadeniam; [odporúčanie 25];*

4. *zriadiť výskumnú skupinu na posúdenie technickej uskutočniteľnosti povinného zabudovania zákonného prístupu (vrátane prístupu k šifrovaným údajom) pre digitálne zariadenia, pričom sa zachová a neohrozí bezpečnosť zariadení a informačné súkromie pre všetkých používateľov a zároveň sa neoslabí ani nenaruší bezpečnosť komunikácie [odporúčanie 26];*

5. *v závislosti od uvedeného mapovania vypracovať záväzné odvetvové normy pre zariadenia uvádzané na trh v EÚ s cieľom integrovať zákonný prístup a podporiť aproximáciu právnych predpisov v tejto oblasti [odporúčanie 25].*

Súčasná spolupráca orgánov presadzovania práva s priemyslom neprináša konkrétne výsledky; posilnenie spolupráce s priemyslom je potrebné na rozvoj zákonných možností prístupu k zariadeniam a aplikáciám pre orgány presadzovania práva. Napríklad v prípade záznamov z monitorovania kamerovým systémom sú orgány presadzovania práva čoraz viac konfrontované so zašifrovanými súbormi, ktoré nemožno analyzovať automatickým softvérom, najmä ak ide o veľké množstvo videozáznamov.

Teoreticky môžu orgány presadzovania práva požiadať o podporu výrobcov zariadení, ktorí môžu zase poskytnúť zdrojový kód svojho softvéru na uľahčenie prístupu k nešifrovaným obsahovým údajom alebo poskytnúť technickú dokumentáciu zariadenia, o ktoré ide pri vyšetrovaní trestných činov.

Europol by mal dobré predpoklady na zhromažďovanie najlepších postupov (ako je zriadenie kontaktných miest pre orgány presadzovania práva) a poznatkov o tom, ako by vlastníci a výrobcovia produktov a výrobcovia hardvéru mohli uľahčiť prístup a dať ich k dispozícii všetkým orgánom presadzovania práva prostredníctvom platformy SIRIUS (alebo rovnocennej platformy).

Zároveň by sa mali zvážiť transparentnejšie riešenia umožňujúce prístup k nešifrovaným údajom na zaistených zariadeniach s cieľom zvýšiť účinnosť vyšetrovaní a zároveň zabezpečiť rovnaké podmienky pre aktérov z daného odvetvia pri súčasnom zachovaní kybernetickej bezpečnosti a ochrane súkromia.

Na základe podrobnej analýzy požiadaviek orgánov presadzovania práva, pokiaľ ide o zákonný prístup, experti naliehavo vyzývajú Európsku komisiu, aby vypracovala *technologický plán*[36], v ktorom sa zhromaždia opatrenia expertov v oblasti technológií, kybernetickej bezpečnosti, ochrany súkromia, normalizácie a bezpečnosti a ktorým sa zabezpečí primeraná koordinácia.

Kľúčovým opatrením v rámci tohto technologického plánu by bolo posúdiť *technickú uskutočniteľnosť povinného zabudovania zákonného prístupu* (vrátane prístupu k šifrovaným údajom a šifrovaným záznamom CCTV) k digitálnym súborom a zariadeniam[37], pričom sa zároveň zabezpečia silné záruky kybernetickej bezpečnosti a neoslabí ani nenaruší bezpečnosť komunikácie. Toto posúdenie by sa uskutočnilo so zapojením všetkých príslušných zainteresovaných strán.

---

[36] V správe sa vo viacerých prípadoch a kapitolách odkazuje na jedinečný „technologický plán“.

[37] Pozri „Moving the Encryption Policy Conversation Forward“ („Pokrok v debate o politike v oblasti šifrovania“) – Carnegieho nadácia pre medzinárodný mier – https://carnegieendowment.org/research/2019/09/moving-the-encryption-policy-conversation-forward?lang=en.

V rozsahu, v akom by takéto posúdenie potvrdilo dostupnosť alebo uskutočniteľnosť povinného zabudovania zákonného prístupu, ktoré spĺňajú uvedené podmienky, by sa v technologickom pláne mal vymedziť aj proces trvalej a dlhodobej *spolupráce s normalizačnými orgánmi*. Účasť orgánov presadzovania práva na tomto procese normalizácie by mohol koordinovať Europol s podporou združenia EACTDA.

Na základe mapovania platných právnych rámcov členských štátov, ktoré určujú povinnosti výrobcov digitálneho hardvéru a softvéru, pokiaľ ide o vyhovenie žiadostiam orgánov presadzovania práva o údaje, by bolo možné posúdiť potrebu *právnych predpisov alebo usmernení a odporúčaní* [na podporu aproximácie právnych predpisov v tejto oblasti].

Kľúčové opatrenia: Experti skupiny na vysokej úrovni vyzývajú na zintenzívnenie spolupráce s priemyslom, odkazujú na príslušné normy v nadchádzajúcich iniciatívach EÚ, ktoré by sa mali podporovať, a na aproximáciu právnych predpisov v oblasti zákonného prístupu v súlade s judikatúrou Súdneho dvora Európskej únie a Európskeho súdu pre ľudské práva.

Aktéri: Europol; Európska komisia	*Harmonogram: od roku 2025*	*Rozpočet: neuvádza sa*

- Experti skupiny na vysokej úrovni vyzývajú **Európsku komisiu**, aby vypracovala špecializovaný **technologický plán** na preskúmanie možností zákonného prístupu k digitálnym zariadeniam.
- Experti skupiny na vysokej úrovni vyzývajú Europol, aby zhromažďoval najlepšie postupy a poznatky o tom, ako by vlastníci a výrobcovia produktov a výrobcovia hardvéru mohli uľahčiť prístup, a dať ich k dispozícii všetkým orgánom presadzovania práva prostredníctvom platformy SIRIUS (alebo rovnocennej platformy).

Kapitola II: Uchovávanie údajov

O ČO IDE?

V minulosti mali získané dôkazy najmä fyzickú podobu, no v súčasnosti uchovávajú poskytovatelia komunikačných služieb obrovské množstvo potenciálnych dôkazov vo forme metaúdajov. Hoci digitálne údaje nie sú jediným dôkazom požadovaným v súvislosti s vyšetrovaním trestných činov, tento druh dôkazov je rozhodujúci – najmä na zistenie totožnosti podozrivých alebo záujmových osôb, ktoré môžu mať relevantné informácie – takmer pri všetkých vyšetrovaniach bez ohľadu na to, či sa týkajú trestných činov spáchaných vo fyzickom alebo digitálnom svete. Najmä v druhom prípade môžu byť komunikačné metaúdaje (najmä IP adresy a čísla portov) často jediným spôsobom, ako identifikovať podozrivého[38].

Na to, aby orgány presadzovania práva mohli vyšetrovať trestné činy v digitálnom veku, je preto potrebné, aby sa digitálne dôkazy sprístupnili v čitateľnom formáte a aby boli v prípade potreby prístupné s náležitým ohľadom na primerané záruky pre trestné konanie, procesné práva a ochranu súkromia a údajov. Údaje sa môžu uchovávať na obchodné účely (ako je účtovanie a fakturácia) alebo na účely presadzovania práva. Uchovávanie údajov môže pomôcť zabezpečiť dostupnosť údajov, aby k nim mali príslušné orgány prístup v súvislosti s vyšetrovaním trestných činov a trestným stíhaním. Údaje uchovávané poskytovateľmi môžu mať kľúčový význam pre účinný boj proti trestnej činnosti a uchovávanie takýchto údajov je predpokladom na umožnenie následného prístupu orgánov presadzovania práva a zabezpečenie toho, aby orgány presadzovania práva mohli viesť vyšetrovanie[39]. Zároveň sa v zásade minimalizácie údajov stanovenej v smernici o súkromí a elektronických komunikáciách[40] a vo všeobecnom nariadení o ochrane údajov (GDPR)[41] stanovuje, že poskytovatelia by mali uchovávať (alebo inak spracúvať) prevádzkové údaje len dovtedy, kým je to potrebné na účely samotnej komunikácie, na fakturáciu alebo v osobitných situáciách na účely marketingu elektronických komunikačných služieb. Akékoľvek iné uchovávanie sa musí riadiť právnym rámcom, ktorý spĺňa požiadavky stanovené v článku 15 smernice o súkromí a elektronických komunikáciách. Tento režim odráža potrebu vyvážiť základné práva na súkromie a ochranu údajov s cieľmi opatrení na presadzovanie práva.

---

38 Odborníci diskutovali o niekoľkých príkladoch relevantnosti digitálnych údajov pri vyšetrovaniach a o počte žiadostí o údaje. Podľa jedného experta všetky vyšetrovania týkajúce sa terorizmu alebo organizovanej trestnej činnosti za posledných päť rokov využívali údaje vyžiadané od poskytovateľov. V roku 2023 bolo v jednom členskom štáte od prevádzkovateľov vyžiadaných viac ako 1 300 000 čísel na identifikáciu v trestnom konaní, pričom takmer všetky žiadosti neskôr potvrdil súdny systém.

39 V rámci tohto dokumentu sa prístup k údajom chápe ako prístup orgánov presadzovania práva, ktorý je v prípade potreby udelený vopred na základe súhlasu súdu na účely vyšetrovania trestných činov a na individuálnom základe.

40 Článok 6, smernica 2002/58/ES.

41 Článok 5 ods. 1 písm. c), nariadenie (EÚ) 2016/679.

V súčasnosti neexistujú žiadne právne predpisy EÚ upravujúce uchovávanie údajov. Súdny dvor Európskej únie v roku 2014 vyhlásil smernicu EÚ o uchovávaní údajov[42] za neplatnú, pričom zdôraznil významné zásahy do základných práv na súkromie a ochranu údajov, ktoré sú [všeobecne a nediferencovane] spojené s uchovávaním údajov pôvodne získaných poskytovateľmi služieb na účely presadzovania práva[43]. V dôsledku toho prešli vnútroštátne právne rámce zmenami, ktoré viedli k podstatným rozdielom v rámci EÚ[44]: zatiaľ čo niektoré členské štáty stále majú zavedené pravidlá, ktorými sa poskytovateľom komunikačných služieb ukladá povinnosť uchovávať určité kategórie údajov na účely presadzovania práva, iné zaviedli zmeny s cieľom splniť kritérium cieleného uchovávania prevádzkových údajov navrhnuté v príslušnej judikatúre;[45] ostatné členské štáty, a to aj v dôsledku následných rozsudkov vnútroštátnych súdov, nemajú zavedené osobitné pravidlá uchovávania údajov na účely presadzovania práva a spoliehajú sa výlučne na údaje uchovávané spoločnosťami na obchodné účely. Podmienky prístupu k takýmto údajom závisia od uplatniteľného vnútroštátneho právneho rámca a od druhu údajov (údaje o účastníkoch, prevádzkové alebo obsahové údaje). Tento nedostatok koherentných a harmonizovaných povinností uchovávania údajov v celej EÚ vedie k nezrovnalostiam medzi členskými štátmi v požiadavkách upravujúcich uchovávanie (a trvanie uchovávania) rôznych druhov metaúdajov poskytovateľmi služieb.

---

42 Smernica 2006/24/ES. Smernica ukladá členským štátom EÚ povinnosť prijať opatrenia na zabezpečenie toho, aby poskytovatelia elektronických komunikačných služieb a sietí uchovávali prevádzkové a lokalizačné údaje a súvisiace údaje potrebné na identifikáciu účastníka alebo registrovaného používateľa počas šiestich mesiacov až dvoch rokov s cieľom umožniť prístup príslušným orgánom na účely vyšetrovania, odhaľovania a stíhania závažných trestných činov, ako sú vymedzené vo vnútroštátnych právnych predpisoch.

43 Prehľad príslušnej judikatúry nájdete na: The future of national data retention obligations – How to apply Digital Rights Ireland at national level? (Budúcnosť vnútroštátnych povinností uchovávať údaje – Ako uplatňovať digitálne práva v Írsku na vnútroštátnej úrovni?) – European Law Blog (Európsky právny blog), V. Franssen; Recalibrating Data Retention in the EU - eucrim (Rekalibrácia uchovávania údajov v EÚ – eucrim); správa Eurojustu/EJCN za rok 2024. The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU (Vplyv judikatúry Súdneho dvora Európskej únie na vnútroštátne úpravy uchovávania údajov a justičnú spoluprácu v EÚ); Cybercrime Judicial Monitor (Justičný monitor počítačovej kriminality) – číslo 6; Cybercrime Judicial Monitor (Justičný monitor počítačovej kriminality) – číslo 9

44 Reakcie členských štátov na vyhlásenie smernice o ochrane údajov za neplatnú sa líšili, pričom opatrenia iniciované na vnútroštátnej úrovni zvýšili rozmanitosť vnútroštátnych systémov uchovávania údajov. Podľa správy Eurojustu/EJCN o uchovávaní údajov z roku 2024 vykonalo v období 2018 – 2022 zmeny vo svojich právnych predpisoch 12 krajín. Respondenti odpovedali, že tieto zmeny boli priamym dôsledkom rozsudkov Súdneho dvora Európskej únie vo veci C-746/18, *Prokuratuur,* a v spojených veciach C-511/18, C-512/18 a C-520/18*, La Quadrature du Net a i*. 23 z 27 členských štátov má zavedené pravidlá uchovávania údajov; sedem členských štátov už zaviedlo pravidlá cieleného uchovávania údajov. Prehľad sa nachádza v štúdii Komisie o uchovávaní neobsahových údajov z elektronických komunikácií na účely presadzovania práva, 2020, s. 39.

45 Súdny dvor rozvinul inštitút cieleného uchovávania prevádzkových a lokalizačných údajov vo viacerých rozsudkoch, pričom rozhodol, že uchovávanie údajov môže byť zlučiteľné s právom Únie, ak je navrhnuté na základe konkrétnych cieľov a na konkrétne účely. Praktické uplatňovanie kritérií navrhnutých Súdnym dvorom na určovanie takýchto cieľov však viedlo k ťažkostiam a bolo napádané na vyšších súdoch v tých členských štátoch, ktoré sa o to pokúsili.

V tých členských štátoch, ktoré nemajú povinnosť uchovávať údaje, je v rámci vyšetrovania trestného činu ťažké a niekedy nemožné identifikovať podozrivú osobu alebo osobu, ktorá môže mať relevantné informácie („záujmová osoba“)[46]. Pridaná hodnota nových pravidiel týkajúcich sa elektronických dôkazov by sa po nadobudnutí účinnosti zvýšila aj vtedy, ak by boli doplnené o povinnosti uchovávať údaje, pretože v opačnom prípade neexistuje záruka, že informácie, na ktoré sa vzťahujú európske príkazy na uchovanie alebo predloženie dôkazov (zahŕňajúce prevádzkové údaje, údaje vyžiadané výlučne na účely identifikácie používateľa a údaje o účastníkoch), budú k dispozícii.

Súčasná situácia ovplyvňuje **orgány presadzovania práva aj poskytovateľov komunikačných služieb**, ale čo je najdôležitejšie, má **vplyv na občanov a obete**, ktorých právo na prístup k spravodlivosti nemožno zabezpečiť, ak sa vyšetrovanie začne, keď už boli údaje vymazané, alebo ak neboli uchovávané[47].

I. Otázky v právomoci jednotlivých členských štátov

V členských štátoch, v ktorých **nie sú zavedené žiadne osobitné povinnosti** týkajúce sa uchovávania údajov na účely presadzovania práva, sa vyšetrovania okrem akýchkoľvek iných dostupných dôkazov opierajú o údaje, ktoré spoločnosti uchovávajú na svoje podnikateľské a obchodné účely. Obchodné údaje podliehajú interným politikám poskytovateľov, pričom spoločnosti uchovávajú prevádzkové údaje počas rôzne dlhých období (napr. približne 6 mesiacov), zatiaľ čo lokalizačné údaje, ktoré zvyčajne nemajú obchodný význam, sa často uchovávajú kratšie. Malé spoločnosti často neuchovávajú účastnícke ani komunikačné metaúdaje vôbec, alebo ich uchovávajú na veľmi krátky čas. V dôsledku toho je vyšetrovanie často pretekom s časom, keďže vyšetrovatelia musia identifikovať poskytovateľa údajov a zaslať žiadosť v súlade s platnými pravidlami pred vymazaním údajov, čo je niekedy záležitosť dní alebo hodín. V niektorých prípadoch spoločnosti neposkytujú informácie o konkrétnych údajoch, ktoré spracúvajú a uchovávajú, čo sťažuje príslušným orgánom predkladať cielené žiadosti pri získavaní údajov. Niektoré hostingové služby umožňujú používateľom prenajímať serverový priestor s použitím fiktívnych údajov, čo znamená, že aj keď uchovávajú údaje o používateľoch, nie sú spoľahlivé[48].

---

46 Pozri príklad uvedený v dokumente Background document Operational challenges faced by law enforcement related to access to data Input to the first plenary meeting of the High-Level Group (HLG) on access to data for effective law enforcement (podkladový dokument Operačné výzvy, ktorým čelia orgány presadzovania práva v súvislosti s prístupom k údajom. Vstup na prvom plenárnom zasadnutí skupiny na vysokej úrovni o prístupe k údajom na účely účinného presadzovania práva), s. 4.

47 V súvislosti s vplyvom na občanov a obete pozri *Dwyer/Commissioner of An Garda Siochána* – [2020] IESC 4 (24/02/2020), najmä bod 9.

48 https://en.wikipedia.org/wiki/Bulletproof_hosting.

Vo väčšine členských štátov právne predpisy o **uchovávaní údajov existujú**. Ako sa však uvádza vyššie, niektoré vnútroštátne právne predpisy boli predmetom zmien v nadväznosti na rozsudky Súdneho dvora Európskej únie, ktoré vyplynuli z vyhlásenia smernice o právach osôb za neplatnú. Tým sa vytvorilo rozmanité prostredie, pretože členské štáty reagovali na rozsudky odlišne. V niektorých členských štátoch sa vyvinulo úsilie o zavedenie cielenej formy uchovávania údajov, ktorú navrhol Súdny dvor Európskej únie ako možné riešenie v oblasti uchovávania údajov. Experti skupiny na vysokej úrovni však zdôraznili, že vykonávanie takýchto kritérií viedlo k právnym a technickým problémom, pokiaľ ide o ich uskutočniteľnosť[49], a poskytovatelia kritizovali náklady súvisiace s technickou implementáciou cieleného uchovávania a všeobecnejšie s často sa meniacimi právnymi predpismi. Ďalším významným právnym problémom na vnútroštátnej úrovni je, že vnútroštátne právne predpisy sa vo väčšine prípadov nevzťahujú na služby OTT (over-the-top). Osobitný prípad služieb OTT sa podrobnejšie preskúma v oddiele 1.3.

II. Cezhraničné otázky v EÚ

Problémy súvisiace s uchovávaním údajov sa vyskytujú aj v súvislosti s cezhraničnými žiadosťami, t. j keď príslušný orgán požaduje údaje od poskytovateľa so sídlom v inom členskom štáte. V prípadoch, ktoré sa týkajú cezhraničných žiadostí, orgány prijímajúcej krajiny nemusia byť schopné vybaviť žiadosť (z dôvodu chýbajúcich údajov alebo príslušných právnych predpisov) vydanú inou krajinou.

Nedostatok harmonizovaných povinností týkajúcich sa uchovávania metaúdajov v celej EÚ vedie k prekážkam pre orgány presadzovania práva v jednom členskom štáte, ktoré **žiadajú údaje** od poskytovateľov so sídlom v iných členských štátoch. Aj keď je uchovávanie údajov na vnútroštátnej úrovni upravené, nie sú zosúladené obdobia uchovávania, ktoré sa v jednotlivých členských štátoch výrazne líšia[50].

---

[49] Hoci Súdny dvor Európskej únie poskytuje určité usmernenia a príklady, ako vykladať **cielené uchovávanie** prevádzkových údajov, judikatúra môže poskytnúť len indície a nie je dostatočne presná na to, aby podrobne opísala možné obmedzenia uchovávania všetkých kategórií údajov. V dôsledku toho bolo Súdnemu dvoru v posledných rokoch predložených niekoľko návrhov na začatie konania namietajúcich voči pravidlám o uchovávaní údajov a členské štáty nie sú schopné zabezpečiť právnu istotu.

[50] V závislosti od údajov a druhu trestnej činnosti sa uchovávanie metaúdajov môže pohybovať od 6 do 72 mesiacov. V správe Eurojustu/EJCN o uchovávaní údajov z roku 2024 respondenti uviedli, že v dôsledku nedostatku uchovávaných údajov, obmedzení z hľadiska kategórie údajov, ktoré možno uchovávať, a krátkych (kratších) období uchovávania je k dispozícii menej údajov. Nedostupnosť údajov následne ovplyvňuje aj schopnosť orgánov vykonávať európske vyšetrovacie príkazy a žiadosti o vzájomnú právnu pomoc.

Rovnako neexistuje harmonizovaný prístup na úrovni EÚ k **vymedzeniu údajov**, ktoré je potrebné uchovávať[51]. Vnútroštátne právne predpisy môžu poskytovateľom služieb ukladať povinnosť uchovávať rôzne kategórie údajov na rôzne účely (dane, audity, presadzovanie práva). Líšia sa aj v tom, ako sú podrobné, pričom niektoré právne predpisy poskytujú podrobné zoznamy neobsahových údajov, ktoré sa majú uchovávať, zatiaľ čo iné obsahujú širšie vymedzenie neobsahových údajov[52]. Poskytovatelia v závislosti od služby, ktorú ponúkajú, a od svojich podnikateľských a obchodných potrieb tiež uchovávajú rôzne druhy údajov počas rôznych časových období. Výsledkom je veľmi rôznorodé prostredie, v ktorom existujú podstatné rozdiely nielen medzi členskými štátmi, ale aj medzi službami.

Takéto rozdiely sú relevantné aj z dôvodu rozdielov medzi členskými štátmi, pokiaľ ide o prístup k uchovávaným údajom: niektoré členské štáty vyžadujú na prístup k niektorým druhom metaúdajov súhlas súdu, zatiaľ čo iné nie. Poskytovatelia služieb uvádzajú, že právna neistota týkajúca sa pravidiel uplatniteľných na sprístupňovanie údajov je jednou z príčin, prečo vybavenie žiadostí orgánov presadzovania práva meška, alebo prečo sa im nevyhovie.

---

[51] Ako sa uvádza v štúdii Komisie o uchovávaní údajov, s. 48: „Hoci sa určité druhy informácií vždy klasifikujú ako údaje o účastníkoch alebo prevádzkové údaje vo všetkých členských štátoch, neexistuje konsenzus o klasifikácii týchto údajových bodov: IP adresy, čísla SIM, identifikačné čísla zariadenia (napr. IMSI, IMEI) a čísla portov pre dynamické IP adresy. V niektorých členských štátoch (EE, FR, IE) sa tieto údajové body klasifikujú ako údaje o účastníkoch, zatiaľ čo iné (DE, ES, IT, PL, SI) ich klasifikujú ako prevádzkové údaje.“

[52] Pozri štúdiu Komisie o uchovávaní údajov, príloha III, kde sa nachádza prehľad údajov uchovávaných v každom členskom štáte.

Príslušné orgány musia dodržiavať vnútroštátne predpisy týkajúce sa poskytovateľa, ktorý má k dispozícii požadované údaje, ale aj osobitné požiadavky stanovené samotnými poskytovateľmi. Ako sa uvádza vo výročnej správe SIRIUS za rok 2022[53], poskytovatelia môžu vyžadovať používanie špecializovaných portálov alebo predkladanie žiadostí podľa konkrétnych predlôh alebo v konkrétnych jazykoch. Môžu tiež požadovať informácie o povahe prípadu, jasný odkaz na vnútroštátny právny základ žiadosti alebo špecifikáciu úzkych časových rámcov pre požadované údaje. Zatiaľ čo niektoré z týchto otázok sa začnú riešiť vykonávaním balíka o elektronických dôkazoch do roku 2026, experti skupiny na vysokej úrovni zdôraznili potrebu súdržnosti medzi týmito pravidlami a akýmkoľvek potenciálnym harmonizovaným rámcom pre uchovávanie údajov. Hoci Európsky inštitút pre telekomunikačné normy (ETSI) vypracoval normy pre formát žiadostí o metaúdaje z interpersonálnych komunikačných služieb založených na číslovaní (tradičné telekomunikácie), poskytovatelia ich v členských štátoch neuplatňujú jednotne. Práca na normách pre prenos údajov od poskytovateľov služieb OTT[54] orgánom presadzovania práva stále prebieha a normy sa zatiaľ nevykonávajú v plnej miere. Okrem toho sa poskytovatelia služieb môžu slobodne rozhodnúť, v akej forme budú údaje používateľov získavať a uchovávať, čo vedie k tomu, že odborníci z praxe dostanú nespracované údaje vo veľmi odlišných formách; to predstavuje značnú záťaž pre orgány presadzovania práva, ktoré by profitovali z racionalizovaných postupov, **komunikačných systémov a formátov** na predkladanie žiadostí a na zasielanie a prijímanie odpovedí na žiadosti a údajov. Normalizované komunikačné systémy a formáty by takisto znížili náklady spoločností na spracovanie žiadostí.

Keď orgány presadzovania práva získajú zákonný prístup k údajom, musia byť schopné ich využívať; údaje preto musia byť **čitateľné**. Poskytovatelia však čoraz častejšie ponúkajú služby, ktoré umožňujú šifrovanie prevádzkových údajov medzi koncovými zariadeniami, a keď tieto údaje na požiadanie poskytnú orgánom presadzovania práva a justičným orgánom, často ich poskytujú v tejto zašifrovanej forme.

---

[53] sirius-eu-digital-evidence-situation-report-2022, s. 14.

[54] V tejto správe sa „komunikačné služby over-the-top (OTT)“ vzťahujú na aplikácie a služby, ktoré poskytujú komunikačné a mediálne služby (ako je posielanie správ, hovory a videohovory) cez internet bez zapojenia alebo kontroly tradičných poskytovateľov telekomunikačných služieb (telekomunikačných operátorov). Medzi bežné príklady komunikačných služieb OTT patria aplikácie na odosielanie správ, ako sú WhatsApp, Telegram, Facebook Messenger; hlasové a videohovorové služby, ako sú Skype, Zoom, Google Meet, Viber; a platformy sociálnych médií, ako sú Instagram a Snapchat (odosielanie správ a zdieľanie médií).

Napokon ďalší vnímaný dôsledok tohto *status quo* súvisí s rizikom, že dôkazy orgánov presadzovania práva budú na súdoch napádané[55]. SDEÚ objasnil, že prípustnosť dôkazov získaných prostredníctvom uchovávania údajov je záležitosťou vnútroštátneho práva[56], pričom podlieha zásadám ekvivalencie a efektivity[57]; Rozdiely medzi vnútroštátnymi úpravami uchovávania údajov preto môžu mať vplyv na prípustnosť dôkazov v cezhraničných konaniach[58].

[55] Pozri kapitolu „Collection and admissibility of evidence“ („Zabezpečovanie a prípustnosť dôkazov“) v správe Eurojustu/EJCN o uchovávaní údajov z roku 2024.

[56] SDEÚ, rozsudok zo 6. októbra 2020, *La Quadrature du Net a i.*, vec C-511/18, EU:C:2020:791, body 222 – 228; rozsudok z 5. apríla 2022, *Commissioner of An Garda Síochána a i.*, vec C-140/20, ECLI:EU:C:2022:258, bod 127.

[57] Tamtiež, bod 223: „...avšak pod podmienkou, že nie sú menej výhodné ako procesné podmienky, ktoré upravujú podobné situácie podľa vnútroštátneho práva (zásada ekvivalencie), a nevedú k praktickému znemožneniu alebo nadmernému sťaženiu výkonu práv priznaných právom Únie (zásada efektivity).“

[58] Vo viacerých súdnych konaniach sa spochybnila prípustnosť neobsahových údajov ako dôkazov. Zhrnutie sa uvádza v štúdii Komisie o uchovávaní údajov, s. 41.

III. Otázky týkajúce sa služieb OTT a iných poskytovateľov

Zatiaľ čo uvedené problémy sa týkajú všetkých poskytovateľov elektronických komunikačných služieb, poskytovatelia služieb OTT predstavujú pre orgány presadzovania práva pri zákonnom prístupe k údajom ešte ďalšie výzvy. Na vnútroštátnej úrovni aj na úrovni EÚ sa poskytovatelia služieb OTT často domnievajú, že nie sú viazaní rovnakými povinnosťami ako poskytovatelia tradičných komunikačných služieb. Hoci poskytovatelia služieb OTT patria do rozsahu pôsobnosti EECC, skutočnosť, že sú často usadení mimo EÚ, a absencia licenčných systémov (t. j. môžu podliehať len všeobecným povoleniam) a sankcií vytvárajú neistotu, pokiaľ ide o ich povinnosť uchovávať údaje vrátane konkrétnych druhov údajov, čím sa presadzovanie práva sťažuje. Okrem toho, hoci poskytovatelia tradičných komunikačných služieb vo väčšine prípadov uchovávajú niektoré údaje na obchodné účely, ktoré umožňujú identifikáciu používateľov (napríklad čísla IP s číslom portu a časovým rámcom), neplatí to pre **poskytovateľov služieb OTT**, ktorí uchovávajú len neobsahové údaje potrebné na ich komerčné účely, v niektorých prípadoch len na krátke obdobie[59]. Poskytovatelia služieb OTT neuchovávajú žiadne neobsahové údaje spojené s dynamickou IP adresou (číslo portu a časový rámec). To môže sťažiť alebo dokonca znemožniť získanie metaúdajov o komunikácii uskutočňovanej prostredníctvom systémov, ako sú WhatsApp alebo Telegram, ktoré sa používajú čoraz viac. Ako už bolo uvedené, typy uchovávaných údajov sa takisto líšia v závislosti od ponúkanej služby. Zatiaľ čo v niektorých prípadoch poskytovatelia vydávajú usmernenia opisujúce druhy údajov, ktoré uchovávajú[60], v iných prípadoch poskytovatelia služieb OTT tieto informácie nezverejňujú. Spolu s nedostatkom povinností týkajúcich sa transparentnosti, pokiaľ ide o druhy údajov, ktoré poskytovatelia generujú, spracúvajú a uchovávajú na obchodné účely, to vedie k častým problémom pre orgány presadzovania práva, keď sa snažia zistiť, či boli údaje uchovávané, kto uchováva aké údaje a aké druhy dátových súborov možno požadovať, a v konečnom dôsledku pri zasielaní žiadostí poskytovateľom.

---

[59] Platí to najmä pre malých poskytovateľov. Podľa štúdie Komisie o uchovávaní údajov, s. 103, sa IP adresy uchovávajú v priemere 30 dní.

[60] Pozri napríklad law-enforcement-guidelines-outside-us.pdf (apple.com).

Rastúci objem žiadostí doručovaných poskytovateľom[61] spolu s potrebou spracúvať veľké dátové súbory zároveň prispieva k meškaniu alebo zamietaniu žiadostí[62]. Okrem príčin vyplývajúcich z rozhodnutí o konkrétnych obchodných modeloch poskytovateľov je to spôsobené aj **obmedzeným počtom mechanizmov spolupráce** medzi orgánmi presadzovania práva a justičnými orgánmi na jednej strane a súkromnými spoločnosťami na strane druhej.

A napokon, hoci nemusia patriť do vymedzenia poskytovateľov komunikačných služieb podľa kódexu EECC, niekoľko vznikajúcich technológií a iných digitálnych aktérov [ako sú výrobcovia automobilov a systémy umelej inteligencie pre veľké jazykové modely (LLM)] generujú a spracúvajú komunikačné metaúdaje, ktoré môžu poskytovať informácie o trestnej činnosti. Napriek rastúcemu množstvu údajov, ktoré tieto služby spracúvajú, v súčasnosti nie sú viazané povinnosťami uchovávania údajov.

MOŽNÉ RIEŠENIA

I. Posilnenie spolupráce medzi poskytovateľmi komunikačných služieb a odborníkmi z praxe

V situácii, keď zabezpečovanie digitálnych dôkazov bráni nedostatok harmonizovaných pravidiel, sa orgány presadzovania práva pri vyšetrovaní často musia spoliehať na **dobrovoľnú spoluprácu** s poskytovateľmi služieb. Hoci toto riešenie pomohlo pri určitých významných vyšetrovaniach[63], je právne neisté a nie je vždy realizovateľné: dobrovoľná spolupráca závisí od typu a veľkosti poskytovateľa služieb, pričom malí poskytovatelia v porovnaní s väčšími často uchovávajú údaje veľmi krátky čas alebo nemajú zdroje na to, aby reagovali na žiadosti orgánov presadzovania práva[64].

---

61 Podľa výročnej správy SIRIUS za rok 2023 sa množstvo žiadostí o údaje adresovaných poskytovateľom služieb každý rok neustále zvyšuje (pozri s. 66 a nasl.).

62 Výročná správa SIRIUS za rok 2023 (poznámka pod čiarou 61) poskytuje prehľad hlavných príčin meškania/zamietnutia žiadostí o elektronické dôkazy (pozri s. 68 a nasl.).

63 Pozri príklady vo výročnej správe SIRIUS za rok 2023 (poznámka pod čiarou 61), s. 19.

64 Vo výročnej správe SIRIUS za rok 2023 (poznámka pod čiarou 61), s. 79, sa uvádza, že vysoký objem žiadostí v rámci dobrovoľnej spolupráce je pre poskytovateľov služieb náročný, a odporúča sa, aby sa zúčastňovali na medzinárodných podujatiach SIRIUS, aby „menší poskytovatelia online služieb mohli využiť odborné znalosti z projektu SIRIUS v oblasti spolupráce s orgánmi s cieľom zlepšiť svoje chápanie tejto záležitosti, štruktúrovať svoje politiky reakcie na žiadosti orgánov a zabezpečiť, aby boli pripravení na nadchádzajúci legislatívny vývoj.“

Partnerstvá a spolupráca s priemyslom sa musia opierať o **jasný právny rámec**, ktorý je základným prvkom akéhokoľvek životaschopného riešenia umožňujúceho orgánom presadzovania práva a justičným orgánom prekonať ťažkosti pri zákonnom prístupe k digitálnym dôkazom. Okrem toho, že obe strany plnia svoje príslušné právne záväzky, je dôležité, aby sa medzi odborníkmi z praxe v oblasti presadzovania práva a poskytovateľmi vytvoril trvalý a dôveryhodný vzťah, aby navzájom chápali svoje potreby a mohli spoločne nájsť uskutočniteľné riešenia. Stabilné **mechanizmy spolupráce** so súkromným sektorom sú potrebné na **zvýšenie transparentnosti**, pokiaľ ide o údaje, ktoré poskytovatelia generujú a uchovávajú, a to, ako dlho sa uchovávajú, ale aj na zabezpečenie **harmonizovanej kategorizácie údajov**, ktoré sa majú uchovávať a ku ktorým sa má pristupovať, na navrhnutie **normalizovaných formátov** pre žiadosti o údaje a na vytvorenie **bezpečných kanálov** priamej výmeny medzi príslušnými orgánmi a poskytovateľmi služieb.

Možno preskúmať niekoľko možností na posilnenie takejto spolupráce, pričom niektoré z nich majú záväznú povahu („hard law“), iné pozostávajú z riešení typu „soft law“. Niektoré z riešení uvedených v tomto oddiele by bolo potrebné posúdiť v kontexte posúdenia vplyvu uvedeného v oddiele II a následne ich ustanoviť zákonmi.

Blok odporúčaní 5

S cieľom zabezpečiť, aby príslušné orgány mohli získavať relevantné údaje identifikáciou správneho držiteľa údajov, aby poskytovatelia služieb takéto žiadosti dostávali v normalizovaných formátoch a aby cezhraničná spolupráca nebola obmedzovaná kolíziou právnych poriadkov, experti odporúčajú:

1. *nadviazanie a posilnenie spolupráce medzi odborníkmi z praxe v oblasti presadzovania práva a poskytovateľmi služieb s cieľom podporiť výmenu informácií, budovanie kapacít a odbornú prípravu a vymedziť zásady a spôsoby spolupráce [odporúčanie 13], napríklad zriadením klíringového strediska, ktoré príslušným orgánom umožní identifikovať príslušných poskytovateľov služieb a lepšie cieliť zákonné žiadosti [odporúčanie 18]. Tento cieľ možno dosiahnuť:*

    a. *stavaním na existujúcich štruktúrach na úrovni EÚ, ako je SIRIUS, Európska justičná sieť (EJS)/Európska justičná sieť na boj proti počítačovej kriminalite (EJCN), internetové fórum EÚ;*

    b. *prostredníctvom memoránd o porozumení s využitím najlepších postupov zavedených v niektorých členských štátoch na vnútroštátnej úrovni [odporúčanie 14];*

2. *podporou pravidiel transparentnosti pre poskytovateľov elektronických komunikačných služieb a iných komunikačných služieb, pokiaľ ide o údaje, ktoré spracúvajú, generujú alebo uchovávajú v rámci svojej podnikateľskej činnosti, a pravidiel informovania orgánov presadzovania práva o tom, aké údaje sú k dispozícii, pričom sa zohľadnia obmedzenia vyplývajúce z dôvernosti vyšetrovaní prostredníctvom dohôd o spolupráci s poskytovateľmi služieb alebo, v prípade potreby, stanovením záväzných povinností [odporúčanie 17, odporúčanie 16];*

3. *vypracovaním racionalizovaných postupov a formátov založených na dohodnutých normách na predkladanie žiadostí poskytovateľom a doručovanie odpovedí štruktúrovaným spôsobom [odporúčanie 15] a podporou určenia jednotných kontaktných miest na spracovanie žiadostí od príslušných orgánov a kontaktov s nimi v rámci platforiem [odporúčanie 36];*

4. *zavedením mechanizmov na zabezpečenie toho, aby cezhraničné žiadosti boli zamerané na poskytovateľov služieb efektívne a aby sa zabránilo možným konfliktom, pričom pôjde o riešenie inšpirované mechanizmami pre elektronické dôkazy a zabezpečí sa súlad takýchto mechanizmov s pravidlami stanovenými v nariadení o elektronických dôkazoch [odporúčanie 19].*

V súčasnosti existujú štruktúry EÚ, ktoré príslušným aktérom umožňujú oboznámiť sa s nástrojmi a najlepšími postupmi. Spojením orgánov presadzovania práva, justičných orgánov a poskytovateľov služieb by projekt SIRIUS mohol uľahčiť výmenu poznatkov a nástrojov týkajúcich sa žiadostí o údaje používateľov, ktoré majú poskytovatelia[65], a – najmä vďaka existujúcej sieti jednotných kontaktných miest SIRIUS – by mohol slúžiť ako platforma na priame prepojenie medzi žiadajúcimi orgánmi a poskytovateľmi[66]. Projekt SIRIUS by mohol slúžiť ako **centrálny register** právnych nástrojov, judikatúry, formátov atď., ako je to v prípade cezhraničného zdieľania elektronických dôkazov[67].

Internetové fórum EÚ[68] by ako existujúce prostredie spolupráce členských štátov, internetového priemyslu a iných partnerov mohlo slúžiť ako priestor, v ktorom by sa medzi príslušnými aktérmi mohli vytvoriť priame kontakty a dôvera na úrovni EÚ, pokiaľ ide o činnosti súvisiace s prístupom k digitálnym údajom. Mohlo by prispieť k vytvoreniu a aktualizácii **otvoreného katalógu** druhov údajov, ktoré poskytovatelia a spracovávatelia údajov získavajú a spracúvajú, ktorý by mohol centrálne spravovať SIRIUS. Takýto katalóg by zmiernil súčasný nedostatok transparentnosti a poskytol by orgánom presadzovania práva a justičným orgánom väčšiu jasnosť, pokiaľ ide o to, o aké údaje môžu požiadať, a zároveň by pôsobil ako klíringové stredisko na určenie toho, komu by sa mala žiadosť zaslať. Okrem toho v prípade, že sa poskytovateľom ukladajú právne povinnosti, by mal katalóg pridanú hodnotu pri monitorovaní a posudzovaní plnenia povinností týkajúcich sa transparentnosti, pokiaľ ide o druhy údajov, ktoré poskytovatelia uchovávajú alebo inak spracúvajú.

---

65 Sieť expertov jednotných kontaktných miest SIRIUS v oblasti zákonných žiadostí o údaje podporuje najlepšie postupy a nabáda krajiny, aby si zriadili vlastné jednotné kontaktné miesta. Jednotné kontaktné miesta sú určené osoby, útvary alebo inštitúcie, ktoré centralizujú, preskúmavajú a predkladajú žiadosti štátnych orgánov poskytovateľom služieb. V súčasnosti je súčasťou tejto siete 36 orgánov presadzovania práva z 25 krajín.

66 Projekt SIRIUS slúži ako kontaktné miesto na získavanie elektronických údajov od poskytovateľov služieb so sídlom v iných jurisdikciách. SIRIUS predstavuje obmedzenú platformu na zdieľanie poznatkov a najlepších postupov pre orgány presadzovania práva a justičné komunity. V rámci projektu SIRIUS sa spravuje aktualizovaný register kontaktných údajov viac ako 1 000 spoločností so zameraním na menších, ťažko vyhľadateľných alebo niekedy neprístupných poskytovateľov služieb. Príslušné orgány sú preto schopné získať viacero adries v rámci jednej transakcie, čo im pomáha efektívnejšie zaobchádzať s veľkými objemami komplexných informácií. Projekt SIRIUS | Europol (europa.eu).

67 SIRIUS je projekt financovaný EÚ, ktorý pomáha orgánom presadzovania práva a justičným orgánom dostať sa k cezhraničným elektronickým dôkazom v kontexte vyšetrovania trestných činov a trestného konania. Tento projekt, ktorý spoločne realizujú Europol a Eurojust v úzkom partnerstve s Európskou justičnou sieťou, je ústredným referenčným bodom v EÚ pre výmenu poznatkov o cezhraničnom prístupe k elektronickým dôkazom. Projekt SIRIUS | Europol (europa.eu).

68 Internetové fórum Európskej únie (EUIF) – Európska komisia (europa.eu).

Využitím synergií s balíkom predpisov o elektronických dôkazoch by sa ušetrili náklady a zdroje a prispelo by sa k úplnému vykonávaniu právnych predpisov o elektronických dôkazoch.
Napríklad podpora orgánov presadzovania práva, aby vytvárali alebo rozširovali kapacitu jednotiek pôsobiacich ako jednotné kontaktné miesta pre (cezhraničné) žiadosti o sprístupnenie údajov, by sa mohla rozšíriť na žiadosti podané na vnútroštátnej úrovni alebo požiadavku poskytovať programy odbornej prípravy pre vyšetrovateľov a špecialistov prvého zásahu.
Rovnako by sa na účely komunikačných metaúdajov uchovávaných na základe vnútroštátnych právnych predpisov mohlo replikovať úsilie, ktoré v súčasnosti prebieha v súvislosti s vykonávaním balíka predpisov o elektronických dôkazoch s cieľom vytvoriť **digitálnu platformu**, ktorá umožní priamu výmenu medzi príslušnými orgánmi a poskytovateľmi.

Členské štáty by mohli zvážiť **memorandá o porozumení** ako nástroje na podporu spolupráce a rozvoj spoločného porozumenia medzi poskytovateľmi služieb, vládou a orgánmi presadzovania práva s cieľom podporiť uplatňovanie vnútroštátnych právnych predpisov. Pozitívne príklady v niektorých členských štátoch by mohli poskytnúť inšpiráciu pre štruktúru memoránd so zapojením všetkých príslušných aktérov (spoločností, agentúr atď.) s cieľom zabezpečiť pokrytie všetkých relevantných aspektov spolupráce (nominácia jednotných kontaktných miest pre poskytovateľov služieb a orgány presadzovania práva, technické potreby, spoločné vymedzenie kategórií údajov, ktoré sa majú poskytovať, spoločné postupy, návrh normalizovaných vzorov žiadostí, bezpečnosť údajov a opatrenia na minimalizáciu údajov atď.)[69]. Ako sa uvádza, **normalizované protokoly** na získavanie údajov od poskytovateľov (vrátane poskytovateľov služieb OTT) a na žiadosti o údaje od príslušných orgánov by boli prospešné pre orgány presadzovania práva, ako aj pre poskytovateľov služieb, ktorí by mohli vytvoriť automatizované mechanizmy na poskytovanie odpovedí, čím sa znížia náklady a ušetrí čas. Napriek tomu, že existujú rozdiely medzi **vnútroštátnymi** a **cezhraničnými žiadosťami** (v rámci elektronických dôkazov), pokiaľ ide o požiadavky, mohli by sa vypracovať postupy a kanály, prostredníctvom ktorých sa údaje požadujú, keďže normalizácia sa týka formátu požadovaných/poskytovaných údajov. Na vývoj takýchto normalizovaných formátov majú najlepšie predpoklady normalizačné orgány ako ETSI. Zapojenie odborníkov členských štátov v oblasti presadzovania práva do týchto procesov je však zatiaľ obmedzené. Z tohto dôvodu by mohla účasť členských štátov na takýchto fórach koordinovať a podporovať už existujúca **európska pracovná skupina pre normalizáciu v oblasti vnútornej bezpečnosti** pod vedením Europolu a Komisie. Práca by mohla vychádzať z existujúcich noriem vypracovaných inštitútom ETSI, ktoré by sa mohli rozšíriť na ďalšie kategórie údajov[70].

---

[69] Memorandum o porozumení Írska zo 6. apríla 2024 je určené na podporu uplatňovania zákona o komunikáciách (uchovávanie údajov) z roku 2011 (v znení zmien). Ministerstvo spravodlivosti vymenovalo nezávislého predsedu, stanovilo mandát a prizvalo zástupcov orgánov presadzovania práva a poskytovateľov služieb.

[70] TS 102 657: Spracúvanie uchovávaných údajov; Odovzdávacie rozhranie na vyžiadanie a dodanie uchovávaných údajov a kategórií uchovávaných údajov (účastník, používanie, zariadenie, prvok siete a fakturačné údaje); TS 103 120: Rozhranie pre informácie o príkaze (definuje elektronické rozhranie medzi dvoma systémami na bezpečnú výmenu informácií týkajúcich sa stanovenia a správy výkonu zákonom požadovaných opatrení; zvyčajne sa používa na zákonné odpočúvanie, ale môže sa použiť na uchovávané údaje; obvykle sa používa medzi poskytovateľom služieb na jednej strane a vládou alebo orgánom presadzovania práva, ktoré sú oprávnené požiadať o zákonné opatrenie, na strane druhej); TS 103 705: Štruktúry údajov pre zákonné zverejňovanie (v štádiu vývoja; len dátové štruktúry, žiadne odovzdávacie rozhranie, žiadna preddefinovaná stromová štruktúra, druhy a informácie vymedzené poskytovateľom služieb).

Kľúčové opatrenia: Experti skupiny na vysokej úrovni vyzývajú na podporu spolupráce a rozvoj spoločného porozumenia medzi poskytovateľmi služieb, vládou a orgánmi presadzovania práva

Aktéri: Európska komisia, členské štáty, Europol (SIRIUS), Eurojust, internetové fórum EÚ

Harmonogram: určí sa

- Experti skupiny na vysokej úrovni vyzývajú **Európsku komisiu, Europol a členské štáty**, aby zhodnotili spôsoby podpory a posilnenia spolupráce medzi orgánmi presadzovania práva a súkromnými spoločnosťami, čím sa podporí trvalý dialóg a vzájomné porozumenie operačných, technických a obchodných potrieb. V kontexte posúdenia vplyvu uvedeného v oddiele II experti skupiny na vysokej úrovni takisto vyzývajú Komisiu, aby zvážila vypracovanie osobitných povinností týkajúcich sa transparentnosti získavania údajov a stálych štruktúr spolupráce.

- Experti skupiny na vysokej úrovni vyzývajú **Európsku komisiu, Europol a Eurojust**, aby zriadili alebo podporovali existujúce platformy na výmenu informácií medzi orgánmi presadzovania práva a súdnictvom na jednej strane a poskytovateľmi komunikačných služieb na strane druhej s cieľom zostaviť katalóg údajov, ktoré generujú a uchovávajú poskytovatelia komunikačných služieb a spracovatelia údajov v rámci svojej podnikateľskej činnosti, ktorý bude spravovať SIRIUS.

- Experti skupiny na vysokej úrovni vyzývajú **členské štáty**, aby preskúmali možnosť uzavrieť dohody o spolupráci a/alebo memorandá o porozumení, v ktorých by sa spojili poskytovatelia služieb, vláda a orgány presadzovania práva s cieľom podporiť uplatňovanie vnútroštátnych právnych predpisov tým, že sa spoločne stanovia zásady a štandardné postupy.

- Experti skupiny na vysokej úrovni vyzývajú **Europol a Európsku komisiu**, aby využili už existujúcu pracovnú skupinu pre normalizáciu v oblasti vnútornej bezpečnosti s cieľom podporiť účasť členských štátov na normalizačných fórach, aby sa prispelo k vymedzeniu príslušných noriem a aby sa spoločne navrhli protokoly s podrobnými postupmi spolupráce s poskytovateľmi služieb.

- Experti skupiny na vysokej úrovni vyzývajú **Európsku komisiu, Europol, Eurojust/EJS a členské štáty**, aby využívali synergie s nástrojmi ako balík predpisov o elektronických dôkazoch na vybudovanie alebo nadobudnutie príslušných nástrojov, napríklad rozšírením využívania aktuálne vyvíjaných digitálnych platforiem tak, aby slúžili ako portály na predkladanie žiadostí.

II. Harmonizácia minimálnych pravidiel uchovávania metaúdajov poskytovateľmi komunikačných služieb a prístupu príslušných orgánov

Experti vo veľkej miere súhlasia s tým, že je potrebný harmonizovaný rámec EÚ upravujúci uchovávanie metaúdajov na účely presadzovania práva. Takýto rámec by poskytoval normalizované riešenia, ako aj jasné a vymáhateľné povinnosti poskytovateľov komunikačných služieb a spracovateľov údajov, pokiaľ ide o to, kedy a ako uchovávať údaje a za akých okolností poskytovať prístup k týmto údajom. Vymedzením jednoznačných pravidiel uchovávania a prístupu by tento rámec slúžil na poskytnutie jasných záruk, pokiaľ ide o základné práva a základné záujmy, pričom by sa zohľadnili dôsledky uplatniteľnej judikatúry, ako aj jasných pravidiel uplatniteľných na poskytovateľov komunikačných služieb, pokiaľ ide o uchovávanie a zdieľanie údajov na účely presadzovania práva. Okrem toho by takýto rámec zabezpečením uchovávania údajov podporil úplné vykonávanie balíka predpisov o elektronických dôkazoch.

Blok odporúčaní 6

S cieľom zabezpečiť, aby boli k dispozícii digitálne dôkazy potrebné na vyšetrovanie a stíhanie trestných činov, aby medzi členskými štátmi nedochádzalo k fragmentácii, pokiaľ ide o pravidlá uplatniteľné na uchovávanie a záruky týkajúce sa základných práv, najmä ochrany súkromia a ochrany údajov, slobody prejavu a práva na obhajobu vrátane práva na riadny proces, a s cieľom zabezpečiť právnu istotu pre príslušné orgány na jednej strane, ako aj pre poskytovateľov elektronických a iných komunikačných služieb na strane druhej, odborníci odporúčajú:

1. *vymedzenie kategórií metaúdajov na základe účelu ich použitia (identifikácia, lokalizácia, stanovenie alebo posúdenie online činnosti záujmovej osoby) [odporúčanie 28] s cieľom zabezpečiť, aby poskytovatelia elektronických komunikačných služieb a iných komunikačných služieb uchovávali údaje dostatočné aspoň na identifikáciu osoby [odporúčanie 27 písm. v)];*
2. *stanovenie minimálnych období uchovávania takýchto údajov;*
3. *navrhnutie podmienok prístupu k uchovávaným údajom [odporúčanie 27 bod iv)], ktoré sa líšia v závislosti od kategórie údajov, kategórie trestného činu (napr. trestné činy, ku ktorým dochádza len na internete) alebo od ohrozenia obetí [odporúčanie 29];*
4. *navrhnutie takýchto právnych, regulačných a technických ustanovení tak, aby sa nimi zabezpečilo úplné dodržiavanie základných práv a slobôd osôb a aby akékoľvek obmedzenie týchto práv bolo nevyhnutné a primerané [odporúčanie 27, vi];*
5. *zabezpečenie toho, aby sa rovnaké pravidlá, povinnosti a záruky vzťahovali na poskytovateľov tradičných komunikačných služieb, služieb OTT a akýchkoľvek iných súčasných alebo budúcich poskytovateľov, ktorí generujú a spracúvajú údaje [odporúčanie 27 body i) a ii)];*
6. *zabezpečenie toho, aby údaje používateľov uchovávané na podnikateľské a obchodné účely boli v rámci príslušných záruk skutočne prístupné orgánom presadzovania práva (odporúčanie 31) a aby príslušné orgány boli schopné údaje zákonne doručené poskytovateľmi čítať [odporúčanie 27 bod iii)];*
7. *zabezpečiť, aby členské štáty mohli presadzovať sankcie voči poskytovateľom elektronických a iných komunikačných služieb, ktorí nespolupracujú, pokiaľ ide o uchovávanie a poskytovanie údajov, napr. prostredníctvom ukladania administratívnych sankcií alebo obmedzení ich schopnosti pôsobiť na trhu EÚ [odporúčanie 30].*

Pri diskusii o **uchovávaní metaúdajov** by sa mali rozlišovať medzi kategóriami údajov, pričom by sa mali rozlišovať údaje potrebné na identifikáciu záujmovej osoby (údaje o účastníkoch[71] a IP adresy zdrojovej komunikácie[72]) od prevádzkových[73] a lokalizačných údajov[74] a pre každú kategóriu by sa mali stanoviť rôzne obdobia uchovávania a záruky. Aj vo fáze prístupu k údajom je cieľom zabezpečiť rovnováhu medzi závažnosťou trestného činu, ktorý sa má vyšetriť, a stupňom narušenia súkromia prostredníctvom opatrení, ktoré sa majú prijať. V súlade s nedávnou judikatúrou[75] by sa mohli preskúmať minimálne požiadavky na všeobecné uchovávanie údajov, ktoré sú dostatočné na zabezpečenie jasnej identifikácie každého používateľa. V prípade prevádzkových a lokalizačných údajov je potrebné preskúmať dodatočné a prísnejšie kritériá.

S cieľom navrhnúť takýto rámec čo najviac nadčasovo a **technologicky neutrálnym** spôsobom by sa kategorizácia údajov, ktoré sa majú uchovávať, mala formulovať na základe na budúcnosť zameraného prístupu vrátane generických dátových súborov údajov založených napríklad na funkciách údajov (údaje, ktoré umožňujú jedinečnú identifikáciu zdroja alebo cieľa komunikácie, údaje, ktoré umožňujú identifikáciu polohy zdroja komunikácie atď.) v kombinácii so zoznamom existujúcich druhov údajov (IP adresa, IMEI atď.). Tento rámec by umožnil riadne posúdiť rušivosť každej kategórie údajov, a tým aj potrebné záruky.

---

71 S určitými výnimkami v prípade malých poskytovateľov sa údaje používateľov vo všeobecnosti už uchovávajú na obchodné účely. V takom prípade a bez toho, aby boli dotknuté primerané záruky, by sa takéto údaje mali sprístupňovať orgánom presadzovania práva.

72 Judikatúra umožňuje všeobecné a nediferencované uchovávanie údajov týkajúcich sa občianskej identity používateľov elektronických komunikácií na ochranu verejných záujmov a všeobecné a nediferencované uchovávanie IP adries s cieľom chrániť národnú bezpečnosť, bojovať proti závažnej trestnej činnosti a predchádzať závažným hrozbám pre verejnú bezpečnosť [rozsudok zo 6. októbra 2020, *La Quadrature du Net a i.*, spojené veci C-511/18, C-512/18 a C-520/18, a rozsudok z 30. apríla 2024, *La Quadrature du Net a i.*, vec C-470/21 („Hadopi“), ECLI:EU:C:2024:370].

73 „Prevádzkové [údaje]“ znamenajú akékoľvek údaje spracovávané na účely prenosu správy v elektronickej komunikačnej sieti alebo na účely fakturácie prenosu (článok 2 smernice 2002/58/ES).

74 [„Lokalizačné údaje“] (neoficiálny preklad) znamenajú akékoľvek údaje spracovávané v elektronickej komunikačnej sieti udávajúce geografickú polohu koncového zariadenia užívateľa verejne dostupnej elektronickej komunikačnej služby (článok 2 smernice 2002/58/ES); lokalizačné údaje zariadenia používateľa by sa mali považovať za lokalizačné údaje iné ako prevádzkové údaje v zmysle článku 9 smernice 2002/58/ES.

75 Rozsudok vo veci Hadopi.

Ako uvádzajú experti a nedávna judikatúra[76], spojenie povinností uchovávania s prísnymi **požiadavkami týkajúcimi sa prístupu k údajom** by poskytlo dodatočné záruky pre základné práva, najmä ochranu súkromia a údajov. Experti skupiny na vysokej úrovni preto diskutovali o potrebe navrhnúť pravidlá prístupu, ktoré sa líšia napríklad v závislosti od druhu a závažnosti trestného činu, stupňa ohrozenia, ktoré trestný čin predstavuje pre obete, účelu prístupu a orgánov príslušných na prístup k údajom. Takýto prístup sa tiež považoval za užitočný spôsob stanovenia osobitných pravidiel vyšetrovania a stíhania trestných činov, ktoré je osobitne náročné vyšetrovať, ako sú trestné činy spáchané výlučne na internete, kde sú digitálne dôkazy jedinými dostupnými dôkazmi.

Po zákonnom prístupe k údajom musia mať žiadajúce orgány možnosť ich prečítať. Poskytovatelia preto musia poskytovať údaje v **čitateľnom formáte**. Poskytovatelia pre prevádzkové a údaje o účastníkoch často ponúkajú služby šifrované medzi koncovými zariadeniami[77] a keď tieto údaje zdieľajú s príslušnými orgánmi, nedešifrujú ich. Experti skupiny na vysokej úrovni zastávali názor, že režim uchovávania údajov by mal zahŕňať povinnosti poskytovateľov služieb poskytovať nešifrované údaje a zároveň zabezpečiť silnú kybernetickú bezpečnosť a úplný súlad s právnymi predpismi o ochrane údajov a súkromia bez toho, aby sa narušilo šifrovanie.

Aby bol rámec uchovávania údajov účinný v súčasnosti aj v budúcnosti, minimálne požiadavky na uchovávanie osobitných kategórií údajov by museli byť uplatniteľné (a vymáhateľné) vo vzťahu ku každému (súčasnému alebo budúcemu) hospodárskemu subjektu poskytujúcemu služby elektronickej komunikácie. S cieľom zohľadniť budúci technologický vývoj by subjekty, na ktoré sa vzťahujú povinnosti týkajúce sa uchovávania údajov, mali zahŕňať poskytovateľov telekomunikačných služieb, poskytovateľov služieb OTT a iných operátorov, ktorí získavajú údaje spojené s konkrétnou fyzickou alebo právnickou osobou, ktorá využíva ich služby, ako sú výrobcovia automobilov alebo systémy AI pre modely LLM. Tieto povinnosti musia byť vymáhateľné a voči poskytovateľom sa musí vyvodzovať zodpovednosť; to by sa mohlo dosiahnuť pomocou rôznych riešení, ktoré by mohli zahŕňať trhové prekážky (licencie na prevádzku) a správne sankcie.

---

[76] V nedávnej veci Hadopi Súdny dvor dospel k záveru, že spojením uchovávania a prístupu je možné súkromie zaručiť.

[77] Pozri oddiel I.

Systém vymáhateľných sankcií pre nespolupracujúcich poskytovateľov a poskytovateľov, ktorí sú hostiteľmi nezákonných služieb, predstavuje základný aspekt akéhokoľvek budúceho rámca EÚ. Vzhľadom na interakciu medzi týmto konkrétnym aspektom a možnými riešeniami, o ktorých sa diskutovalo v súvislosti so zákonným odpočúvaním, sa o sankciách bude diskutovať na ďalšom zasadnutí o zákonnom odpočúvaní.

Zatiaľ čo pre väčšinu poskytovateľov by si povinnosti uchovávať a poskytovať údaje vyžadovali najmä technickú implementáciu (t. j. sprístupnenie údajov získaných alebo spracúvaných na obchodné účely príslušným orgánom), znamenalo by to štandardné uloženie povinnosti zaviesť postupy registrácie používateľov poskytovateľom, ktorí v súčasnosti svojich používateľov neregistrujú, pretože nemajú žiadnu takúto obchodnú potrebu (ako napríklad poskytovatelia služieb OTT). Experti skupiny na vysokej úrovni považovali takéto povinnosti za pozitívne v kontexte diskusií o potrebe zvýšiť **transparentnosť poskytovateľov** a posilniť vyvodzovanie zodpovednosti voči nim, pokiaľ ide o údaje, ktoré získavajú a uchovávajú, a to na ako dlho ich uchovávajú. Existujúce povinnosti týkajúce sa kategorizácie v rámci iných nástrojov (všeobecné nariadenie o ochrane údajov) môžu poskytnúť prehľad o údajoch spracúvaných týmito poskytovateľmi.

Kľúčové opatrenia: Experti skupiny na vysokej úrovni vyzývajú na vytvorenie nového rámca EÚ na uchovávanie údajov a prístup k nim

Aktéri: Európska komisia, Rada, Európsky parlament *Harmonogram: 2025 – 2026*

- Experti skupiny na vysokej úrovni naliehavo vyzývajú **Európsku komisiu**, aby začala proces posúdenia vplyvu s cieľom vyhodnotiť rôzne možnosti posilnenia kapacity príslušných orgánov účinne vyšetrovať a stíhať trestné činy prostredníctvom prístupu k historickým metaúdajom generovaným a uchovávaným poskytovateľmi komunikácií. Posúdenie vplyvu by sa malo vzťahovať aj na požiadavky subsidiarity, vplyv na základné práva a vnútorný trh a vzťah k iným existujúcim právnym nástrojom. Malo by slúžiť ako základ pre legislatívny návrh, ktorý by sa mal prijať prostredníctvom riadneho legislatívneho postupu.

Kapitola III: Zákonné odpočúvanie

O ČO IDE?

„Zákonné odpočúvanie komunikačnej prevádzky“ znamená, keď tretia strana – orgán alebo iný subjekt splnomocnený zákonom alebo na základe zákona – získava utajený prístup k údajom z podozrivej komunikácie. Hoci zákonné odpočúvanie bolo v minulosti relevantné najmä pre telefonické hovory, rastúci prechod od tradičných hlasových volaní k službám zasielania správ a iným formám elektronickej komunikácie priniesol nové výzvy.

Európskym kódexom elektronických komunikácií sa tento prechod zohľadnil a rozšírila sa ním pôsobnosť časti právneho rámca, ktorá sa vzťahuje na tradičné telekomunikácie, na spoločnosti, ktoré ponúkajú internetové služby prostredníctvom telekomunikačnej infraštruktúry, ktorú nevlastnia ani nespravujú, vrátane interpersonálnych komunikačných služieb nezávislých od číslovania. V praxi to znamená, že poskytovatelia interpersonálnych komunikačných služieb nezávislých od číslovania môžu potenciálne podliehať rovnakému právnemu rámcu, aký sa uplatňuje na tradičných telekomunikačných operátorov, a to aj v prípade zákonného odpočúvania. Členské štáty môžu vyžadovať, aby prevádzkovatelia umožnili zákonné odpočúvanie elektronických komunikácií príslušnými vnútroštátnymi orgánmi v súlade s nariadením (EÚ) 2016/679 a so smernicou 2002/58/ES, ktoré obsahujú ustanovenia o dôvernosti komunikácií a výnimky z nej. V rámci všeobecného režimu udeľovania povolení podľa EECC môžu členské štáty túto požiadavku reformulovať.

Zákonný prístup sa nemusí odohrávať len na sieťovej úrovni, ako to bolo v prípade tradičných telefonických hovorov a textových správ (SMS), ale aj na zariadení používateľa (pred odoslaním informácií) alebo na úrovni doručenia (napr. keď sa správy uchovávajú v cloude). V súvislosti s touto správou sa zákonné odpočúvanie vzťahuje na tieto tri prípady použitia a týka sa údajov sprístupnených v reálnom čase alebo s malým oneskorením.

Je dôležité rozlišovať medzi odpočúvacími technológiami, ktoré **implementoval komunikačný operátor**, a technológiami, ktoré môžu orgány presadzovania práva použiť samostatne. Do vymedzenia pojmu „**zákonné odpočúvanie**“ v normách ETSI je zahrnutý len prvý prípad [v tejto správe označovaný ako „odpočúvanie na úrovni operátora“], v ktorom sa na získavanie odpočúvaných údajov a ich doručovanie žiadajúcim orgánom vyžaduje, aby komunikačný operátor nainštaloval technické systémy. Druhý prípad [v tejto správe označovaný ako „**taktické odpočúvanie**“] sa vzťahuje na nástroje, ktoré si nevyžadujú trvalú fyzickú inštaláciu v sieti, ako sú zachytávače IMSI[78] alebo softvér na odpočúvanie údajov v smartfónoch. Z týchto prípadov použitia vyplývajú rôzne úrovne rušivosti a problémy rôznej povahy a nevzťahuje sa na ne rovnaký právny režim.

Hoci zákonné odpočúvanie tradičnej telekomunikačnej prevádzky zostáva základným nástrojom pri mnohých vyšetrovaniach[79], účinnosť tohto opatrenia sa výrazne znížila, keďže telekomunikačné služby v súčasnosti väčšinou poskytujú iné subjekty: podľa rôznych zdrojov sa približne 97 % všetkých mobilných správ teraz zasiela prostredníctvom aplikácií na odosielanie správ, ako sú WhatsApp, Facebook Messenger a WeChat, zatiaľ čo tradičné SMS a MMS predstavujú len približne 3 % správ. Okrem toho sa v roku 2023 viac ako 90 % komunikácií OTT uskutočnilo prostredníctvom služieb šifrovaných medzi koncovými zariadeniami[80].

Experti sa zhodujú na týchto trendoch: po prvé, páchatelia trestnej činnosti začali prechádzať z tradičných komunikačných operátorov na hlavných poskytovateľov služieb OTT; potom začali najvýznamnejší páchatelia trestnej činnosti postupne využívať špecializované siete používané na trestnú činnosť (ako sú Encrochat a Sky ECC); a od roku 2020 sa mnohí z nich po narušení veľkých šifrovaných komunikačných sietí používaných na trestnú činnosť rozhodli vrátiť k bežným službám OTT šifrovaným medzi koncovými zariadeniami.

---

78 Zachytávače IMSI sú sledovacie zariadenia, ktoré napodobňujú stožiare mobilných vysielačov a odpočúvajú signál mobilného telefónu, medzinárodné identifikačné kódy mobilného účastníka (IMSI) a komunikačné údaje.

79 V posledných rokoch sa v Európe výrazne a stabilne zvyšuje počet žiadostí o zákonné odpočúvanie. Krajiny ako Nemecko, Francúzsko a Spojené kráľovstvo zaznamenali mimoriadne vysoký počet takýchto žiadostí, pričom len samotné Nemecko zaznamenalo výrazný nárast. Napríklad v roku 2023 spoločnosť Deutsche Telekom vykázala viac ako 31 000 žiadostí o odpočúvanie, čo predstavuje nárast z približne 26 000 žiadostí o odpočúvanie v roku 2022 (https://www.telekom.com/en/company/data-privacy-and-security/news/germany-363566).

80 Zdroje: Comparitech a Statista.

V tejto súvislosti čelia poskytovatelia komunikačných služieb pri odpovediach na žiadosti o zákonné odpočúvanie takým výzvam, že ledva dokážu splniť základné požiadavky týkajúce sa zákonného odpočúvania vymedzené v Budapeštianskom dohovore o počítačovej kriminalite[81]. V dôsledku toho sa operačná hodnota tradičného zákonného odpočúvania často obmedzuje na taktické poznatky, ako je určenie toho, či je zariadenie zapnuté alebo nie, polohu sieťovej antény, alebo určenie toho, kto je v spojení s kým; zákonné odpočúvanie obsahových údajov prenášaných prostredníctvom poskytovateľov služieb OTT však najčastejšie nie je možné.

V dôsledku toho orgány presadzovania práva často nemajú prístup k obsahu komunikácie, ktorá je predmetom odpočúvania[82], ani ho nemôžu čítať, ani zistiť, kto používa danú internetovú službu v reálnom čase, a filtrovať relevantné informácie. Táto výrazná strata prístupu k prenášaným údajom ovplyvňuje vyšetrovania viacerými spôsobmi:

- závažné ťažkosti pri predchádzaní trestnej činnosti, mapovaní zločineckých organizácií a prisudzovaní trestnej činnosti páchanej online alebo offline;
- orgány presadzovania práva intenzívnejšie využívajú tzv. špeciálne techniky[83], ktoré sú pre príslušníkov často rušivejšie a oveľa nebezpečnejšie, napríklad keď súdny orgán prikáže inštaláciu kamier alebo mikrofónov v blízkosti cieľa;
- orgány presadzovania práva intenzívnejšie využívajú vyšetrovacie techniky, ktoré sú menej cielené: bez prístupu k obsahu komunikácie alebo presných geolokalizačných údajov musia vyšetrovatelia často vyšetrovať **všetky** osoby spájané s osobou podozrivou z páchania trestnej činnosti.

V tejto súvislosti experti skupiny na vysokej úrovni upozornili na štyri kľúčové kategórie výziev.

---

81 https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2008/137/ [články 20 a 21]

82 Jeden expert uviedol, že obsahové údaje nie sú dostupné prostredníctvom tradičného zákonného odpočúvania v 99 % prípadov.

83 Takzvané špeciálne techniky zahŕňajú celý rad taktických prostriedkov na získanie informácií o cieli záujmu pomocou kamier, mikrofónov, vzdialeného prístupu k zariadeniam, sledovačov GPS atď.

I. Zákonné odpočúvanie komunikácie uskutočňované prostredníctvom netradičných poskytovateľov komunikácie

Väčšina členských štátov zaviedla určitú formu regulácie, ktorou sa upravuje zákonné odpočúvanie a stanovujú sa povinnosti poskytovateľov komunikačných služieb použiť spôsobilosti odpočúvania[84]. Zatiaľ čo podmienky vydávania príkazov na zákonné odpočúvanie sa v jednotlivých krajinách výrazne líšia, povinnosti vzťahujúce sa na operátorov sú často podobné[85]; musia byť schopní odpočúvať všetky relevantné komunikácie pochádzajúce od určeného cieľa na území svojho štátu bez akýchkoľvek výpadkov a musia poskytovať infraštruktúru potrebnú na získanie odpočúvaných údajov a ich prenos na účely presadzovania práva.

Keď prevádzkovatelia prenosových sietí (poskytovatelia komunikačných služieb, ktorí vlastnia sieť a majú prístup k jej infraštruktúre) poskytujú aj komunikačné služby (telefónne hovory, SMS atď.), najčastejšie sú povinnosti týkajúce sa zákonného odpočúvania schopní splniť[86]. Vo väčšine prípadov vychádzajú z noriem ETSI a spoliehajú sa na poskytovateľov špecializovaných technológií, aby riadili svoje vlastné obmedzenia vrátane nákladovej efektívnosti, minimálneho vplyvu na sieťovú infraštruktúru, interoperability, spoľahlivosti a bezpečnosti.

V prípade služieb OTT je situácia zložitejšia: zákonné odpočúvanie môžu vykonávať prevádzkovatelia prenosových sietí alebo poskytovatelia služieb OTT.

Keď je odpočúvanie komunikácie prostredníctvom služieb OTT implementované na úrovni prenosovej siete, jeho účinnosť je často obmedzená. Po prvé, prevádzkovateľ prenosovej siete nemusí byť schopný identifikovať komunikáciu cieľa (napr. pri pripojení prostredníctvom verejnej Wi-Fi). Okrem toho služby OTT často používajú svoje vlastné protokoly, ktoré je potrebné dekódovať systémami zákonného odpočúvania, čo si vyžaduje vyššie náklady, viac času a zložitejší proces. Napokon to, že poskytovatelia služieb OTT používajú šifrovania medzi koncovými zariadeniami, spôsobuje, že prístup k obsahovým údajom je veľmi problematický a čoraz viac bráni prístupu k metaúdajom, keďže veľká väčšina krajín sa domnieva, že povinnosť prevádzkovateľov prenosových sietí poskytovať nešifrované informácie zaniká, keď šifrovanie vykonáva tretia strana, ako sa uvádza v Budapeštianskom dohovore.

---

84 Pozri „Lawful interception – a market access barrier in the European Union“ („Zákonné odpočúvanie – prekážka prístupu na trh v Európskej únii“), Vadim Doronin. In: Computer Law & Security Review 51 (2023) 105867.

85 I keď existujú rozdiely v povinnostiach týkajúcich sa obsahových alebo neobsahových údajov.

86 Hoci funkcie, ako sú home routing, slicing alebo Rich Communication Services, môžu obmedzovať schopnosť prevádzkovateľov prenosových sietí plniť si svoje povinnosti (pozri oddiel o technologických výzvach).

Vymedzenie pojmu „elektronické komunikačné služby“ podľa kódexu EECC, ktoré od roku 2018 zahŕňa NI-ICS, sa používa formou odkazu v článku 5 ods. 1 smernice o súkromí a elektronických komunikáciách. To zase znamená, že pojem elektronické komunikačné služby, ktorý je v súčasnosti už širší (v porovnaní s tým, keď bola prijatá smernica o súkromí a elektronických komunikáciách), umožňuje členským štátom, aby sa na účely vykonania zákonného odpočúvania spoliehali priamo na poskytovateľov služieb OTT[87]. Členské štáty doteraz túto možnosť využívali nerovnomerne, pričom niektoré z nich stanovili podobné povinnosti pre všetky typy poskytovateľov elektronických komunikačných služieb vrátane poskytovateľov služieb OTT, zatiaľ čo iné poskytovateľov služieb OTT vylúčili[88]. **V praxi populárne služby OTT bez ohľadu na existujúce povinnosti nevyvinuli technické mechanizmy, ktorými by reagovali na žiadosti orgánov členských štátov EÚ o zákonné odpočúvanie**, a to najmä z právnych dôvodov[89].

Naproti tomu Spojené kráľovstvo na základe zákona o vyšetrovacích právomociach vytvorilo rámec pre zákonné odpočúvanie komunikácie v rámci služieb OTT, ktorý sa vďaka prijatiu dohody o prístupe k údajom medzi Spojeným kráľovstvom a USA vzťahuje aj na služby OTT so sídlom v USA. Podľa príslušných orgánov Spojeného kráľovstva to výrazne ovplyvňuje predchádzanie trestnej činnosti a jej vyšetrovanie.

Experti z vnútroštátnych orgánov napokon jasne uviedli, že taktické odpočúvanie založené na využívaní zraniteľností nie je ani účinnou, ani žiaducou alternatívou vymáhateľných pravidiel zákonného odpočúvania uplatniteľných na poskytovateľov služieb OTT a malo by sa obmedziť na konkrétne prípady so silnými zárukami vymedzenými vo vnútroštátnych právnych predpisoch, aby sa zabezpečila proporcionalita.

---

87 Hoci stále prebiehajú diskusie o presnom rozsahu uplatniteľnosti a výklady sa v jednotlivých členských štátoch líšia.

88 Pozri „Lawful interception – a market access barrier in the European Union“ („Zákonné odpočúvanie – prekážka prístupu na trh v Európskej únii“), Vadim Doronin. In: Computer Law & Security Review 51 (2023) 105867.

89 Nie je to podložené štatistikou, keďže vnútroštátne orgány veľmi zriedka zasielajú poskytovateľom služieb OTT žiadosti o zákonné odpočúvanie, pretože si dobre uvedomujú, že je nepravdepodobné, že by to prinieslo výsledky.

II. Cezhraničné žiadosti

Cezhraničné žiadosti o zákonné odpočúvanie adresované poskytovateľom služieb OTT a v menšej miere poskytovateľom tradičných komunikačných služieb predstavujú pre orgány presadzovania práva niekoľko výziev.

Pokiaľ ide o poskytovateľov tradičných komunikačných služieb, orgány čelia predovšetkým organizačným výzvam. Po prvé, nástroje medzinárodnej spolupráce – najmä mechanizmy vzájomnej právnej pomoci – môžu byť nepraktické pri naliehavých odpočúvaniach, ktoré si vyžadujú súhlas a vykonanie v priebehu hodín, nie dní alebo týždňov[90]. Dôvodom je počet krokov, ktoré je potrebné prijať na zabezpečenie súladu s právnymi predpismi tak v dožadujúcom, ako aj v dožiadanom členskom štáte. Celkovo panuje názor, že proces vzájomnej právnej pomoci je neefektívny a zaťažujúci, ak sa uplatňuje na zákonné odpočúvanie. Európsky vyšetrovací príkaz (EVP), ktorý sa začal uplatňovať v roku 2017, nahradil tradičné postupy vzájomnej právnej pomoci v EÚ[91] stanovením prísnych lehôt[92] na zabezpečenie požadovaných dôkazov, obmedzením dôvodov zamietnutia takýchto žiadostí a zavedením jednotného vzorového formulára, ktorý by orgány mohli používať na vyžiadanie dôkazov. Okrem toho, ak na vykonanie odpočúvania nie je potrebná žiadna technická pomoc od členského štátu, v ktorom sa nachádza cieľ odpočúvania, tento členský štát je o odpočúvaní upovedomený prostredníctvom vzorového formulára a má možnosť namietať proti nemu do 96 hodín. V zásadnej veci C-670/22 si SDEÚ osvojil širokú koncepciu „odpočúvania telekomunikačnej prevádzky“, pričom rozhodol, že infiltrácia koncových zariadení na účely získavania údajov o prenose dát, polohe a komunikácii z internetovej komunikačnej služby predstavuje „odpočúvanie telekomunikačnej prevádzky“. Experti sa však napriek tomu domnievajú, že významné zlepšenia, ktoré priniesol EVP, neuspokojujú potrebu rýchleho a harmonizovaného cezhraničného prístupu k údajom v pohybe.

Okrem toho orgány členských štátov uviedli, že existujúca technická architektúra často nie je vhodná na účely vykonávania zákonného odpočúvania v jednom členskom štáte a prenosu údajov do iného členského štátu v takmer reálnom čase. V niektorých prípadoch, keď sa vykonávajú príslušné organizačné protokoly, objem údajov, ktoré sa majú prenášať, jednoducho nie je kompatibilný so šírkou pásma, ktorá je k dispozícii prostredníctvom zabezpečených komunikačných kanálov.

---

90 Experti spomenuli prípady, keď sa prípad skončil pred účinným vykonaním cezhraničného zákonného odpočúvania, alebo prípady, keď sa na vybavenie žiadostí o vzájomnú právnu pomoc čakalo viac ako 8 mesiacov.

91 S výnimkou DK a IE, na ktoré sa smernica o EVP nevzťahuje.

92 30 dní na uznanie EVP a ďalších 90 dní na jeho vykonanie.

Odpočúvanie komunikácie OTT predstavuje v porovnaní s odpočúvaním telefonickej komunikácie, pri ktorom poskytovatelia ponúkajú svoje služby na presne vymedzenom území, zložité jurisdikčné problémy. Tradičné telekomunikačné služby sú viazané na konkrétnu fyzickú sieťovú infraštruktúru, čím sa zabezpečuje, že poskytovateľ služieb má zariadenia a právnu prítomnosť v krajine, v ktorej dochádza k odpočúvaniu. Takáto lokalizovaná situácia znižuje riziko kolízie právnych poriadkov v rámci EÚ a uľahčuje dodržiavanie predpisov.

Naopak v prípade služieb OTT sa môžu žiadajúci orgán, cieľ odpočúvania, miesto fyzického vykonania a miesto usadenia spoločnosti nachádzať v niekoľkých rôznych jurisdikciách. Vzájomné pôsobenie medzi právnymi rámcami v týchto jurisdikciách by potenciálne mohlo viesť ku kolízii právnych poriadkov[93].

Experti z policajných a justičných orgánov nemajú žiadne pochybnosti: vybavovanie žiadostí o zákonné odpočúvanie prostredníctvom medzinárodných nástrojov nie je schodným riešením. Ak orgány presadzovania práva obchádzajú proces vzájomnej právnej pomoci a namiesto toho zasielajú príkazy priamo poskytovateľom služieb podľa svojich vnútroštátnych právnych predpisov, poskytovatelia služieb OTT, ako sú Microsoft, META alebo Google, môžu čeliť protichodným právnym požiadavkám. Napríklad v mnohých prípadoch má žiadajúci členský štát pravidlá upravujúce zákonný prístup, ktoré sú v rozpore s írskym právom[94], ktorým sa riadi niekoľko významných poskytovateľov služieb OTT, keďže majú sídlo v Írsku, ale môžu sa riadiť aj vnútroštátnym právom v členských štátoch, v ktorých poskytujú svoje služby.

Tieto výzvy možno účinne riešiť prostredníctvom spoločných opatrení a určitého stupňa harmonizácie pravidiel zákonného odpočúvania na úrovni EÚ s cieľom uľahčiť a urýchliť cezhraničné žiadosti týkajúce sa zákonného odpočúvania. To by bolo predpokladom riešenia ďalších výziev organizačnej a technickej povahy, ktorých riešenia možno nájsť, keď sú pravidlá jasne stanovené a uskutočniteľné.

---

93 Pozri „LE interception concerns under the EECC“ („Problémy s odpočúvaním na účely presadzovania práva podľa EECC“), Microsoft, január 2020.

94 Írske právo zakazuje poskytovateľom služieb OTT zapájať sa do odpočúvania v reálnom čase.

III. Technológie

Bez ohľadu na právne úvahy má vývoj komunikačných technológií vplyv na technickú schopnosť orgánov presadzovania práva odpočúvať komunikáciu prostredníctvom služieb poskytovaných priamo poskytovateľmi komunikačných služieb alebo poskytovateľmi služieb OTT.

Pokiaľ ide o poskytovateľov tradičných komunikačných služieb, spôsobilosti zákonného odpočúvania zvyčajne vyvíjajú poskytovatelia technológií na základe noriem ETSI a sú začlenené do 3GPP[95]. V dôsledku toho môžu dobre vybavené policajné zbory uspokojivo zvládnuť odpočúvanie tradičnej komunikácie – volaní a SMS správ – a potenciálne môžu odpočúvať internetovú komunikáciu službami poskytovanými prostredníctvom sietí poskytovateľov komunikačných služieb alebo poskytovateľov služieb OTT.

Zvyšujúca sa zložitosť komunikačných infraštruktúr a protokolov v oblasti 5G, ako je virtualizácia, network slicing, edge computing a prvky zvyšujúce súkromie, však predstavujú pre tradičných operátorov nové technologické výzvy[96]. Experti skupiny na vysokej úrovni poukázali najmä na výzvy súvisiace s technológiou Home Routing[97] a protokolom RCS[98].

Z výhľadového hľadiska a na základe skúseností so sieťou 5G experti skupiny na vysokej úrovni očakávajú výzvy spojené s budúcim zavádzaním 6G (plánované na obdobie po roku 2030), ktoré zájde o krok ďalej, pokiaľ ide o prvky zvyšujúce súkromie[99], prípadne bude zahŕňať šifrovanie medzi koncovými zariadeniami ako štandard, čo by spolu mohlo sťažiť odpočúvanie.
Nové komunikačné technológie ako internet vecí, satelitná komunikácia a rozvoj kvantovej výpočtovej techniky[100] zároveň so sebou prinášajú ďalší súbor výziev, ktoré treba predvídať.

---

95 Projekt partnerstva tretej generácie, ktorý poskytuje základ pre rozvoj komunikačných technológií, ako sú 5G, internet vecí a mobilné širokopásmové pripojenie.

96 Pozri „Law enforcement and judicial aspects related to 5G“ („Aspekty presadzovania práva a justičné aspekty súvisiace s 5G“), koordinátor EÚ pre boj proti terorizmu, 2019. https://data.consilium.europa.eu/doc/document/ST-8983-2019-INIT/en/pdf.

97 Europol – Position paper on Home routing (stanovisko k technológii Home Routing) (europa.eu).

98 Protokol RCS umožňuje výmenu skupinových chatov, videosúborov, audiosúborov a obrázkov s vysokým rozlíšením; často sa používa namiesto SMS. V závislosti od jeho vykonávania môže byť zákonné odpočúvanie správ RCS nemožné, čo má významný vplyv na presadzovanie práva (viac ako 1 miliarda aktívnych používateľov protokolu RCS v roku 2023).

99 Pozri plán 6G: https://5g-ppp.eu/wp-content/uploads/2021/06/WhitePaper-6G-Europe.pdf.

100 The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement (Druhá kvantová revolúcia: vplyv kvantovej výpočtovej techniky a kvantových technológií na presadzovanie práva), Europol (europa.eu).

Experti skupiny na vysokej úrovni napokon zdôraznili, že jednou z hlavných technických výziev, ktorej čelia orgány presadzovania práva, je šifrovanie medzi koncovými zariadeniami, najmä v prípade komunikácie OTT, pričom viac ako 80 % komunikácie prebieha prostredníctvom služieb šifrovaných medzi koncovými zariadeniami (živá komunikácia a úložisko záloh), čím sa vyšetrovateľom bráni v prístupe k obsahu komunikácie. Experti zároveň súhlasia aj s tým, že šifrovanie medzi koncovými zariadeniami sa považuje za spoľahlivé bezpečnostné opatrenie, ktoré účinne chráni občanov pred rôznymi formami trestnej činnosti. Šifrovanie medzi koncovými zariadeniami zabezpečuje, aby prístup k obsahu svojich správ mali len komunikujúci používatelia, čím účinne chráni pred nezákonným odpočúvaním, krádežou údajov, štátnou špionážou a inými formami neoprávneného prístupu hackerov, páchateľov počítačovej kriminality alebo dokonca samotných poskytovateľov služieb.

Vyčíslenie výziev, ktorým čelia orgány presadzovania práva pri monitorovaní komunikácie páchateľov trestnej činnosti a teroristov pomocou šifrovania medzi koncovými zariadeniami, je zložité. Dôvodom je, že orgány presadzovania práva sa často rozhodnú neinvestovať čas a zdroje do získania súdnych príkazov na elektronické sledovanie na platformách, o ktorých je známe, že štandardne používajú šifrovanie medzi koncovými zariadeniami[101]; počet skutočných žiadostí o zákonné odpočúvanie obsahových údajov, ktoré nemožno vykonať z dôvodu šifrovania medzi koncovými zariadeniami, je preto veľmi nízky a nie je relevantný. Orgány presadzovania práva vnímajú túto nedostatočnú spôsobilosť sledovania ako významný mŕtvy uhol a zraniteľnosť, ktorú si zločinci a teroristi plne uvedomujú a ktorú aktívne využívajú, ako sa ukázalo v prípadoch EncroChat[102] a Sky ECC, ktoré viedli k tisícom zatknutí v celej Európe vrátane mnohých vysokopostavených zločincov. Táto obava bola vyjadrená okrem iného vo viacerých vyhláseniach európskych policajných prezidentov[103] a skupiny G7[104]. Na ilustráciu vplyvu straty prístupu k obsahovým údajom experti poukázali na niekoľko verejných príkladov týkajúcich sa okrem iného terorizmu[105], obchodovania s drogami[106] a znásilnení[107], kde šifrovanie výrazne obmedzilo schopnosť orgánov presadzovania práva predchádzať závažnej a organizovanej trestnej činnosti a bojovať proti nej.

Zástupcovia orgánov presadzovania práva by uprednostnili prístup, ktorý by od spoločností vyžadoval, aby im za prísnych podmienok poskytovali prístup k nešifrovaným údajom. Treba však poznamenať, že experti na kybernetickú bezpečnosť vyjadrili obavy, že takéto riešenia by ohrozili kybernetickú bezpečnosť. Niektorí experti na presadzovanie práva uviedli, že v niektorých prípadoch sa šifrovanie zaviedlo spôsobom, ktorý je zlučiteľný s kybernetickou bezpečnosťou, ako aj s potrebou udržiavať niektoré služby, ako sú aktualizácie operačného systému, skenovanie obsahu (napr. e-maily alebo webové relácie) na účely kybernetickej bezpečnosti alebo kľúčové mechanizmy obnovy, keď sa používateľ rozhodne pre túto funkciu.

---

101 Manpearl, 2017.

102 Pre ďalšie informácie o EncroChat a Sky ECC pozri Europol a Eurojust, Third Report of the Observatory Function on Encryption (Tretia správa monitorovacieho útvaru o šifrovaní), jún 2021.

103 https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC-%231384205-v1-Joint_Declaration_of_the_European_Police_Chiefs.PDF

104 https://www.gov.uk/government/publications/g7-interior-and-security-ministers-meeting-september-2021/g7-london-interior-commitments-accessible-version

105 V marci 2017 vykonal Khalid Masood, 52-ročný muž, v centre Londýna teroristický útok inšpirovaný islamistami, pri ktorom šesť ľudí zahynulo a 29 bolo zranených. Hoci správy o incidente naznačovali, že Masood čin plánoval a vykonal sám, zistilo sa, že niekoľko minút pred uskutočnením útoku poslal PDF dokument s názvom „Jihad“ veľkému počtu svojich kontaktov na WhatsApp a iMessage, pričom obe aplikácie boli a stále sú automaticky štandardne šifrované medzi koncovými zariadeniami. Zdroje: Max Hill, „The Westminster Bridge Terrorist Attack“ („Teroristický útok na Westminsterskom moste“) (London: The Stationery Office, 2018); BBC News, „WhatsApp Must Not Be a „Place for Terrorists to Hide“ („WhatsApp nesmie slúžiť ako skrýša pre teroristov“), 26. marca 2017.

106 Experti spomenuli významné prípady obchodovania s drogami, pri ktorých nebolo možné dosiahnuť pokrok, kým sa nezískal prístup k šifrovanej komunikácii prostredníctvom nástrojov Encrochat a Sky ECC.

107 V jednom prípade v Spojenom kráľovstve, ktorý priťahoval publicitu, bolo sťažené policajné vyšetrovanie prípadu znásilnenia, pretože podozrivé osoby používali na komunikáciu WhatsApp a šifrovanie medzi koncovými zariadeniami sťažilo prístup ku kľúčovým dôkazom. Neschopnosť orgánov presadzovania práva dešifrovať správy WhatsApp bez súhlasu používateľa bránila vyšetrovaniu.

Na tomto základe sa experti na presadzovanie práva zhodli na tom, že výzvy, ktoré predstavuje šifrovanie, si vyžadujú mnohostranný prístup, ktorý vyvažuje práva na súkromie a bezpečnosť a potrebu, aby orgány presadzovania práva mali prístup k údajom s cieľom bojovať proti trestnej činnosti a chrániť životy a telesnú integritu a majetok ľudí. Hoci je nepravdepodobné, že by všetky relevantné obavy mohlo rozptýliť jediné riešenie, kombinácia prístupov by mohla pomôcť tento problém zmierniť.

IV. Poskytovatelia komunikačných služieb trestnej povahy

Páchatelia trestnej činnosti využívajú na utajenie svojej komunikácie bežné platformy šifrované medzi koncovými zariadeniami; môžu sa však tiež rozhodnúť využívať zabezpečené komunikačné kanály osobitne určené na trestnú činnosť (ďalej len „CCC“ – criminal communication channels – komunikačné kanály používané na trestnú činnosť)[108]. EncroChat a Sky ECC sú známe CCC, v rámci ktorých sa predávali telefóny s integrovanou službou šifrovania medzi koncovými zariadeniami prispôsobenou na utajenie trestnej činnosti; boli propagované na dark webe. Obe platformy boli v rokoch 2020 a 2021 zlikvidované vďaka medzinárodným spoločným operáciám orgánov presadzovania práva, ktoré odhalili ich rozsiahle zapojenie do organizovanej trestnej činnosti. Takisto sa zlikvidovalo niekoľko podobných platforiem, ako je Phantom Secure[109] a Exclu[110], zatiaľ čo mnohé menšie platformy sú stále v prevádzke a poskytujú bezpečné centrá na výmenu informácií o trestnej činnosti. V tejto roztrieštenej situácii je nevyhnutné, aby orgány presadzovania práva boli schopné identifikovať CCC, monitorovať a blokovať ich činnosť, likvidovať ich a stavať zločincov pred súd.

[108] https://www.eurojust.europa.eu/sites/default/files/Documents/pdf/joint_ep_ej_third_report_of_the_observatory_function_on_encryption_en.pdf

[109] https://www.fbi.gov/news/stories/phantom-secure-takedown-031618

[110] New strike against encrypted criminal communications with dismantling of Exclu tool (Ďalší úder proti šifrovanej kriminálnej komunikácii – likvidácia nástroja Exclu) | Eurojust | Agentúra Európskej únie pre justičnú spoluprácu v trestných veciach (europa.eu)

Pretože odpočúvanie na úrovni operátora nie je pri tomto type nepoctivého poskytovateľa komunikačných služieb možné, na účely presadzovania práva sú potrebné relevantné spôsobilosti taktického odpočúvania – nástroje a odborné znalosti – na cielené monitorovanie ich používateľov, a to aj napriek šifrovaniu. Experti na presadzovanie práva trvali na významných výzvach, rizikách a obmedzeniach spojených s vývojom a používaním takýchto techník, ktoré nie sú škálovateľné a mali by sa šetriť na tie najdôležitejšie prípady. Vnútroštátne orgány v závislosti od svojich kapacít a právneho rámca používajú rôzne prístupy vrátane nástrojov vyvinutých interne, zakúpených od tretích strán alebo prevádzkovaných ako služba; bez ohľadu na to, ktorú možnosť využívajú, experti sa zhodujú, že na používanie takýchto nástrojov je potrebné mať zavedené rôzne záruky. To môže zahŕňať úvahy o lepšom dohľade nad nástrojmi, ich hodnotení a certifikácii, ako aj o solídnom rámci riadenia zraniteľnosti, pričom sa v plnej miere rešpektuje procesná autonómia členských štátov v trestných veciach a ich výlučná právomoc, pokiaľ ide o národnú bezpečnosť.

Vyšetrovacie orgány čelia aj právnym problémom, ako sú ťažkosti s kriminalizáciou poskytovateľov komunikačných služieb a hostingových služieb, ktorí ponúkajú predovšetkým zločinecké služby (keďže všetka prevádzka je šifrovaná), čo je potrebný prvý krok pred prijatím súdneho alebo správneho opatrenia. Okrem toho členské štáty musia mať možnosť ukladať kanálom CCC sankcie s cieľom obmedziť alebo zablokovať prístup k takýmto službám v EÚ, a tým poraziť ich zločinecký obchodný model. Bude to potrebné, ak a keď sa na služby OTT začnú vzťahovať povinnosti týkajúce sa zákonného odpočúvania, aby sa zabránilo tomu, že páchatelia trestnej činnosti sa vrátia k nepoctivým poskytovateľom komunikačných služieb.

Napokon, na súdoch sú napadnuté rôzne aspekty vecí, ako sú veci proti EncroChat a Sky ECC. Požiadavky na používanie údajov získaných odpočúvaním v inom členskom štáte ako dôkazov sa v rámci EÚ značne líšia, čo vedie k právnej neistote pri podobných operáciách vykonávaných jedným členským štátom s potenciálnym vplyvom na mnohé iné.

MOŽNÉ RIEŠENIA

I. Zabezpečiť vykonateľnosť žiadostí o zákonné odpočúvanie pre všetky typy poskytovateľov elektronických komunikačných služieb

V EÚ sú spôsobilosti zákonného odpočúvania obmedzené na poskytovateľov tradičných komunikačných služieb, zatiaľ čo väčšina komunikácie sa v súčasnosti uskutočňuje prostredníctvom poskytovateľov netradičných komunikačných služieb[111]. Bez ohľadu na to, či komunikačnú službu poskytuje vlastník infraštruktúry, schopnosť orgánov presadzovania práva vykonávať zákonné odpočúvanie komunikácie záujmovej osoby by mala byť rovnaká. Alternatívne riešenia, ako napríklad zákonné odpočúvanie NI-ICS a iných komunikačných služieb výlučne na úrovni prenosovej siete, spoliehanie sa na nástroje medzinárodnej spolupráce pri zákonnom odpočúvaní služieb poskytovateľov NI-ICS alebo rozsiahle využívanie taktického odpočúvania, nie sú realizovateľné[112].

V dôsledku toho experti skupiny na vysokej úrovni považujú za prioritu zabezpečiť, aby sa povinnosti týkajúce sa zákonného odpočúvania dostupných údajov uplatňovali rovnakým spôsobom na poskytovateľov tradičných a netradičných komunikácií a aby boli rovnako vymáhateľné. Harmonizácia takýchto povinností by mala slúžiť na prekonanie výziev súvisiacich s vybavovaním cezhraničných žiadostí.

V záujme splnenia tohto cieľa a postupného presunu smerom k aproximácii a harmonizácii pravidiel zákonného odpočúvania v EÚ navrhujú experti skupiny na vysokej úrovni postupný prístup: najprv by sa mali odsúhlasiť zásady štrukturalizácie na úrovni EÚ (krok 1); Komisia by potom mala podporiť vykonávanie týchto zásad (krok 2); a napokon, na základe ďalšieho posúdenia sa zásady môžu kodifikovať v právnom nástroji (krok 3).

---

111 V Spojenom kráľovstve dosiahol počet zaslaných SMS a MMS v roku 2022 36 miliárd, zatiaľ čo počet online správ bol 1,3 bilióna [WhatsAppening in the world of online communications? (Čo sa deje vo svete online komunikácie?) – Ofcom].

112 Pozri oddiel o výzvach.

Krok 1: Dohoda o spoločnom základnom scenári

Po prvé, je potrebné dospieť k spoločnému chápaniu toho, na ktoré kategórie elektronických komunikačných služieb sa môžu vzťahovať vnútroštátne povinnosti týkajúce sa zákonného odpočúvania podľa pravidiel smernice o súkromí a elektronických komunikáciách a všeobecného nariadenia o ochrane údajov.

Po druhé, je potrebné dosiahnuť dohodu o operačných požiadavkách na vysokej úrovni, v ktorej sa jasne uvedie, čo sa očakáva od vnútroštátnych orgánov, pokiaľ ide o zákonné odpočúvanie, a aké by mali byť súvisiace záruky. Ako dobrý základ na vymedzenie požiadaviek orgánov presadzovania práva sa identifikoval dokument LEON[113]. Tento dokument by mali sprevádzať požiadavky týkajúce sa napríklad proporcionality, dohľadu a transparentnosti, pričom by sa malo prípadne rozlišovať medzi pravidlami uplatniteľnými na obsahové a neobsahové údaje, a to pri plnom rešpektovaní kybernetickej bezpečnosti a ochrany údajov a súkromia a bez toho, aby sa narušilo šifrovanie. Prípadné zriadenie *ad hoc* skupiny expertov vrátane expertov na kybernetickú oblasť, ochranu súkromia a presadzovanie práva by mohlo zabezpečiť, aby sa požiadavky v prípade potreby aktualizovali, a to prípadne na základe práce pracovnej skupiny Europolu pre normalizáciu v oblasti vnútornej bezpečnosti, v ktorej by sa malo pokračovať.

Po tretie, pojem miestnej príslušnosti treba spresniť, pokiaľ ide o jeho uplatniteľnosť na služby OTT, pričom treba zohľadniť rozdielne výklady medzi vnútroštátnymi orgánmi a, čo je najdôležitejšie, medzi vnútroštátnymi orgánmi a poskytovateľmi služieb OTT. Mali by sa napríklad spresniť pravidlá uplatniteľné na prípady, keď poloha cieľa nie je istá. Potrebné sú aj usmernenia o tom, kto môže posudzovať zákonnosť žiadosti, napríklad pokiaľ ide o úlohu poskytovateľov služieb v tejto súvislosti. V neposlednom rade, hoci prevažná väčšina súdnych rozhodnutí doteraz potvrdila zákonnosť procesných úkonov proti EncroChat a Sky ECC, viaceré súdne konania stále prebiehajú[114], čo môže mať veľký vplyv na odsúdenie vysokopostavených zločincov. Preto môže byť potrebné uľahčiť prípustnosť dôkazov získaných opatreniami taktického odpočúvania medzi členskými štátmi, vzájomné uznávanie rozsudkov a justičných rozhodnutí a policajnú a justičnú spoluprácu v trestných veciach.

---

[113] Dokument LEON (Law Enforcement – Operational Needs for Lawful Access to Communications – Presadzovanie práva – operačné potreby v oblasti zákonného prístupu ku komunikáciám) je výsledkom práce švédskych orgánov presadzovania práva v úzkej spolupráci so zástupcami orgánov presadzovania práva v členských štátoch EÚ, Severnej Amerike a Austrálii. Má za cieľ identifikovať a opísať potreby v oblasti presadzovania práva, pokiaľ ide o zákonný prístup k obsahu komunikácií, údajom súvisiacim s obsahom a informáciám o účastníkoch. Pozri *poznámku predsedníctva Rady s názvom Law Enforcement Operational Needs for Lawful Access to Communication (LEON) (Operačné potreby v oblasti presadzovania práva, pokiaľ ide o zákonný prístup ku komunikáciám)*, 6050/23 zo 16. februára 2023.

[114] Pozri veci T-1180/23, T-148/24, T-167/24, T-484/24 a T-560/24.

Blok odporúčaní 7

S cieľom dohodnúť sa na úrovni EÚ na spoločných zásadách zákonného odpočúvania dostupných údajov, ktoré sa vzťahujú na všetky typy poskytovateľov elektronických komunikačných služieb, experti odporúčajú:

1. *spresniť vymedzenie a rozsah zákonného odpočúvania v súlade s existujúcimi aktmi EÚ a inými relevantnými európskymi a medzinárodnými nástrojmi, ako je Budapeštiansky dohovor o počítačovej kriminalite [odporúčanie 38];*

2. *inšpirovať sa dokumentom LEON s cieľom vymedziť spoločné operačné požiadavky [odporúčanie 21];*

3. *určiť potrebné záruky [odporúčanie 17, odporúčanie 41];*

4. *riešiť hľadisko kybernetickej bezpečnosti tak, aby žiadne opatrenie nezahŕňalo povinnosť poskytovateľov prispôsobiť svoje systémy IKT spôsobom, ktorý by mal negatívny vplyv na kybernetickú bezpečnosť ich používateľov [odporúčanie 41];*

5. *objasniť pojem miestnej príslušnosti vo vzťahu k údajom na riešenie potenciálnych kolízií právnych poriadkov [odporúčanie 39] a podporiť prijatie minimálnych pravidiel na úrovni EÚ, ktoré by v relevantných prípadoch umožňovali prípustnosť dôkazov získaných opatreniami taktického odpočúvania medzi členskými štátmi, a to v rozsahu potrebnom na uľahčenie vzájomného uznávania rozsudkov a justičných rozhodnutí a policajnej a justičnej spolupráce v trestných veciach [odporúčanie 42].*

Je potrebné zvážiť najlepší prístup k zhromaždeniu a odsúhlaseniu spoločných zásad, ako sa uvádza v bloku odporúčaní 7, a určiť najrelevantnejší nástroj na ich zdieľanie. Pri pohľade späť zohralo uznesenie Rady o zákonnom odpočúvaní zo 17. januára 1995[115] zásadnú úlohu pri uľahčovaní harmonizácie riešení zákonného odpočúvania, keďže poskytlo odkaz na normy, ktoré pre túto oblasť vypracoval inštitút ETSI. Podobný prístup, možno prostredníctvom odporúčania Komisie alebo Rady, by mohol byť rovnako prospešný.

[115] https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A31996G1104

Kľúčové opatrenia: Experti skupiny na vysokej úrovni vyzývajú EÚ, aby v roku 2025 vydala odporúčanie o prístupe k údajom v reálnom čase

Harmonogram: 2025 *Rozpočet: určí sa*

- Experti skupiny na vysokej úrovni vyzývajú Európsku komisiu, aby vydala odporúčanie, v ktorom spresní pojem zákonného odpočúvania[116] pre poskytovateľov elektronických komunikačných služieb a podrobne opíše rôzne požiadavky, ktoré sa môžu vzťahovať na zákonné odpočúvanie dostupných neobsahových a obsahových údajov pri plnom rešpektovaní kybernetickej bezpečnosti, ochrany údajov a súkromia bez toho, aby sa narušilo šifrovanie, pričom by sa vychádzalo zo spoločných operačných požiadaviek vymedzených v dokumente LEON.

Krok 2: Poskytovanie podpory EÚ na zabezpečenie rovnakých podmienok a posilnenie cezhraničnej spolupráce

Spoločné zásady stanovené v kroku 1 by boli základom pre technickú, právnu a organizačnú harmonizáciu na úrovni EÚ. Ich premietnutie do konkrétnych výsledkov si vyžaduje koordináciu a finančnú podporu zo strany Komisie. To by zahŕňalo vytvorenie osobitného procesu založeného na existujúcich pracovných skupinách a v prípade potreby vytvorenie nových pracovných skupín, zabezpečenie koordinácie s príslušnými zainteresovanými stranami vrátane poskytovateľov služieb OTT a zástupcov odvetvia, podávanie správ príslušným orgánom, najmä Rade a Európskemu parlamentu, a zabezpečenie transparentnosti vo vzťahu k verejnosti. Mohlo by to zahŕňať aj financovanie cielených štúdií priamo alebo prostredníctvom relevantných partnerstiev, napr. s príslušnými agentúrami alebo akademickými partnermi.

[116] Obmedzené na odpočúvanie na úrovni operátora, ako je vymedzené vyššie.

Experti skupiny na vysokej úrovni okrem toho zdôraznili naliehavú potrebu zlepšiť efektívnosť cezhraničných žiadostí o zákonné odpočúvanie podľa súčasného rámca a zároveň vykonávať uvedenú prácu. Tento cieľ by zahŕňal:

- posúdenie súčasných obmedzení EVP[117] a prácu na zlepšení operačnej efektívnosti;
- riešenie technických a organizačných obmedzení týkajúcich sa cezhraničnej výmeny dôkazov získaných zákonným odpočúvaním, čo by si zase vyžadovalo ďalšiu prácu na:
    - mapovaní problému (aké sú obmedzenia, ktoré členské štáty sa s nimi stretávajú atď.),
    - normalizácii štruktúr údajov, mechanizmov dôvery a filtrovania údajov s cieľom zabrániť prenosu irelevantných údajov a dodržiavať zásady ochrany údajov týkajúce sa obmedzenia účelu, proporcionality a minimalizácie údajov,
    - návrhoch a kapacite cezhraničných prostriedkov prenosu,
    - identifikácii súvisiacich systémov financovania;
- uľahčenie cezhraničných žiadostí o zákonné odpočúvanie určením a odbornou prípravou jednotných kontaktných miest v koordinácii so širšou prácou na týchto miestach a prístupom k digitálnym dôkazom, pričom významnú úlohu by zohrával projekt SIRIUS;
- v relevantných prípadoch podporu dvojstranných dohôd medzi členskými štátmi a USA ako predpokladu na uľahčenie priamych žiadostí vnútroštátnych orgánov o všeobecné zahŕňanie poskytovateľov služieb OTT, keďže rozsah pôsobnosti dohody medzi EÚ a USA o cezhraničnom prístupe k elektronickým dôkazom, o ktorej sa v súčasnosti rokuje, podľa smerníc na rokovania nezahŕňa zákonné odpočúvanie, čo znamená, že na riešenie kolízie právnych poriadkov sú potrebné osobitné dohody.

[117] V smernici Európskeho parlamentu a Rady 2014/41/EÚ z 3. apríla 2014 o európskom vyšetrovacom príkaze v trestných veciach („smernica o EVP“) sa používa termín „telekomunikačná prevádzka“; zatiaľ čo väčšina členských štátov ho interpretuje v širšom zmysle v súlade s aktualizáciou EECC, mohla by sa v tejto súvislosti zvážiť a ďalej posúdiť prípadná potreba zmeniť smernicu o EVP.

Experti napokon vyzvali, aby sa zvážili opatrenia, ktorými by sa mohli zlepšiť odrádzajúce opatrenia prijaté vnútroštátnymi orgánmi proti nespolupracujúcim poskytovateľom elektronických komunikačných služieb. Experti vyzvali najmä na posúdenie uskutočniteľnosti a primeranosti možných technických riešení.

Blok odporúčaní 8

S cieľom zabezpečiť, aby široká škála poskytovateľov elektronických komunikačných služieb vrátane poskytovateľov služieb OTT reagovala na žiadosti o zákonné odpočúvanie podľa vnútroštátnych právnych predpisoch, odborníci odporúčajú tieto opatrenia:

1. *podpora vykonávania zásad vymedzených v odporúčaní 1.1 prostredníctvom koordinácie a financovania;*

2. *preskúmanie toho, ako by EVP mohol lepšie podporiť účinné cezhraničné žiadosti o zákonné odpočúvanie, napr. zlepšením právnej istoty, skrátením lehôt na odpoveď na príkazy a podporou jednotného používania EVP [odporúčanie 40];*

3. *budovanie mechanizmov (interoperabilita a kybernetická bezpečnosť) a infraštruktúr (šírka pásma a škálovateľnosť), ktoré sú zlučiteľné s cezhraničným prenosom veľkých dátových súborov v reálnom čase [odporúčanie 9];*

4. *podpora určovania jednotných kontaktných miest v EÚ na vybavovanie žiadostí od orgánov verejnej moci a udržiavanie kontaktov s nimi s cieľom uľahčiť presadzovanie povinností týkajúcich sa zákonného odpočúvania a vytvoriť mechanizmy na účinné zameriavanie sa na cezhraničné žiadosti [odporúčania 19 a 36];*

5. *podpora rozvoja dvojstranných dohôd o prístupe k údajom v reálnom čase s tretími krajinami, najmä so Spojenými štátmi [odporúčanie 38.4].*

Účinné vykonávanie odporúčania EÚ o zákonnom odpočúvaní by sa mohlo podporiť viacerými činnosťami.

Kľúčové opatrenia: Experti skupiny na vysokej úrovni vyzývajú Komisiu, aby vykonávanie odporúčania EÚ o zákonnom odpočúvaní spojila s primeranou koordináciou a financovaním

- Experti skupiny na vysokej úrovni vyzývajú Komisiu, aby navrhla jasný plán na podporu vykonávania odporúčania EÚ o zákonnom odpočúvaní, a to aj z hľadiska finančného plánovania.

Krok 3: Posúdenie možnosti právneho nástroja o zákonnom odpočúvaní

Môže sa ukázať, že samotná koordinácia nebude na dosiahnutie potrebnej úrovne harmonizácie postačovať, aj keď ju doplnia opatrenia na zefektívnenie existujúcich právnych nástrojov. Na zabezpečenie vykonateľnosti žiadostí a právnej istoty, odstránenie kolízie právnych poriadkov a zníženie administratívnej záťaže spojenej s kontrolami súladu a zákonnosti môže byť potrebný nový súbor pravidiel. Okrem toho rozdiely medzi pravidlami zákonného odpočúvania v rámci EÚ vytvárajú zaťažujúce požiadavky na regulované subjekty, ako sú poskytovatelia služieb OTT, čo môže vytvárať prekážky prístupu na trh pre poskytovateľov komunikačných služieb[118]. V tejto súvislosti by harmonizované pravidlá EÚ o zákonnom odpočúvaní dostupných údajov pomohli vybudovať budúcu digitálnu infraštruktúru Európy, pričom by sa uprednostnil model, v ktorom telekomunikačná infraštruktúra ponúka potenciálne pokrytie celého kontinentu[119].

Prechod na internetovú komunikáciu je silným podnetom na ustanovenie harmonizovaných pravidiel prístupu na úrovni EÚ; mala by sa však starostlivo posúdiť prijateľnosť, uskutočniteľnosť a vplyv právneho nástroja na priemysel, kybernetickú bezpečnosť a bezpečnosť, pričom by sa mali zohľadniť súčasné rozdiely medzi právnymi režimami členských štátov týkajúcimi sa zákonného odpočúvania. Experti skupiny na vysokej úrovni uviedli, že potenciálny nástroj by mal: i) byť v súlade so zásadami stanovenými v odporúčaní 1.1; ii) plne zohľadňovať aspekt základných práv a zvrchovanosť štátov v trestných veciach a otázkach národnej bezpečnosti; a iii) inšpirovať sa prácou, ktorá sa vykonala v súvislosti s balíkom predpisov o elektronických dôkazoch.

Experti skupiny na vysokej úrovni sa zhodli na tom, že akákoľvek iniciatíva na podporu alebo presadzovanie pravidiel zákonného odpočúvania týkajúcich sa všetkých typov elektronických komunikačných služieb by mala obsahovať jasný a vykonateľný rámec na prijatie opatrení proti poskytovateľom komunikačných služieb, ktorí pôsobia nezákonne, a/alebo odmietajú akúkoľvek formu spolupráce s orgánmi presadzovania práva. Ak by takýto rámec neexistoval, pravidlá by boli ohrozené a zločinci by masovo presunuli svoju komunikáciu k poskytovateľom, ktorí predpisy nedodržiavajú. V každej budúcej iniciatíve EÚ by sa v tejto súvislosti mal zvážiť rozdiel medzi poskytovateľmi služieb OTT, ktorí si neplnia svoje právne povinnosti, a poskytovateľmi elektronických komunikačných služieb, ktorí zámerne ponúkajú služby prispôsobené trestnej činnosti. Okrem toho by každá iniciatíva mala zohľadniť aj *acquis* EÚ, najmä akt o digitálnych službách.

---

118 Pozri „Lawful interception – a market access barrier in the European Union“ („Zákonné odpočúvanie – prekážka prístupu na trh v Európskej únii“), Vadim Doronin. In: Computer Law & Security Review 51 (2023) 105867.

119 Biela kniha – Ako splniť potreby digitálnej infraštruktúry v Európe? | Formovanie digitálnej budúcnosti Európy (europa.eu)

Takáto iniciatíva by mohla zahŕňať správne alebo justičné opatrenia. Experti skupiny na vysokej úrovni vyzvali na hĺbkovú reflexiu o tejto otázke, ktorá by sa zaoberala obavami týkajúcimi sa základných práv a kybernetickej bezpečnosti, ako aj zložitými súvisiacimi technologickými výzvami.

Blok odporúčaní 9

Na základe ďalšej analýzy a posúdenia vplyvu experti odporúčajú ***vypracovať nástroj EÚ na zákonné odpočúvanie (pozostávajúci zo soft law nástrojov alebo záväzných právnych nástrojov) na účely presadzovania práva****, ktorým by sa stanovili vymáhateľné povinnosti pre poskytovateľov elektronických komunikačných služieb v EÚ. Odporúčajú, aby tento potenciálny nástroj: [odporúčanie 38]*

1. *dodržiaval zásady dohodnuté v bloku odporúčaní 7;*
2. *bol technologicky neutrálny [odporúčanie 21];*
3. *na účely presadzovania spolupráce podporoval harmonizáciu trestnoprávnych opatrení na úrovni EÚ vrátane trestu odňatia slobody proti nespolupracujúcim poskytovateľom elektronických komunikačných služieb [odporúčanie 34];*
4. *plne zohľadňoval aspekt základných práv a zvrchovanosť štátov v trestných veciach a otázkach národnej bezpečnosti [odporúčanie 38];*
5. *bol inšpirovaný prácou vykonanou v súvislosti s prijímaním pravidiel týkajúcich sa elektronických dôkazov [odporúčanie 38 bod iv)];*
6. *poskytovateľom služieb ukladal povinnosti zapínať alebo vypínať niektoré funkcie ich služieb, aby bolo možné získať informácie po doručení súdneho príkazu (napríklad uchovávať geolokalizáciu konkrétneho používateľa, na ktorého sa vzťahuje zákonná žiadosť)[odporúčanie 32];*
7. *zahŕňal mechanizmy na zabezpečenie toho, aby členské štáty mohli presadzovať sankcie voči nespolupracujúcim poskytovateľom elektronických komunikačných služieb (správne alebo trestnoprávne opatrenia v závislosti od toho, či poskytovateľ len nespolupracuje alebo ponúka službu trestnej povahy) v súlade s pravidlami aktu o digitálnych službách a prípadne nad ich rámec, a aby takéto sankcie pôsobili na takéto subjekty odrádzajúco [odporúčanie 33].*

Presadzovanie zásad stanovených v odporúčaní EÚ o zákonnom odpočúvaní by bolo dôležitým krokom k harmonizovanejším a vymáhateľnejším pravidlám v tejto oblasti. Stále však môže byť potrebný právny nástroj na zlepšenie právnej istoty, zabezpečenie zavedenia potrebných záruk pre všetky príslušné elektronické komunikačné služby pri vykonávaní zákonného odpočúvania a na zabezpečenie toho, aby poskytovatelia elektronických komunikačných služieb, ktorí nie sú ochotní presadzovať pravidlá stanovené členskými štátmi, boli k tomu donútené.

Kľúčové opatrenia: Experti skupiny na vysokej úrovni vyzývajú Komisiu, aby posúdila ďalší vývoj legislatívneho rámca o zákonnom odpočúvaní na účely presadzovania práva

- Experti skupiny na vysokej úrovni vyzývajú Európsku komisiu, aby pred možným posúdením vplyvu posúdila možnosť právneho nástroja EÚ o zákonnom odpočúvaní, pričom nadviaže na prácu vykonanú v rámci prípravy nariadenia a smernice EÚ o elektronických dôkazoch a zameria sa na identifikáciu potenciálnych technologicky neutrálnych riešení.

II. Riešenie technologických výziev

Mnohé výzvy, ktorým čelia orgány presadzovania práva, pokiaľ ide o prístup k údajom, vyplývajú z toho, aké ťažké je pre ne predvídať technologický vývoj a prispôsobiť sa mu. Dôvodom je, že na rozdiel od aktérov v iných odvetviach, ako je obrana alebo kozmický priestor, orgány presadzovania práva na to nemajú potrebné zdroje ani silné vzťahy s priemyslom a nie je pre ne ani zvykom, že by ich potrebovali. V mnohých prípadoch sa aktéri v oblasti vnútornej bezpečnosti snažia vyplniť technologické medzery reaktívnym spôsobom alebo sa najčastejšie pokúšajú pokryť svoje potreby štandardnou technológiou, ktorá je k dispozícii a cenovo dostupná. Na podporu prechodu od reaktívneho prístupu k proaktívnejšiemu je potrebné riešiť technologické výzvy štruktúrovaným, výhľadovo orientovaným a multidisciplinárnym spôsobom s dvoma hlavnými prioritami: z pohľadu vnútroštátnych orgánov je nevyhnutné zabezpečiť, aby orgány presadzovania práva mali prístup k príslušným kapacitám na získanie a spracovanie prenášaných dostupných údajov; pre operátorov a poskytovateľov technológií je zase nevyhnutné, aby mohli plniť svoje povinnosti, pokiaľ ide o prístup k údajom, súkromie a kybernetickú bezpečnosť, a aby sa chránili ich záujmy.

Odborníci preto navrhujú predvídať technologické výzvy prostredníctvom komplexnej a výhľadovej politiky založenej na **technologickom pláne pre zákonný prístup**, v ktorom sa stanovia ciele a vymedzia činnosti spolu s ich financovaním na dosiahnutie týchto cieľov.

Pokiaľ ide o budovanie kapacít, hoci výzvy sú odlišné, prístup, ktorý navrhujú experti, je často podobný ako pri digitálnej forenznej analýze, uchovávaní údajov a zákonnom odpočúvaní[120], a vychádza z rovnakých odporúčaní, pričom existuje silná požiadavka na plánovanie zamerané na ciele s cieľom riadiť možnosti financovania s užším zapojením priemyselných aktérov a kľúčových zainteresovaných strán, ako je Európske inovačné centrum pre vnútornú bezpečnosť.

Odborníci na presadzovanie práva však zdôraznili dve skutočnosti, ktoré sú špecifické pre zákonné odpočúvanie.

- Zvýšené používanie metaúdajov – napr. lokalizačných údajov, záznamov o hovoroch a záhlaví e-mailov – môže predstavovať ďalšie vyšetrovacie stopy. **S čoraz väčším počtom zariadení pripojených na internet sa zvýši objem generovaných údajov, čo ponúkne viac príležitostí na identifikáciu vzorcov správania.** Experti vyzvali na intenzívnejší výskum, inovácie a využívanie, pokiaľ ide o **rozšírené používanie metaúdajov**, napríklad prostredníctvom umelej inteligencie, ako spôsob zmiernenia nedostatočného prístupu k údajom o obsahu. Zároveň poukázali na riziká pre súkromie spojené s rozsiahlym spracúvaním hromadných osobných metaúdajov umelou inteligenciou, ktoré treba vyvážiť cieleným využívaním obsahových údajov. Experti na presadzovanie práva však jasne uvádzajú, že len samotné metaúdaje nemôžu úplne nahradiť dôkaznú hodnotu obsahu komunikácie na preukázanie úmyslu.

- Keď páchatelia trestnej činnosti používajú špecializované komunikačné platformy šifrované medzi koncovými zariadeniami, orgány presadzovania práva musia používať taktické riešenia založené na využívaní **zraniteľností** na získanie prístupu ku komunikácii podozrivých osôb. Viaceré orgány presadzovania práva už fungujú na základe právneho rámca, ktorý umožňuje odpočúvanie na koncových bodoch komunikácie, a majú na to technológiu, a v tejto súvislosti existuje priestor na ďalší pokrok. Ten by mohol zahŕňať podporu vývoja nástrojov vytvorených v EÚ a umožnenie orgánom presadzovania práva, aby ich získali a používali na základe existujúceho právneho rámca.

  Experti na presadzovanie práva však uvádzajú, že táto metóda by sa nemala rozširovať ako primárny prostriedok získavania dôkazov, keďže taktické odpočúvanie nie je škálovateľné ani bezproblémové. Napríklad by mohli vzniknúť problémy s jurisdikciou na základe polohy cieľa. Okrem toho využívanie zraniteľností, ktoré nemožno zverejniť, je nevyhnutne v rozpore so základnými zásadami kybernetickej bezpečnosti.

[120] Podrobne opísané v kapitole o digitálnej forenznej analýze.

Pokiaľ ide o zákonný prístup už v štádiu návrhu, experti na presadzovanie práva navrhli obozretný prístup, keďže od priemyselných aktérov by sa nemalo vyžadovať, aby do služby integrovali akýkoľvek systém, ktorý by mohol všeobecne alebo systematicky oslabiť šifrovanie pre všetkých jej používateľov; zákonný prístup by mal zostať cielený na konkrétnu komunikáciu. Zhodli sa na relevantnosti celkového cieľa, ale trvali na tom, že je potrebné napredovať postupne a zapájať všetky príslušné kategórie zainteresovaných strán vrátane expertov na technológie, kybernetickú bezpečnosť a súkromie, pričom sa zohľadnia potenciálne riziká a citlivosť verejnej diskusie. Dôrazne odporúčali najmä zaujať prístup založený na dôkazoch a starostlivo posudzovať dostupnosť technických riešení, ktoré neoslabujú kybernetickú bezpečnosť komunikácií ani nemajú negatívny vplyv na kybernetickú bezpečnosť operátorov.

Blok odporúčaní 10

S cieľom riešiť technologické výzvy zákonného odpočúvania experti odporúčajú vypracovať ***technologický plán pre zákonný prístup***[121]*, ktorým sa najmä:*

1. *spoja experti v oblasti technológií, kybernetickej bezpečnosti, ochrany súkromia, normalizácie a bezpečnosti a zabezpečí primeraná koordinácia, prípadne prostredníctvom stálej štruktúry [odporúčanie 22];*
2. *podporí výskum, vývoj a zavádzanie nástrojov na získavanie údajov a prístup k údajom vrátane dešifrovacích spôsobilostí, ako aj kapacít na analýzu údajov*[122] *založených na umelej inteligencii [odporúčanie 4];*
3. *podporí koordinovaný prístup k normalizácii, ktorým by sa podľa vhodnosti zohľadňovali potreby zákonného prístupu k údajom a ktorým by sa tiež [odporúčania 15, 16 a 20]:*
    a. *podporovalo zapojenie odborníkov z praxe zo všetkých relevantných komunít do príslušných normalizačných skupín;*
    b. *doplnili budúce iniciatívy o primerané normalizačné opatrenia (na podporu technologicky neutrálneho prístupu);*
    c. *pokryli komunikačné technológie ako celok, internet vecí (vrátane napríklad prepojených automobilov) a akákoľvek forma pripojenia (vrátane napríklad satelitnej komunikácie);*
4. *posilní koordinácia EÚ s priemyslom s cieľom riešiť situácie, v ktorých existujú technologické riešenia, ktoré sa však neimplementovali; v takýchto prípadoch*[123] *sú potrebné jasné usmernenia a uľahčenie dialógu na úrovni EÚ [odporúčanie 24];*
5. *zavedie zákonný prístup už v štádiu návrhu so zreteľom na všetky relevantné technológie v súlade s potrebami orgánov presadzovania práva, pričom sa zároveň zabezpečí silná bezpečnosť a kybernetická bezpečnosť a splnenie právnych povinností týkajúcich sa zákonného prístupu [odporúčanie 22];*
6. *dôkladne vyriešia výzvy súvisiace so šifrovaním:*
    a. *zabezpečením toho, aby prípadné nové povinnosti a/alebo normy neviedli priamo ani nepriamo k povinnosti poskytovateľov oslabiť bezpečnosť komunikácie tým, že vo všeobecnosti narušia alebo oslabia šifrovanie medzi koncovými zariadeniami [odporúčanie 23];*
    b. *zabezpečením toho, aby zákonný prístup už v štádiu návrhu nemal negatívny vplyv na stav bezpečnosti príslušných hardvérových alebo softvérových architektúr [odporúčanie 23];*
    c. *koordinovaným úsilím a podporou financovania zo strany EÚ s cieľom vypracovať metodiku vývoja opatrení v oblasti cieleného zákonného prístupu, narábania s nimi a ich využívania na riešenie prípadov, keď prístup k údajom nie je možný prostredníctvom spolupráce s poskytovateľmi elektronických komunikačných služieb [odporúčanie 10].*

---

[121] Technologický plán by sa mal vzťahovať na tri pracovné okruhy: digitálna forenzná analýza, uchovávanie údajov a zákonné odpočúvanie.

[122] Toto odporúčanie sa vzťahuje aj na prístup k údajom na zariadení (pozri oddiel o digitálnej forenznej analýze), ale prípady použitia sú mierne odlišné.

[123] Napríklad ak dohody o home-routingu alebo konkrétny druh implementácie protokolu RCS neumožňujú zákonné odpočúvanie.

Hoci niektoré iniciatívy, ktoré navrhli experti skupiny na vysokej úrovni, už čiastočne existujú, existuje silná potreba lepšie štruktúrovať strednodobú a dlhodobú technologickú politiku v oblasti zákonného prístupu v rámci technologického plánu, a to cielenými míľnikmi a súvisiacim nástrojom monitorovania. Tento prístup by sa mal vzťahovať nielen na prístup k prenášaným údajom, ale aj na digitálnu forenznú analýzu a uchovávanie údajov.

Technologický plán by mal byť orientovaný na budúcnosť, vymáhateľný, zameraný na prioritné témy a zakotvený v digitálnej stratégii EÚ. Mal by zahŕňať všetky príslušné kategórie zainteresovaných strán, najmä inštitúcie, orgány, úrady a agentúry EÚ, vnútroštátne orgány, akademickú obec vo všetkých relevantných oblastiach, priemysel a mimovládne organizácie v úzkom partnerstve a mal by mať jasnú správu.

Kľúčové opatrenia: Experti skupiny na vysokej úrovni naliehavo vyzývajú Komisiu, aby predložila a začala vykonávať technologický plán prístupu k údajom

- Experti skupiny na vysokej úrovni vyzývajú Európsku komisiu, aby vypracovala a začala vykonávať technologický plán zameraný na výzvy v oblasti šifrovania, v ktorom sa budú riešiť všetky relevantné aspekty vrátane technologických a trhových aspektov a aspektov kybernetickej bezpečnosti, základných práv, normalizácie, presadzovania práva a výskumu. Tento technologický plán by mal byť k dispozícii v roku 2025 a mal by vychádzať zo všetkých relevantných odborných znalostí členských štátov a inštitúcií, orgánov, úradov a agentúr EÚ vrátane oblasti kybernetickej bezpečnosti, ochrany údajov a súkromia.