Svet
Evropske unije

Bruselj, 13. marec 2025
(OR. en)

15941/2/24
REV 2

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

DOPIS

Pošiljatelj:	predsedstvo
Prejemnik:	delegacije
Št. predh. dok.:	11281/24
Zadeva:	Sklepno poročilo skupine na visoki ravni za dostop do podatkov za učinkovito odkrivanje in pregon

V imenu sopredsedojočih skupini na visoki ravni za dostop do podatkov za učinkovito odkrivanje in pregon vam v prilogi pošiljamo sklepno poročilo te skupine.

Ta revidirana različica odraža redakcijske spremembe, uvedene med jezikovnim pregledom.

PRILOGA

Sklepno poročilo skupine na visoki ravni za dostop do podatkov za učinkovito odkrivanje in pregon

15. november 2024

Izražena mnenja so mnenja strokovnjakov skupine na visoki ravni in ne bi smela šteti za uradno stališče Evropske komisije ali Sveta.

Priporočila skupine na visoki ravni za dostop do podatkov za učinkovito odkrivanje in pregon je treba izvajati ob polnem spoštovanju pristojnosti držav članic. Uporabljajo se le za dejavnosti odkrivanja in pregona ter komercialna orodja, ki se uporabljajo za pravosodne namene, in ne posegajo v izključne pristojnosti držav članic za nacionalno varnost. Posledično so suvereni instrumenti in instrumenti, ki so v uporabi in/ali razviti izključno za namene notranje varnosti, izključeni iz področja uporabe teh priporočil.

Vsebina

Povzetek

Evropska unija je območje svobode, varnosti in pravice, kjer se spoštujejo temeljne pravice ter različni pravni sistemi in tradicije držav članic. Cilj tega območja je zagotoviti visoko raven varnosti[1] z ukrepi za preprečevanje kriminala in boj proti njemu ter omogočiti lažje usklajevanje in sodelovanje med organi odkrivanja in pregona ter pravosodnimi in drugimi pristojnimi organi.

Zaradi tehnološkega razvoja in digitalizacije naših družb se je vsakdanje življenje državljanov in državljank občutno spremenilo, organi odkrivanja in pregona ter pravosodni organ pa se srečujejo z novimi izzivi z vidika zagotavljanja visoke ravni varnosti, tako na nacionalni ravni kot tudi na ravni EU. V današnji digitalni dobi ima skoraj vsaka kriminalna preiskava digitalno komponento. To vprašanje je bilo aprila 2023 obravnavano v preglednem dokumentu, pripravljenem za strokovno skupino na visoki ravni za dostop do podatkov za učinkovito odkrivanje in pregon:

> Tehnologije in orodja […] zlorabljajo tudi v kriminalne namene. Zaradi teh sprememb je vse težje ohranjati učinkovito odkrivanje in pregon povsod v EU za namene zaščite javne varnosti, preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj ter izpolnitve legitimnih pričakovanja žrtev glede pravice in odškodnine. Če ne bomo ustrezno ukrepali, obstaja resna nevarnost, da bo ta zdajšnji trend storilcem kaznivih dejanj omogočil, da prekinejo komunikacijo na javnih kanalih […]. To resno ogroža varnost posameznikov in družbe, saj lahko navsezadnje ovira pozitivno obveznost držav, da še naprej zagotavljajo pravno državo in demokratično družbo[2].

[1] V tem dokumentu pojem „varnost“ pomeni boj proti kriminalu ali preprečevanje groženj javni varnosti.

[2] 8281/23, 13. april 2023.

Pravica do spoštovanja zasebnega in družinskega življenja, doma in komunikacij ter pravica do varstva osebnih podatkov sta zagotovljeni z Listino EU o temeljnih pravicah. Zaupnost komunikacij, tako pisnih kot tudi telefonskih, je pomemben dosežek demokratičnih družb, saj zagotavlja, da se niti država niti zasebni akterji ne smejo vmešavati v svobodo izražanja ljudi, in omogoča vzpostavitev uspešne civilne družbe. Uživanje teh pravic je lahko zakonsko omejeno, zlasti z ukrepi za zaščito nacionalne varnosti, obrambe ali javne varnosti ter za preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj ali nedovoljene uporabe elektronskih komunikacijskih sistemov, če so ti ukrepi v demokratični družbi potrebni, primerni in sorazmerni. Zato lahko organi odkrivanja in pregona ter pravosodni organi odpirajo in berejo pisna sporočila, prestrezajo telefonske klice in prisluškujejo pogovorom, če se jim to zdi potrebno, sorazmerno in upravičeno ter če so takšni ukrepi v skladu z veljavnimi pravnimi določbami in se pri njihovem izvajanju ustrezno spoštujejo njihove temeljne pravice. Ta možnost bi morala biti na voljo vsem pristojnim organom ne glede na stopnjo tehnološkega razvoja. Zaradi širjenja novih oblik medosebne komunikacij v zadnjih letih se mora celotna družba prilagajati novim resničnostim. Zagotoviti moramo, da komunikacija med državljani in državljankami ostane zaščitena, hkrati pa organom odkrivanja in pregona ter pravosodnim organom omogočiti, da še naprej izpolnjujejo svojo dolžnost varovanja državljanov in državljank s preprečevanjem hudih kaznivih dejanj, organiziranega kriminala in terorizma ter bojem proti njim. Prilagajanje je nujno, zato strokovnjaki pozivajo oblikovalce politik, naj ukrepajo takoj, saj organi odkrivanja in pregona že zaostajajo za tehnološkim razvojem, kar neposredno vpliva na njihovo sposobnost zagotavljanja pravic državljanov in državljank.

Ministri in ministrice za notranje zadeve so na neformalni seji Sveta za pravosodje in notranje zadeve 26. januarja 2023 razmišljali o izzivih, ki jih tehnološki razvoj predstavlja za odkrivanje in pregon v digitalni dobi. Izrazili so tudi zaskrbljenost, da veljavna pravila in njihova razlaga v sodni praksi, skupaj s praktičnimi in operativnimi ovirami, vse bolj otežujejo opravljanje dela organov odkrivanja in pregona, zlasti ko gre za hrambo in dostop do podatkov, potrebnih za preiskovanje in pregon kaznivih dejanj[3].

[3] Glej 7184/1/23 REV 1 z dne 23. marca 2023, v katerem so navedene vse pripombe držav članic.

Po tej razpravi je Svet potrdil ustanovitev skupine za oblikovanje strateške, v prihodnost usmerjene vizije za učinkovit in zakonit dostop do podatkov, elektronskih dokazov in informacij v digitalni dobi za pravosodne organe in organe odkrivanja in pregona, tj. **skupine na visoki ravni za dostop do podatkov za učinkovito odkrivanje in pregon (HLG)**[4].

Naloga skupine na visoki ravni je bila poiskati rešitve za izziv, povezan z omogočanjem zakonitega dostopa do podatkov, da bi z učinkovitimi rešitvami, ki bi bile odgovor na izzive prihodnosti, zagotovili visoko raven varnosti za vse prebivalce in prebivalke EU ter hkrati zagotovili spoštovanje temeljnih pravic, vključno s pravicami do zasebnosti in varstva podatkov, ter visoko raven kibernetske varnosti.

42 priporočil[5], ki so glavni rezultat dela skupine na visoki ravni, je bilo pripravljenih v času, ko je vse več pozivov k spletni odgovornosti. Priporočila se nanašajo na sedanje in pričakovane izzive glede na tehnološki razvoj, njihov namen pa je omogočiti celovit pristop EU k zagotavljanju učinkovitih kazenskih preiskav in pregona. Priporočila so razvrščena v tri sklope: **krepitev zmogljivosti; sodelovanje z industrijo in standardizacija in zakonodajni ukrepi.** V njih so poudarjeni izzivi, s katerimi se soočajo organi odkrivanja in pregona pri dostopu do podatkov v berljivi obliki za namene kazenskih preiskav, ki so posledica neusklajenih obveznosti hrambe podatkov in strogih zahtev sodne prakse EU, vse večje uporabe šifriranja od konca do konca in nesodelovanja nekaterih netradicionalnih telekomunikacijskih storitev. V njih so sicer pozdravljena pravila o e-dokazih, vendar je opozorjeno, da imajo omejitve pri obravnavanju izzivov, ki jih prinaša šifriranje, pozvano pa je tudi k tesnejšemu sodelovanju med organi odkrivanja in pregona in pravosodnimi organi ter ponudniki storitev, da se vzpostavi stalen dialog in medsebojno razumevanje operativnih, tehničnih in poslovnih potreb ter odpravijo težave pri dostopu do šifriranih podatkov. Po mnenju strokovnjakov bo tesnejše sodelovanje med organi odkrivanja in pregona ter ponudniki storitev do določene mere izboljšalo stanje, vendar pa je treba obveznosti ponudnikov storitev glede sodelovanja kot rešitev, ki bi bila odgovor na izzive prihodnosti, uveljaviti tudi z zakonodajo, ne da bi pri tem na splošen ali sistematičen način oslabili šifriranja za uporabnike storitev.

---

4 Skupina na visoki ravni za dostop do podatkov za učinkovito odkrivanje in pregon –Evropska komisija (europa.eu).

5 Priporočila skupine na visoki ravni.

Ministri in ministrice za notranje zadeve so na seji Sveta 13. junija 2024 **izmenjali mnenja** o priporočilih skupine na visoki ravni, na splošno pozdravili delo strokovnjakov te skupine in poudarili, da je treba hitro nadaljevati delo v zvezi z dostopom do podatkov za učinkovito odkrivanje in pregon[6]. Opredelili so naslednje prednostne naloge: (1) vzpostavitev usklajenega pravnega okvira EU za hrambo podatkov za namene odkrivanja in pregona; (2) vzpostavitev pravil za učinkovit dostop do podatkov, ki se nanašajo na medosebno elektronsko komunikacijo; in (3) vzpostavitev pravno in tehnično zanesljivih rešitev za dostop do šifrirane elektronske komunikacije v posameznih primerih in na podlagi sodne odločbe za namene preprečevanja, preiskovanja in pregona hudih kaznivih dejanj in organiziranega kriminala ter terorizma.

Ministri in ministrice so se zavzeli tudi za okrepitev vpliva EU na standardizacijo protokolov in tehnologij ter za usklajen pristop k certificiranju orodij in postopkov na področju digitalne forenzike. Nazadnje so vztrajali, da je za izvajanje priporočil treba pripraviti kažipot, ki bi vključeval jasno časovnico, oceno izvedljivosti in ustrezna finančna sredstva. Kot pomembno je bilo ocenjeno tudi usklajevanje izvajanja posameznih priporočil.

Namen tega sklepnega poročila je podrobno opisati izzive, ki so jih opredelili strokovnjaki, ter določiti možnosti za nadaljevanje dela in **operacionalizacijo priporočil**. V njem je opisanih več ključnih vprašanj, ki so jih opredelili strokovnjaki in so v skladu z mandatom skupine na visoki ravni usmerjala tri delovne sklope.

Prvič, dostop do podatkov je ključnega pomena za **digitalno forenziko**, s katero organi odkrivanja in pregona lahko zbirajo in analizirajo dokaze, pridobljene iz elektronskih naprav. Ti podatki zagotavljajo zanesljive informacije o kriminalnih dejavnostih in identifikaciji odgovornih za kriminalna dejanja. Zaradi hitrega napredka in široke uporabe nekaterih tehnologij, kot je šifriranje, morajo organi odkrivanja in pregona okrepiti svoje vire, znanja in tehnične rešitve za dostop do šifriranih podatkov. V zvezi s tem in v zvezi z uporabo komercialnih rešitev lahko učinkovito čezmejno sodelovanje zagotovi podporo z izmenjavo strokovnega znanja, razvojem standardiziranih orodij in postopkov ter združevanjem virov. Kljub temu pa so se strokovnjaki strinjali, da samo razvoj zmogljivosti ne bo izboljšal zmogljivosti odkrivanja in pregona. Nekateri strokovnjaki so menili, da je omogočanje dostopa do podatkov v berljivi obliki v jasno reguliranih okoliščinah bolj trajnostna dolgoročna rešitev.

[6] 11281/24, 21. junij 2024.

Drugič, potrebna je usklajena in dosledna zakonodaja o **hrambi podatkov**, ki je v celoti skladna s temeljnimi pravicami, da se organom odkrivanja in pregona omogoči učinkovito preiskovanje in pregon kaznivih dejanj. Zaradi hitrega razvoja tehnologij je pravočasen dostop organov odkrivanja in pregona do ustreznih podatkov, ki jih hranijo ponudniki, vse bolj dragocen. Dostop do komunikacijskih metapodatkov, ki jih hranijo ponudniki storitev, je še posebej bistven za identifikacijo osumljencev in razumevanje njihovih dejavnosti, njegov pomen za nadaljevanje preiskav pa je že bil dokazan.

Tretjič, **zakonito prestrezanje** je bistveno za učinkovito preiskovanje in pregon organiziranega kriminala in terorističnih skupin. Organi lahko na podlagi sodnih odločb in ob popolnem spoštovanju temeljnih pravic od ponudnikov storitev zahtevajo, da posredujejo vsebino komunikacije, ta vsebina pa daje neprecenljiv vpogled v kriminalne dejavnosti. Upoštevajoč prehod s tradicionalnih ponudnikov komunikacij na povrhnje storitve (OTT), kot so opredeljene v Evropskem zakoniku o elektronskih komunikacijah (EZEK)[7], in dejstvo, da se storilci kaznivih dejanj vse bolj selijo na šifrirane platforme med koncema („end-to-end“)[8], je za zakonit dostop do komunikacij v realnem času potrebna ocena potrebe po jasnih pravilih za sodelovanje med organi odkrivanja in pregona in tehnološkimi podjetji ter okrepljeno sodelovanje na ravni EU, da bi lahko olajšali čezmejne zahteve.

Priporočila in vsebina tega sklepnega poročila odražajo samo **pričakovanja in zahteve strokovnjakov skupine na visoki ravni**.

S tem poročilom je **skupina na visoki ravni zaključila svoje delo** ter poziva Komisijo, države članice, Evropski parlament in vse zadevne deležnike, naj se pri pripravi ukrepov za reševanje vprašanja dostopa do podatkov za učinkovito odkrivanje in pregon zgledujejo po priporočilih in poročilu. Takšne ukrepe bi morala spremljati močna utemeljitev, ki bi dokazovala nujnost sprejetja pomembnih ukrepov za zagotovitev učinkovitega zakonitega dostopa do podatkov. Strokovnjaki spodbujajo vse institucije in organe EU, naj to delo brez odlašanja nadaljujejo, in sicer z izvajanjem konkretnih pobud iz namenskega kažipota.

---

7 Direktiva (EU) 2018/1972 z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah razširja del pravnega okvira, ki se uporablja za tradicionalne telekomunikacije, na podjetja, ki ponujajo internetne storitve prek telekomunikacijske infrastrukture, ki je nimajo v lasti oziroma je ne upravljajo, vključno z medosebnimi komunikacijskimi storitvami, neodvisnimi od številke (NI-ICS).

8 *Internet Organised Crime Threat Assessment, Europol* (Ocena ogroženosti zaradi internetnega organiziranega kriminala, Europol) (IOCTA), 2024.

Zakoniti dostop*:* ključni izzivi

Naši sposobnosti za boj proti kriminalu in ohranjanje varnosti EU sta se v zadnjih letih na številnih področjih izboljšali. Sodelovanje na področju odkrivanja in pregona ter pravosodno sodelovanje sta postali učinkovitejši, uvedeni so bili nova zakonodaja ter orodja za boj proti hudim kaznivim dejanjem in organiziranemu kriminalu, hkrati pa so bila okrepljena skupna prizadevanja za boj proti tihotapljenju migrantov, trgovini z ljudmi, strelnemu orožju in drogam, korupciji in drugim hudim kaznivim dejanjem.

Vendar se organi odkrivanja in pregona vsak dan soočajo z novimi izzivi pri zagotavljanju varnosti naših državljanov in državljank, zlasti tistih, ki jih prinaša digitalizacija naše družbe.

Digitalne tehnologije spreminjajo naše življenje – od našega načina komuniciranja do življenja in dela –, družbeni vidiki tega prehoda pa sežejo globoko. Digitalizacija lahko zagotovi rešitve za številne izzive, s katerimi se soočajo Evropa in Evropejci, ter ponuja številne priložnosti – priložnosti za ustvarjanje delovnih mest, spodbujanje izobraževanja, povečanje konkurenčnosti in spodbujanje inovacij, boj proti podnebnim spremembam, olajšanje zelenega prehoda in še veliko več.

Hkrati digitalizacija zagotavlja tudi pogoje, v katerih lahko storilci kaznivih dejanj izkoristijo tehnološki napredek za izvajanje kaznivih dejanj na spletu in zunaj njega. Šifrirane naprave in aplikacije, novi komunikacijski operaterji, navidezna zasebna omrežja (VPN) itd. so zasnovani tako, da varujejo zasebnost zakonitih uporabnikov. Vendar poleg tega storilcem kaznivih dejanj zagotavljajo učinkovita sredstva za prikrivanje njihovih identitet, trženje s kriminalom povezanih proizvodov in storitev, , usmerjanje plačil ter prikrivanje njihovih dejavnosti in komunikacij, s čimer se učinkovito izogibajo odkrivanju, preiskovanju in pregonu. Čeprav obstajajo orodja in storitve, ki so namensko izdelani in se uporabljajo predvsem za izvajanje nezakonitih dejavnosti, obstajajo dokazi, da storilci kaznivih dejanj vse pogosteje izkoriščajo ukrepe za varstvo zasebnosti, ki jih zagotavljajo zakonite elektronske komunikacijske storitve. ***Organi odkrivanja in pregona v zvezi s tem pogosto zaostajajo za storilci kaznivih dejanj, saj nimajo ustreznega osebja, orodij in sredstev za učinkovito reševanje tega izziva***. Zaradi tega razvoja dogodkov je dostop do podatkov za namene odkrivanja in pregona v zadnjih letih ključni izziv pri kazenskih preiskavah in pregonu. Kljub temu so bili doseženi izjemni uspehi; organom odkrivanja in pregona je npr. uspelo razvozlati šifrirana komunikacijska omrežja kriminalnega značaja, kot sta EncroChat in SkyECC, ter nadaljujejo izvajanje operacij, kot je „Desert Light“, v okviru katere je bil novembra 2022 razbit „superkartel“ trgovcev s kokainom. Europolova platforma za dešifriranje je v zadnjih nekaj letih podprla več preiskav na visoki ravni, kar je prispevalo k uspešnim ukrepom odkrivanja in pregona proti terorizmu ter hudim kaznivim dejanjem in organiziranemu kriminalu.

Vendar se za temi uspešnimi zgodbami skrivajo številne zapoznele in neuspešne preiskave, saj strokovnjaki poročajo o stalnih izzivih v zvezi s pravočasnim izpolnjevanjem operativnih potreb.

Zakoniti dostop organom omogoča, da ciljno spremljajo in prestrezajo komunikacijo med storilci kaznivih dejanj ter onemogočajo njihova dejanja, s čimer se otežuje uporaba tehnologije za kriminalne namene. Nasprotno pa se bodo organi odkrivanja in pregona brez trdnega pravnega okvira in ustreznih virov še naprej spopadali z nepremostljivimi težavami, obstaja pa tudi tveganje, da bi ključni dokazi iz različnih razlogov ostali nedosegljivi.

- **Podatki niso vedno na voljo**, zlasti kadar so izbrisani, zaradi nedoslednih in neustreznih pravil o hrambi podatkov za namene odkrivanja in pregona. Ta vrzel resno ovira preiskave hudih kaznivih dejanj in organiziranega kriminala. Dejansko je v raziskavi, izvedeni leta 2023[9] v okviru projekta SIRIUS, skoraj polovica preiskovalcev, s katerimi je bilo opravljeno posvetovanje, kot glavno oviro navedla, da ni usklajene ureditve hrambe podatkov. Brez usklajenih pravil obstaja tveganje, da ključni podatki ostanejo nedosegljivi, kar spodkopava prizadevanja za učinkovit boj proti kriminalu.

- **Podatkov ni mogoče pridobiti**, zlasti če je pridobivanje iz naprave neuspešno. Ker ni potrebnih znanj in spretnosti, ustreznih orodij ter zadostnega sodelovanja s proizvajalci naprave in med njimi, je digitalna forenzika težavna, draga in zamudna, če ne v celoti neizvedljiva. Ta pomembna pomanjkljivost ovira učinkovite preiskave. Brez naprednih forenzičnih zmogljivosti in spretnosti ter izboljšanega sodelovanja z industrijo in med nacionalnimi organi ključni digitalni dokazi ostajajo nedostopni, kar močno vpliva na prizadevanja na področju odkrivanja in pregona.

- **Podatkov ni mogoče vedno prebrati** zaradi šifriranja. Številne službe za varstvo zaupnosti komunikacij in zasebnosti ter za kibernetsko varnost zdaj uporabljajo šifriranje od konca do konca, vendar lahko to organom odkrivanja in pregona zelo oteži dostop do komunikacijskih podatkov. To pomeni, da tudi če so podatki prestreženi zakonito, jih pogosto ni mogoče dešifrirati. Če teh podatkov ni mogoče prebrati, ostajajo pomembni dokazi skriti, zaradi česar je veliko težje preiskovati kazniva dejanja.

[9] SIRIUS *Cross-Border Access to Electronic Evidence (SIRIUS project*) (Čezmejni dostop do elektronskih dokazov (projekt SIRIUS)), https://www.europol.europa.eu/operations-services-innovation/sirius-project.

- **Podatkov ni mogoče vedno analizirati**, npr. tehnologija in/ali človeški viri niso vedno na voljo za pregledovanje velikih količin podatkov ali filtriranje in analiziranje zaseženih podatkov na učinkovit način, ki je združljiv s temeljnimi vrednotami EU ter pravnimi okviri EU in držav članic.

- **Podatkov ni mogoče pridobiti** zaradi kolizije zakonov med jurisdikcijami. Podatki pogosto potujejo preko mednarodnih meja, kar prinaša zapletene izzive v zvezi s sodno pristojnostjo. Različne države imajo različne zakone in predpise v zvezi z dostopom do podatkov, zaradi česar je težko pridobiti podatke, shranjene v tujini. Nova uredba in direktiva EU o e-dokazih sta pomemben korak k temu, da se to olajša, vendar je za celovito izvajanje teh ukrepov potrebno še veliko dela – brez njunega doslednega izvajanja pa dostop do ključnih podatkov iz drugih držav še vedno ostaja velik izziv na področju odkrivanja in pregona.

To so nekateri od vsakodnevnih izzivov, s katerimi se danes soočajo organi odkrivanja in pregona.

Storilci kaznivih dejanj nenehno prilagajajo svoje vedenje, da jih ne bi bilo mogoče odkriti. Razpoložljivi statistični podatki[10] kažejo, da (storilci kaznivih dejanj)vse pogosteje prehajajo na zakonite šifrirane platforme od konca do konca. Ko pa so učinkoviti protiukrepi odkriti, obstaja verjetnost, da bodo storilci kaznivih dejanj ponovno prešli na druge komunikacijske kanale. Zato je bistveno, da so organi odkrivanja in pregona ob pomoči strokovnjakov iz vseh zadevnih skupnosti sposobni spremljati tehnološki razvoj in predvideti spremembe v kriminalnem vedenju, kot so tiste, povezane s 6G, internetom stvari in satelitskimi komunikacijami. Da bi se lahko soočili s podobnimi izzivi v prihodnosti, je treba poleg tega ohraniti in prilagoditi zmogljivosti, ki so omogočile uspešne operacije proti namenskim kriminalnim komunikacijskim storitvam (npr. EncroChat, Ghost ECC).

[10] Europol IOCTA 2024.

Organi odkrivanja in pregona morajo imeti vse več možnosti za zakonit dostop do digitalnih informacij. Ker se storilci kaznivih dejanj vse bolj zanašajo na spletne storitve, število zahtevkov za podatke od ponudnikov spletnih storitev narašča; njihovo število se je med leti 2017 in 2022 dejansko potrojilo[11]. Komunikacijski podatki (tako metapodatki kot podatki o vsebini) so ključni za številne kazenske preiskave. Dostop do digitalnih dokazov naj bi imel ključno vlogo v 85 % preiskav[12]. Z novim sklopom pravil o čezmejnem dostopu do elektronskih dokazov se bo povečala zmožnost pristojnih organov za dostop do teh podatkov. Vendar lahko ta pravila delujejo le, če so podatki na voljo v berljivi obliki. Prav tako sta dostop do podatkov, shranjenih v zaseženih napravah, in zakonito prestrezanje komunikacij še vedno izjemen izziv, tako s pravnega vidika kot v praksi. Kar zadeva učinkovito prestrezanje podatkov v tranzitu v čezmejnih primerih, lahko države članice za pravosodno sodelovanje sicer zaprosijo prek Konvencije o medsebojni pravni pomoči v kazenskih zadevah[13] in evropskega preiskovalnega naloga[14]; vendar sta bila ta instrumenta zamišljena predvsem za izmenjavo fizičnih dokazov, njuna učinkovitost pa je lahko glede na tehnološki razvoj omejena.

Za zakoniti dostop morajo veljati strogi pogoji, določeni v nacionalnem pravu, pravu EU in mednarodnem pravu, in vzpostavljeni morajo biti pregledni in odgovorni postopki za urejanje takega dostopa, vključno s preprečevanjem kakršnega koli nezakonitega razkritja poslovnih skrivnosti, pri čemer je treba zagotoviti, da se v primeru zakonitega razkritja sprejmejo ustrezni ukrepi za ohranitev njihove zaupnosti.

Zakoniti dostop mora v celoti spoštovati načeli nujnosti in sorazmernosti, po potrebi pa ga mora odobriti sodišče ali neodvisni organ. Dostop do podatkov je treba uravnotežiti z zanesljivimi ukrepi za varstvo zasebnosti in kibernetsko varnost (npr. šifriranje, požarni zidovi ter protivirusna programska oprema in programska oprema, namenjena varovanju pred zlonamerno programsko opremo). Zagotavljanje, da je dostop do podatkov omejen tako, da je dovoljen samo za namene preiskave, prispeva k varovanju zasebnosti posameznih uporabnikov.

---

11 Projekt SIRIUS.

12 *Commission Impact Assessment on the Proposals for an e-Evidence Regulation and an e-Evidence Directive* (Ocena učinka predloga uredbe o elektronskih dokazih in direktive o elektronskih dokazih, ki jo je opravila Komisija) (17. april 2018).

13 MLA - Council of Europe standards - PC-OC (coe.int).

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

Čeprav je zakonit dostop do podatkov za namene odkrivanja in preiskovanja v središču zagotavljanja najvišje možne ravni varnosti naših državljanov in državljank, to ne sme biti na račun temeljnih pravic ali kibernetske varnosti sistemov in proizvodov. Glede zaščite osebne integritete in varnosti ljudi na eni strani ter njihovimi pravicami na drugi strani se ne sme sklepati kompromisov; treba je najti ravnovesje, ki zagotavlja, da ena ne posega v drugo. Dolžnost tako EU kot držav članic je zagotoviti, da lahko državljani in državljanke uživajo visoko raven varstva svojih temeljnih pravic in da se v vsakdanjem življenju počutijo varne. Tehnološki razvoj ne sme ustvariti varnih zatočišč za storilce kaznivih dejanj: kadar obstaja razumen sum, da je bilo ali bo storjeno kaznivo dejanje, morajo imeti organi odkrivanja in pregona dostop do orodij, ki jim omogočajo dostop do zadevnih podatkov.

V Evropski konvenciji o človekovih pravicah, nacionalnih ustavah in Listini EU o temeljnih pravicah je priznana pravica vsakega posameznika do zasebnega življenja in priznanje, da to vključuje posameznikovo komunikacijo. Listina EU o temeljnih pravicah določa tudi pravico do varstva podatkov. Pravici do zasebnosti in varstva osebnih podatkov nista absolutni pravici, temveč ju je treba upoštevati glede na njuno vlogo v družbi[15]. Javni organi ne smejo posegati v uveljavljanje teh pravic, ***razen če je tako poseganje skladno z zakonom, spoštuje bistvo pravic ter je nujno potrebno in sorazmerno v demokratični družbi***. Pod temi pogoji se lahko omejita pravici do zasebnosti in varstva osebnih podatkov, tudi v interesu nacionalne in javne varnosti ter za preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj.

Visoka stopnja prevzemanja odgovornosti je ključnega pomena. V naših demokratičnih družbah so zakonodajalci odgovorni za vzpostavitev pogojev za takšno prevzemanje odgovornosti ob zagotavljanju visoke ravni zasebnosti in varnosti. ***Zasebnost in varnost se med seboj ne izključujeta***.

Rešitve za zagotovitev zakonitega dostopa v utemeljenih primerih je treba osnovati v sodelovanju z vsemi ustreznimi deležniki, vključno z industrijo, da bi spodbudili inovacije in močno kibernetsko varnost. ***Te rešitve morajo biti oblikovane ob ustreznem upoštevanju vseh ustreznih potreb in zahtev ter jih ni mogoče prepustiti izključno presoji tehnoloških podjetij***.

---

[15] Sodba z dne 30. aprila 2024, *La Quadrature du Net in drugi*, Zadeva C-470/21, EU:C:2024:370, točka 70.

Preden se lahko sprejmejo nadaljnji ukrepi, je treba opraviti tehnične ocene, da bi odpravili pomisleke nekaterih strokovnjakov za kibernetsko varnost glede kompleksnosti zagotavljanja zakonitega dostopa ob hkratnem ohranjanju močne kibernetske varnosti. ***Kibernetska varnost proizvodov in storitev ter zakonit dostop do podatkov izhajata iz pravnih obveznosti in morata soobstajati***. Zahteve glede zakonitega dostopa je treba izvajati na podlagi jasnih standardov, razvitih s strani vseh ustreznih deležnikov (vključno s predstavniki industrije, strokovnjaki za varstvo podatkov in kibernetsko varnost ter strokovnimi delavci na področju odkrivanja in pregona), ki odražajo ustrezne pravne zahteve, in na podlagi ustrezno ocenjenih možnih rešitev, s čimer se zagotovi, da zakonit dostop ne ogroža varnosti proizvodov in storitev.

Številna podjetja in ponudniki storitev zaradi pravne negotovosti, povezane s prostovoljnimi ukrepi, in tveganja morebitnega nasprotovanja njihovih uporabnikov ***oklevajo pri sodelovanju z organi odkrivanja in pregona***. Ta nenaklonjenost ovira preiskave. Poleg tega zaradi vtisa, da dajejo uporabniki prednost zasebnosti pred javno varnostjo, akterji iz industrije morda niso naklonjeni temu, da bi odprli kanale za komuniciranje z organi odkrivanja in pregona ter vzpostavili prilagojene mehanizme, ki zagotavljajo zakonit dostop. Za reševanje tega vprašanja je potreben jasen pravni okvir za zakonit dostop do podatkov. V obstoječi zakonodaji obstajajo precejšnje ovire, ki otežujejo zagotavljanje takega dostopa, zlasti na prostovoljni podlagi.

Sodelovanje med podjetji in organi odkrivanja in pregona je neustrezno in pomanjkljivo ter ga je treba dopolniti z jasnimi pravili. ***Brez jasnih in izvršljivih pravnih obveznosti podjetja pogosto ne morejo pomagati organom odkrivanja in pregona pri dostopu do podatkov***.

Ker ni učinkovitih rešitev za zagotovitev zakonitega dostopa, ***se rešitve, ki temeljijo na ranljivosti, pogosto obravnavajo kot edina možnost***.

Kadar se prestreženi podatki (in po možnosti drugi podatki, pridobljeni iz naprave) obdelujejo z orodji, ki jih oblikujejo zasebna podjetja, ne glede na zagotovila, ki jih ta podjetja dajo, nacionalni organi nimajo dejanskega vpogleda v to, kateri podatki se pregledujejo in kako, ter se morajo zanašati izključno na potrdila, ki jih izda vlada države, v kateri imajo sedež podjetja, ki zagotavljajo storitev prestrezanja. Potreba, da ranljivost ostane tajna, zato da se ohrani učinkovitost orodij/storitev, to težavo še zaostruje. To vprašanje je zlasti zaskrbljujoče, kadar ima ponudnik sedež zunaj EU.

In nenazadnje, zasebna podjetja, ki zagotavljajo storitve na področju vsiljivih preiskovalnih tehnik, imajo interes, da čim bolj povečajo svoje dobičke, zato se lahko odločijo, da svoja orodja prodajo režimom, ki niso demokratični (kot je bilo v primeru škandala Hacking Team[16]).

Druga možnost je, da ***organi odkrivanja in pregona*** zaradi izzivov pri dostopu do podatkov ***sprejmejo bolj vsiljive preiskovalne ukrepe***. V takih primerih so organi odkrivanja in pregona prisiljeni uporabiti ukrepe, ki predstavljajo večji vdor v zasebnost, kot so fizični nadzor namesto dostopa do geolokacijskih podatkov in hišne preiskave namesto zakonitega prestrezanja.

Nezmožnost organov odkrivanja in pregona, da dostopajo do podatkov, lahko povzroči znatno izgubo zaupanja javnosti v pravosodni sistem. Če so preiskave zapoznele ali kompromitirane, lahko državljani in državljanke menijo, da je sistem neučinkovit. To spodkopavanje zaupanja lahko ogrozi javni red in mir ter zmanjša pripravljenost javnosti, da prispeva k prizadevanjem na področju odkrivanja in pregona.

Zakonit dostop organom odkrivanja in pregona na koncu ***omogoča zbiranje dokazov, da bi žrtvam zagotovili pravico in jih zaščitili pred nadaljnjo škodo***. Podatki so lahko pomembni za odkrivanje in pregon vseh vrst kaznivih dejanj, tako na spletu kot zunaj njega. Posamezniki so lahko izpostavljeni hudim oblikam kibernetskega nadlegovanja, kraji identitete, goljufiji itd., ki so posledica kriminalne zlorabe digitalnih tehnologij, storitev in komunikacij. Te izkušnje imajo lahko hude čustvene in duševne posledice za žrtve ter zaostrujejo že obstoječe neenakosti in ranljivosti.

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

V vsaki kazenski preiskavi so potrebni dokazi za identifikacijo storilca ali za dokazovanje njegove odgovornosti pred sodnikom. Pomagajo lahko tudi razbremeniti državljana, če je bil neupravičeno obtožen. Če preiskovalci in tožilci ne morejo dostopati do potrebnih informacij, morda ne bodo mogli nadaljevati svojih preiskav in identificirati storilca, kar žrtvi povzroča dodatne stiske in finančne izgube ter spodkopava zaupanje v pravosodni sistem. Zgolj tradicionalni fizični dokazi ne zadostujejo vedno za vzpostavitev povezav in iskanje sledi. ***Organi odkrivanja in pregona ter sodstvo morajo biti prilagojeni digitalni dobi. Le tako bodo lahko v celoti zaščitili našo družbo in gospodarstvo*** pred vse večjimi grožnjami, ki izhajajo iz kibernetskih napadov in hibridnih groženj ter dejavnosti organiziranega kriminala.

Če organi odkrivanja in pregona ne morejo učinkovito dostopati do podatkov, je njihova sposobnost, da zagotavljajo varnost in ujamejo storilce najhujših kaznivih dejanj, znatno oslabljena. ***Organom odkrivanja in pregona bi bilo treba zagotoviti zakonit in strogo nadzorovan učinkovit dostop do podatkov z zanesljivimi jamstvi za varstvo zasebnosti in kibernetsko varnost, da bi preprečili, odkrivali, preiskovali in preganjali kazniva dejanja; tako bi jim omogočili, da zagotovijo varnost ter državljanom in državljankam EU omogočijo varno življenje in sodno varstvo v primeru kaznivih dejanj, storjenih zoper njih***.

Poglavje I: Digitalna forenzika

KAKŠNE SO TEŽAVE?

Digitalna forenzika se nanaša na zbiranje, analizo in hrambo digitalnih dokazov (tako komunikacijskih metapodatkov kot podatkov o vsebini), shranjenih v kateri koli digitalni obliki v elektronski napravi, vključno z informacijami iz trdih diskov računalnika, mobilnih telefonov, pametnih naprav, navigacijskih sistemov vozil in elektronskih vratnih ključavnic kot tudi podatki, shranjeni v oblaku in drugih digitalnih napravah.

Ker je dostop do komunikacijskih podatkov vse težji, postaja pridobivanje informacij iz zaseženih naprav (ali omrežij povezanih naprav) vse pomembnejše za kazenske preiskave. Z dostopom do podatkov v mirovanju v napravah so lahko organom odkrivanja in pregona zagotovljene kakovostnejše informacije, npr. o identiteti članov organiziranih kriminalnih združb, kot druge tehnike, kot je zakonito prestrezanje. Nekateri strokovnjaki trdijo, da ni mogoče vnaprej vedeti, kateri podatki so pomembni za posamezno preiskavo: celo tiste informacije, ki se morda na začetku zdijo nepomembne, se lahko v nadaljevanju preiskave izkažejo za bistvene. Dostop do vseh podatkov v napravi je lahko pomemben tudi za potrditev nedolžnosti osumljenca in zaščito pravic tožene stranke[17]. Poleg tega morajo biti preiskovalne metode vedno sorazmerne.

Kronično **pomanjkanje virov** in zmogljivosti, s katerim se na tem področju soočajo organi odkrivanja in pregona, je še resnejše zaradi uvajanje novih tehnologij (npr. novih vrst naprav, interneta stvari in računalništva v oblaku), ki zahtevajo nove spretnosti ter orodja. Čeprav je v agencijah in institucijah držav članic že na voljo veliko strokovnega znanja na področju digitalne forenzike, je to znanje razpršeno in ni jasnih mehanizmov za izmenjavo in razširjanje zmogljivosti, kar pomeni, da ostaja omejeno v ločenih silosih.

[17] Strokovnjak je omenil primer, v katerem je bila analiza dejavnosti naprave ključna pri dokazovanju, da osumljenec ni mogel biti vpleten v umor.

Pomanjkanje **primerljivih kapacitet digitalnih forenzičnih laboratorijev** ter splošno pomanjkanje **standardiziranih forenzičnih postopkov** in mehanizmov, ki bi omogočali **priznavanje spretnosti in strokovnega znanja strokovnjakov za digitalno forenziko**, lahko ovira čezmejno sodelovanje.

Strokovnjaki skupine na visoki ravni so jasno povedali, da je privzeto **šifriranje** podatkov v napravah glavni izziv, s katerim se srečujejo organi odkrivanja in pregona. Ti ne morejo dostopati do podatkov, shranjenih v nekaterih vrstah sodobnih naprav, ki so zaščitene s kriptoprocesorji[18] ali z močnimi šifrirnimi algoritmi in zapletenimi gesli, niti z uporabo najmočnejših platform za dešifriranje. Šifriranje ter drugi ukrepi na področju kibernetske varnosti in zasebnosti so potrebni za zaščito informacijskih sistemov ter komunikacij in osebnih podatkov, vendar ti ukrepi – zlasti vse večja uporaba šifriranja – zmanjšujejo zmožnost organov odkrivanja in pregona za zbiranje dokazov.

Države članice imajo na tem področju omejeno **strokovno znanje in zmogljivosti**; skoraj vse navajajo pomanjkanje tehničnih rešitev za izpolnitev potreb strokovnih delavcev in velika večina meni, da so njihove spretnosti in finančna sredstva nezadostni. Sposobnosti organov odkrivanja in pregona za dešifriranje informacij, shranjenih v zaseženih napravah, se med državami članicami zelo razlikujejo, pri čemer je njihova stopnja uspešnosti v nekaterih primerih 15- do 20-odstotna, včasih pa so uspešni v več kot dveh tretjinah primerov. Tam, kjer so zmogljivosti, so običajno neučinkoviti pri dešifriranju podatkov, ki so bili zavarovani z močnimi gesli, in datotek, zaščitenih v posebnih šifriranih vsebnikih. Tudi v primerih, ko je dešifriranje uspešno, se pogosto ne izvede pravočasno. Oprema za dešifriranje je draga in visoko specializirana, strojna oprema pa porablja zmogljivosti.

Večina oddelkov za digitalno forenziko v organih odkrivanja in pregona se pri dostopu do podatkov na napravah zanaša na komercialne rešitve, kar ustvarja dodatne izzive, saj te rešitve težko sledijo tehnološkemu razvoju in hitro postanejo zastarele, visoki stroški licenc znatno zmanjšujejo število pooblaščenih uporabnikov, pogosto so razvite zunaj Evrope in so lahko slabo prilagojene potrebam organov odkrivanja in pregona iz EU ali morda ne izpolnjujejo standardov EU za prevzemanje odgovornosti na področju digitalne forenzike.

[18] Kot je varnostni čip T2 na novejših prenosnih računalnikih Apple.

Organi odkrivanja in pregona pogosto nimajo druge možnosti, kot da izkoristijo **ranljivosti** za pridobitev dostopa do ključev za dešifriranje na napravah. Vendar je treba preiskovalne tehnike, ki temeljijo na tem pristopu, uskladiti s ciljem zagotavljanja varnejše strojne in programske opreme, kot je določeno v aktu o kibernetski odpornosti; sheme za obvladovanje in razkrivanje ranljivosti bi ublažile nenamerne posledice takih tehnik. Strokovnjaki so preučili alternativne rešitve, kot je, da se osumljencem naloži obveznost, da preiskovalnim organom predajo elemente, potrebne za dostop v ustreznih napravah (npr. gesla). Nacionalni pravni okviri, ki se uporabljajo v takih primerih, se zelo razlikujejo, in le tri države članice so navedle, da imajo posebne zakonodajne določbe, ki osumljenca obvezujejo, da zagotovi dostop do šifriranih ključev ali dešifriranih podatkov[19]. Nekatere države članice osumljencem nalagajo obveznosti, da dajo na voljo nekatere biometrične podatke (npr. prstne odtise), s čimer omogočijo dostop do naprave; v drugih primerih morajo osumljenci razkriti svoje geslo. Na splošno to ostaja področje, ki ga je treba dodatno oceniti.

Nekatere zgoraj opredeljene težave se lahko ublažijo z **združevanjem kapacitet držav članic** ob upoštevanju njihove izključne pristojnosti na področju nacionalne varnosti. Vendar se ta rešitev še naprej pušča ob strani, včasih zaradi pravnih omejitev (v sedmih državah članicah obstajajo omejitve glede izmenjave orodij, pet od njih pa je prepoznalo omejitve glede uporabe orodij, ki bi si jih izmenjevale z drugimi državami članicami), na splošno pa zaradi pomanjkanja vzpostavljenih mehanizmov za izmenjavo orodij ali skupno nabavo licenc.

V preteklosti so imeli organi odkrivanja in pregona proste **kanale za komuniciranje s proizvajalci, ponudniki in dobavitelji**. To jim je omogočilo, da so vzpostavili protokole o sodelovanju, ki so jim omogočili boljše razumevanje na novo uvedenega tehnološkega razvoja in posledično olajšali ukrepe kazenskega pregona, hkrati pa je zagotavljalo kibernetsko varnost. Glede na hitrost uvajanja novih tehnologij in vstopanja novih podjetij na trg so se razmere spremenile in sodelovanje z industrijo ni več prisotno.

S sprejetjem ustreznih standardov bi omogočili, da bi se lahko protokoli za proizvode in tehnična arhitektura oblikovali ob upoštevanju pomislekov in tehničnih zahtev organov odkrivanja in pregona že v zgodnji fazi. Vendar **sodelovanje organov odkrivanja in pregona v ustreznih organih za standardizacijo** ni zadostno, kar vpliva na njihovo zmožnost učinkovitega sodelovanja pri razvoju prihodnjih tehnoloških standardov.

---

[19] Eurojust Cybercrime Judicial Monitor (Issue 4), december 2018, str. 34, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_cybercime_judicial_monitor_4_2018.pdf.

MOŽNE REŠITVE

I. Povečanje in racionalizacija prizadevanj za okrepitev zmogljivosti na področju orodij digitalne forenzike

Države članice že imajo strokovno znanje in zmogljivost za izvajanje digitalne forenzike; vendar lahko ustrezne nacionalne institucije in organi z izmenjavo in združevanjem svojih tehničnih rešitev izkoristijo izkušnje drugih agencij in dosežejo znatno ekonomijo obsega, s tem pa zmanjšajo potrebna finančna sredstva. Države članice lahko v ta namen nadalje preučijo rešitve na področju orodij digitalne forenzike ter usposabljanja in razvoja spretnosti.

Sklop priporočil 1

Za okrepitev sodelovanja in skupne zmogljivosti na področju digitalne forenzike strokovnjaki priporočajo:

1. *evidentiranje in povezovanje obstoječih mrež za digitalno forenziko ter ustanovitev sekretariata [priporočilo 1];*
2. *boljši dostop do znanja in razširjanje znanja med strokovnjaki [priporočilo 1];*
3. *razmislek o mehanizmih za združevanje znanja [priporočilo 2];*
4. *povečanje financiranja za raziskave in razvoj z jasnimi rezultati [priporočilo 4];*
5. *promoviranje Europolovega odložišča orodij kot osrednjega vozlišča za izmenjavo orodij [priporočilo 4];*
6. *olajšanje izmenjave rešitev in orodij digitalne forenzike med državami članicami v okolju zaupanja (ob upoštevanju nacionalnih pravil) [priporočilo 2];*
7. *razvoj mehanizma na ravni EU za skupni nakup licenc za orodja digitalne forenzike, da bi si jih izmenjevali med državami članicami [priporočilo 3];*
8. *spodbujanje sodelovanja s proizvajalci in razvijalci orodij digitalne forenzike za racionalizacijo strukture in formata podatkov, ki jih organi odkrivanja in pregona pridobijo z uporabo teh orodij, po možnosti v skladu z dogovorjenimi standardi [priporočilo 12];*
9. *vzpostavitev mehanizma/sheme za ocenjevanje in – kadar je ustrezno – certificiranje komercialno dostopnih orodij digitalne forenzike na ravni EU, ob upoštevanju morebitnih negativnih učinkov na preiskovanje in pregon, kot je dodajanje nepotrebnega bremena [priporočilo 5].*

Več organizacij, mrež, združenj in projektov združuje strokovne delavce in različne kategorije partnerjev za povečanje zmogljivosti organov EU za odkrivanje in pregon na področju digitalnih preiskav:

- *Evropska mreža inštitutov za forenzične znanosti* (ENFSI)[20] je glavna evropska mreža, ki med drugim zajema digitalno forenziko; ima 73 članov iz 39 držav, ti člani pa sodelujejo v delovnih skupinah, npr. za forenzično informacijsko tehnologijo in digitalno tehnologijo preslikovanja;

- *Evropsko združenje za razvoj tehnologij za boj proti kibernetski kriminaliteti* (EACTDA)[21] združuje organe odkrivanja in pregona, raziskovalne in tehnološke organizacije, industrijske partnerje in akademske kroge iz številnih držav članic, da bi se olajšala uporaba rezultatov varnostnih raziskovalnih projektov ter zagotovila v celoti preizkušena programska orodja, pripravljena za delovanje, brez stroškov licenc, in dostop do izvorne kode za organizacije EU za javno varnost;

- Evropski urad za boj proti goljufijam (OLAF) od leta 2007 nacionalnim organom odkrivanja in pregona nudi posebno usposabljanje za digitalne forenzike in analitike (*Digital Forensics and Analysts Training (DFAT)*), s posebnim poudarkom na goljufijah, korupciji in drugih nezakonitih dejavnostih, ki škodijo finančnim interesom Evropske unije; vsako leto se usposablja približno 175 strokovnjakov za digitalno forenziko, s čimer se oblikuje trdna skupnost na tem področju kriminala;

- drugi projekti, kot sta *CYCLOPES*[22] in *I-LEAD*[23], niso stalne strukture, kljub temu pa združujejo strokovnjake in zagotavljajo ustrezno analizo vrzeli.

Žal pa obstoječe stalne mreže ne združujejo enot za digitalno forenziko organov odkrivanja in pregona iz EU ter organizacij, ki z njimi tesno sodelujejo (npr. Center za kibernetsko varnost in preiskovanje kibernetske kriminalitete na Univerzi v Dublinu (UCD) ali litovski center odličnosti za kibernetsko kriminaliteto za usposabljanje, raziskave in izobraževanje).

---

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/en.

Europol (zlasti Europolov inovacijski laboratorij skupaj z Evropskim centrom za boj proti kibernetski kriminaliteti) do neke mere že sodeluje z vsemi zgoraj navedenimi mrežami in je dokazal, da je sposoben združiti znatno število strokovnih delavcev, npr. v obliki osrednjih skupin Evropskega potrjevalnega odbora za inovacije (EuCB), ki organizira *forum strokovnjakov za forenziko*[24] ter vzpostavlja stike med strokovnjaki in ustreznimi partnerji, npr. prek *foruma za kibernetske inovacije*[25].

Europol zagotavlja tudi pripravljeno infrastrukturo, tj. Europolovo platformo za strokovnjake (EPE), ki omogoča sodelovanje in izmenjavo znanja med strokovnjaki o posebnih temah.

Ključni ukrep: strokovnjaki skupine na visoki ravni pozivajo k okrepitvi zmogljivosti Europola na področju digitalne forenzike

Akterji: Europol, Evropska komisija, države članice	*Časovni okvir: 2028*	*Proračun: o njem se bo razpravljalo pozneje, odvisno od izida tekočih razprav o naslednjem večletnem finančnem okviru.*

- Strokovnjaki skupine na visoki ravni v okviru znatne okrepitve Europola, napovedane v političnih usmeritvah Evropske komisije za obdobje 2024–2029, pozivajo k povečanju zmogljivosti Europola, da bi državam članicam pomagali pri **združevanju virov, znanja in strokovnega znanja ter izmenjavi rešitev in orodij digitalne forenzike** v okolju zaupanja. Izključiti bi bilo treba nacionalna orodja in orodja, ki se uporabljajo in/ali razvijajo izključno za namene nacionalne varnosti.
- Strokovnjaki skupine na visoki ravni pozivajo Europol, naj **prevzame vlogo vozlišča** za dostop do ustreznega operativnega strokovnega znanja na tem področju in po možnosti **vzpostavi projekt, podoben projektu SIRIUS, na področju digitalne forenzike**, da bi olajšali izmenjavo znanja in izkušenj ter najboljših praks.
- Strokovnjaki skupine na visoki ravni pozivajo Europol, naj okrepi svojo vlogo pri **usklajevanju organizacij in projektov**, ki prispevajo k ustvarjanju znanja na področju digitalne forenzike na ravni EU, pod vodstvom Evropskega potrjevalnega odbora in ob upoštevanju prispevka drugih ustreznih agencij.

[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.

Obstaja več finančnih instrumentov za podporo raziskavam in razvoju orodij na področju digitalne forenzike.

- Evropska komisija v okviru *Sklada za notranjo varnost (ISF)* redno objavlja javne razpise za zbiranje predlogov na področju kibernetske kriminalitete in digitalnih preiskav. Kljub precej omejenemu proračunu (v sedanjem večletnem finančnem okviru je bilo tem ukrepom dodeljenih približno 15 milijonov EUR), so se projekti, izbrani v okviru teh razpisov, izkazali za ciljno usmerjene in uspešne.

  Približno dve tretjini proračuna ISF se dodelita v okviru deljenega upravljanja, pri čemer države članice izberejo, katere projekte bodo financirale, in prevzamejo odgovornost za vsakodnevno upravljanje. Zato imajo države članice možnost, da podprejo projekte na področju digitalne forenzike v okviru svojih nacionalnih programov.

- *Cilj sklopa Obzorje Evropa za civilno varnost za družbo*, ki ima skupni proračun v višini 1 596 milijard EUR za obdobje sedmih let, je spodbujati varne evropske družbe v kontekstu sprememb brez primere ter vse večje svetovne soodvisnosti in groženj, hkrati pa krepiti evropsko kulturo svobode in pravice. V zadnjih letih je podprl več pomembnih raziskovalnih projektov, kot sta FORMOBILE[26] in EXFILES[27], ki so pomagali strokovnim delavcem pri njihovih vsakodnevnih dejavnostih.

- *Program Digitalna Evropa* je glavni instrument financiranja EU, namenjen krepitvi digitalne infrastrukture EU z različnimi pobudami. Program, katerega skupni proračun za obdobje 2021–2027 znaša 7,5 milijarde EUR, namenja znatna sredstva zlasti kibernetski varnosti in zajema tudi digitalno forenziko.

[26] FORMOBILE – *From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices* (Od mobilnih telefonov do sodišča – celovita veriga forenzičnih preiskav, ciljno usmerjena na mobilne naprave): https://cordis.europa.eu/project/id/832800.

[27] EXFILES – *Europe fights against crime and terrorism* (Evropa se bori proti kriminalu in terorizmu): https://exfiles.eu/.

Europolova platforma za dešifriranje je vodilni projekt v okviru ISF. Ta platforma, ki jo je Europol vzpostavil leta 2020 v tesnem sodelovanju s Skupnim raziskovalnim središčem Evropske komisije, podpira nacionalne organe odkrivanja in pregona z dešifriranjem njihovih digitalnih dokazov. Njen cilj je organom odkrivanja in pregona zagotoviti trajnostno rešitev za dostop do tehničnih virov in virov IT, ki jih potrebujejo. V zadnjih nekaj letih se je platforma uporabljala v številnih večjih primerih in je v skoraj polovici primerov prinesla ključne rezultate, kar je privedlo do več zgodb o uspehu. Leta 2023 je platforma uspešno podprla 37 preiskav (v zvezi s spolnim izkoriščanjem otrok, terorizmom, kibernetsko kriminaliteto, organiziranim kriminalom, tihotapljenjem drog in goljufijami ter odmevnimi finančnimi preiskavami), vključno s prednostnimi preiskavami, kot so preiskave v zvezi z SkyECC in Encrochat. Platforma je postala bistveno orodje organov odkrivanja in pregona, vendar ne zadostuje za obravnavo vseh vprašanj, povezanih z dešifriranjem, s katerimi se srečujejo organi EU.

Ključni ukrep: strokovnjaki skupine na visoki ravni pozivajo k nadaljnjemu razvoju in spodbujanju uporabe zmogljivosti EU za dešifriranje

Akterja: Evropska komisija, Europol	*Časovni okvir: 2028*	*Proračun: določijo ga države članice (npr. v okviru nacionalnih programov ISF).*

- Strokovnjaki skupine na visoki ravni pozivajo Evropsko komisijo, naj podpre zmožnost nacionalnih organov, da zbirajo visokokakovostne spremne informacije, pri čemer naj spoštuje izključno pristojnost držav članic na področju nacionalne varnosti, in sicer z namenskim financiranjem (npr. v okviru nacionalnih programov ISF) in izmenjavo najboljših praks, da bi lahko prispevali k povečanju učinkovitosti Europolove platforme za dešifriranje.
- Strokovnjaki skupine na visoki ravni pozivajo Evropsko komisijo, naj podpre Europolove naložbe v vzdrževanje tehničnih zmogljivosti in krepitev zmogljivosti za dešifriranje, pri čemer naj sledi tehnološkemu razvoju in upošteva raziskave na področju kvantne kriptografije.
- Strokovnjaki skupine na visoki ravni pozivajo Evropsko komisijo, naj finančno podpre države članice pri razvoju **nacionalnih in regionalnih zmogljivosti za dešifriranje**, da bi dopolnili prizadevanja Europola.

Obstoječi programi financiranja EU nudijo znatno podporo organom odkrivanja in pregona. Nadaljnje izboljšanje teh priložnosti bi povečalo njihov prispevek k povečanju zmogljivosti oddelkov za digitalno forenziko ter zmanjšanju vezanosti na ponudnika in odvisnosti organov odkrivanja in pregona od orodij „črne skrinjice“ (tj. orodij, ki obdelujejo podatke, ne da bi zaupanja vredni organi lahko preverili, kako delujejo), razvitih zunaj EU.

Koraki v ciklu dejavnosti (raziskave, razvoj, uvajanje), ki bi jih bilo treba storiti, da bi zagotovili oprijemljivo dodano vrednost organov odkrivanja in pregona, so podprti z različnimi shemami. Da bi v celoti izkoristili priložnosti, ki so na voljo na ravni EU, bi se morali nacionalne uprave, organi odkrivanja in pregona ter strokovni delavci zavedati funkcij in ciljev vsakega posameznega programa in mehanizma.

Program Obzorje Evropa je podprl različne uspešne projekte z dejavnim sodelovanjem strokovnjakov na področju odkrivanja in pregona. Ker pa je to raziskovalni program, bi bilo treba prilagoditi pričakovanja glede pripravljenosti razvitih orodij za operativno uporabo.

Namen projekta *Tools4LEAs*, ki ga financira ISF in upravlja EACTDA, je olajšati uvajanje rezultatov varnostnih raziskovalnih projektov ter zagotoviti v celoti preizkušena programska orodja, pripravljena za delovanje, brez stroškov licenc, in dostop do izvorne kode za organizacije EU za javno varnost. Ta projekt je najprimernejši za nadgradnjo rezultatov raziskovalnih projektov za pomoč pri zagotavljanju operativnih orodij. Pri njem sodeluje Europol in skupaj z vsemi končnimi uporabniki, ki so člani EACTDA, usmerja njegovo delo.

Evropski potrjevalni odbor je ustanovil več kot 15 osrednjih skupin držav članic za skupno izkoriščanje novih tehnologij in soustvarjanje inovativnih orodij. Države članice so osrednje skupine Evropskega potrjevalnega odbora izkoristile za usklajevanje dela razvoja inovativnih orodij, ki se financirajo z nepovratnimi sredstvi ISF, kot so MARIT-D, ProfID in spletni pajki. Osrednje skupine so idealen okvir, v katerem lahko države članice usklajujejo soustvarjanje digitalnih preiskovalnih orodij.

Evropska komisija s ciljno usmerjenimi *razpisi za zbiranje predlogov v okviru ISF* za notranjo varnost še naprej financira projekte, ki so znatno prispevali k uspehu operativnih ukrepov. V okviru projekta CERBERUS so bile npr. ugotovljene ranljivosti v sistemu EncroChat, kar je francoski žandarmeriji ob podpori nizozemskega nacionalnega forenzičnega inštituta in UCD omogočilo, da so sistem ukinili. Projekt FREETOOL[28], ki ga je vodil Center za kibernetsko varnost in preiskovanje kibernetske kriminalitete (UCD), je omogočil razvoj vrste brezplačnih orodij za preiskovanje kibernetske kriminalitete[29], prilagojenih izpolnjevanju posebnih zahtev organov odkrivanja in pregona pri digitalnih preiskavah in analizah. Ta orodja so bila razvita v partnerstvu z organi odkrivanja in pregona in so prosto dostopna skupnosti organov odkrivanja in pregona. 3 000 uporabnikov iz več kot 100 organov odkrivanja in pregona iz več deset jurisdikcij se je prijavilo za dostop do orodij, ki jih je na ravni organizacij sprejelo tudi več organov odkrivanja in pregona in se uporabljajo v odmevnih preiskavah. *Program za pravosodje* zajema tudi pravosodno sodelovanje v kazenskih zadevah in bi lahko spodbujal čezmejno sodelovanje pri uporabi digitalnih preiskovalnih orodij.

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

[29] Orodja zajemajo različne faze preiskave: predhodno zbiranje odprtokodnih podatkov (OSINT), forenzično preiskavo podatkov v živo, analizo spomina, naknadno zbiranje odprtokodnih podatkov in ohranjanje spletnih virov, avtomatizirano pridobivanje datotek/artefaktov, forenzično poročanje, obdelavo medijev in geolokacijo.

Europolovo odložišče orodij (ETR) se je od svoje ustanovitve dalje razvilo tako, da zajema več kot 40 naprednih orodij, ki evropskim organom odkrivanja in pregona zagotavljajo neposreden dostop do najsodobnejših tehnologij. Vsak mesec so dodana nova orodja, odložišče pa je postalo glavni vir za strokovnjake EU, ki iščejo programsko opremo za pomoč pri svojih preiskavah. ETR ima trenutno več kot 2 700 uporabnikov, izvedenih pa je bilo 7 800 prenosov njegovih različnih orodij. Nacionalne preiskovalne enote orodja pogosto uporabljajo za podporo številnim operacijam, tudi na različnih področjih kriminala, kot so trgovina z ljudmi, huda kazniva dejanja in organizirani kriminal, kibernetska kriminaliteta ter spolna zloraba otrok na spletu. ETR ponuja neposredno možnost izkoriščanja projektov, ki jih financira EU ter ponujajo konkretne in dobre rezultate ter katerih ustvarjalci so pripravljeni izdati dovoljenje Europolu, da jih deli z vsemi evropskimi organi odkrivanja in pregona. Izbrani partnerji iz projektov INSPECTr, Tools4LEAs in FORMOBILE so že uporabljali skupna orodja preko odložišča ETR. Europol se usklajuje z Agencijo EU za usposabljanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (CEPOL), da bi uporabnikom ponudili usposabljanje o orodjih ETR.

Poleg tega bi moral program Digitalna Evropa vse bolj spodbujati sinergije in dopolnjevanje med področji kibernetske varnosti in boja proti kibernetski kriminaliteti, ki se pogosto opirata na ista orodja in tehnike digitalne forenzike.

Trenutno ni mehanizma, ki bi skrbel, da orodja digitalne forenzike izpolnjujejo standarde odgovornosti in forenzične standarde v EU. Tak mehanizem bi moral zagotavljati tehnično oceno, s katero bi zagotovili, da se v celoti spoštujejo sorazmernost (tj. zagotovitev dokazov, da orodje omogoča dostop do ciljno usmerjenih informacij, s čimer se analiza omeji le na to, kar je potrebno), preglednost in pravice tožene stranke (tj. dokazovanje, da orodje pridobiva verodostojne in točne informacije, kar je zagotovilo za zagovornike in neodvisne forenzične strokovnjake, ki pričajo na sodišču) ter druge zakonske zahteve (npr. skladnost z aktom o umetni inteligenci). To bi povečalo zanesljivost dokazov na sodišču – tako na nacionalni kot na čezmejni ravni – s čimer bi se okrepilo čezmejno sodelovanje.

Ključni ukrep: strokovnjaki skupine na visoki ravni pozivajo k ciljno usmerjenemu financiranju projektov za raziskovanje, razvoj in uvajanje orodij digitalne forenzike

Akterji: Evropska komisija, Europol, države članice, EACTDA, ENFSI	*Časovni okvir: od leta 2024 naprej*	*Proračun:*

- Strokovnjaki skupine na visoki ravni pozivajo države članice, **naj projekte na področju digitalne forenzike, ki se financirajo v okviru njihovih nacionalnih programov ISF, vključijo v obstoječe mehanizme** (npr. EMPACT) ali mreže (npr. ECTEG, EACTDA), da bi izkoristili izkušnje strokovnjakov iz drugih držav članic ter hkrati spodbujali razširjanje in uvajanje rezultatov s strani drugih organov odkrivanja in pregona.

- Strokovnjaki skupine na visoki ravni pozdravljajo trenutna prizadevanja Evropske komisije za podporo raziskovanju, razvoju in uporabi orodij digitalne forenzike s financiranjem v okviru ustreznih finančnih programov: **Obzorje Evropa**, **Digitalna Evropa** in **ISF**. Evropska komisija bo glede na razpoložljiva sredstva vsaki dve leti objavila **javne razpise za zbiranje predlogov** na področju kibernetske kriminalitete in digitalnih preiskav v okviru ISF.

- Strokovnjaki skupine na visoki ravni pozdravljajo stalna prizadevanja Evropske komisije za financiranje **EACTDA** v okviru ISF, da bi EACTDA lahko zagotovila v celoti preizkušena programska orodja, pripravljena za delovanje, brez stroškov licenc, in dostop do izvorne kode za organizacije EU za javno varnost.

- Strokovnjaki skupine na visoki ravni pozdravljajo stalna prizadevanja Evropske komisije za spodbujanje uporabe **Europolovega odložišča orodij** kot osrednjega vozlišča za razširjanje orodij v okviru možnosti financiranja; poleg tega spodbujajo **Europolov inovacijski laboratorij**, naj si še naprej prizadeva, da bi organom EU za odkrivanje in pregon zagotovili zaupanja vredna, varna, brezplačna, enostavna in skalabilna preiskovalna orodja.

- Strokovnjaki skupine na visoki ravni pozivajo k nadaljnjemu razmisleku o **vzpostavitvi shem za ocenjevanje in po potrebi certificiranje** komercialno dostopnih orodij digitalne forenzike na ravni EU. To se lahko npr. izvede **v okviru evropske mreže inštitutov za forenzične znanosti**.

Licence za orodja digitalne forenzike so drage in si jih nekateri organi odkrivanja in pregona včasih ne morejo privoščiti. Skupno javno naročanje licenc, ki se nato lahko razdelijo med organe v različnih državah članicah, lahko omogoči pogajanja o nižjih cenah.

V sklopu projekta *iProcureNet*[30], ki se financira v okviru programa Obzorje Evropa, sta bila vzpostavljena metodologija za skupno javno naročanje na področju varnosti in mreža organov za javno naročanje v državah članicah. *Inovacijsko vozlišče EU za notranjo varnost* bi bilo glede na svojo sestavo in organizacijo svojega dela primerno, da spremlja določitev skupnih potreb s strani držav članic in opredeli, katera orodja bi bila najbolj uporabna, če se vzpostavi namensko delovno področje digitalne forenzike.

Orodja digitalne forenzike s seboj prinašajo še druge težave, poleg stroškov. Podatki, pridobljeni s temi orodji, so lahko npr. strukturirani ali predstavljeni v obliki, ki ni skladna z obstoječimi domačimi informacijskimi sistemi, ki se uporabljajo za nadaljnjo obdelavo (npr. analizo ali izmenjavo podatkov). Zato je treba oblikovati sklop skupnih zahtev držav članic glede strukture in oblike podatkov, pridobljenih z orodji digitalne forenzike. Na podlagi tega bi lahko organi držav članic sodelovali v razpravah s ponudniki orodij digitalne forenzike, da bi se lahko njihove zahteve ustrezno upoštevale, npr. v okviru postopkov skupnega javnega naročanja, kot je opisano zgoraj.

Ključni ukrep: strokovnjaki skupine na visoki ravni poudarjajo, da je pri pridobivanju orodij digitalne forenzike potrebna boljša stroškovna učinkovitost

Akterji: države članice, Evropska komisija, inovacijsko vozlišče EU za notranjo varnost, Europol	*Časovni okvir: od leta 2025 naprej (skupno javno naročanje)*	*Proračun: ni na voljo*

- Strokovnjaki skupine na visoki ravni pozivajo Evropsko komisijo, naj:
  - podpre države članice pri **opredelitvi orodij digitalne forenzike**, ki so najbolj potrebna za učinkovite preiskave (po možnosti v okviru inovacijskega vozlišča EU za notranjo varnost);
  - podpre **sodelovanje med operativnimi enotami in kontaktnimi točkami v organih za javna naročila,** ki so združene v projektu iProcureNet;
  - vzpostavi **pilotne skupne nakupe licenc za orodja digitalne forenzike**.
- Strokovnjaki skupine na visoki ravni menijo, da lahko **Europol** pomaga državam članicam pri določitvi **skupnih zahtev glede strukture in oblike podatkov, pridobljenih** z orodji digitalne forenzike, ter na tej podlagi spodbuja sodelovanje med ustreznimi nacionalnimi organi in strokovnjaki, da se jim omogoči sodelovanje s proizvajalci in razvijalci teh orodij, da se lahko dogovorijo o standardih, zahteve držav članic pa se lahko ustrezno upoštevajo.

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

II. Izmenjava zmogljivosti in občutljivih orodij

Trenutno je izkoriščanje ranljivosti za dostop do ključev za dešifriranje na napravah še vedno glavna možnost, ki jo imajo organi odkrivanja in pregona za dostop do šifriranih vsebin, saj je razpoložljivost zmogljivosti za dešifriranje omejena (npr. Europolova platforma za dešifriranje) in ni učinkovitega sodelovanja z industrijo ali posebnega pravnega okvira za zagotovitev zakonitega dostopa do informacij na digitalnih napravah.

Tudi če so ti pogoji (nekateri od njih) do neke mere vzpostavljeni, se bodo storilci kaznivih dejanj verjetno zanašali na namenske šifrirane naprave za prikrivanje informacij ali nezakonitih vsebin. Zato bo v bližnji prihodnosti še vedno treba uporabljati in si po možnosti izmenjevati občutljiva orodja[31] in zmogljivosti.

Sklop priporočil 2

Za izmenjavo občutljivih orodij in odgovorno upravljanje s tem povezanih zmogljivosti strokovnjaki priporočajo:

1. *razmislek o vzpostavitvi mehanizmov za zagotovitev izmenjave občutljivih orodij na način, ki v celoti spoštuje nacionalna pravila [priporočilo 1];*
2. *vzpostavitev procesa za izmenjavo zmogljivosti, ki bi lahko vključeval izkoriščanje ranljivosti, s čimer bi se omogočilo združevanje znanja in virov, ob zagotavljanju, da se spoštujeta zaupnost in občutljivost informacij [priporočilo 6];*
3. *morebitno preučitev evropskega pristopa k upravljanju in razkrivanju ranljivosti, s katerimi se soočajo organi odkrivanja in pregona, na podlagi obstoječih dobrih praks [priporočilo 2].*

Evropska komisija je prek programa Obzorje Evropa in IFS podprla projekta (*EXFILES* in *ForRES*[32]), namenjena ranljivosti in izkoriščanju programske opreme, s čimer je strokovnjakom na področju odkrivanja in pregona zagotovila orodja in protokole za hitro in dosledno pridobivanje podatkov, ki so kljub temu skladni z vsemi ustreznimi pravnimi določbami.

[31] „Občutljiva orodja“ se nanašajo tako na orodja digitalne forenzike kot na taktična orodja za prestrezanje.

[32] https://forres.eu.

Izmenjava občutljivih orodij in s tem povezanih zmogljivosti med zaupanja vrednimi evropskimi partnerji olajšuje operativno sodelovanje, omogoča vzajemno pridobivanje znanja in ustvarja ekonomije obsega, s čimer se zmanjšujejo potrebni viri.

Čeprav je izkoriščanje ranljivosti včasih še vedno ključnega pomena za preiskave, ga je treba v skladu z ustreznim nacionalnim pravnim okvirom uporabljati skrajno previdno, saj vpliva na varnostno stanje strojne in programske opreme.

Ključni ukrep: strokovnjaki skupine na visoki ravni pozivajo k podpori pri izmenjavi občutljivih orodij in odgovornem upravljanju s tem povezanih zmogljivosti

Akterji: države članice, Evropska komisija	*Časovni okvir: od leta 2024 naprej*	*Proračun: ni na voljo*

- Strokovnjaki skupine na visoki ravni pozivajo Evropsko komisijo, naj še naprej podpira projekte, namenjene izmenjavi občutljivih orodij (orodij digitalne forenzike in taktičnih orodij za prestrezanje) in združevanju virov prek ustreznih programov financiranja; Komisija bi lahko podprla tudi **vzpostavitev nadnacionalne platforme za strukturiranje in izmenjavo znanja**.

- Strokovnjaki skupine na visoki ravni pozivajo Skupno raziskovalno središče Evropske komisije, naj preuči izvedljivost določitve **evropskega pristopa k upravljanju in razkrivanju ranljivosti**, ki jih obravnavajo organi odkrivanja in pregona, na podlagi obstoječih dobrih praks.

III. Kolektivne naložbe za razvoj spretnosti ter izboljšanje strokovnega znanja na področju digitalne forenzike

Ustrezno osebje s področja odkrivanja in pregona bi moralo biti usposobljeno za uporabo preiskovalnih orodij in tehnik, ki se uporabljajo pri njihovih preiskavah, njihovo strokovno znanje pa bi bilo treba dokazati s certifikatom. Njihove zahtevane in dokumentirane kompetence bi morale odražati njihovo vlogo in vključevati vsaj področje digitalne forenzike za generične mobilne naprave (agnostične z vidika orodij), nadzorne verige/vsebin dokazov ter osnovno poznavanje vrst pridobivanja, analiz, poročanja in navzočnosti na obravnavi. Dokumentacija bi morala odražati, ali so te kompetence pridobljene z usposabljanjem ali na delovnem mestu.

Sklop priporočil 3

Za podporo razvoju spretnosti in strokovnega znanja na področju digitalne forenzike, vključno z dešifriranjem in standardizacijo, strokovnjaki priporočajo:

1. *povečanje števila priložnosti za usposabljanje strokovnjakov [priporočilo 7];*
2. *vzpostavitev sistema certificiranja na ravni EU za strokovnjake za digitalno forenziko, da se zajamčita kakovost in enotnost zagotovljenega tehničnega usposabljanja [priporočilo 7];*
3. *vlaganje v zapolnitev vrzeli v tehničnih spretnostih pri standardizaciji ter povečanje ozaveščenosti s sklepanjem dogovorov z akademskimi krogi in drugimi ustreznimi inštituti [priporočilo 8].*

CEPOL izvaja tečaje usposabljanja o več pomembnih temah[33]. Evropska skupina za usposabljanje in izobraževanje na področju kibernetske kriminalitete (ECTEG)[34] pripravlja tečaje o kibernetski kriminaliteti in digitalni forenziki ter jih brezplačno daje na voljo agenciji CEPOL in nacionalnim organom odkrivanja in pregona.

ECTEG je razvila *Decrypt*, ki je namenjen usposabljanju za krepitev zmogljivosti organov odkrivanja in pregona držav članic EU za zakonito dešifriranje z izpopolnjenimi strategijami za zakonito ravnanje s šifriranimi dokazi. Decrypt lahko uvede CEPOL kot tudi nacionalne enote z uporabo infrastrukture, ki jo da na voljo Skupno raziskovalno središče.

---

33 Usposabljanje preiskovalcev za digitalno forenziko, mobilno forenziko, forenziko podatkov v živo in forenziko za Mac.

34 ECTEG je neprofitna organizacija, ki združuje 30 organov odkrivanja in pregona iz 20 evropskih držav, mednarodnih organov in akademskih krogov. S podporo ISF razvija, spodbuja in izmenjuje vire, rešitve in gradivo za usposabljanje. Glej https://www.ecteg.eu/.

Prav tako je pomembno, da se tistim, ki se prvi odzovejo, zagotovijo osnovne spretnosti na področju digitalne forenzike. ECTEG je med drugim vzpostavila tudi projekt *eFirst (*„Izobraževanje organov odkrivanja in pregona, ki se prvi odzovejo, o bistvenih elementih kibernetike“*)*. eFirst je spletni modul za samostojno usposabljanje, namenjen policistom, ki delujejo na terenu (v patrulji, na kraju kaznivega dejanja, v hišnih preiskavah), ali policistom, ki so zadolženi za sprejem prve pritožbe žrtve. Zagotavlja osnovno znanje o kibernetski kriminaliteti in digitalni forenziki. Uporablja se lahko tudi kot podlaga za tečaje v živo na policijskih akademijah.

Cerificiranje profilov strokovnjakov zagotavlja, da ima vsaka oseba potrebno znanje in spretnosti. Strokovnjake spodbuja, da razvijejo svoje spretnosti ter spremljajo razvoj na svojem področju, podpira pa tudi poklicno napredovanje in priznavanje osebnih dosežkov. To vodi h kakovostnejšemu in natančnejšemu delu. Poleg tega se lahko s certificiranjem oseb:

- zagotovi jasen in pregleden opis spretnosti in kompetenc strokovnjakov za digitalno forenziko, kar bo strokovnim delavcem in vodjem enot omogočilo, da ugotovijo, kdo mora izpolnjevati potrebne zahteve za učinkovito opravljanje ustreznih nalog;

- olajša razvoj in usmerja organizacija tečajev usposabljanja na nacionalni in regionalni ravni ter ravni EU; primerljivo usposabljanje policistov v vseh državah članicah EU zagotavlja, da imajo vsi policisti dostop do usklajene ravni znanja in spretnosti, ne glede na državo, iz katere prihajajo;

- prispeva k preglednejšim sodnim postopkom;

- poveča zaupanje med preiskovalci in drugimi akterji ter tako okrepi mednarodno sodelovanje med nacionalnimi organi odkrivanja in pregona.

CEPOL je začel razvijati *sektorski okvir kvalifikacij* za policijsko delo, ki se osredotoča na čezmejno sodelovanje. Ta model se lahko uporabi v praksi na podlagi dela, ki ga je ECTEG opravila v zvezi s certificiranjem strokovnjakov za digitalno forenziko v okviru *projekta globalnega certificiranja na področju kibernetske kriminalitete*[35].

Tako ECTEG kot EACTDA del svojih virov vlagata v podporo učinkovitemu *sodelovanju ustreznih strokovnjakov na področju odkrivanja in pregona v postopkih standardizacije*, npr. z omogočanjem pridobivanja potrebnih spretnosti.

Ključni ukrep: strokovnjaki skupine na visoki ravni pozivajo k izboljšanju tehničnih spretnosti ter certificiranju profilov

Akterji: CEPOL, ECTEG	*Časovni okvir: ukrepi, ki se izvajajo; certifikacijska shema za strokovnjake za digitalno forenziko naj bi bila pripravljena do leta 2026*	*Proračun:*

- Strokovnjaki skupine na visoki ravni pozivajo CEPOL, naj še naprej **izvaja** tečaje usposabljanja (zlasti tečaje za izvajalce usposabljanj).
- Strokovnjaki skupine na visoki ravni pozivajo ECTEG, naj še naprej **razvija, posodablja in pilotno izvaja** tečaje usposabljanja o digitalni forenziki za strokovnjake in osebe, ki se prve odzovejo, s posebnim poudarkom na dešifriranju.
- Strokovnjaki skupine na visoki ravni pozdravljajo trenutna prizadevanja Komisije (v zvezi z odprtimi razpisi za zbiranje predlogov v okviru ISF) za podporo ECTEG ter **uvedbo** tečajev usposabljanja na regionalni ravni.
- Skupina na visoki ravni poziva ECTEG, naj še naprej preučuje možnost vzpostavitve sistema certificiranja na ravni EU za strokovnjake za digitalno forenziko, CEPOL pa, naj čim bolj sodeluje v teh prizadevanjih na podlagi svojega dela v zvezi s **sektorskim okvirom kvalifikacij** za policijsko delo in **globalnim certificiranjem na področju kibernetske kriminalitete**.
- Skupina na visoki ravni poziva ECTEG, naj ustreznim strokovnim delavcem še naprej olajšuje pridobivanje **kompetenc in strokovnega znanja v zvezi s postopki standardizacije**.

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

IV. Olajšanje zakonitega dostopa

Brez standardov, ki bi urejali vgrajen zakoniti dostop, morajo organi odkrivanja in pregona vse pogosteje izkoriščati ranljivosti, da bi pridobili dostop do zaseženih naprav, na katerih so informacije zaščitene s šifriranjem. Čeprav lahko ta metoda prinaša napredek pri preiskavah, je povezana z visokimi stroški. Zato je treba razmisliti o možnih alternativah.

Sklop priporočil 4

Da bi vzpostavili mehanizme za sodelovanje z ustreznimi industrijskimi partnerji in preučili možnost uvedbe zavezujočih standardov in približevanja zakonodaje na področju zakonitega dostopa v skladu s sodno prakso Sodišča Evropske unije (SEU) in Evropskega sodišča za človekove pravice, strokovnjaki priporočajo:

1. *razvoj platforme (SIRIUS ali enakovredne platforme) za izmenjavo orodij, najboljših praks in znanja o tem, kako lastnikom in proizvajalcem proizvodov ter proizvajalcem strojne opreme odobriti dostop do podatkov [priporočilo 11];*

2. *evidentiranje kontaktnih točk organov odkrivanja in pregona pri proizvajalcih digitalne strojne in programske opreme [priporočilo 11];*

3. *celovito evidentiranje obstoječe zakonodaje v državah članicah in razvoj priročnika EU o njej, da se podrobno opredelijo pravne odgovornosti proizvajalcev digitalne strojne in programske opreme, da izpolnijo zahteve organov odkrivanja in pregona za podatke, ob upoštevanju posebnih scenarijev in zahtev, ki podjetja prisilijo, da uporabijo naprave za dostop [priporočilo 25];*

4. *ustanovitev raziskovalne skupine, ki bi ocenila tehnično izvedljivost obveznosti vgrajenega zakonitega dostopa (vključno za dostop do šifriranih podatkov) za digitalne naprave, ob hkratnem ohranjanju varnosti naprav in zasebnosti informacij za vse uporabnike brez njunega ogrožanja ter brez slabšanja ali spodkopavanja varnosti komunikacij [priporočilo 26];*

5. *razvoj zavezujočih industrijskih standardov za naprave, dane na trg v EU, odvisno od zgoraj navedenega evidentiranja, za vključitev zakonitega dostopa in spodbudo približevanju zakonodaje na tem področju [priporočilo 25].*

Sedanje sodelovanje organov odkrivanja in pregona z industrijo ne prispeva h konkretnim rezultatom; za razvoj zakonitih poti do dostopa organov odkrivanja in pregona do naprav in aplikacij je treba okrepiti sodelovanje z industrijo. V primeru posnetkov videonadzora se organi odkrivanja in pregona npr. vse pogosteje srečujejo s šifriranimi datotekami, ki jih ni mogoče analizirati z avtomatsko programsko opremo, zlasti kadar gre za velike količine videoposnetkov.

Teoretično lahko organi odkrivanja in pregona zaprosijo za podporo proizvajalce naprav, ki lahko nato zagotovijo izvorno kodo svoje programske opreme, da olajšajo dostop do nekodiranih podatkov o vsebini, ali zagotovijo tehnično dokumentacijo o opremi, ki se je pojavila v kazenskih preiskavah.

Europol bi lahko zbiral najboljše prakse (kot je vzpostavitev kontaktnih točk za organe odkrivanja in pregona) in znanje o tem, kako bi lahko lastniki in proizvajalci proizvodov ter proizvajalci strojne opreme olajšali dostop in jih dali na voljo vsem organom odkrivanja in pregona preko platforme SIRIUS (ali enakovredne platforme).

Hkrati bi bilo treba razmisliti o preglednejših rešitvah, ki bi omogočile dostop do nekodiranih podatkov na zaseženih napravah, da bi povečali učinkovitost preiskav in obenem zagotovili enake konkurenčne pogoje za akterje v industriji, pri tem pa ohranili kibernetsko varnost in varovali zasebnost.

Strokovnjaki na podlagi podrobne analize zahtev organov odkrivanja in pregona za zakonit dostop pozivajo Evropsko komisijo, naj pripravi *tehnološki kažipot*[36], ki bo združeval ukrepe strokovnjakov za tehnologijo, kibernetsko varnost, zasebnost, standardizacijo in varnost ter zagotavljal ustrezno usklajevanje.

Ključni ukrep v okviru tega tehnološkega kažipota bi bil oceniti *tehnično izvedljivost vgrajenih obveznosti zakonitega dostopa* (vključno z dostopom do šifriranih podatkov in šifriranih posnetkov CCTV) za digitalne datoteke in naprave[37], ob hkratnem zagotavljanju strogih zaščitnih ukrepov za kibernetsko varnost in brez slabšanja ali ogrožanja varnosti komunikacij. Ta ocena bi se izvedla ob sodelovanju vseh zadevnih deležnikov.

---

[36] Poročilo se v več primerih in poglavjih sklicuje na edinstven „tehnološki kažipot“.

[37] Glej „*Moving the Encryption Policy Conversation Forward*“ (Nadaljevanje pogovora o politiki šifriranja) - Carnegie Endowment for International Peace - https://carnegieendowment.org/research/2019/09/moving-the-encryption-policy-conversation-forward?lang=en.

Tehnološki kažipot bi moral v obsegu, v katerem je taka ocena potrdila razpoložljivost ali izvedljivost vgrajenih zakonitih obveznosti dostopa, ki izpolnjujejo zgoraj navedene pogoje, opredeliti tudi postopek za trajno in dolgoročno *sodelovanje z organi za standardizacijo*. Sodelovanje organov odkrivanja in pregona v tem postopku standardizacije bi lahko ob podpori EACTDA usklajeval Europol.

Na podlagi evidentiranja obstoječih pravnih okvirov držav članic, ki določajo odgovornosti proizvajalcev digitalne strojne in programske opreme v zvezi s skladnostjo z zahtevami organov odkrivanja in pregona za podatke, bi bilo mogoče oceniti potrebo po *zakonodaji ali smernicah in priporočilih* [spodbujanje približevanja zakonodaje na tem področju].

Ključni ukrep: strokovnjaki skupine na visoki ravni pozivajo k okrepitvi sodelovanja z industrijo, spodbujanju ustreznih standardov v prihodnjih pobudah EU ter približevanju zakonodaje na področju zakonitega dostopa v skladu s sodno prakso Sodišča Evropske unije in Evropskega sodišča za človekove pravice

Akterji: Europol, Evropska komisija	*Časovni okvir: od leta 2025 naprej*	*Proračun: ni na voljo*

- Strokovnjaki skupine na visoki ravni pozivajo **Evropsko komisijo**, naj pripravi namenski **tehnološki kažipot** za preučitev možnosti za zakonit dostop do digitalnih naprav.
- Strokovnjaki skupine na visoki ravni pozivajo **Europol**, naj zbere najboljše prakse in znanje o tem, kako bi lahko lastniki in proizvajalci proizvodov ter proizvajalci strojne opreme olajšali dostop in ga dali na voljo vsem organom odkrivanja in pregona prek platforme **SIRIUS** (ali enakovredne platforme).

Poglavje II: Hramba podatkov

KAKŠNE SO TEŽAVE?

Medtem ko so se v preteklosti dokazi zbirali predvsem v fizični obliki, ponudniki komunikacij danes hranijo ogromno potencialnih dokazov v obliki metapodatkov. Čeprav digitalni podatki niso edini dokazi, ki se zahtevajo v okviru kazenskih preiskav, je ta vrsta dokazov ključna – zlasti za ugotavljanje identitete osumljencev ali operativno zanimivih oseb, ki imajo morda ustrezne informacije – v skoraj vseh preiskavah, ne glede na to, ali se nanašajo na kazniva dejanja, storjena v fizičnem ali digitalnem svetu. Zlasti v zvezi s slednjimi so lahko komunikacijski metapodatki (zlasti naslovi IP in številke vrat) pogosto edini način za identifikacijo osumljenca[38].

Da bi lahko organi odkrivanja in pregona preiskovali kazniva dejanja v digitalni dobi, morajo biti digitalni dokazi na voljo v berljivi obliki in dostopni, kadar je to potrebno, pri čemer je treba ustrezno upoštevati vse zaščitne ukrepe za kazenske postopke, procesne pravice ter zasebnost in varstvo podatkov. Podatki se lahko hranijo za poslovne namene (kot sta zaračunavanje in izdajanje računov) ali za namene odkrivanja in pregona. Hramba podatkov lahko pomaga zagotoviti razpoložljivost podatkov, tako da lahko pristojni organi do njih dostopajo v okviru kazenskih preiskav in pregona. Podatki, ki jih hranijo ponudniki, so lahko ključnega pomena za učinkovit boj proti kriminalu, hranjenje takih podatkov pa je predpogoj za to, da se nato organom odkrivanja in pregona omogoči dostop in zagotovi, da lahko izvajajo preiskave[39]. Istočasno v skladu z načelom minimalizacije podatkov, določenim v direktivi o zasebnosti in elektronskih komunikacijah[40] in splošni uredbi o varstvu podatkov (GDPR)[41], velja, da bi morali ponudniki hraniti (ali drugače obdelovati) podatke o prometu le toliko časa, kolikor je potrebno za namene same komunikacije, za zaračunavanje ali v posebnih primerih za namene trženja elektronskih komunikacijskih storitev. Vsako drugo hranjenje mora urejati pravni okvir, ki izpolnjuje zahteve iz člena 15 direktive o zasebnosti in elektronskih komunikacijah. Ta ureditev odraža potrebo po uravnoteženju temeljnih pravic do zasebnosti in varstva podatkov z nameni ukrepov za odkrivanje in pregon.

---

38 Strokovnjaki so razpravljali o več primerih relevantnosti digitalnih podatkov v preiskavah in številu zahtev za podatke. Po navedbah enega od njih so v zadnjih petih letih v vseh preiskavah v zvezi s terorizmom ali organiziranim kriminalom uporabili podatke, ki so jih zahtevali od ponudnikov. Leta 2023 so v eni od držav članic za identifikacijo v kazenskih postopkih od operaterjev zahtevali več kot 1 300 000 številk, skoraj vse zahteve pa je pozneje potrdil pravosodni sistem.

39 Za namene tega dokumenta se dostop do podatkov razume kot dostop, odobren organom odkrivanja in pregona na podlagi predhodne sodne odobritve, kadar je to potrebno, za namene kazenskih preiskav in za vsak primer posebej.

40 Člen 6 Direktive 2002/58/ES.

41 Člen 5(1)(c) Uredbe (EU) 2016/679.

Trenutno ni zakonodaje EU, ki bi urejala hrambo podatkov. Sodišče Evropske unije je leta 2014 razveljavilo direktivo EU o hrambi podatkov[42], pri čemer je opozorilo na precejšnje posege v temeljno pravico do zasebnosti in varstva podatkov, neločljivo povezane s [splošnim in neselektivnim] shranjevanjem podatkov, ki so jih prvotno zbrali ponudniki storitev, za namene odkrivanja in pregona[43]. Zato so se nacionalni pravni okviri spremenili, kar je povzročilo znatne razlike v EU[44]: medtem ko v nekaterih državah članicah še vedno veljajo pravila, v skladu s katerimi morajo ponudniki komunikacij hraniti nekatere kategorije podatkov za namene odkrivanja in pregona, so druge uvedle spremembe, da bi izpolnile merilo ciljne hrambe podatkov o prometu, predlagano v sodni praksi[45]; nekatere druge, tudi zaradi poznejših sodb nacionalnih sodišč, nimajo posebnih pravil o hrambi podatkov za namene odkrivanja in pregona ter se zanašajo izključno na podatke, ki jih podjetja hranijo za poslovne namene. Pogoji za dostop do takih podatkov so odvisni od veljavnega nacionalnega pravnega okvira in vrste podatkov (naročniki, podatki o prometu ali vsebini). Kot posledica tega, da ni skladnih in usklajenih obveznosti glede hrambe podatkov po vsej EU, se zahteve držav članic glede hrambe (in trajanja hrambe) različnih vrst metapodatkov s strani ponudnikov storitev razlikujejo.

---

42 Direktiva 2006/24/ES. V skladu z Direktivo morajo države članice EU sprejeti ukrepe, s katerimi zagotovijo, da ponudniki elektronskih komunikacijskih storitev in omrežij hranijo podatke o prometu in lokaciji ter s tem povezane podatke, potrebne za identifikacijo naročnika ali registriranega uporabnika, za obdobje od šest mesecev do dveh let, da se pristojnim organom omogoči dostop za namene preiskovanja, odkrivanja in pregona hudih kaznivih dejanj, kot so opredeljena v nacionalni zakonodaji.

43 Za pregled ustrezne sodne prakse glej: *The future of national data retention obligations – How to apply Digital Rights Ireland at national level?* (Prihodnost obveznosti glede hrambe podatkov – Kako uporabljati digitalne pravice Irske na nacionalni ravni?) – European Law Blog, V. Franssen; *Recalibrating Data Retention in the EU* (Prilagoditev hrambe podatkov v EU) - eucrim; Poročilo Eurojusta/EJCN 2024. *The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU* (Učinek sodne prakse Sodišča Evropske unije na nacionalne ureditve hrambe podatkov in pravosodno sodelovanje v EU); *Cybercrime Judicial Monitor - Issue 6* (Zbornik pravosodne prakse, povezane s kibernetsko kriminaliteto – 6. izdaja); *Cybercrime Judicial Monitor - Issue 9* (Zbornik pravosodne prakse, povezane s kibernetsko kriminaliteto, 9. izdaja)

44 Odzivi držav članic na razveljavitev direktive o hrambi podatkov so se razlikovali, ukrepi, uvedeni na nacionalni ravni, pa so povečali raznolikost nacionalnih sistemov hrambe podatkov. Glede na Poročilo Eurojusta/EJCN o hrambi podatkov iz leta 2024 je v obdobju 2018–2022 svojo zakonodajo spremenilo 12 držav. Sodelujoči so odgovorili, da so te spremembe neposredna posledica zadev Sodišča Evropske unije C-746/18, *Prokuratuur*, in združenih zadev C-511/18, C-512/18 in C-520/18, *La Quadrature du Net in drugi*. 23 od 27 držav članic ima vzpostavljena pravila o hrambi podatkov; sedem držav članic je že uvedlo ciljno usmerjena pravila o hrambi podatkov. Za pregled glej *Commission Study on the retention of electronic communications non-content data for law enforcement purposes* (Študija Komisije o hrambi nevsebinskih podatkov o elektronskih komunikacijah za namene odkrivanja in pregona), 2020, str. 39.

45 Sodišče je v več sodbah razvilo koncept ciljne hrambe podatkov o prometu in lokaciji, pri čemer je odločilo, da je hramba podatkov lahko združljiva s pravom Unije, če je zasnovana na podlagi posebnih ciljev in za posebne namene. Vendar je praktična uporaba meril, ki jih je Sodišče predlagalo za oblikovanje takih ciljev, povzročila težave in izzive na višjih sodiščih v tistih državah članicah, ki so to poskušale.

V državah članicah, ki nimajo obveznosti hrambe podatkov, je težko ali včasih nemogoče identificirati osumljenca ali osebo, ki bi lahko imela pomembne informacije („operativno zanimiva oseba“) v kazenski preiskavi[46]. Dodana vrednost novih pravil o elektronskih dokazih bi se – ko bodo začela veljati – povečala tudi, če bi bila dopolnjena z obveznostmi hrambe podatkov, saj sicer ni nobenega jamstva, da bodo na voljo informacije, ki so predmet evropskega naloga za zavarovanje elektronskih dokazov ali evropskega naloga za predložitev dokazov (kar zajema podatke o prometu, podatke, ki se zahtevajo izključno za identifikacijo uporabnika, in podatke o naročnikih).

Sedanje okoliščine vplivajo na **organe odkrivanja in pregona** ter **ponudnike komunikacij**, predvsem pa na **državljane in državljanke ter na žrtve**, katerih pravice do dostopa do pravnega varstva ni mogoče zagotoviti, če se preiskave začnejo, ko so bili podatki že izbrisani ali če niso bili shranjeni[47].

I. Vprašanja, ki so v pristojnosti posameznih držav članic

V državah članicah, **v katerih ni posebnih obveznosti** glede hrambe podatkov za namene odkrivanja in pregona, preiskave temeljijo na podatkih, ki jih podjetja hranijo za svoje poslovne in komercialne namene, poleg vseh drugih razpoložljivih dokazov. Za komercialne podatke veljajo notranje politike ponudnikov, pri čemer podjetja hranijo podatke o prometu za različna obdobja (npr. približno 6 mesecev), podatke o lokaciji, ki običajno niso poslovno pomembni, pa pogosto hranijo krajši čas. Manjša podjetja pogosto sploh ne shranjujejo metapodatkov o naročnikih ali komunikacijah ali jih hranijo zelo kratek čas. Zato so preiskave pogosto tekma s časom, saj morajo preiskovalci pred izbrisom podatkov včasih zgolj v nekaj dneh ali urah identificirati pošiljatelja podatkov in posredovati zahtevo v skladu z veljavnimi pravili. V nekaterih primerih podjetja ne zagotavljajo informacij o specifičnih podatkih, ki jih obdelujejo in hranijo, zaradi česar pristojni organi pri iskanju podatkov težko predložijo ciljne zahteve. Nekatere storitve gostovanja uporabnikom omogočajo najem strežniškega prostora z uporabo fiktivnih podatkov, kar pomeni, da, tudi če shranjujejo podatke uporabnikov, niso zanesljive[48].

---

46 Glej primer iz *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* (Operativni izzivi, s katerimi se soočajo organi odkrivanja in pregona – gradivo za prvo plenarno sejo Skupine na visoki ravni za dostop do podatkov za učinkovito odkrivanje in pregon; referenčni dokument), str. 4.

47 V zvezi z vplivom na državljane in državljanke ter na žrtve glej zadevo *Dwyer/The Commissioner of the Garda Síochána* – [2020] IESC 4 (24. februar 2020), zlasti točko 9.

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

V večini držav članic je v veljavi zakonodaja o **hrambi podatkov**. Vendar, kot je opisano zgoraj, so se nekatere nacionalne zakonodaje spremenile na podlagi sodb Sodišča Evropske unije, ki so izhajale iz razveljavitve direktive o hrambi podatkov. To je ustvarilo raznoliko okolje, pri čemer se države članice različno odzivajo na sodbe. V nekaterih državah članicah so si prizadevali za uvedbo ciljne oblike hrambe, ki jo je Sodišče Evropske unije predlagalo kot možno pot v zvezi s hrambo podatkov. Vendar so strokovnjaki skupine na visoki ravni poudarili, da je implementacija takih meril povzročila pravne in tehnične težave, kar zadeva njihovo izvedljivost[49], ponudniki pa so kritizirali stroške, povezane s tehnično implementacijo ciljne hrambe in, splošneje, s pogostim spreminjanjem zakonodaje. Druga pomembna pravna težava na nacionalni ravni je, da nacionalna zakonodaja v večini primerov ne zajema povrhnjih storitev (OTT-storitev). Posebni primer OTT-storitev bo podrobneje obravnavan v oddelku 1.3.

II. Čezmejne težave v EU

Težave v zvezi s hrambo podatkov se pojavljajo tudi pri čezmejnih zahtevah, tj. kadar pristojni organ zahteva podatke od ponudnika s sedežem v drugi državi članici. V primerih, ki vključujejo čezmejne zahteve, organi v državi prejemnici morda ne bodo mogli izvršiti zahteve (ker ni podatkov ali ustreznih pravnih predpisov), ki jo je izdala druga država.

Zaradi neusklajenosti obveznosti glede hrambe metapodatkov v EU sta ovirana odkrivanje in pregon v državi članici, ki **želi dobiti podatke** od ponudnikov s sedežem v drugih državah članicah. Tudi kadar so na nacionalni ravni v veljavi ureditve hrambe podatkov, med nacionalnimi sistemi ni skladnosti glede obdobja hrambe, ki se med državami članicami močno razlikuje[50].

---

[49] Sodišče Evropske unije sicer daje nekaj smernic in primerov, kako razumeti **ciljno hrambo** podatkov o prometu, vendar lahko sodna praksa zgolj daje napotke in ni dovolj natančna, da bi podrobno opredelila morebitne omejitve hrambe za vse kategorije podatkov. Posledično je bilo Sodišču v zadnjih letih predloženih več zadev zoper pravila o hrambi podatkov, države članice pa ne morejo zagotoviti pravne varnosti.

[50] Glede na podatke in vrsto kaznivega dejanja se lahko metapodatki hranijo 6 do 72 mesecev. V poročilu Eurojusta/EJCN o hrambi podatkov iz leta 2024 so sodelujoči navedli, da je bilo zaradi nehranjenja podatkov, omejitev za kategorije podatkov, ki jih je mogoče hraniti, in kratkih obdobij hranjenja na voljo manj podatkov. Nerazpoložljivost podatkov posledično vpliva tudi na zmožnost organov, da izvršujejo evropske preiskovalne naloge in se odzivajo na prošnje za medsebojno pravno pomoč.

Prav tako na ravni EU ni usklajenega pristopa k **opredelitvi podatkov**, ki jih je treba hraniti[51]. Nacionalna zakonodaja lahko od ponudnikov storitev zahteva, da hranijo različne kategorije podatkov za različne namene (davki, revizije, odkrivanje in pregon). Zakonodaje se razlikujejo tudi glede stopnje podrobnosti, ki jo zagotavljajo v zvezi s tem, saj nekatere med njimi vsebujejo podrobne sezname nevsebinskih podatkov, ki jih je treba hraniti, druge pa širše opredelitve nevsebinskih podatkov[52]. Poleg tega ponudniki glede na storitve, ki jih ponujajo, ter svoje poslovne in komercialne potrebe hranijo različne vrste podatkov za različna časovna obdobja. Zato je okolje zelo raznoliko, pri čemer so velike razlike ne le med državami članicami, temveč tudi med storitvami.

Take razlike so relevantne tudi zato, ker so med državami članicami razlike tudi pri dostopanju do hranjenih podatkov: v nekaterih državah članicah je za dostop do nekaterih vrst metapodatkov potrebno dovoljenje, v drugih pa ne. Ponudniki storitev poročajo, da je pravna negotovost glede pravil, ki se uporabljajo za razkritje podatkov, eden od vzrokov za zamude in neizpolnjevanje zahtev organov odkrivanja in pregona.

---

[51] Kot je navedeno v študiji Komisije o hrambi podatkov, str. 48: Čeprav so nekatere vrste informacij vedno klasificirane kot podatki o naročnikih ali prometu v vseh državah članicah, ni soglasja o klasifikaciji naslednjih podatkovnih točk: IP-naslovov IP, številk SIM, identifikacijskih številk naprave (npr. IMSI, IMEI) in številk vrat za dinamične IP-naslove. V nekaterih državah članicah (EE, FR, IE) so te podatkovne točke klasificirane kot podatki o naročnikih, v drugih (DE, ES, IT, PL, SI) pa kot podatki o prometu.

[52] Za pregled podatkov, ki se hranijo v posamezni državi članici, glej študijo Komisije o hrambi podatkov, Priloga III.

Pristojni organi morajo upoštevati nacionalne predpise, ki se uporabljajo za ponudnika, ki hrani zahtevane podatke, pa tudi posebne zahteve, ki jih določijo ponudniki sami. Kot je navedeno v letnem poročilu SIRIUS za leto 2022[53], lahko ponudniki zahtevajo, da se uporabijo namenski portal ali da se zahteve predložijo na določenih predlogah ali v določenih jezikih. Zahtevajo lahko tudi informacije o naravi zadeve, jasen sklic na nacionalno pravno podlago za zahtevo ali določitev kratkih časovnih okvirov za zahtevane podatke. Nekatera od teh vprašanj bodo sicer obravnavana z implementacijo svežnja o elektronskih dokazih do leta 2026, vendar so strokovnjaki skupine na visoki ravni poudarili potrebo po skladnosti teh pravil z morebitnim usklajenim okvirom za hrambo podatkov. Čeprav je Evropski inštitut za telekomunikacijske standarde (ETSI) razvil standarde za format zahtev za metapodatke medosebnih komunikacijskih storitev na podlagi številke (tradicionalne telekomunikacije), jih ponudniki v državah članicah ne uporabljajo dosledno. Standardi za prenos podatkov od ponudnikov OTT-storitev[54] do organov odkrivanja in pregona še niso dokončno oblikovani in se ne izvajajo v celoti. Poleg tega se lahko ponudniki storitev sami odločijo, v kakšni obliki bodo zbirali in shranjevali podatke uporabnikov, kar pomeni, da strokovni delavci prejemajo neobdelane podatke v zelo različnih oblikah; to ustvarja precejšnje breme za organe odkrivanja in pregona, ki bi jim bili v pomoč poenostavljeni postopki, **komunikacijski sistemi in formati** za predložitev zahtev ter za pošiljanje in prejemanje odgovorov na nanje, pa tudi podatkov. S standardiziranimi komunikacijskimi sistemi in formati bi se zmanjšali tudi stroški, ki jih imajo podjetja z obdelavo zahtev.

Ko organi odkrivanja in pregona pridobijo zakonit dostop do podatkov, jih morajo biti sposobni izkoriščati; zato morajo biti podatki **berljivi**. Vendar ponudniki vse pogosteje ponujajo storitve, ki omogočajo šifriranje podatkov o prometu od konca do konca, in kadar te podatke na zahtevo posredujejo organom odkrivanja in pregona ter pravosodnim organom, jih pogosto zagotovijo v tej šifrirani obliki.

---

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

[54] V tem poročilu se povrhnje komunikacijske storitve (OTT-storitve) nanašajo na aplikacije in storitve, s katerimi se zagotavljajo komunikacijske in medijske storitve (kot so pošiljanje sporočil ter govorni in video klici) prek interneta brez sodelovanja ali nadzora tradicionalnih ponudnikov telekomunikacijskih storitev (telekomunikacijski operaterji). Običajni primeri komunikacijskih OTT-storitev vključujejo aplikacije za pošiljanje sporočil, kot so WhatsApp, Telegram in Facebook Messenger, storitve govornih in videoklicev, kot so Skype, Zoom, Google Meet, Viber, ter platforme družbenih medijev, kot sta Instagram in Snapchat (pošiljanje sporočil in souporaba medijev).

Poleg tega ima ta *status quo* domnevno še eno posledico, in sicer tveganje, da bodo **dokazi** organov odkrivanja in pregona **izpodbijani** na sodišču[55]. Sodišče Evropske unije je pojasnilo, da je dopustnost dokazov, pridobljenih s hrambo podatkov, stvar nacionalnega prava[56], ob upoštevanju načel enakovrednosti in učinkovitosti[57]. Razlike med nacionalnimi ureditvami hrambe podatkov lahko torej vplivajo na dopustnost dokazov v čezmejnih postopkih[58].

[55] Glej poglavje „Collection and admissibility of evidence“ (*Zbiranje in dopustnost dokazov*) v poročilu Eurojusta/EJCN o hrambi podatkov iz leta 2024.

[56] Sodišče Evropske unije, sodba z dne 6. oktobra 2020, *La Quadrature du Net in drugi*, C-511/18, ECLI:EU:C:2020:791, točke 222–228; sodba z dne 5. aprila 2022, *Commissioner of An Garda Síochána in drugi*, zadeva C-140/20, ECLI:EU:C:2022:258, točka 127.

[57] Prav tam, točka 223: „... pod pogojem, da ta pravila niso manj ugodna od tistih, ki urejajo podobne položaje v nacionalnem pravu (načelo enakovrednosti), in da v praksi ne onemogočajo ali pretirano otežujejo uresničevanja pravic, ki jih podeljuje pravo Unije (načelo učinkovitosti).“

[58] V več sodnih zadevah je bila izpodbijana dopustnost nevsebinskih podatkov kot dokazov. Za povzetek glej študijo Komisije o hrambi podatkov, str. 41.

III. Vprašanja v zvezi z OTT-ponudniki in drugimi ponudniki

Navedena vprašanja se nanašajo na vse ponudnike elektronskih komunikacijskih storitev, vendar OTT-ponudniki za organe odkrivanja in pregona predstavljajo dodatne izzive pri zakonitem dostopu do podatkov. Tako na nacionalni ravni kot na ravni EU OTT-ponudniki pogosto menijo, da zanje ne veljajo enake obveznosti kot za tradicionalne ponudnike komunikacij. Čeprav OTT-ponudniki spadajo na področje uporabe EZEK, dejstvo, da imajo pogosto sedež zunaj EU, ter dejstvo, da ni sistemov licenciranja (tj. zanje lahko veljajo samo splošna dovoljenja) in sankcij, ustvarjata negotovost glede njihovih obveznosti hrambe podatkov, vključno s posebnimi vrstami podatkov, in otežujeta uveljavljanje skladnosti. Poleg tega tradicionalni ponudniki komunikacij v večini primerov za poslovne namene hranijo določene podatke, ki omogočajo identifikacijo uporabnikov (kot so številke IP s številko vrat in časovnim okvirom), kar pa ne velja za **ponudnike OTT-storitev**, ki hranijo le nevsebinske podatke, potrebne za njihove komercialne namene, v nekaterih primerih le za kratko obdobje[59]. OTT-ponudniki ne hranijo nobenih nevsebinskih podatkov, povezanih z dinamičnim naslovom IP (številka vrat in časovni okvir). To lahko oteži ali celo onemogoči pridobivanje metapodatkov o komunikacijah, ki potekajo prek sistemov, kot sta WhatsApp ali Telegram, ki se vse pogosteje uporabljata. Kot je navedeno, se tudi vrste hranjenih podatkov razlikujejo glede na ponujeno storitev. Medtem ko ponudniki v nekaterih primerih izdajo smernice, v katerih so opisane vrste podatkov, ki jih hranijo[60], v drugih primerih OTT-ponudniki teh informacij ne razkrijejo. To skupaj z dejstvom, da, kar zadeva vrste podatkov, ki jih ponudniki ustvarjajo, obdelujejo in shranjujejo za poslovne namene, ni **obveznosti glede preglednosti**, organom odkrivanja in pregona pogosto povzroča težave pri ugotavljanju, ali so bili podatki shranjeni, kdo hrani katere podatke in katere vrste naborov podatkov je mogoče zahtevati, in v končni fazi tudi pri pošiljanju zahtev ponudnikom.

---

59 To velja zlasti za manjše ponudnike. V skladu s študijo Komisije o hrambi podatkov, str. 103, se IP-naslovi v povprečju hranijo 30 dni.

60 Glej na primer law-enforcement-guidelines-outside-us.pdf (apple.com).

Hkrati vse večji obseg zahtev, ki jih prejmejo ponudniki[61], skupaj s potrebo po obdelavi obsežnih naborov podatkov, prispeva k temu, da so zahteve odložene ali zavrnjene[62]. Poleg vzrokov, ki izhajajo iz odločitev ponudnikov v zvezi s posebnimi poslovnimi modeli, je to tudi posledica **omejenega števila mehanizmov za sodelovanje** med organi odkrivanja in pregona ter pravosodnimi organi na eni strani ter zasebnimi podjetji na drugi strani.

Čeprav morda ne spadajo v opredelitev ponudnikov komunikacijskih storitev iz EZEK, nekatere nastajajoče tehnologije in drugi digitalni akterji (kot so proizvajalci avtomobilov in umetnointeligenčni sistemi velikega jezikovnega modela) ustvarjajo in obdelujejo komunikacijske metapodatke, ki lahko zagotovijo informacije o kriminalnih dejavnostih. Kljub vse večji količini podatkov, ki se obdelujejo v okviru teh storitev, trenutno zanje ne veljajo obveznosti hrambe podatkov.

MOŽNE REŠITVE

I. Krepitev sodelovanja med ponudniki komunikacijskih storitev in strokovnimi delavci

Ker je zbiranje podatkov zaradi neusklajenosti pravil ovirano, se morajo organi odkrivanja in pregona pri izvajanju preiskav pogosto zanašati na **prostovoljno sodelovanje** s ponudniki storitev. Čeprav je ta rešitev pripomogla k nekaterim odmevnim preiskavam[63], je pravno negotova in ni vedno izvedljiva: prostovoljno sodelovanje je odvisno od vrste in velikosti ponudnika storitev, pri čemer majhni ponudniki pogosto hranijo podatke zelo kratek čas v primerjavi z večjimi ponudniki ali pa nimajo sredstev za odzivanje na zahteve organov odkrivanja pregona[64].

---

61 Glede na letno poročilo SIRIUS za leto 2023 se obseg zahtev za podatke, naslovljenih na ponudnike storitev, iz leta v leto stalno povečuje (glej str. 66 in naslednje strani).

62 Letno poročilo SIRIUS za leto 2023 (opomba 61) vsebuje pregled glavnih vzrokov za zamude/zavrnitev zahtev za elektronske dokaze (glej str. 68 in naslednje strani).

63 Glej primere iz letnega poročila SIRIUS za leto 2023 (opomba 61), str. 19.

64 V letnem poročilu SIRIUS za leto 2023 (opomba 61), str. 79, je navedeno, da velik obseg zahtev na podlagi prostovoljnega sodelovanja pomeni izziv za ponudnike storitev, zato je priporočeno, da sodelujejo na mednarodnih dogodkih SIRIUS, tako da lahko manjši izvajalci storitev izkoristijo strokovno znanje v okviru projekta SIRIUS na področju sodelovanja z organi, da bi izboljšali svoje razumevanje zadeve, oblikovali svoje politike za odzivanje na zahteve organov in zagotovili, da bodo pripravljeni na prihodnji razvoj zakonodaje.

Partnerstva in sodelovanje z industrijo je treba podpreti z **jasnim pravnim okvirom** kot bistvenim sestavnim delom vsake izvedljive rešitve, ki organom odkrivanja in pregona ter pravosodnim organom omogoča premagovanje težav pri zakonitem dostopu do digitalnih dokazov. Poleg tega, da obe strani izpolnjujeta svoje pravne obveznosti, je pomembno, da se vzpostavi stalen in zaupanja vreden odnos med strokovnimi delavci na področju odkrivanja in pregona ter ponudniki, tako da bodo razumeli potrebe drug drugega in skupaj našli izvedljive rešitve. Potrebni so stabilni **mehanizmi za sodelovanje** z zasebnim sektorjem, da se **poveča preglednost** podatkov, ki jih ponudniki ustvarjajo in hranijo, ter trajanja hrambe, pa tudi da se zagotovi **usklajena kategorizacija podatkov**, ki jih je treba hraniti in do njih dostopati, da se oblikujejo **standardizirani formati** za zahtevanje podatkov in vzpostavijo **varni kanali** za neposredno izmenjavo med pristojnimi organi in ponudniki storitev.

Preučiti je mogoče več možnosti za okrepitev takega sodelovanja, od katerih so nekatere zavezujoče (trdo pravo), druge pa rešitve mehkega prava. Nekatere rešitve, navedene v tem oddelku, bi bilo treba oceniti v okviru ocene učinka iz oddelka II in jih nato določiti z zakonom.

Sklop priporočil 5

Da bi zagotovili, da lahko pristojni organi z identifikacijo pravih imetnikov podatkov zahtevajo ustrezne podatke, da ponudniki storitev take zahteve prejmejo v standardiziranih oblikah in da čezmejno sodelovanja ni ovirano zaradi kolizije zakonov, strokovnjaki priporočajo:

1. *vzpostavitev in krepitev sodelovanja med strokovnimi delavci organov odkrivanja in pregona ter ponudniki storitev, da se podprejo izmenjava informacij, krepitev zmogljivosti in usposabljanje ter opredelijo načela in načini sodelovanja [priporočilo 13], npr. z vzpostavitvijo potrjevalnega urada, ki bi pristojnim organom omogočal, da identificirajo zadevne ponudnike storitev in bolje usmerijo zakonite zahteve [priporočilo 18]. To je mogoče doseči z:*

    a. *nadgradnjo obstoječih struktur na ravni EU, kot so SIRIUS, Evropska pravosodna mreža (EJN) / Evropska pravosodna mreža za kibernetsko kriminaliteto (EJCN), internetni forum EU;*

    b. *memorandumi o soglasju in z uporabo dobrih praks, uveljavljenih v nekaterih državah članicah na nacionalni ravni [priporočilo 14];*

2. *spodbujanjem pravil o preglednosti za ponudnike elektronskih komunikacijskih storitev in drugih komunikacijskih storitev, kar zadeva podatke, ki jih obdelujejo, ustvarjajo ali hranijo v okviru svojega poslovanja, ter obveščanje organov odkrivanja in pregona o tem, kateri podatki so na voljo, ob upoštevanju omejitev zaradi zaupnosti preiskav, in sicer na podlagi sporazumov o sodelovanju s ponudniki storitev ali po potrebi z določitvijo obveznih obveznosti [priporočilo 17, priporočilo 16];*

3. *razvojem poenostavljenih postopkov in formatov na podlagi dogovorjenih standardov za strukturirano predložitev zahtev ponudnikom in prejemanje odgovorov [priporočilo 15] ter s spodbujanjem, da se v okviru platform določijo enotne kontaktne točke za obdelavo zahtev pristojnih organov in stike z njimi [priporočilo 36];*

4. *vzpostavitvijo mehanizmov, ki bi zagotavljali, da so čezmejne zahteve naslovljene na ponudnike storitev na način, ki je učinkovit in preprečuje morebitne spore, pri čemer naj bi se zgledovali po mehanizmih za elektronske dokaze in zagotavljali skladnost takih mehanizmov s pravili, določenimi v uredbi o elektronskih dokazih [priporočilo 19].*

Trenutno so na voljo strukture EU, ki zadevnim akterjem omogočajo, da se seznanijo z orodji in dobrimi praksami. Projekt SIRIUS bi lahko z združevanjem organov odkrivanja in pregona, pravosodnih organov in ponudnikov storitev olajšal izmenjavo znanja in orodij v zvezi z zahtevami po podatkih uporabnikov, ki jih hranijo ponudniki[65], predvsem zaradi obstoječe mreže enotnih kontaktnih točk SIRIUS pa bi lahko služil kot platforma za neposredno povezavo med organi, ki zahtevajo podatke, in ponudniki[66]. SIRIUS bi lahko služil kot **centralno odložišče** pravnih instrumentov, sodne prakse, formatov itd., kot velja za čezmejno izmenjavo e-dokazov[67].

Internetni forum EU[68] bi lahko kot obstoječe sodelovalno okolje za države članice, internetno industrijo in druge partnerje služil kot prostor, kjer bi lahko na ravni EU vzpostavili neposredne stike in zaupanje med ustreznimi akterji v zvezi z dejavnostmi, povezanimi z dostopom do digitalnih podatkov. Prispeval bi lahko k vzpostavitvi in posodabljanju **odprtega kataloga** vrst podatkov, ki jih zbirajo in obdelujejo ponudniki in obdelovalci podatkov, po možnosti pa bi ga centralno upravljal SIRIUS. Tak katalog bi ublažil trenutno nepreglednost, organom odkrivanja in pregona ter pravosodnim organom pa zagotovil večjo jasnost glede tega, katere podatke lahko zahtevajo; hkrati bi deloval kot posredovalnica za identificiranje subjekta, ki bi mu bilo treba poslati zahtevo. Poleg tega bi v primeru, da bi bile ponudnikom naložene pravne obveznosti, katalog zagotovil dodano vrednost pri spremljanju in ocenjevanju izvajanja obveznosti glede preglednosti v zvezi z vrstami podatkov, ki jih ponudniki hranijo ali kako drugače obdelujejo.

---

65 Mreža enotnih kontaktnih točk SIRIUS, ki združuje strokovnjake za zakonite zahteve, promovira dobre prakse in spodbuja države, naj vzpostavijo lastne enotne kontaktne točke. Enotne kontaktne točke so osebe, enote ali institucije, ki so imenovane v ta namen ter ki centralizirajo, pregledujejo in ponudnikom storitev predložijo zahteve vladnih organov. Trenutno je v to mrežo vključenih 36 organov odkrivanja in pregona iz 25 držav.

66 Projekt SIRIUS služi kot vstopna točka za pridobivanje elektronskih podatkov od ponudnikov storitev s sedežem v drugih jurisdikcijah. SIRIUS zagotavlja omejeno platformo za izmenjavo znanja in dobrih praks za organe odkrivanja in pregona ter pravosodne skupnosti. Projekt SIRIUS vzdržuje posodobljeno odložišče kontaktnih podatkov več kot 1 000 podjetij, osredotočeno na manjše, težko dostopne ali občasno nedostopne ponudnike storitev. Pristojni organi lahko zato pridobijo več naslovov z eno samo transakcijo, kar jim pomaga učinkoviteje obravnavati velike količine kompleksnih informacij. Projekt SIRIUS | Europol (europa.eu).

67 SIRIUS je projekt, ki ga financira EU in ki organom za odkrivanje in pregon ter pravosodnim organom pomaga pri dostopu do čezmejnih elektronskih dokazov v okviru kazenskih preiskav in postopkov. Projekt SIRIUS, ki ga skupaj izvajata Europol in Eurojust v tesnem sodelovanju z EJN, je osrednja referenčna točka v EU za izmenjavo znanja o čezmejnem dostopu do elektronskih dokazov. Projekt SIRIUS | Europol (europa.eu).

68 Internetni forum Evropske unije (EUIF) – Evropska komisija (europa.eu).

Z izkoriščanjem sinergij s svežnjem o elektronskih dokazih bi prihranili stroške in vire ter prispevali k celovitemu izvajanju zakonodaje o elektronskih dokazih. Spodbujanje organov odkrivanja in pregona k vzpostavljanju ali povečanju zmogljivosti enot, ki delujejo kot enotne kontaktne točke za (čezmejne) zahteve za razkritje podatkov, bi lahko npr. razširili na zahteve na nacionalni ravni ali zahtevo po zagotavljanju programov usposabljanja za preiskovalce in osebe, ki se prve odzovejo. Prav tako bi lahko aktualna prizadevanja v okviru izvajanja svežnja o elektronskih dokazih, da bi vzpostavili **digitalno platformo**, ki bi omogočala neposredno izmenjavo med pristojnimi organi in ponudniki, replicirali za namene komunikacijskih metapodatkov, ki se hranijo na podlagi nacionalne zakonodaje.

Države članice bi lahko razmislile o vzpostavitvi **memorandumov o soglasju** kot instrumentov za spodbujanje sodelovanja in razvoj skupnega razumevanja med ponudniki storitev, vlado ter organi odkrivanja in pregona v podporo izvajanju nacionalne zakonodaje. Pri njihovem strukturiranju bi se lahko zgledovali po pozitivnih primerih v nekaterih državah članicah, pri čemer naj bi vključili vseh ustrezne akterje (podjetja, agencije itd.), da bi zagotovili, da so zajeti vsi pomembni vidiki sodelovanja (imenovanje enotnih kontaktnih točk za ponudnike storitev ter organe odkrivanja in pregona, tehnične potrebe, skupna opredelitev kategorij podatkov, ki jih je treba zagotoviti, skupni postopki, priprava standardiziranih vzorcev zahtev, varnost podatkov in ukrepi za minimalizacijo podatkov itd.)[69]. Kot je navedeno, bi bili **standardizirani protokoli** za zbiranje podatkov od ponudnikov (vključno s ponudniki OTT-storitev) in za zahteve pristojnih organov za podatke koristni tako za organe odkrivanja in pregona kot za ponudnike storitev, ki bi lahko vzpostavili avtomatizirane mehanizme za zagotavljanje odzivov, zmanjšanje stroškov in prihranek časa. Kljub razlikam med **nacionalnimi** in **čezmejnimi zahtevami** (na podlagi okvira za elektronske dokaze), kar zadeva predpise, bi bilo mogoče razviti delovne postopke in kanale, prek katerih se zahtevajo podatki, saj se standardizacija nanaša na obliko zahtevanih/prejetih podatkov. Za razvoj takih standardiziranih oblik so najprimernejši organi za standardizacijo, kot je ETSI. Vendar strokovnjaki organov odkrivanja in pregona iz držav članic v teh postopkih zaenkrat sodelujejo le v omejenem obsegu. Zato bi lahko obstoječa **Evropska delovna skupina za standardizacijo na področju notranje varnosti**, ki jo vodita Europol in Komisija, usklajevala in spodbujala sodelovanje držav članic v takih forumih. Delo bi lahko temeljilo na obstoječih standardih, ki jih je razvil ETSI in bi se lahko razširili na druge kategorije podatkov[70].

---

[69] Irski memorandum o soglasju z dne 6. aprila 2024 naj bi podprl izvajanje zakona o komunikacijah (hramba podatkov) iz leta 2011 (kot je bil spremenjen). Ministrstvo za pravosodje je imenovalo neodvisnega predsednika, določilo pristojnosti in k sodelovanju povabilo predstavnike organov odkrivanja in pregona ter ponudnikov storitev.

[70] TS 102 657: Ravnanje s hranjenimi podatki; Izročilni vmesnik za zahteve in izročitev hranjenih podatkov ter kategorije hranjenih podatkov (naročnik, uporaba, oprema, omrežni element in podatki o obračunu); TS 103 120: Vmesnik za informacije o nalogu (opredeljuje elektronski vmesnik med dvema sistemoma za varno izmenjavo informacij v zvezi z vzpostavitvijo in upravljanjem zakonitih zahtevanih ukrepov; običajno se uporablja za zakonito prestrezanje, vendar se lahko uporablja tudi za hranjene podatke; običajno se uporablja med ponudnikom storitev na eni strani ter vlado ali organom odkrivanja in pregona, ki ima pravico zahtevati zakoniti ukrep, na drugi strani); TS 103 705: Strukture podatkov za zakonito razkritje (v fazi razvoja; samo podatkovne strukture, brez izročilnega vmesnika, brez vnaprej določene drevesne strukture ter opredeljene vrste in informacij s strani ponudnika storitev).

Ključni ukrep: Strokovnjaki skupine na visoki ravni pozivajo k spodbujanju sodelovanja in razvoju skupnega razumevanja med ponudniki storitev, vlado ter organi odkrivanja in pregona

Akterji: Evropska komisija, države članice, Europol (SIRIUS), Eurojust, internetni forum EU

Časovni okvir: še ni določeno

- Strokovnjaki skupine na visoki ravni pozivajo **Evropsko komisijo**, **Europol** in **države članice**, naj ocenijo načine za spodbujanje in krepitev sodelovanja med organi odkrivanja in pregona ter zasebnimi podjetji ter spodbujajo stalen dialog in vzajemno razumevanje operativnih, tehničnih in poslovnih potreb. Poleg tega glede na oceno učinka iz oddelka II pozivajo Komisijo, naj razmisli o razvoju posebnih obveznosti v zvezi s preglednostjo zbiranja podatkov in stalnih struktur sodelovanja.

- Strokovnjaki skupine na visoki ravni pozivajo **Evropsko komisijo**, **Europol** in **Eurojust**, naj vzpostavijo ali spodbujajo obstoječe platforme za izmenjavo med organi odkrivanja in pregona ter sodstvom na eni strani ter ponudniki komunikacijskih storitev na drugi strani, pripravijo pa naj tudi katalog podatkov, ki jih ponudniki komunikacij in obdelovalci podatkov ustvarijo in hranijo v okviru svojih poslovnih dejavnosti, ki naj bi ga upravljal SIRIUS.

- Strokovnjaki skupine na visoki ravni pozivajo **države članice**, naj preučijo možnost sklenitve sporazumov o sodelovanju in/ali memorandumov o soglasju, ki bi združevali ponudnike storitev, vlade ter organe odkrivanja in pregona, da bi z določitvijo načel in standardnih praks podprli izvajanje nacionalne zakonodaje.

- Strokovnjaki skupine na visoki ravni pozivajo **Europol** in **Evropsko komisijo**, naj uporabita obstoječo Delovno skupino za standardizacijo na področju notranje varnosti, da bi spodbudili sodelovanje držav članic v forumih za standardizacijo, prispevali k opredelitvi ustreznih standardov in skupaj oblikovali protokole, v katerih bi bili podrobno opredeljeni postopki za sodelovanje s ponudniki storitev.

- Strokovnjaki skupine na visoki ravni pozivajo **Evropsko komisijo**, **Europol**, **Eurojust/EJN** in **države članice**, naj izkoristijo sinergije z instrumenti, kot je sveženj o elektronskih dokazih, da bi oblikovali ali pridobili ustrezna orodja, npr. z razširitvijo uporabe digitalnih platform, ki se razvijajo, da bi se uporabljale kot portali za predložitev zahtev.

II. Uskladitev minimalnih pravil za hrambo metapodatkov s strani ponudnikov komunikacij in dostop pristojnih organov

Strokovnjaki se večinoma strinjajo, da je potreben usklajen okvir EU, ki bo urejal hrambo metapodatkov za namene odkrivanja in pregona. Tak okvir bi zagotovil standardizirane rešitve ter jasne in izvršljive obveznosti za ponudnike komunikacij in upravljavce podatkov v zvezi s tem, kdaj in kako hraniti podatke ter v kakšnih okoliščinah zagotoviti dostop do teh podatkov. Z opredelitvijo jasnih pravil o hrambi in dostopu bi ta okvir služil zagotavljanju jasnih zaščitnih ukrepov za temeljne pravice in bistvene interese ob upoštevanju navedb veljavne sodne prakse ter jasnosti pravil, ki se uporabljajo za ponudnike komunikacij za hrambo in souporabo podatkov za namene odkrivanja in pregona. Poleg tega bi tak okvir z zagotavljanjem hrambe podatkov podprl celovito izvajanje svežnja o elektronskih dokazih.

Sklop priporočil 6

Da bi zagotovili, da so na voljo digitalni dokazi, potrebni za preiskovanje in pregon kaznivih dejanj, da med državami članicami ni razdrobljenosti v zvezi s pravili, ki se uporabljajo za hrambo, in zaščitnimi ukrepi v zvezi s temeljnimi pravicami, zlasti zasebnostjo in varstvom podatkov, svobodo izražanja in pravicami tožene stranke, vključno s pravico do dolžnega pravnega postopanja, ter da bi zagotovili pravno varnost za pristojne organe na eni strani ter ponudnike elektronskih in drugih komunikacijskih storitev na drugi strani, strokovnjaki priporočajo:

1. *opredelitev kategorij metapodatkov na podlagi namena njihove uporabe (opredelitev, lociranje, ugotavljanje ali ocenjevanje spletne dejavnosti operativno zanimive osebe) [priporočilo 28], da se zagotovi, da ponudniki elektronskih komunikacijskih storitev in drugih komunikacijskih storitev hranijo podatke, ki zadostujejo vsaj za identifikacijo subjekta [priporočilo 27, točka (v)];*
2. *določitev najkrajšega obdobja hrambe takih podatkov;*
3. *oblikovanje pogojev za dostop do hranjenih podatkov [priporočilo 27, točka (iv)], ki se razlikujejo glede na kategorijo podatkov, kategorijo kaznivega dejanja (npr. kazniva dejanja, ki se zgodijo le na internetu) ali grožnjo žrtvam [priporočilo 29];*
4. *oblikovanje takih pravnih, regulativnih in tehničnih določb tako, da zagotavljajo dosledno spoštovanje temeljnih pravic in svoboščin udeležencev ter da je vsaka omejitev teh pravic potrebna in sorazmerna [priporočilo 27, vi];*
5. *zagotavljanje, da se enaka pravila, obveznosti in zaščitni ukrepi uporabljajo za tradicionalne ponudnike komunikacijskih storitev, OTT-storitev in vse druge obstoječe ali prihodnje ponudnike, ki ustvarjajo in obdelujejo podatke [priporočilo 27, točki (i) in (ii)];*
6. *zagotavljanje, da so podatki uporabnikov, shranjeni za komercialne in poslovne namene, ob ustreznih zaščitnih ukrepih dejansko dostopni organom odkrivanja in pregona(priporočilo 31) in da lahko pristojni organi berejo podatke, ki so jih zakonito prejeli od ponudnikov [priporočilo 27, točka (iii)];*
7. *zagotavljanje, da lahko države članice izvršujejo sankcije proti ponudnikom elektronskih in drugih komunikacijskih storitev, ki ne sodelujejo v zvezi s hrambo in zagotavljanjem podatkov, npr. z izvajanjem upravnih sankcij ali omejitvami njihove zmogljivosti za delovanje na trgu EU [priporočilo 30].*

V zvezi s **hrambo metapodatkov** bi bilo treba razlikovati med kategorijami podatkov, tj. med podatki, potrebnimi za identifikacijo operativno zanimive osebe (podatki o naročnikih[71] in naslovi IP izvorne komunikacije[72]), ter podatki o prometu[73] in lokaciji[74], ter zagotoviti različna obdobja hrambe in zaščitne ukrepe za vsako kategorijo. Tudi v fazi dostopa do podatkov je cilj zagotoviti ravnovesje med resnostjo kaznivega dejanja, ki ga je treba preiskati, in stopnjo poseganja v zasebnost z ukrepi, ki jih je treba sprejeti. V skladu z nedavno sodno prakso[75] bi bilo mogoče preučiti minimalne zahteve za splošno hrambo podatkov, ki zadostujejo za zagotovitev jasne identifikacije vsakega uporabnika. Za podatke o prometu in lokaciji je treba preučiti dodatna in strožja merila.

Da bi tak okvir oblikovali na način, ki bo kos izzivom prihodnosti in **tehnološko nevtralen**, bi bilo treba kategorizacijo podatkov, ki jih je treba hraniti, oblikovati na podlagi pristopa, usmerjenega v prihodnost, vključno s splošnimi nabori podatkov, ki temeljijo npr. na funkcijah podatkov (podatki, ki omogočajo edinstveno identifikacijo komunikacijskega vira ali namembnega kraja, podatki, ki omogočajo identifikacijo lokacije komunikacijskega vira itd.), skupaj s seznamom obstoječih vrst podatkov (naslov IP, IMEI itd.). Ta okvir bi omogočil ustrezno oceno invazivnosti posamezne kategorije podatkov in s tem potrebnih zaščitnih ukrepov.

---

[71] Z nekaterimi izjemami v primeru majhnih ponudnikov se podatki o uporabnikih običajno že hranijo za poslovne namene. V tem primeru in brez poseganja v sorazmerne zaščitne ukrepe bi bilo treba take podatke dati na voljo organom odkrivanja in pregona.

[72] Sodna praksa omogoča splošno in nediferencirano hrambo podatkov v zvezi s civilno identiteto uporabnikov elektronskih komunikacij za zaščito javnih interesov ter splošno in nediferencirano hrambo IP-naslovov za zaščito nacionalne varnosti, boj proti hudim kaznivim dejanjem in preprečevanje resnih groženj javni varnosti (sodba z dne 6. oktobra 2020, *La Quadrature du Net in drugi*, združene zadeve C-511/18, C-512/18 in C-520/18, in sodba z dne 30. aprila 2024, *La Quadrature du Net in drugi*, zadeva C- 470/21 („Hadopi“), ECLI:EU:C:2024:370).

[73] „Podatki o prometu“ pomenijo katere koli podatke, obdelane za namen prenosa sporočila po elektronskem komunikacijskem omrežju ali zaradi zaračunavanja tega sporočila (člen 2 Direktive 2002/58/EC).

[74] „Podatki o lokaciji" pomenijo vsakršne podatke, obdelane v elektronskem komunikacijskem omrežju, ki podajajo zemljepisni položaj terminalske opreme uporabnika javno razpoložljive elektronske komunikacijske storitve (člen 2 Direktive 2002/58/EC); podatke o lokaciji opreme uporabnika bi bilo treba obravnavati kot podatke o lokaciji, ki niso podatki o prometu, kot je opredeljeno v členu 9 Direktive 2002/58/ES.

[75] Sodba v zadevi Hadopi.

Glede na ugotovitve strokovnjakov in nedavno sodno prakso[76] bi z združitvijo obveznosti hrambe s strogimi **zahtevami glede dostopa do podatkov** zagotovili dodatne zaščitne ukrepe za temeljne pravice, zlasti za zasebnost in varstvo podatkov. Zato so strokovnjaki skupine na visoki ravni razpravljali o potrebi po oblikovanju pravil o dostopu, ki se razlikujejo npr. glede na vrsto in resnost kaznivega dejanja, stopnjo ogroženosti, ki jo kaznivo dejanje pomeni za žrtve, namen dostopa in organe, pristojne za dostop do podatkov. Tak pristop se je štel tudi za koristen način za določitev posebnih pravil za preiskovanje in pregon kaznivih dejanj, ki jih je še posebej težko preiskati, kot so tista, storjena izključno na internetu, kjer so edini razpoložljivi dokazi digitalni dokazi.

Ko so podatki zakonito dostopni, jih morajo imeti organi, ki zahtevajo podatke, možnost brati. Zato morajo ponudniki podatke zagotoviti v **razumljivi obliki**. Ponudniki za podatke o prometu in naročnikih pogosto ponujajo šifrirane storitve od konca do konca[77] in teh podatkov ne dešifrirajo, ko jih delijo s pristojnimi organi. Strokovnjaki skupine na visoki ravni so menili, da bi morala ureditev hrambe podatkov vključevati obveznost za ponudnike storitev, da zagotovijo nekodirane podatke, hkrati pa zagotovijo močno kibernetsko varnost in popolno skladnost z zakonodajo o varstvu podatkov in zasebnosti, ne da bi pri tem ogrozili šifriranje.

Da bi bil okvir hrambe podatkov tako zdaj kot v prihodnosti učinkovit, bi morale minimalne zahteve za hrambo posebnih kategorij podatkov veljati (in biti izvršljive) za vse (sedanji ali prihodnji) gospodarske subjekte, ki zagotavljajo elektronske komunikacijske storitve. Da bi upoštevali prihodnji tehnološki razvoj, bi morali subjekti, za katere veljajo obveznosti hrambe podatkov, vključevati ponudnike telekomunikacijskih storitev, OTT-ponudnike in druge operaterje, ki zbirajo podatke, povezane z določeno fizično ali pravno osebo, ki uporablja njihovo storitev, kot so proizvajalci avtomobilov ali umetnointeligenčni sistemi velikega jezikovnega modela. Te obveznosti morajo biti izvršljive in obstajati mora odgovornost ponudnikov; to bi lahko dosegli z različnimi rešitvami, ki bi lahko vključevale tržne ovire (dovoljenja za delovanje) in upravne sankcije.

---

[76] Sodišče je v nedavni zadevi Hadopi ugotovilo, da je zasebnost mogoče zagotoviti s kombinacijo hrambe in dostopa.

[77] Glej oddelek I.

Sistem izvršljivih sankcij za nesodelujoče ponudnike in ponudnike, ki gostijo nezakonite storitve, je bistven vidik vsakega prihodnjega okvira EU. Glede na interakcijo med tem posebnim vidikom in možnimi rešitvami, obravnavanimi v kontekstu zakonitega prestrezanja, je treba o sankcijah razpravljati na naslednjem sestanku o zakonitem prestrezanju.

Večina ponudnikov bi obveznost hrambe in zagotavljanja podatkov izpolnila predvsem s tehničnim izvajanjem (tj. dajanjem podatkov, zbranih ali obdelanih za poslovne namene, na voljo pristojnim organom), ponudnikom, ki trenutno ne registrirajo svojih uporabnikov, ker to za njihov posel ni potrebno (kot so OTT-ponudniki), pa bi s tem samodejno naložili postopke registracije uporabnikov. Po mnenju strokovnjakov skupine na visoki ravni so tovrstne obveznosti pozitivne glede na razprave o potrebnem povečanju **preglednosti in odgovornosti** ponudnikov v zvezi s podatki, ki jih zbirajo in shranjujejo, ter trajanjem njihove hrambe. Obstoječe obveznosti za kategorizacijo v okviru drugih instrumentov (splošna uredba o varstvu podatkov) lahko zagotovijo vpogled v podatke, ki jih obdelujejo ti ponudniki.

Ključni ukrep: Strokovnjaki skupine na visoki ravni pozivajo k novemu okviru EU za hrambo podatkov in dostop do njih

Akterji: Evropska komisija, Svet, Evropski parlament

Časovni okvir: 2025–2026

- Strokovnjaki skupine na visoki ravni pozivajo **Evropsko komisijo**, naj začne postopek za oceno učinka, da bi ocenila različne možnosti za okrepitev zmogljivosti pristojnih organov za učinkovito preiskovanje in pregon kaznivih dejanj z dostopom do zgodovinskih metapodatkov, ki jih ustvarijo in hranijo ponudniki komunikacij. Ocena učinka bi morala zajemati tudi zahteve glede subsidiarnosti, učinek na temeljne pravice in notranji trg ter povezavo z drugimi obstoječimi pravnimi instrumenti. Služiti bi morala kot podlaga za zakonodajni predlog, ki naj bi bil sprejet po rednem zakonodajnem postopku.

Poglavje III: Zakonito prestrezanje

KAKŠNE SO TEŽAVE?

„Zakonito prestrezanje komunikacij“ se nanaša na tretjo osebo – organ ali drug subjekt, pooblaščen z zakonom ali na njegovi podlagi –, ki pridobi prikrit dostop do podatkov iz sumljive komunikacije. Medtem ko je bilo zakonito prestrezanje v preteklosti relevantno zlasti za telefonske klice, vse pogostejše prehajanje s tradicionalnih govornih klicev na storitve sporočanja in druge oblike elektronskih komunikacij prinaša nove izzive.

V EZEK je to prehajanje priznano, hkrati pa je tisti del pravnega okvira, ki se uporablja za tradicionalne telekomunikacije, razširjen na podjetja, ki ponujajo internetne storitve, vključno z medosebnimi komunikacijskimi storitvami, neodvisnimi od številke (NI-ICS), prek telekomunikacijske infrastrukture, ki je nimajo v lasti oziroma je ne upravljajo. V praksi to pomeni, da se lahko za ponudnike NI-ICS uporablja isti pravni okvir, kot se je uporabljal za tradicionalne telekomunikacijske operaterje, tudi ko gre za zakonito prestrezanje. Države članice lahko zahtevajo, da operaterji nacionalnim pristojnim organom dovolijo zakonito prestrezanje elektronskih komunikacij v skladu z Uredbo (EU) 2016/679 in Direktivo 2002/58/ES, ki vsebujeta določbe o zaupnosti komunikacij in izjeme od njih. Na podlagi režima splošne odobritve v okviru EZEK lahko to zahtevo formulirajo tudi na novo.

Ni nujno, da se zakonit dostop opravi na ravni omrežja, kot je nekdaj veljalo za tradicionalne telefonske klice in besedilna (SMS) sporočila, temveč se lahko opravi tudi na napravi uporabnika (preden so informacije poslane) ali na ravni destinacije (npr. ko se sporočila shranijo v oblaku). V tem poročilu zakonito prestrezanje zajema te tri primere uporabe in zadeva podatke, do katerih se dostopa v realnem času ali z le malo zamude.

Razlikovati je treba med tehnologijami prestrezanja, ki jih **uporablja komunikacijski operater**, in tehnologijami, ki jih lahko avtonomno uporabljajo organi odkrivanja in pregona. V opredelitev pojma „zakonito prestrezanje“ v standardih ETSI je vključeno le prvo prestrezanje [v tem poročilu imenovano „**prestrezanje na ravni operaterja**“], ki zahteva, da komunikacijski operater namesti tehnične sisteme za zbiranje prestreženih podatkov in njihovo posredovanje organom prosilcem“. Slednje [v tem poročilu imenovano „**taktično prestrezanje**“] se nanaša na orodja, ki ne zahtevajo trajne fizične namestitve na omrežju, denimo IMSI lovilce[78] ali programsko opremo za prestrezanje podatkov na pametnih telefonih. Navedeni primeri uporabe implicirajo drugačne stopnje invazivnosti in izzive drugačne narave ter ne spadajo v isto pravno ureditev.

Čeprav je zakonito prestrezanje tradicionalnih telekomunikacij še vedno bistveno orodje v številnih preiskavah[79], se je učinkovitost tega ukrepa drastično zmanjšala, saj telekomunikacijske storitve zdaj večinoma zagotavljajo drugi akterji: iz različnih virov je razvidno, da se približno 97 % vseh mobilnih sporočil danes pošilja prek aplikacij za pošiljanje sporočil, kot so WhatsApp, Facebook Messenger in WeChat, medtem ko tradicionalna sporočila SMS in MMS predstavljajo le približno 3 % sporočil. Poleg tega je bilo v letu 2023 več kot 90 % OTT-komunikacij izvedenih prek storitev, šifriranih od konca do konca[80].

Strokovnjaki so si enotni glede naslednjih trendov: najprej so storilci kaznivih dejanj začeli prehajati s tradicionalnih komunikacijskih operaterjev na osrednje OTT-ponudnike, nato so glavni med njimi postopoma začeli uporabljati namenska kriminalna omrežja (kot sta Encrochat in Sky ECC), od leta 2020 naprej, tj. po ukinitvi večjih šifriranih kriminalnih komunikacijskih omrežij, pa se številni odločajo za vrnitev na redne OTT, šifrirane od konca do konca.

---

78 IMSI lovilci so nadzorne naprave, ki posnemajo telekomunikacijske stolpe za prestrezanje signalov mobilnih telefonov, in sicer z zajemanjem številk mednarodnih identitet mobilnih naročnikov (IMSI) in komunikacijskih podatkov.

79 V zadnjih letih se število zahtev za zakonito prestrezanje v Evropi močno in stalno povečuje. Takih zahtev je zlasti veliko v državah, kot so Nemčija, Francija in Združeno kraljestvo, pri čemer še posebej izstopa Nemčija. Tako je npr. Deutsche Telekom leta 2023 poročal o več kot 31 000 zahtevah za prestrezanje, kar je več kot leta 2022, ko jih je bilo približno 26 000 (https://www.telekom.com/en/company/data-privacy-and-security/news/germany-363566).

80 Vira: Comparitech in Statista.

V zvezi s tem se ponudniki komunikacij pri odzivanju na zahteve za zakonito prestrezanje soočajo s takimi izzivi, da le stežka izpolnijo bistvene zahteve zakonitega prestrezanja, kot so opredeljene v Budimpeški konvenciji o kibernetski kriminaliteti[81]. Zato je operativna vrednost tradicionalnega zakonitega prestrezanja pogosto omejena na taktične vpoglede, kot so ugotavljanje, ali je naprava vklopljena ali izklopljena, lokacija omrežne antene ali kdo je povezan s kom; vendar zakonito prestrezanje podatkov o vsebini, poslanih prek ponudnikov OTT-storitev, najpogosteje ni mogoče.

Zato organi odkrivanja in pregona pogosto ne morejo dostopati do ciljnih komunikacij in prebrati njihove vsebine[82] niti razumeti, kdo uporablja določeno internetno storitev v realnem času, ali filtrirati ustreznih informacij. Ta pomembna izguba dostopa do podatkov v tranzitu vpliva na preiskave na več načinov:

- velike težave pri preprečevanju kaznivih dejanj, evidentiranju kriminalnih združb in pripisovanju kriminalnih dejavnosti, storjenih na spletu ali zunaj njega;
- večja uporaba tako imenovanih posebnih tehnik[83], ki so pogosto invazivnejše in za uradnike veliko nevarnejše, s strani organov odkrivanja in pregona, npr. kadar pravosodni organ predpiše namestitev kamer ali mikrofonov blizu tarče;
- večja uporaba preiskovalnih tehnik, ki so manj ciljno usmerjene, s strani organov odkrivanja in pregona: če nimajo dostopa do vsebine komunikacij ali natančnih podatkov o geolokaciji, morajo preiskovalci pogosto preiskati **vse** osebe, povezane s posameznikom, osumljenim kriminalnih dejavnosti.

Glede na navedeno so strokovnjaki skupine na visoki ravni opozorili na štiri ključne kategorije izzivov:

---

81 https://rm.coe.int/1680081561 [člena 20 in 21].

82 En strokovnjak je navedel, da podatki o vsebini prek tradicionalnega zakonitega prestrezanja v 99 % zadev niso na voljo.

83 Tako imenovane posebne tehnike zajemajo vrsto taktičnih sredstev za pridobivanje informacij o operativno zanimivi tarči s kamerami, mikrofoni, daljinskim dostopom na napravah, sledilniki GPS itd.

I. Zakonito prestrezanje komunikacij, ki potekajo prek netradicionalnih ponudnikov komunikacij

Večina držav članic je uvedla tako ali drugačno obliko regulacije, s katero se ureja zakonito prestrezanje, in za ponudnike komunikacijskih storitev določila obveznosti uporabe zmogljivosti za prestrezanje[84]. Čeprav se pogoji za izdajanje odredb o zakonitem prestrezanju med državami zelo razlikujejo, so obveznosti, ki veljajo za operaterje, pogosto podobne[85]: zmožni morajo biti neprekinjeno prestrezati vse relevantne komunikacije določene tarče na državnih tleh, poleg tega pa morajo zagotavljati infrastrukturo, potrebno za zbiranje in posredovanje prestreženih podatkov organom odkrivanja in pregona.

Kadar operaterji telekomunikacijskih omrežij (ponudniki komunikacij, ki so lastniki omrežja in lahko dostopajo do njegove infrastrukture) zagotavljajo tudi komunikacijske storitve (telefonske klice, sporočila SMS itd.), so najpogosteje zmožni izpolnjevati obveznosti zakonitega prestrezanja[86]. V večini primerov gradijo na standardih ETSI, pri obvladovanju lastnih omejitev, vključno s stroškovno učinkovitostjo, minimalnim vplivom na omrežno infrastrukturo, interoperabilnostjo, zanesljivostjo in varnostjo, pa se opirajo na ponudnike specializirane tehnologije.

Pri OTT-storitvah je situacija kompleksnejša: zakonito prestrezanje lahko izvajajo bodisi operaterji telekomunikacijskih omrežij ali OTT-ponudnik, ki storitev opravlja.

Kadar se prestrezanje komunikacij prek OTT-storitev izvaja na ravni telekomunikacijskega omrežja, je njegova učinkovitost pogosto omejena. Prvič, operater morda ne bo mogel identificirati tarčinih komunikacij (npr. pri povezovanju prek javnega brezžičnega omrežja). Poleg tega OTT-storitve pogosto uporabljajo lastniške protokole, ki jih je treba dekodirati s sistemi za zakonito prestrezanje, kar proces podraži, podaljša in dodatno zaplete. In nenazadnje, uporaba šifriranja od konca do konca s strani OTT-ponudnikov močno otežuje dostop do podatkov o vsebini in vse bolj preprečuje dostop do metapodatkov, saj velika večina držav meni, da obveznost operaterjev telekomunikacijskih omrežij, da zagotavljajo nekodirane informacije, preneha obstajati, kadar šifriranje izvaja tretja oseba, v skladu z Budimpeško konvencijo.

---

84 Glej „*Lawful interception – A market access barrier in the European Union*“ (Zakonito prestrezanje – ovira za dostop na trg v Evropski uniji), Vadim Doronin v reviji Computer Law & Security Review (št. 51, 2023, članek 105867).

85 Čeprav obstajajo razlike, kar zadeva obveznosti v zvezi s podatki o vsebini ali z nevsebinskimi podatki.

86 Čeprav lahko funkcije, kot so usmerjanje v domača omrežja („Home Routing“), rezinjenje („slicing“) ali bogate komunikacijske storitve („Rich Communication Services“ – RCS), ovirajo zmožnost operaterjev telekomunikacijskih omrežij, da izpolnjujejo svoje obveznosti (glej razdelek o tehnoloških izzivih).

Opredelitev pojma „elektronske komunikacijske storitve“, ki od leta 2018 vključuje tudi NI-ICS, iz EZEK se uporablja kot sklicevanje v členu 5(1) Direktive o zasebnosti in elektronskih komunikacijah. To pa pomeni, da zdaj širši koncept elektronskih komunikacijskih storitev (v primerjavi s trenutkom, ko je bila sprejeta Direktiva o zasebnosti in elektronskih komunikacijah) državam članicam omogoča, da se pri izvajanju zakonitega prestrezanja opirajo neposredno na OTT-ponudnike[87]. Države članice so to možnost doslej koristile neenakomerno, pri čemer so nekatere uvedle podobne obveznosti za vse vrste ponudnikov elektronskih komunikacijskih storitev, vključno z OTT-ponudniki, medtem ko druge OTT-ponudnike izključujejo[88]. **V praksi osrednji ponudniki OTT-storitev ne glede na obstoječe obveznosti niso razvili tehničnih mehanizmov za odzivanje na zahteve organov držav članic EU za zakonito prestrezanje**, zlasti iz pravnih razlogov[89].

Nasprotno pa je Združeno kraljestvo v skladu z zakonom o preiskovalnih pooblastilih vzpostavilo okvir za zakonito prestrezanje OTT-komunikacij, ki se zaradi sprejetja sporazuma med Združenim kraljestvom in ZDA o dostopu do podatkov uporablja tudi za ponudnike OTT-storitev s sedežem v ZDA. Po mnenju ustreznih organov Združenega kraljestva to pomembno prispeva k preprečevanju in preiskovanju kaznivih dejanj.

In nenazadnje, strokovnjaki iz nacionalnih organov so pojasnili, da taktično prestrezanje, ki temelji na izkoriščanju ranljivosti, ni niti učinkovita niti zaželena alternativa izvršljivim pravilom o zakonitem prestrezanju, ki se uporabljajo za OTT-ponudnike, in bi moralo biti omejeno na specifične zadeve, pri čemer bi morala biti vzpostavljena močna jamstva, opredeljena v nacionalni zakonodaji, da se zagotovi sorazmernost.

---

87 Čeprav še vedno potekajo razprave o natančnem področju uporabe in se razlage med državami članicami razlikujejo.

88 Glej „*Lawful interception – A market access barrier in the European Union*“ (Zakonito prestrezanje – ovira za dostop na trg v Evropski uniji), Vadim Doronin v reviji Computer Law & Security Review (št. 51, 2023, članek 105867).

89 To ni podprto s statističnimi podatki, saj nacionalni organi zahteve za zakonito prestrezanje zelo redko pošiljajo OTT-ponudnikom, dobro zavedajoč se, da to verjetno ne bo prineslo rezultatov.

II. Čezmejne zahteve

Čezmejne zahteve za zakonito prestrezanje, naslovljene na ponudnike OTT-storitev in – v manjši meri – na tradicionalne ponudnike komunikacijskih storitev, za organe odkrivanja in pregona predstavljajo več izzivov.

Kar zadeva tradicionalne ponudnike komunikacijskih storitev, se organi soočajo predvsem z organizacijskimi izzivi. Prvič, instrumenti mednarodnega sodelovanja, zlasti mehanizmi medsebojne pravne pomoči, so lahko nepraktični za nujna prestrezanja, ki jih je treba odobriti in izvesti v nekaj urah in ne dneh ali tednih[90]. Razlog za to je število ukrepov, ki jih je treba sprejeti za zagotovitev skladnosti z zakonodajo tako v državi članici prosilki kot v državi članici prejemnici. Splošno mnenje je, da je postopek medsebojne pravne pomoči, kadar se uporablja za zakonito prestrezanje, neučinkovit in obremenjujoč. Evropski preiskovalni nalog (EPN), ki se je začel uporabljati leta 2017, je nadomestil tradicionalne postopke medsebojne pravne pomoči v EU[91], pri čemer so bili določeni strogi roki[92] za zbiranje zahtevanih dokazov, omejeni razlogi za zavrnitev takih zahtev in uveden enoten standardni obrazec, na podlagi katerega lahko organi zaprosijo za pomoč pri pridobivanju dokazov. Poleg tega, kadar za izvedbo prestrezanja ni potrebna tehnična pomoč države članice, v kateri se nahaja oseba, katere komunikacije se prestrezajo, je ta država članica o prestrezanju uradno obveščena s standardnim obrazcem in ima možnost, da v 96 urah temu ugovarja. Sodišče Evropske unije je v prelomni zadevi C-670/22 sprejelo širok koncept „prestrezanja telekomunikacij“, pri čemer je menilo, da je „prestrezanje telekomunikacij“ prikrit poseg v terminalske naprave za namene zbiranja podatkov o prometu, lokaciji in komunikaciji iz internetne komunikacijske storitve. Strokovnjaki kljub temu menijo, da sicer pomembne izboljšave, ki jih je prinesel EPN, ne zadoščajo za izpolnitev potrebe po hitrem in harmoniziranem čezmejnem dostopu do podatkov v gibanju.

Poleg tega so organi držav članic poročali, da obstoječa tehnična arhitektura pogosto ni primerna za namen izvajanja zakonitega prestrezanja v eni državi članici in prenosa podatkov v skoraj realnem času v drugo državo članico. V nekaterih primerih, kadar so vzpostavljeni ustrezni organizacijski protokoli, količina podatkov, ki jih je treba prenesti, preprosto ni združljiva s pasovno širino, ki je na voljo prek varnih komunikacijskih kanalov.

---

[90] Strokovnjaki so omenili zadeve, ki so se končale še pred uspešno izvedbo čezmejnega zakonitega prestrezanja, ali zadeve, v katerih je bil zaostanek v zvezi z medsebojno pravno pomočjo večji od osmih mesecev.

[91] Razen na Danskem in Irskem, kjer se EPN ne uporablja.

[92] 30 dni za priznanje EPN in dodatnih 90 dni za njegovo izvršitev.

Prestrezanje OTT-komunikacij prinaša kompleksne težave v zvezi s pristojnostjo v primerjavi s prestrezanjem telefonskih komunikacij, kjer ponudniki svoje storitve ponujajo na natančno določenem ozemlju. Tradicionalne telekomunikacijske storitve so vezane na specifično fizično omrežno infrastrukturo, kar zagotavlja, da ima ponudnik storitev tako zmogljivosti kot pravno prisotnost v državi, v kateri pride do prestrezanja. Ta lokalizirana ureditev zmanjšuje tveganje pravnih sporov znotraj EU in poenostavlja skladnost.

Nasprotno pa lahko v primeru OTT-storitev organ prosilec, tarča prestrezanja, fizična izvedba in sedež podjetja obsegajo več različnih jurisdikcij. Medsebojni vpliv pravnih okvirov v teh jurisdikcijah bi lahko povzročil kolizijo zakonov[93].

Za strokovnjake iz policijskih in pravosodnih organov ni nobenega dvoma: izvajanje zahtev za zakonito prestrezanje prek mednarodnih instrumentov ni izvedljiva rešitev. Če organi odkrivanja in pregona zaobidejo postopek medsebojne pravne pomoči in namesto tega vročajo naloge neposredno ponudnikom storitev v skladu s svojo notranjo zakonodajo, so lahko OTT-ponudniki, kot so Microsoft, META ali Google, soočeni z nasprotujočimi si pravnimi zahtevami. V številnih primerih bi imela npr. država članica prosilka pravila, ki urejajo zakonit dostop in so v nasprotju z irskim pravom[94], ki ureja več glavnih OTT-ponudnikov, saj imajo sedež na Irskem, hkrati pa jih lahko ureja tudi notranje pravo v državah članicah, v katerih zagotavljajo storitve.

Te izzive je mogoče učinkovito reševati s skupnimi ukrepi in z določeno stopnjo harmonizacije pravil o zakonitem prestrezanju na ravni EU, da bi olajšali in pospešili čezmejne zahteve za zakonito prestrezanje. To bi bil predpogoj za obravnavo drugih organizacijskih in tehničnih izzivov, za katere je mogoče najti rešitve, kadar so pravila jasno določena in izvedljiva.

---

93 Glej „*LE interception concerns under the EECC*“ (Vprašanja v zvezi s prestrezanjem v okviru odkrivanja in pregona v skladu z EZEK), Microsoft, januar 2020.

94 Irska zakonodaja OTT-ponudnikom prepoveduje prestrezanje v živo.

III. Tehnologija

Razvoj komunikacijskih tehnologij – ne glede na pravne vidike – vpliva na tehnično zmožnost organov odkrivanja in pregona za prestrezanje komunikacij prek storitev, ki jih neposredno zagotavljajo ponudniki komunikacijskih storitev ali ponudniki OTT-storitev.

Za tradicionalne ponudnike komunikacij zmogljivosti za zakonito prestrezanje običajno razvijejo ponudniki tehnologije na podlagi standardov ETSI in so vključene v 3GPP[95]. Zato lahko dobro opremljene policijske službe zadovoljivo prestrezajo tradicionalne komunikacije (govorna sporočila in sporočila SMS), potencialno pa lahko prestrežejo tudi internetne komunikacije prek storitev, ki se zagotavljajo prek njihovih omrežij.

Vendar vse večja kompleksnost komunikacijske infrastrukture in protokolov 5G, kot so virtualizacija, omrežno rezinjenje, računalništvo na robu in funkcije za boljše varovanje zasebnosti, predstavlja nove tehnološke izzive za tradicionalne operaterje[96]. Strokovnjaki skupine na visoki ravni so omenjali zlasti izzive, povezane z usmerjanjem v domača omrežja[97] in z RCS[98].

Strokovnjaki skupine na visoki ravni – iz zornega kota, usmerjenega v prihodnost, in na podlagi izkušenj z omrežjem 5G – pričakujejo izzive v povezavi s prihodnjo uvedbo omrežja 6G (predvideni po letu 2030), ki bo šlo še korak dlje, kar zadeva funkcije za boljše varovanje zasebnosti[99], in bo morda standardno vključevalo šifriranje od konca do konca, zaradi vsega navedenega pa bi lahko bilo prestrezanje težavnejše. Obenem nove komunikacijske tehnologije, kot so internet stvari, satelitske komunikacije in razvoj kvantnega računalništva[100], s seboj prinašajo dodatne izzive, ki jih je treba predvideti.

---

95 *Third Generation Partnership Project* (partnerski projekt tretje generacije), ki je temelj za razvoj komunikacijskih tehnologij, kot so 5G, internet stvari in mobilne širokopasovne povezave.

96 Glej „*Law enforcement and judicial aspects related to 5G*“ (Odkrivanje in pregon ter pravosodni vidiki, povezani s 5G), koordinator EU za boj proti terorizmu, 2019 (https://data.consilium.europa.eu/doc/document/ST-8983-2019-INIT/en/pdf).

97 Europol - Position paper on Home routing.pdf (*Europol – Dokument o stališču glede usmerjanja v domača omrežja.pdf*) (europa.eu).

98 Protokol RCS omogoča izmenjavo skupinskih klepetov, video- in avdioposnetkov in slik visoke ločljivosti; pogosto se uporablja namesto sporočil SMS. Zakonito prestrezanje sporočil RCS je – odvisno od njegove izvedbe – morda nemogoče, kar znatno vpliva na odkrivanje in pregon (v letu 2023 je imel RCS več kot eno milijardo aktivnih uporabnikov).

99 Glej časovni načrt za omrežje 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* (Druga kvantna revolucija: vpliv kvantnega računalništva in kvantnih tehnologij na odkrivanje in pregon) | Europol (europa.eu).

In nenazadnje, strokovnjaki skupine na visoki ravni so poudarili, da eden od glavnih tehničnih izzivov, s katerimi se soočajo organi odkrivanja in pregona, izhaja iz šifriranja od konca do konca, zlasti za OTT-komunikacije, saj več kot 80 % komunikacij poteka prek storitev, šifriranih od konca do konca (komunikacije v živo in shranjevanje varnostnih kopij), kar preiskovalcem preprečuje dostop do vsebine komunikacij. Hkrati se strokovnjaki strinjajo, da šifriranje od konca do konca velja za robusten varnostni ukrep, ki državljane učinkovito ščiti pred različnimi oblikami kriminala. Z zagotavljanjem, da lahko samo uporabniki, ki komunicirajo, dostopajo do vsebine svojih sporočil, šifriranje od konca do konca učinkovito ščiti pred nezakonitim prisluškovanjem, krajo podatkov, vohunjenjem ob podpori države in drugimi oblikami nedovoljenega dostopa hekerjev, storilcev kaznivih dejanj kibernetske kriminalitete ali celo samih ponudnikov storitev.

Težko je količinsko opredeliti izzive, s katerimi se organi odkrivanja in pregona soočajo pri spremljanju komunikacij storilcev kaznivih dejanj in teroristov, ki uporabljajo šifriranje od konca do konca. Organi odkrivanja in pregona se namreč pogosto odločijo, da ne bodo namenili časa in sredstev za pridobitev sodnih odločb za elektronski nadzor na platformah, za katere je znano, da privzeto uporabljajo šifriranje od konca do konca[101]; zato je število uspešnih zahtev za zakonito prestrezanje podatkov o vsebini, ki jih ni mogoče izvesti zaradi šifriranja od konca do konca, zelo majhno in ni pomenljivo. Organi odkrivanja in pregona menijo, da je to pomanjkanje zmogljivosti za nadzor precejšnja šibka točka in ranljivost, ki se ju storilci kaznivih dejanj in teroristi dobro zavedajo in ju tudi dejavno izkoriščajo, kot se je pokazalo v zadevah EncroChat[102] in Sky ECC, v katerih je prišlo do več tisoč aretacij po vsej Evropi, tudi številnih vidnih storilcev kaznivih dejanj. Na ta pomislek so v več izjavah med drugim spomnili tudi evropski policijski načelniki[103] in skupina G7[104]. Strokovnjaki so, da bi ponazorili vpliv izgube dostopa do podatkov o vsebini, navedli več javnih primerov, med drugim primerov terorizma[105], nedovoljenega prometa s prepovedanimi drogami[106] in posilstva[107], pri katerih je šifriranje bistveno oviralo zmožnost organov odkrivanja in pregona za preprečevanje hudih kaznivih dejanj in organiziranega kriminala ter boj proti njim.

Predstavniki organov odkrivanja in pregona se zavzemajo za pristop, ki od podjetij zahteva, da organom odkrivanja in pregona zagotovijo dostop do nekodiranih podatkov pod strogimi pogoji. Ob tem je treba opozoriti, da so strokovnjaki za kibernetsko varnost izrazili zaskrbljenost, da bi take rešitve ogrozile kibernetsko varnost. Nekateri strokovnjaki s področja odkrivanja in pregona so navedli, da je v nekaterih primerih šifriranje izvedeno na način, ki je združljiv tako s kibernetsko varnostjo kot s potrebo po ohranitvi nekaterih storitev, kot so posodobitve operacijskih sistemov, skeniranje vsebine (npr. elektronskih sporočil ali spletnih sej) za namene kibernetske varnosti ali ključni obnovitveni mehanizmi, kadar se uporabnik odloči za to funkcijo.

---

101 Manpearl, 2017.

102 Za več informacij o EncroChat in Sky ECC glej Europol in Eurojust, „*Third Report of the Observatory Function on Encryption*“ (Tretje poročilo opazovalne funkcije za šifriranje), junij 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 Marca 2017 je 52-letni Khalid Masood v centru Londona izvedel teroristično napad, katerega motiv je bil povezan z islamizmom in v katerem je umrlo šest ljudi, 29 pa jih je bilo ranjenih. Čeprav je bilo iz poročil o incidentu mogoče razumeti, da je Masood napad načrtoval in izvedel sam, je bilo ugotovljeno, da je le nekaj minut pred napadom velikemu številu svojih stikov na aplikacijah WhatsApp in iMessage, ki sta bili – in sta še vedno – privzeto šifrirani od konca do konca, poslal dokument v formatu PDF z naslovom „*Jihad*“ (Džihad). Vira: Max Hill, „*The Westminster Bridge Terrorist Attack*“ (Teroristični napad na Westminstrskem mostu) (London: The Stationery Office, 2018); BBC News, „*WhatsApp Must Not Be a ‚Place for Terrorists to Hide*“‘ (WhatsApp ne sme biti ‚mesto, kjer se skrivajo teroristi‘), 26. marec 2017.

106 Strokovnjaki so omenili večje primere nedovoljenega prometa s prepovedanimi drogami, pri katerih ni bilo mogoče doseči napredka, dokler ni bil pridobljen dostop do šifrirane komunikacije prek storitev Encrochat in Sky ECC.

107 V odmevni zadevi v Združenem kraljestvu so bile policijske preiskave primera posilstva ovirane, ker so osumljenci za komunikacijo uporabljali WhatsApp, šifriranje od konca do konca pa je otežilo dostop do ključnih dokazov. Preiskava je bila ovirana zaradi nezmožnosti organov odkrivanja in pregona, da sporočila, poslana z aplikacijo WhatsApp, dešifrirajo brez privolitve uporabnika.

Na podlagi tega so se strokovnjaki s področja odkrivanja in pregona strinjali, da izzivi, ki jih prinaša šifriranje, zahtevajo večplasten pristop, ki ohranja ravnotežje med pravicami do zasebnosti, varnostjo in potrebo po tem, da imajo organi odkrivanja in pregona dostop do podatkov zaradi boja proti kriminalu ter zaščite življenj, telesne celovitosti in premoženja ljudi. Malo je verjetno, da bi enotna rešitev naslovila vse zadevne pomisleke, zato pa bi lahko težavo pomagala ublažiti kombinacija pristopov.

IV. Ponudniki komunikacij kazenske narave

Storilci kaznivih dejanj za prikrivanje svojih komunikacij uporabljajo osrednje platforme, šifrirane od konca do konca; lahko pa se odločijo tudi za uporabo varnih komunikacijskih kanalov, posebej zasnovanih za kriminalno dejavnost (imenovanih „CCC“ za „criminal communication channels“ (kriminalni komunikacijski kanali))[108]. Tako EncroChat kot Sky ECC sta dobro znana kriminalna komunikacijska kanala, prek katerih so prodajali telefone z integrirano storitvijo sporočanja, šifrirano od konca do konca ter prilagojeno za prikrivanje kriminalnih dejavnosti in promovirano na temnem spletu. Obe platformi sta bili v letih 2020 in 2021 ukinjeni zahvaljujoč skupnim mednarodnim operacijam odkrivanja in pregona, ki so razkrile njuno obsežno vpletenost v organizirani kriminal. Ukinjenih je bilo tudi več drugih podobnih platform, kot sta Phantom Secure[109] in Exclu[110], medtem ko številne manjše platforme še vedno delujejo in še naprej predstavljajo varna vozlišča za izmenjavo kriminalnih informacij. V tem razdrobljenem okolju je bistvenega pomena, da so organi odkrivanja in pregona zmožni prepoznati kriminalne komunikacijske kanale, spremljati in blokirati njihovo dejavnost, jih ukiniti ter privesti storilce kaznivih dejanj pred sodišče.

---

[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* (Nov napad na šifrirane kriminalne komunikacije z ukinitvijo orodja Exclu) | Eurojust | Agencija Evropske unije za pravosodno sodelovanje v kazenskih zadevah (europa.eu).

Medtem ko prestrezanje na ravni operaterja za to vrsto nepoštenega ponudnika komunikacij ni mogoče, organi odkrivanja in pregona potrebujejo ustrezne zmogljivosti za taktično prestrezanje (orodja in strokovno znanje), da lahko – šifriranju navkljub – ciljno spremljajo svoje uporabnike. Strokovnjaki s področja odkrivanja in pregona so omenjali pomembne izzive, tveganja in omejitve, povezane z razvojem in uporabo takih tehnik, ki niso skalabilne in bi jih bilo treba ohraniti za najpomembnejše zadeve. Nacionalni organi – odvisno od svojih zmogljivosti in pravnega okvira – uporabljajo različne pristope, vključno z orodji, ki jih razvijejo sami, kupijo od tretjih oseb ali uporabljajo kot storitev; ne glede na to, za katero možnost se odločijo, pa so si strokovnjaki enotni, da so za uporabo takih orodij potrebna jamstva in zaščitni ukrepi. Med drugim bi se lahko razmislilo o boljšem nadzoru, evalvaciji in certificiranju orodij, pa tudi o trdnem okviru za obvladovanje ranljivosti, ob doslednem upoštevanju postopkovne avtonomije držav članic v kazenskih zadevah in njihove izključne pristojnosti na področju nacionalne varnosti.

Preiskovalni organi se soočajo tudi s pravnimi izzivi, kot so težave pri inkriminaciji ponudnikov komunikacij in storitev gostovanja, ki ponujajo predvsem kriminalne storitve (saj je ves promet šifriran), kar je nujen prvi korak pred sprejetjem sodnih ali upravnih ukrepov. Poleg tega morajo imeti države članice možnost, da kriminalnim komunikacijskim kanalom naložijo sankcije, da bi omejile ali blokirale dostop do takih storitev v EU in tako onemogočile njihov kriminalni poslovni model. To bo potrebno, ko in če bodo za OTT-storitve začele veljati obveznosti zakonitega prestrezanja, s čimer bi preprečili vrnitev storilcev kaznivih dejanj k nepoštenim ponudnikom komunikacij.

In nenazadnje, različni vidiki zadev, kot sta tisti proti družbama EncroChat in Sky ECC, se izpodbijajo pred sodišči. Zahteve za uporabo podatkov, prestreženih v drugi državi članici, kot dokazov se po EU zelo razlikujejo, kar povzroča pravno negotovost za podobne operacije, ki jih izvaja ena država članica in bi lahko vplivale na mnoge druge.

MOŽNE REŠITVE

I. Zagotoviti izvršljivost zahtev za zakonito prestrezanje za vse vrste ponudnikov elektronskih komunikacijskih storitev

V EU so zmogljivosti za zakonito prestrezanje omejene na tradicionalne ponudnike komunikacij, medtem ko večina komunikacij trenutno poteka prek netradicionalnih ponudnikov komunikacij[111]. Ne glede na to, ali komunikacijsko storitev zagotavlja lastnik infrastrukture ali ne, bi morala biti zmožnost organov odkrivanja in pregona za zakonito prestrezanje komunikacij operativno zanimive osebe enaka. Alternativne rešitve, kot je izvajanje zakonitega prestrezanja na NI-ICS in drugih komunikacijskih storitvah izključno na ravni telekomunikacijskega omrežja, opiranje na instrumente mednarodnega sodelovanja za izvajanje zakonitega prestrezanja pri ponudnikih NI-ICS ali obsežna uporaba taktičnega prestrezanja, niso izvedljive[112].

Zato strokovnjaki skupine na visoki ravni menijo, da je prednostna naloga zagotoviti, da se obveznosti glede zakonitega prestrezanja razpoložljivih podatkov uporabljajo na enak način za tradicionalne in netradicionalne ponudnike komunikacij ter da so enako izvršljive. Harmonizacija takih obveznosti bi morala biti namenjena premoščanju izzivov, povezanih z izvrševanjem čezmejnih zahtev.

Za dosego tega cilja ter postopen primik k približevanju in harmonizaciji pravil o zakonitem prestrezanju v EU strokovnjaki skupine na visoki ravni predlagajo progresiven pristop: najprej bi se bilo treba dogovoriti o načelih strukturiranja na ravni EU (prvi korak), nato bi morala Komisija podpreti izvajanje teh načel (drugi korak), na koncu pa se lahko načela na podlagi nadaljnje ocene kodificirajo v pravnem instrumentu (tretji korak).

---

111 V Združenem kraljestvu je bilo leta 2022 poslanih 36 milijard sporočil SMS in MMS, medtem ko je bilo spletnih sporočil 1,3 bilijona (*WhatsAppening in the world of online communications?* (Kaj se dogaja v svetu spletnih komunikacij?) – Ofcom).

112 Glej razdelek o izzivih.

Prvi korak: dogovor o skupnem izhodišču

Prvič, oblikovati je treba skupno razumevanje tega, za katere kategorije elektronskih komunikacijskih storitev lahko veljajo domače obveznosti glede zakonitega prestrezanja v skladu s pravili iz Direktive o zasebnosti in elektronskih komunikacijah ter iz splošne uredbe o varstvu podatkov.

Drugič, doseči je treba dogovor o operativnih zahtevah na visoki ravni, v katerem je jasno navedeno, kaj nacionalni organi pričakujejo v smislu zakonitega prestrezanja in kakšni bi morali biti s tem povezani zaščitni ukrepi. LEON[113] je bil opredeljen kot dobra podlaga za opredelitev zahtev odkrivanja in pregona. Temu dokumentu bi morale biti priložene zahteve glede npr. sorazmernosti, nadzora in preglednosti, po možnosti z razlikovanjem med pravili, ki veljajo za podatke o vsebini in nevsebinske podatke, ob doslednem spoštovanju kibernetske varnosti, varstva podatkov in zasebnosti ter brez ogrožanja šifriranja. Z morebitno ustanovitvijo ad hoc skupine strokovnjakov, tudi strokovnjakov za kibernetiko, zasebnost ter odkrivanje in pregon, bi lahko zagotovili, da se zahteve po potrebi posodabljajo, po možnosti na podlagi dela Europolove Delovne skupine za standardizacijo na področju notranje varnosti, ki bi ga bilo treba nadaljevati.

Tretjič, koncept krajevne pristojnosti je treba pojasniti z vidika njegove uporabe za OTT-storitve, pri tem pa upoštevati različne razlage nacionalnih organov, pa tudi – kar je najpomembneje – nacionalnih organov in OTT-ponudnikov. Pojasniti bi bilo treba npr. pravila, ki veljajo za primere, ko je lokacija tarče nejasna. Potrebne so tudi smernice o tem, kdo lahko oceni zakonitost zahteve, npr. glede vloge ponudnikov storitev v tem okviru. In ne nazadnje, čeprav je bila z veliko večino dosedanjih odločb sodišča potrjena zakonitost procesnih dejanj zoper EncroChat in Sky ECC, je več sodnih zadev še vedno v teku[114] in bi lahko pomembno vplivalo na obsodbo vidnih storilcev kaznivih dejanj. Zato bo morda treba olajšati dopustnost dokazov, pridobljenih z ukrepi taktičnega prestrezanja med državami članicami, vzajemnim priznavanjem sodb in sodnih odločb ter policijskim in pravosodnim sodelovanjem v kazenskih zadevah.

---

[113] Dokument LEON (*Law Enforcement – Operational Needs for Lawful Access to Communications* (Odkrivanje in pregon – operativne potrebe po zakonitem dostopu do komunikacij)) je rezultat dela, ki so ga švedski organi odkrivanja in pregona opravili v tesnem sodelovanju s predstavniki organov odkrivanja in pregona iz držav članic EU ter Severne Amerike in Avstralije. Cilj je opredeliti in opisati potrebe organov odkrivanja in pregona po zakonitem dostopu do vsebine komunikacij, podatkov, povezanih z vsebino, in informacij o naročnikih. Glej *Sporočilo predsedstva Sveta o operativnih potrebah organov odkrivanja in pregona po zakonitem dostopu do komunikacij (LEON)*, 6050/23 z dne 16. februarja 2023.

[114] Glej zadeve T-1180/23, T-148/24, T-167/24, T-484/24 in T-560/24.

Sklop priporočil 7

Da bi na ravni EU dosegli dogovor o skupnih načelih za zakonito prestrezanje razpoložljivih podatkov, ki bi veljala za vse vrste ponudnikov elektronskih komunikacijskih storitev, strokovnjaki priporočajo:

1. *pojasnitev opredelitve in področja uporabe zakonitega prestrezanja v skladu z obstoječimi akti EU ter drugimi ustreznimi evropskimi in mednarodnimi instrumenti, kakršen je Budimpeška konvencija o kibernetski kriminaliteti [priporočilo 38];*

2. *opredelitev skupnih operativnih zahtev po zgledu dokumenta LEON [priporočilo 21];*

3. *opredelitev potrebnih zaščitnih ukrepov [priporočilo 17, priporočilo 41];*

4. *takšno obravnavo vidika kibernetske varnosti, da se ponudnikom z nobenim ukrepom ne naloži obveznost prilagoditve njihovih sistemov IKT na način, ki bi negativno vplival na kibernetsko varnost njihovih uporabnikov [priporočilo 41];*

5. *pojasnitev koncepta krajevne pristojnosti za podatke, da se obravnava morebitna kolizija zakonov [priporočilo 39], ter spodbujanje sprejetja minimalnih pravil na ravni EU, ki omogočajo dopustnost dokazov, ki so po potrebi pridobljeni z ukrepi taktičnega prestrezanja med državami članicami, in sicer v obsegu, ki je potreben za lažje vzajemno priznavanje sodb in sodnih odločb ter policijsko in pravosodno sodelovanje v kazenskih zadevah [priporočilo 42].*

Razmisliti je treba o najboljšem pristopu k oblikovanju skupnih načel in dogovarjanju o njih, kot je navedeno v sklopu priporočil 7, ter o opredelitvi najustreznejšega instrumenta za izmenjavo teh načel. Če pogledamo v preteklost, je bila Resolucija Sveta o zakonitem prestrezanju z dne 17. januarja 1995[115] ključnega pomena za lažjo harmonizacijo rešitev za zakonito prestrezanje, saj je zagotovila referenco za standarde za zakonito prestrezanje, ki jih je razvil ETSI. Podoben pristop, po možnosti s priporočilom Komisije ali Sveta, bi lahko bil enako koristen.

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

Ključni ukrep: strokovnjaki skupine na visoki ravni pozivajo EU, naj v letu 2025 izda priporočilo o dostopu do podatkov v realnem času

Časovni okvir: 2025 *Proračun: še ni določen*

- Strokovnjaki skupine na visoki ravni pozivajo Evropsko komisijo, naj izda priporočilo, v katerem bo pojasnjen pojem zakonitega prestrezanja[116] za ponudnike elektronskih komunikacijskih storitev in podrobno opisane različne zahteve, ki lahko veljajo za zakonito prestrezanje razpoložljivih nevsebinskih podatkov in podatkov o vsebini, ob doslednem spoštovanju kibernetske varnosti, varstva podatkov in zasebnosti, brez ogrožanja šifriranja ter na podlagi skupnih operativnih zahtev, kot so opredeljene v dokumentu LEON.

Drugi korak: zagotovitev podpore EU za to, da se zagotovijo enaki konkurenčni pogoji in okrepi čezmejno sodelovanje

Skupna načela, določena v prvem koraku, bi bila podlaga za tehnično, pravno in organizacijsko harmonizacijo na ravni EU. Za njihovo prevedbo v konkretne rezultate sta potrebna usklajevanje in finančna podpora Komisije. Med drugim bi bili potrebni vzpostavitev namenskega procesa, izhajanje iz obstoječih delovnih skupin in po potrebi oblikovanje novih, zagotavljanje usklajevanja z ustreznimi deležniki, vključno z OTT-ponudniki in predstavniki industrije, poročanje ustreznim organom, zlasti Svetu in Evropskemu parlamentu, ter zagotavljanje preglednosti v odnosu do javnosti, morda pa tudi financiranje ciljno usmerjenih študij bodisi neposredno bodisi prek ustreznih partnerstev, npr. z ustreznimi agencijami ali akademskimi partnerji.

[116] Omejeno na prestrezanje na ravni operaterja, kot je opredeljeno zgoraj.

Strokovnjaki skupine na visoki ravni so poudarili tudi, da je poleg zgoraj opisanega dela nujno potrebno tudi izboljšanje učinkovitosti čezmejnih zahtev za zakonito prestrezanje v sedanjem okviru. Ta cilj bi med drugim vključeval:

- oceno sedanjih omejitev EPN[117] in prizadevanja za izboljšanje operativne učinkovitosti;
- obravnavo tehničnih in organizacijskih omejitev, ki se nanašajo na čezmejno izmenjavo dokazov, zbranih z zakonitim prestrezanjem, zaradi česar bi bilo posledično potrebno nadaljnje delo, kar zadeva:
    - evidentiranje problema (katere so omejitve, katere države članice se z njimi srečujejo itn.),
    - standardizacijo podatkovnih struktur, mehanizmov zaupanja in filtriranja podatkov, da se prepreči prenos nerelevantnih podatkov in podpirajo načela varstva podatkov glede omejitve namena, sorazmernosti in najmanjšega obsega podatkov,
    - zasnovo in zmogljivost čezmejnih načinov prenosa,
    - opredelitev s tem povezanih shem financiranja;
- olajševanje čezmejnih zahtev za zakonito prestrezanje z določitvijo in usposabljanjem enotnih kontaktnih točk ob usklajevanju s širšim delom v zvezi s enotnimi kontaktnimi točkami in dostopom do digitalnih dokazov, pri čemer ima pomembno vlogo projekt SIRIUS;
- spodbujanje dvostranskih sporazumov med državami članicami in ZDA, kjer je ustrezno, kot predpogoja za olajšanje neposrednih zahtev nacionalnih organov osrednjim ponudnikom OTT-storitev, saj področje uporabe sporazuma med EU in ZDA o čezmejnem dostopu do elektronskih dokazov, o katerem trenutno potekajo pogajanja, v skladu s pogajalskimi smernicami ne zajema zakonitega prestrezanja, kar pomeni, da so za obravnavo kolizije zakonov potrebni posebni sporazumi.

[117] Direktiva Evropskega parlamenta in Sveta 2014/41/EU z dne 3. aprila 2014 o evropskem preiskovalnem nalogu v kazenskih zadevah (v nadaljnjem besedilu: direktiva o EPN) se nanaša na „telekomunikacije“; čeprav večina držav članic EPN razlaga širše, v skladu s posodobitvijo EZEK, bi lahko preučili in dodatno ocenili morebitno potrebo po njegovi spremembi v tej zvezi.

In nenazadnje, strokovnjaki so pozvali k razmisleku o ukrepih, s katerimi bi lahko izboljšali odvračilne ukrepe, ki jih nacionalni organi sprejmejo proti nekooperativnim ponudnikom elektronskih komunikacijskih storitev. Še posebej so pozvali k oceni izvedljivosti in sorazmernosti možnih tehničnih rešitev.

Sklop priporočil 8

Da bi zagotovili, da se na zahteve za zakonito prestrezanje, kot so določene v nacionalni zakonodaji, odzove širok nabor ponudnikov elektronskih komunikacijskih storitev, vključno z OTT-ponudniki, strokovnjaki priporočajo:

1. *podporo izvajanju načel, opredeljenih v priporočilu 1.1, z usklajevanjem in financiranjem;*
2. *preučitev, kako bi lahko z EPN bolje podprli čezmejne zahteve za učinkovito zakonito prestrezanje, npr. z izboljšanjem pravne varnosti, skrajšanjem rokov za odzivanje na naloge in spodbujanjem enotne uporabe EPN [priporočilo 40];*
3. *vzpostavitev mehanizmov (interoperabilnost in kibernetska varnost) in infrastruktur (pasovna širina in skalabilnost), ki so združljivi s čezmejnim prenosom velikih naborov podatkov v realnem času [priporočilo 9];*
4. *spodbujanje določitve enotnih kontaktnih točk v EU za obravnavo zahtev javnih organov in za stike z njimi, da se olajša izvrševanje obveznosti v zvezi z zakonitim prestrezanjem in vzpostavijo mehanizmi za učinkovito ciljno usmeritev čezmejnih zahtev [priporočili 19 in 36];*
5. *spodbujanje oblikovanja dvostranskih sporazumov s tretjimi državami, zlasti z Združenimi državami, o dostopu do podatkov v realnem času [priporočilo 38.4].*

Uspešno izvajanje priporočila EU o zakonitem prestrezanju bi lahko podprli s številnimi dejavnostmi.

Ključni ukrep: strokovnjaki skupine na visoki ravni pozivajo Komisijo, naj izvajanje priporočila EU o zakonitem prestrezanju spremljata ustrezno usklajevanje in financiranje

- Strokovnjaki skupine na visoki ravni pozivajo Komisijo, naj predlaga jasen načrt za podporo izvajanju priporočila EU o zakonitem prestrezanju, tudi z vidika finančnega načrtovanja.

Tretji korak: ocena možnosti pravnega instrumenta o zakonitem prestrezanju

Sámo usklajevanje se lahko izkaže za nezadostno za dosego potrebne ravni harmonizacije, četudi ga dopolnjujejo ukrepi za povečanje učinkovitosti obstoječih pravnih instrumentov. Morda bo potreben nov sklop pravil za zagotovitev izvršljivosti zahtev in pravne varnosti, za odpravo kolizije zakonov in za zmanjšanje upravnega bremena, povezanega s pregledi skladnosti in zakonitosti. Poleg tega razlike med pravili o zakonitem prestrezanju po EU reguliranim subjektom, kot so OTT-ponudniki, nalagajo obremenjujoče zahteve, kar bi lahko ustvarilo ovire za dostop ponudnikov komunikacij na trg[118]. S tega vidika bi s harmoniziranimi pravili EU o zakonitem prestrezanju razpoložljivih podatkov lažje zgradili prihodnjo evropsko digitalno infrastrukturo, pri čemer bi dali prednost modelu, pri katerem telekomunikacijska infrastruktura ponuja potencialno pokritost celotne celine[119].

Prehod na internetne komunikacije je močna spodbuda za določitev harmoniziranih pravil za dostop na ravni EU; vendar bi bilo treba skrbno oceniti sprejemljivost in izvedljivost pravnega instrumenta, pa tudi njegov z industrijo, kibernetsko varnostjo in varnostjo povezan učinek, upoštevaje sedanje razlike med pravnimi ureditvami držav članic na področju zakonitega prestrezanja. Strokovnjaki skupine na visoki ravni so navedli, da bi moral morebitni instrument: (i) biti v skladu z načeli, določenimi v priporočilu 1.1; (ii) v celoti upoštevati vidik temeljnih pravic ter suverenost držav na področjih kazenskih zadev in nacionalne varnosti, obenem pa (iii) se zgledovati po delu, opravljenem v zvezi s svežnjem o elektronskih dokazih.

Strokovnjaki skupine na visoki ravni so se strinjali, da bi morala vsaka pobuda za spodbujanje ali uvedbo pravil o zakonitem prestrezanju vseh vrst elektronskih komunikacijskih storitev vsebovati jasen in izvršljiv okvir za ukrepanje proti ponudnikom komunikacij, ki delujejo nezakonito in/ali zavračajo kakršno koli obliko sodelovanja z organi odkrivanja in pregona. Če takega okvira ne bi bilo, bi bila pravila oslabljena, storilci kaznivih dejanj pa bi svoje komunikacije množično prenesli na ponudnike, ki ne izpolnjujejo zahtev. Pri vsaki prihodnji pobudi EU v zvezi s tem bi bilo treba upoštevati razliko med OTT-ponudniki, ki ne izpolnjujejo svojih pravnih obveznosti, in ponudniki elektronskih komunikacijskih storitev, ki namerno predlagajo storitve, prilagojene kriminalnim dejavnostim. Poleg tega bi bilo treba upoštevati tudi pravni red EU, zlasti akt o digitalnih storitvah.

---

118 Glej „*Lawful interception – A market access barrier in the European Union*“ (Zakonito prestrezanje – ovira za dostop na trg v Evropski uniji), Vadim Doronin v reviji Computer Law & Security Review (št. 51, 2023, članek 105867).

119 *White Paper - How to master Europe's digital infrastructure needs?* (Bela knjiga – Kako obvladati potrebe po digitalni infrastrukturi v Evropi?) | *Shaping Europe's digital future* (Oblikovanje digitalne prihodnosti Evrope) (europa.eu).

Tovrstna pobuda bi lahko zajemala upravne ali sodne ukrepe. Strokovnjaki skupine na visoki ravni so pozvali k poglobljenemu razmisleku o zadevi, v okviru katerega bi obravnavali tako temeljne pravice kot vprašanja kibernetske varnosti ter s tem povezane kompleksne tehnološke izzive.

Sklop priporočil 9

Strokovnjaki na podlagi nadaljnje analize in ocene učinka priporočajo ***zasnovanje instrumenta EU o zakonitem prestrezanju (sestavljenega iz mehkega prava ali zavezujočih pravnih instrumentov) za namene odkrivanja in pregona****, v katerem bi se določile izvršljive obveznosti za ponudnike elektronskih komunikacijskih storitev v EU. Priporočajo še, naj ta morebitni instrument: [priporočilo 38]*

1. *upošteva načela, dogovorjena v sklopu priporočil 7;*
2. *bo tehnološko nevtralen [priporočilo 21];*
3. *spodbuja harmonizacijo ukrepov kazenskega prava, vključno z zaporno kaznijo, na ravni EU zoper nekooperativne ponudnike elektronskih komunikacijskih storitev za uveljavitev sodelovanja [priporočilo 34];*
4. *v celoti upošteva vidik temeljnih pravic ter suverenost držav na področjih kazenskih zadev in nacionalne varnosti [priporočilo 38];*
5. *se zgleduje po delu, opravljenem v okviru sprejetja pravil o elektronskih dokazih [priporočilo 38, točka (iv)];*
6. *naloži obveznosti ponudnikom storitev, da v okviru svojih storitev vklopijo ali izklopijo nekatere funkcije, da bi po prejemu naloga pridobili informacije (npr. shranitev geolokacije določenega uporabnika po tem, ko je bila v zvezi z njim izdana zahteva po zakonitem dostopu) [priporočilo 32];*
7. *vključuje mehanizme za zagotovitev, da lahko države članice izvršujejo sankcije zoper nekooperativne ponudnike elektronskih komunikacijskih storitev (bodisi ukrepe upravnega ali ukrepe kazenskega prava, odvisno od tega, ali je ponudnik zgolj nekooperativen ali ponuja storitev kazenske narave) – v skladu s pravili iz akta o digitalnih storitvah in po možnosti izhajajoč iz njih – ter da take sankcije odvračajo od teh subjektov [priporočilo 33].*

Izvrševanje načel iz priporočila EU o zakonitem prestrezanju bi bil pomemben korak k bolj harmoniziranim in bolj izvršljivim pravilom o zakonitem prestrezanju. Vendar bo morda še vedno potreben pravni instrument, da bi izboljšali pravno varnost in zagotovili, da bi pri izvajanju zakonitega prestrezanja poskrbeli za vzpostavitev potrebnih zaščitnih ukrepov za vse zadevne ponudnike elektronskih komunikacijskih storitev ter da so tisti ponudniki elektronskih komunikacijskih storitev, ki niso pripravljeni izvrševati pravil, ki jih določijo države članice, to primorani storiti.

Ključni ukrep: strokovnjaki skupine na visoki ravni pozivajo Komisijo, naj oceni nadaljnji razvoj zakonodajnega okvira za zakonito prestrezanje za namene odkrivanja in pregona

- Strokovnjaki skupine na visoki ravni pozivajo Evropsko komisijo, naj pred morebitno oceno učinka oceni možnost pravnega instrumenta EU o zakonitem prestrezanju, pri čemer naj izhaja iz dela, opravljenega pri pripravi na uredbo in direktivo EU o elektronskih dokazih, ter se osredotoči na opredelitev morebitnih tehnološko nevtralnih rešitev.

II. Obravnavati tehnološke izzive

Številni izzivi, s katerimi se soočajo organi odkrivanja in pregona v zvezi z dostopom do podatkov, izhajajo iz dejstva, da je težko predvideti tehnološki razvoj in se mu prilagoditi. To je zato, ker organi odkrivanja in pregona v nasprotju z akterji v drugih sektorjih, kot sta obramba ali vesolje, nimajo sredstev ali tesnega odnosa z industrijo, ki jih v ta namen potrebujejo, hkrati pa niso vajeni, da bi to sploh potrebovali. V številnih primerih skušajo akterji na področju notranje varnosti zapolniti tehnološke vrzeli reaktivno, še pogosteje pa skušajo svoje potrebe zadovoljiti s standardno tehnologijo, ki je dostopna in cenovno ugodna. Da bi spodbudili prehod z reaktivnega na bolj proaktiven pristop, je treba tehnološke izzive obravnavati na strukturiran, v prihodnost usmerjen in večdisciplinaren način, z dvema glavnima prednostnima nalogama: z vidika nacionalnih organov je bistveno zagotoviti, da imajo organi odkrivanja in pregona dostop do ustreznih zmogljivosti za pridobivanje in obdelavo razpoložljivih podatkov v tranzitu, medtem kot je za operaterje in ponudnike tehnologije ključno, da lahko izpolnijo svoje obveznosti glede dostopa do podatkov, zasebnosti in kibernetske varnosti ter da se ohranijo njihovi interesi.

Strokovnjaki zato predlagajo anticipacijo tehnoloških izzivov s celovito in v prihodnost usmerjeno politiko, in sicer na podlagi **tehnološkega kažipota za zakoniti dostop**, v katerem bodo določeni cilji in okvirne dejavnosti ter s tem povezana finančna sredstva za doseganje teh ciljev.

Kar zadeva krepitev zmogljivosti, je – čeprav so izzivi drugačni – pristop za digitalno forenziko, hrambo podatkov in zakonito prestrezanje[120], kot ga predlagajo strokovnjaki, pogosto podoben ter sloni na istih priporočilih, z odločno zahtevo po načrtovanju, temelječem na ciljih, za usmerjanje možnosti financiranja ob tesnejšem sodelovanju industrijskih akterjev in ključnih deležnikov, kot je inovacijsko vozlišče EU za notranjo varnost.

Vendar so strokovnjaki s področja odkrivanja in pregona vztrajali pri dveh elementih, specifičnih za zakonito prestrezanje:

- večja uporaba metapodatkov – npr. podatkov o lokaciji, seznama klicev in glav elektronskih sporočil – lahko zagotovi dodatne preiskovalne sledi. **Ker je z internetom povezanih vse več naprav, se količina ustvarjenih podatkov povečuje, kar nudi več priložnosti za opredelitev vedenjskih vzorcev.** Strokovnjaki so pozvali k več raziskavam, inovacijam in uvajanja v zvezi z **razširjeno uporabo metapodatkov**, npr. z umetno inteligenco, da bi ublažili pomanjkanje dostopa do podatkov o vsebini. Hkrati so omenjali tveganja za zasebnost, povezana z obsežno obdelavo masovnih osebnih metapodatkov z umetno inteligenco, ki jih je treba uravnotežiti s ciljno usmerjenim izkoriščanjem podatkov o vsebini. Vendar so strokovnjaki s področja odkrivanja in pregona jasni, da metapodatki sami ne morejo v celoti nadomestiti dokazne vrednosti vsebine komunikacij za dokazovanje namena;

- kadar storilci kaznivih dejanj uporabljajo namenske komunikacijske platforme, šifrirane od konca do konca, morajo organi odkrivanja in pregona za pridobitev dostopa do komunikacij osumljencev uporabiti taktične rešitve, ki temeljijo na izkoriščanju **ranljivosti**. Številni organi odkrivanja in pregona že delujejo v skladu s pravnim okvirom, ki omogoča prestrezanje na komunikacijskih končnih točkah, in imajo za to tudi tehnologijo, pri čemer je v zvezi s tem možen nadaljnji napredek. To bi lahko bila med drugim podpora razvoju v EU narejenih orodij ter omogočanje organom odkrivanja in pregona, da jih pridobijo in uporabijo v skladu z obstoječim pravnim okvirom.

  Vendar so strokovnjaki s področja odkrivanja in pregona opozorili, da te metode ne bi smeli razširiti kot osnovnega načina za zbiranje dokazov, saj taktično prestrezanje ni niti skalabilno niti neproblematično. Težave v zvezi s pristojnostjo bi se lahko npr. pojavile na podlagi lokacije tarče. Poleg tega je izkoriščanje ranljivosti, ki jih ni mogoče razkriti, nujno v nasprotju s temeljnimi načeli kibernetske varnosti.

[120] Podrobno opisano v poglavju o digitalni forenziki.

Kar zadeva vgrajen zakoniti dostop, so strokovnjaki s področja odkrivanja in pregona predlagali previden pristop, saj se od akterjev iz industrije ne bi smelo zahtevati združitve kakršnega koli sistema, za katerega je verjetno, da bi na splošen ali sistematičen način oslabil šifriranje za vse uporabnike storitve; zakoniti dostop bi moral ostati ciljno usmerjen in temeljiti na posamezni komunikaciji. Strinjali so se glede pomembnosti splošnega cilja, hkrati pa vztrajali, da je treba napredovati postopoma in vključiti vse ustrezne kategorije deležnikov, vključno s strokovnjaki za tehnologijo, kibernetsko varnost in zasebnost, ob upoštevanju morebitnih tveganj in občutljivosti javne razprave. Zlasti so odločno priporočili uporabo pristopa, ki temelji na dokazih, in skrbno oceno razpoložljivosti tehničnih rešitev, ki ne oslabijo kibernetske varnosti komunikacij ali negativno vplivajo na kibernetsko varnost operaterjev.

Sklop priporočil 10

Da bi obravnavali tehnološke izzive zakonitega prestrezanja, strokovnjaki priporočajo razvoj ***tehnološkega kažipota za zakoniti dostop***[121]*, ki bo zlasti:*

1. *združeval strokovnjake za tehnologijo, kibernetsko varnost, zasebnost, standardizacijo in varnost ter zagotavljal ustrezno usklajevanje, potencialno prek stalne strukture [priporočilo 22];*
2. *spodbujal raziskave, razvoj in uvajanje orodij za pridobivanje podatkov in dostop do njih, vključno z zmogljivostmi za dešifriranje ter zmogljivostmi, ki temeljijo na umetni inteligenci, za analizo podatkov*[122] *[priporočilo 4];*
3. *spodbujal usklajen pristop k standardizaciji, v okviru katerega bi se, če je to primerno, upoštevale potrebe po zakonitem dostopu do podatkov, hkrati pa [priporočila 15, 16 in 20]:*
    a. *spodbujalo vključevanje strokovnih delavcev iz vseh zadevnih skupnosti v ustrezne skupine za standardizacijo;*
    b. *prihodnje pobude pospremile z ustreznimi standardizacijskimi ukrepi (da bi spodbudili tehnološko nevtralen pristop);*
    c. *zajeli komunikacijske tehnologije na splošno, internet stvari (vključno npr. s povezanimi avtomobili) in vse oblike povezljivosti (vključno npr. s satelitsko komunikacijo);*
4. *izboljšal usklajevanje EU z industrijo zaradi obravnave primerov, v katerih tehnološke rešitve sicer obstajajo, vendar se ne izvajajo; v takih primerih*[123] *so potrebni jasne smernice in dialog, omogočen na ravni EU [priporočilo 24];*
5. *izvajal vgrajen zakoniti dostop v zvezi z vsemi zadevnimi tehnologijami v skladu s potrebami, ki jih izrazijo organi odkrivanja in pregona, ob hkratnem zagotavljanju močne varnosti in kibernetske varnosti ter izpolnjevanja pravnih obveznosti glede zakonitega dostopa [priporočilo 22];*
6. *temeljito obravnaval izzive šifriranja, in sicer z:*
    a. *zagotavljanjem, da morebitne nove obveznosti in/ali standardi niti neposredno niti posredno ne ustvarjajo obveznosti za ponudnike, ki slabijo varnost komunikacij, tako da na splošno spodkopavajo ali slabijo šifriranje od konca do konca [priporočilo 23];*
    b. *zagotavljanjem, da vgrajen zakoniti dostop ne bi negativno vplival na varnostno držo zadevne strojne ali programske opreme [priporočilo 23];*
    c. *usklajenim in s finančnimi sredstvi EU podprtim prizadevanjem za pripravo metodologije za razvoj, obravnavanje in uporabo ciljno usmerjenega zakonitega dostopa, da bi obravnavali primere, v katerih dostop do podatkov prek sodelovanja s ponudniki elektronskih komunikacijskih storitev ni mogoč [priporočilo 10].*

---

121 Tehnološki kažipot bi moral zajemati tri delovna področja: digitalno forenziko, hrambo podatkov in zakonito prestrezanje.

122 To priporočilo velja tudi za dostop do podatkov na napravi (glej razdelek o digitalni forenziki), le da se primeri uporabe nekoliko razlikujejo.

123 Npr. kadar sporazumi o usmerjanju v domača omrežja ali specifična vrsta izvajanja RCS ne dopuščajo zakonitega prestrezanja.

Nekatere pobude, ki so jih predlagali strokovnjaki skupine na visoki ravni, sicer delno že obstajajo, vendar je nujno, da se v tehnološkem kažipotu bolje strukturira srednje- in dolgoročna tehnološka politika o zakonitem dostopu, in sicer z usmerjenimi cilji in s tem povezanim instrumentom za spremljanje. S tem pristopom ne bi smeli zajeti le dostopa do podatkov v tranzitu, temveč tudi digitalno forenziko in hrambo podatkov.

Tehnološki kažipot bi moral biti usmerjen v prihodnost, izvršljiv, osredotočen na prednostne teme in vpet v digitalno strategijo EU. Vanj bi morale biti vključene vse ustrezne kategorije deležnikov, zlasti institucije, organi in agencije EU, nacionalni organi, akademiki z vseh ustreznih področij, industrija ter nevladne organizacije, odlikovati pa bi ga moralo jasno vodenje.

Ključni ukrep: strokovnjaki skupine na visoki ravni pozivajo Komisijo, naj predstavi in izvaja tehnološki kažipot za dostop do podatkov

- Strokovnjaki skupine na visoki ravni pozivajo Evropsko komisijo, naj predstavi in izvaja tehnološki kažipot, ki se bo osredotočal na izzive šifriranja in v katerem bodo obravnavani vsi pomembni vidiki, vključno z vidiki tehnologije, trga, kibernetske varnosti, temeljnih pravic, standardizacije, odkrivanja in pregona ter raziskav. Ta tehnološki kažipot bi moral biti na voljo leta 2025 in bi moral temeljiti na vsem ustreznem strokovnem znanju držav članic ter institucij in agencij EU, tudi s področij kibernetske varnosti, varstva podatkov in zasebnosti.