EUROOPAN
KOMISSIO

Bryssel 24.6.2025
COM(2025) 349 final

# KOMISSION TIEDONANTO EUROOPAN PARLAMENTILLE, NEUVOSTOLLE, EUROOPAN TALOUS- JA SOSIAALIKOMITEALLE JA ALUEIDEN KOMITEALLE

## Etenemissuunnitelma – lainvalvontaviranomaisten laillinen ja tosiasiallinen pääsy dataan

## Johdanto

Kuten eurooppalaisessa sisäisen turvallisuuden strategiassa (ProtectEU)[1] todetaan, **turvallisuus on peruskallio, jolle kaikki vapautemme rakentuvat**. Demokratia, oikeusvaltioperiaate, perusoikeudet, eurooppalaisten hyvinvointi, kilpailukyky ja vauraus ovat kaikki riippuvaisia siitä, miten pystymme takaamaan perusturvallisuuden.

EU:lla ja jäsenvaltioilla on velvollisuus taata, että kansalaiset saavat nauttia **korkeatasoisesta turvallisuudesta jokapäiväisessä elämässään**. Lainvalvonta- ja oikeusviranomaisilla on oltava tätä varten tarvittavat välineet, jotta ne voivat seurata laitonta toimintaa, tunnistaa rikoksentekijöitä, hajottaa rikollisverkostoja ja suojella uhreja sekä viime kädessä varmistaa rikosoikeuden täytäntöönpanon kaikkia perusoikeuksia kunnioittaen.

Terrorismilla, järjestäytyneellä rikollisuudella, verkkohuijauksilla, huumausainekaupalla, lasten seksuaalisella hyväksikäytöllä, verkossa tapahtuvalla seksuaalisella kiristämisellä, kiristysohjelmilla ja monilla muilla rikoksilla on eräs yhteinen piirre: ne jättävät **digitaalisia jälkiä**. Kuten Europol toteaa vakavaa ja järjestäytynyttä rikollisuutta koskevassa EU:n uhkakuva-arviossa (SOCTA) vuodelle 2025, lähes kaikilla vakavan ja järjestäytyneen rikollisuuden muodoilla on digitaalinen jalanjälki.[2] **Nykyään noin 85 prosenttia rikostutkinnoista perustuu sähköiseen todistusaineistoon.**[3] Palveluntarjoajille osoitettujen tietopyyntöjen määrä on kolminkertaistunut vuosina 2017–2022, ja tietojen tarve vain kasvaa.[4]

Vaikka viime aikoina on nähty merkittäviä esimerkkejä siitä, että lainvalvonta- ja oikeusviranomaiset ovat onnistuneet puuttumaan rikollisten viestintäverkkoihin[5], monet muut tutkinnat **viivästyvät tai epäonnistuvat, koska digitaalista todistusaineistoa ei ole oikea-aikaisesti saatavilla**.[6] Lainvalvontaviranomaiset ja oikeuslaitos ovat viimeisten kymmenen vuoden aikana joutuneet antamaan jalansijaa rikollisille, koska rikolliset käyttävät sellaisten palveluntarjoajien tarjoamia välineitä ja tuotteita, jotka ovat ottaneet käyttöön toimenpiteitä laillisiin pyyntöihin perustuvan yhteistyön estämiseksi.[7]

**Kriittisiä rikostodisteita** jää saamatta, koska[8]

- palveluntarjoajat **poistavat ne** muutaman päivän kuluessa henkilötietojen ja yksityisyyden suojaa koskevien velvoitteidensa tai liiketoimintaan liittyvien tarpeidensa vuoksi

[1] EUR-Lex – 52025DC0148 – FI - EUR-Lex.
[2] Vakavaa ja järjestäytynyttä rikollisuutta koskeva Euroopan unionin uhkakuva-arvio vuodelle 2025, EU-SOCTA-2025.pdf.
[3] Commission Impact Assessment on the Proposals for an e-evidence Regulation and an e-evidence Directive (17. huhtikuuta 2018), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2018:0119:FIN:FI:PDF.
[4] Vuoden 2023 SIRIUS-kertomus, https://www.eurojust.europa.eu/sites/default/files/assets/sirius-eueesr-2023.pdf, s. 69.
[5] Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized |Europol joint_ep_ej_third_report_of_the_observatory_function_on_encryption_en.pdf / Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe | Europol.
[6] Raportti, tehokkaan lainvalvonnan edellyttämää tietojen saatavuutta käsittelevä korkean tason työryhmä – Euroopan komissio.
[7] Tehokkaan lainvalvonnan edellyttämää tietojen saatavuutta käsittelevän korkean tason työryhmän loppuraportti (15. marraskuuta 2024).
[8] Common Challenges in Cybercrime, 2024, Europolin ja Eurojustin katsaus.

- niitä **ei voida hankkia** lainkäyttöalueiden välisten lainvalintaa koskevien ristiriitojen vuoksi, sillä datan saatavuutta koskevat lait ja määräykset vaihtelevat eri maiden välillä, mikä vaikeuttaa ulkomailla säilytetyn datan hankkimista
- niitä **ei voida hankkia rikostutkinnassa takavarikoiduista laitteista**, koska **digitaalinen rikostutkinta** on vaikeaa ellei jopa täysin mahdotonta
- niitä **ei voida lukea**, koska data on salattu
- niitä **ei voida analysoida tehokkaasti ja laillisesti**, sillä käytettävissä ei ole sopivia teknologioita tai riittävästi henkilöresursseja, jotta suuria takavarikoituja datamääriä voitaisiin suodattaa ja analysoida tehokkaasti ilman ristiriitoja EU:n ja jäsenvaltioiden oikeudellisen kehyksen kanssa.

Näihin haasteisiin vastaamiseksi perustettiin vuonna 2023 **tehokkaan lainvalvonnan edellyttämää tietojen saatavuutta käsittelevä korkean tason työryhmä**, jäljempänä ’korkean tason työryhmä’, joka antoi 42 suositusta vuoden 2024 toukokuussa ja marraskuussa. **EU:n oikeus- ja sisäasioiden neuvosto** hyväksyi korkean tason työryhmän suositukset[9] 13. kesäkuuta 2024 ja tämän jälkeen joulukuussa 2024 päätelmät, joissa komissiota kehotettiin laatimaan etenemissuunnitelma. Etenemissuunnitelman oli määrä perustua korkean tason työryhmän työhön ja sen esittämiin suosituksiin sellaisten toimenpiteiden käyttöönotosta, joilla varmistetaan lainvalvontaviranomaisten laillinen ja tosiasiallinen pääsy dataan.[10] Tällä tiedonannolla vastataan neuvoston kehotukseen.

Koska digitalisaatio ulottuu koko ajan laajemmalle ja tarjoaa rikollisille jatkuvasti uusia välineitä, on olennaisen tärkeää luoda **laillista datan saatavuutta** koskeva säännöstö, jotta varmistetaan, että rikolliset saatetaan oikeuden eteen. Tässä etenemissuunnitelmassa ”laillisella saatavuudella” tarkoitetaan lainmukaista pääsyä digitaaliseen tietoon, jota lainvalvontaviranomaiset tarvitsevat rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy.

Jotta dataan pääsy olisi laillista, sen on oltava **välttämätöntä ja oikeasuhteista, siinä on kunnioitettava perusoikeuksia** ja varmistettava yksityisyyden ja henkilötietojen asianmukainen suoja, sen on perustuttava **selkeisiin, tarkkoihin ja helposti käytettävissä oleviin sääntöihin, jotka on vahvistettu laissa**, sen on kuuluttava riippumattomien **valvontamekanismien** piiriin ja sen yhteydessä on tarjottava **tehokkaita oikeussuojakeinoja** henkilöille, joihin dataan pääsy voi vaikuttaa. Yhtä tärkeää on huolehtia siitä, että digitaaliset järjestelmät pysyvät **kyberturvallisina** ja suojassa luvattomalta käytöltä, jotta voidaan suojautua kyberuhkilta.

## I. Digitaalisen todistusaineiston saatavuuden varmistaminen: datan säilyttäminen[11]

[9] Tehokkaan lainvalvonnan edellyttämää tietojen saatavuutta käsittelevän korkean tason työryhmän suositukset.

[10] Neuvoston päätelmät tehokkaan lainvalvonnan edellyttämästä tietojen saatavuudesta (12. joulukuuta 2024) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/fi/pdf; neuvoston päätelmät tulevista painopisteistä Euroopan unionin ja sen jäsenvaltioiden yhteisten terrorisminvastaisten toimien vahvistamiseksi (12. joulukuuta 2024) https://data.consilium.europa.eu/doc/document/ST-16820-2024-INIT/fi/pdf.

[11] Datan säilyttämisellä tarkoitetaan sitä, että palveluntarjoajat säilyttävät tietyn ajan tiettyjä tarjoamiensa viestintäpalvelujen yhteydessä käsiteltyjä muita kuin sisältötietoja, jotta toimivaltaiset viranomaiset voivat käyttää niitä rikostutkinnassa asianmukaisten suojatoimenpiteiden mukaisesti ja varmistaa rikosoikeuden toteutumisen.

Espanjassa ratkaistiin vuonna 2019 nuoren naisen katoamista koskeva rikostutkinta viestintäpalvelujen tarjoajan kansallisen oikeudellisen velvoitteen mukaisesti tallentamien sijaintitietojen ansiosta. Näiden tietojen avulla tutkijat pystyivät paikantamaan kadonneen naisen, selvittämään, että kidnappauksesta epäilty oli myös kyseisellä alueella, ja sulkemaan pois muita epäiltyjä.[12] Viestintään liittyvät muut kuin sisältötiedot (esim. tilaaja- ja sijaintitiedot, päivämäärä, kellonaika, kesto, lähettäjä ja vastaanottaja sekä viestien koko) ovat keskeisessä asemassa useimmissa rikoksiin liittyvissä tutkinta- ja syytetoimissa. Nämä tiedot voivat olla ratkaisevia uhrien, epäiltyjen ja syytettyjen tunnistamisessa ja paikantamisessa, rikoksen selvittämisessä ja epäiltyjen poissulkemisessa.

EU:n yksityisyyden suojaa ja tietosuojaa koskevan lainsäädännön mukaisesti sähköisten viestintäpalvelujen tarjoajat saavat tallentaa viestintään liittyviä muita kuin sisältötietoja, jotka kulkevat kyseisten palveluntarjoajien järjestelmien kautta, vain niin kauan kuin se on tarpeen tiettyjä nimenomaisia ja laillisia liiketoimintatarkoituksia varten. Oikeudelliset velvoitteet voivat kuitenkin edellyttää, että viestintäpalvelujen tarjoajat säilyttävät nämä tiedot muita tarkoituksia varten, esimerkiksi jos niitä tarvitaan rikosten ennalta estämisessä, tutkimisessa tai paljastamisessa tai rikoksiin liittyvissä syytetoimissa.

EU:n tietojen säilyttämistä koskeva direktiivi[13] kumottiin vuonna 2014[14], minkä jälkeen palveluntarjoajien tietojen säilyttämisvelvollisuutta koskevasta lainsäädännöstä on tullut hajanaista ja epätasaista. Tietojen säilyttämistä koskevat jäsenvaltioiden säännöt eroavat toisistaan siinä, minkä tyyppisiä sähköisiä viestejä palveluntarjoajien on säilytettävä, mitä tietoluokkia säännöt kattavat ja kuinka kauan tietoja on säilytettävä.[15] Lisäksi joissakin jäsenvaltioissa ei ole lainkaan tietojen säilyttämistä koskevia lakeja. Lainvalvonta- ja oikeusviranomaiset kohtaavat työssään oikeudellisia ja toiminnallisia esteitä. Sähköisten viestintäpalvelujen tarjoajille, erityisesti pienille palveluntarjoajille, koituu myös lisäkustannuksia ja esteitä silloin, kun ne tarjoavat palvelujaan kaikkialla EU:ssa, koska niiden on noudatettava erilaisia oikeudellisia vaatimuksia eri jäsenvaltioissa.

Korkean tason työryhmä suositteli siksi **datan säilyttämistä koskevan yhdenmukaistetun EU:n kehyksen** luomista sen varmistamiseksi, että rikosten tutkinnassa ja rikoksiin liittyvissä syytetoimissa tarvittava digitaalinen todistusaineisto on käytettävissä. Yhdenmukaistetulla EU:n järjestelmällä pyrittäisiin vähentämään jäsenvaltioiden välistä hajanaisuutta datan säilyttämistä koskevien sääntöjen ja perusoikeuksiin, erityisesti yksityisyyteen ja tietosuojaan sekä puolustautumisoikeuksiin, myös oikeudenmukaista oikeudenkäyntiä koskevaan oikeuteen, liittyvien takeiden osalta.. Tällainen oikeudellinen kehys takaisi siten myös oikeusvarmuuden toimivaltaisille viranomaisille ja palveluntarjoajille.[16]

***Keskeinen toimi***

[12] La cobertura del móvil de Diana Quer desmonta la versión del Chicle: no la abordó donde él dijo que estaba robando gasolina | España.

[13] https://eur-lex.europa.eu/eli/dir/2006/24/oj.

[14] Unionin tuomioistuimen (suuri jaosto) tuomio 8.4.2014. Digital Rights Ireland Ltd vastaan Minister for Communications, Marine and Natural Resources ym.

[15] Ks. yleiskatsaus The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU | Eurojust |Euroopan unionin rikosoikeudellisen yhteistyön virasto ja Euroopan komission tutkimus ”Study on the retention of electronic communications non-content data for law enforcement purposes”.

[16] Suositusjoukko 6, korkean tason työryhmän loppuraportti.

- **<u>Komissio</u> laatii vuonna 2025 vaikutustenarvioinnin datan säilyttämistä koskevien EU:n sääntöjen päivittämiseksi tarpeen mukaan.**

Korkean tason työryhmä totesi, että **<u>lainvalvonta-alan toimijoiden ja palveluntarjoajien välisiä synergioita on vahvistettava</u>**.[17]

Tätä varten **Euroopan unionin lainvalvontayhteistyövirastoa (Europol) ja Euroopan unionin rikosoikeudellisen yhteistyön virastoa (Eurojust)** kehotetaan jatkamaan ja laajentamaan pyrkimyksiään **helpottaa yhteistyötä sekä tietojen ja parhaiden käytäntöjen vaihtoa toimijoiden ja palveluntarjoajien välillä SIRIUS-hankkeen**[18] kautta komission jatkuvalla tuella. SIRIUS-hankkeesta on tullut tärkein tietolähde, jolla **tuetaan lainvalvonta-alan toimijoita ja oikeusviranomaisia EU:ssa ja sen ulkopuolella** kolmansiin maihin sijoittautuneiden **verkkopalvelujen tarjoajien tallentaman sähköisen todistusaineiston saannissa**. SIRIUS-foorumissa on yli 8 000 jäsentä, jotka edustavat lainvalvonta- ja oikeusviranomaisia 47 maasta eri puolilta maailmaa, ja se on tukenut suoraan lähes 70:tä poliisioperaatiota.

Europolin ja Eurojustin olisi hyödynnettävä SIRIUS-hanketta samassa tarkoituksessa kehittääkseen yhteistyössä **yksityisen sektorin kanssa luettelon datasta, jota sähköisissä viestintäpalveluissa käsitellään laillisesti liiketoimintatarkoituksiin**. Tämä auttaa toimivaltaisia viranomaisia määrittämään, mitä tietoja on saatavilla laillisten tiedonsaantipyyntöjen perusteella, tunnistamaan asiaankuuluvat palveluntarjoajat ja kohdentamaan lailliset tiedonsaantipyynnöt paremmin, mikä säästää sekä viranomaisten että palveluntarjoajien aikaa ja kustannuksia.

***Keskeiset toimet***

- **<u>Europolia ja Eurojustia</u> kehotetaan hyödyntämään komission jatkuvan tuen avulla SIRIUS-hanketta tehostaakseen yhteistyötä sähköisten viestintäpalvelujen tarjoajien kanssa.**

- **<u>Europolia ja Eurojustia</u> kehotetaan kehittämään yhteistyössä yksityisen sektorin kanssa luettelo datasta, jota sähköisten viestintäpalvelujen tarjoajat käsittelevät liiketoimintatarkoituksiin (vuoden 2025 viimeisestä neljänneksestä alkaen).**

## <u>II. Todisteiden hankkiminen eri järjestelmistä ja lainkäyttöalueilta: laillinen tietojen sieppaus</u>

Laillinen ja reaaliaikainen pääsy viestintätietoihin on olennaisen tärkeää rikollisten pysäyttämiseksi verkossa ja sen ulkopuolella. Ranskan ja Alankomaiden yhteinen tutkintaryhmä sulki vuonna 2020 salatun EncroChat-puhelinverkon, jota järjestäytyneet rikollisryhmät käyttivät laajasti. Yhteisessä tutkinnassa siepattiin reaaliaikaisesti miljoonia viestejä, joita vakavia rikoksia suunnitelleet rikolliset vaihtoivat keskenään, sekä jaettiin kyseisiä viestejä muiden viranomaisten kanssa ja analysoitiin niitä. Saatujen tietojen ansiosta lainvalvontaviranomaiset ovat kaikkialla Euroopassa ja muualla maailmassa torjuneet rikollista toimintaa, muun muassa väkivaltaisia hyökkäyksiä, korruptiota, murhayrityksiä ja

[17] Suositusjoukko 5, korkean tason työryhmän loppuraportti.
[18] SIRIUS-hanke | Europol.

laajamittaista huumausainekauppaa. Tietyissä viesteissä viitattiin aikomuksiin toteuttaa välittömiä väkivaltarikoksia, ja viestien ansiosta lainvalvontaviranomaiset pystyivät estämään ne.[19] Eurooppalainen tutkintamääräys helpotti näiden todisteiden tehokasta jakamista.[20]

EncroChat-tapaus osoittaa, että reaaliaikainen pääsy viestinnän sisältötietoihin on olennaista järjestäytyneiden rikollisryhmien tehokkaassa tutkinnassa ja syytteeseenpanossa. Tämä tapaus on kuitenkin edelleen yksi harvoista menestystarinoista: korkean tason työryhmä totesi, että laillisen tietojen sieppauksen[21] tehokkuus on heikentynyt huomattavasti, kun viestinnässä on siirrytty perinteisistä puheluista ja tekstiviesteistä avoimen internetin kautta jaettaviin (OTT) viestintäpalveluihin, joita tarjotaan sovellusten avulla. Tällä hetkellä noin 97 prosenttia kaikista matkapuhelinviesteistä lähetetään viestintäsovellusten kautta, kun taas perinteisiä teksti- ja multimediaviestejä on vain noin kolme prosenttia viesteistä.[22] Korkean tason työryhmä totesi myös, että vuodesta 2020 lähtien useat rikollisryhmät ovat päättäneet siirtyä takaisin tavallisiin läpisalattuihin OTT-viestintäpalveluihin joissakin merkittävissä rikollisten käyttämissä viestintäverkoissa esiintyneiden häiriöiden vuoksi.[23]

Kansalliset säännöt, joilla asetetaan laillista tietojen sieppausta koskevia velvoitteita, ovat EU:ssa hajanaisia.[24] Korkean tason työryhmä huomautti, että vaikka joissakin jäsenvaltioissa asetetaan samanlaisia velvoitteita kaikentyyppisille sähköisille viestintäpalveluille, myös OTT-viestintäpalveluille, toisissa jäsenvaltioissa niitä ei sisällytetä velvoitteiden piiriin. Lisäksi palveluntarjoajat eivät useinkaan ole sijoittautuneet pyynnön esittävän viranomaisen jäsenvaltioon, mikä voi aiheuttaa monimutkaisia lainkäyttövaltakysymyksiä, lainvalintaa koskevia ristiriitoja ja täytäntöönpanon haasteita.[25] Näin ollen tällaisten viestintäpalvelujen sisältö ei käytännössä ole saatavilla.

Eurooppalainen tutkintamääräys ja muut yhteistyövälineet voivat auttaa ratkaisemaan rajat ylittävän tietojen sieppauksen haasteita joissakin osissa EU:ta. Jäsenvaltioiden viranomaisilla on kuitenkin edelleen ongelmia niiden käytössä: näillä välineillä ei voida tukea tietojen sieppausta, jos palvelua tarjotaan joko jäsenvaltioista, jotka eivät osallistu kyseiseen välineeseen, tai kolmannesta maasta. Tämän vuoksi korkean tason työryhmä suositteli useita toimenpiteitä sen varmistamiseksi, että monet palveluntarjoajat, myös OTT-palvelujen tarjoajat, vastaavat laillista tietojen sieppausta koskeviin pyyntöihin.[26]

Vastauksena suositukseen **komissio ehdottaa keinoja parantaa toimenpiteitä, joilla tehostetaan tietojen sieppausta koskevaa rajat ylittävää yhteistyötä** sekä viranomaisten kesken että viranomaisten ja palveluntarjoajien välillä. Korkean tason työryhmän suositusten mukaisesti komissio pyrkii ensisijaisesti parantamaan olemassa olevia välineitä, erityisesti eurooppalaista tutkintamääräystä, ja vapaaehtoista yhteistyötä (jos kolmansien maiden kanssa

[19] Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe | Europol; Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée.
[20] Eurooppalainen tutkintamääräys | Eurojust |Euroopan unionin rikosoikeudellisen yhteistyön virasto.
[21] Tässä tiedonannossa laillisilla sieppaustekniikoilla tarkoitetaan tekniikoita, jotka viestintäoperaattori ottaa käyttöön mahdollistaakseen reaaliaikaisen pääsyn viestintätietoihin tutkintatoimissa, sekä tekniikoita, joita lainvalvontaviranomaiset voivat ottaa käyttöön itsenäisesti.
[22] Korkean tason työryhmän loppuraportti, s. 38.
[23] Järjestäytynyttä verkkorikollisuutta koskeva uhka-arvio (IOCTA) 2024.
[24] Ks. digitaalista infrastruktuuria koskeva EU:n valkoinen kirja, s. 14; Lettan raportti sisämarkkinoista, s. 59, ja Draghin raportti EU:n kilpailukyvystä, s. 70, 74 ja 76.
[25] Korkean tason työryhmän loppuraportti, s. 41.
[26] Suositusjoukko 8, korkean tason työryhmän loppuraportti.

ei ole lainvalintaa koskevia ristiriitoja tai ne on poistettu). Jäsenvaltioiden olisi viime kädessä voitava panna täytäntöön laillista tietojen sieppausta koskevia velvoitteita kansallisen lainsäädännön mukaisesti kaikille viestintäpalvelujen tarjoajille, jotka aikovat tarjota palveluja kotimaassa, riippumatta palveluntarjoajien sijainnista ja siitä, ovatko tarjottavat palvelut perinteisiä vai internetpohjaisia televiestintäpalveluja.

Joillakin jäsenvaltioilla ei myöskään ole tarvittavaa verkkokapasiteettia tietojen jakamiseksi rajat ylittävässä yhteistyössä. Siksi **komissio selvittää jäsenvaltioiden tarpeita** ja tukee sellaisten suojattujen verkkojen käyttöönottoa asianomaisissa jäsenvaltioissa, joiden kaistanleveys on riittävä suurten datamäärien siirtämiseen reaaliaikaisesti. Tätä aloitetta voitaisiin rahoittaa EU:n ohjelmista.

***Keskeiset toimet***

**Komissio aikoo**

- **ehdottaa toimenpiteitä, joilla parannetaan laillista tietojen sieppausta koskevien rajat ylittävien pyyntöjen tehokkuutta olemassa olevilla välineillä, muun muassa arvioimalla tarvetta vahvistaa edelleen eurooppalaista tutkintamääräystä (vuoteen 2027 mennessä)**

- **kartoittaa toimenpiteitä, joilla luodaan tasapuoliset toimintaedellytykset kaikentyyppisille viestintäpalvelujen tarjoajille laillista tietojen sieppausta koskevien velvoitteiden täytäntöönpanossa**

- **määrittää tehokkaimman tavan puuttua yhteistyöhaluttomia viestintäpalvelujen tarjoajia koskevaan ongelmaan**

- **tukea jäsenvaltioiden, Europolin ja muiden turvallisuusvirastojen väliseen suojattuun tietojenvaihtoon tarkoitettujen valmiuksien käyttöönottoa (vuosina 2026–2028).**

**Jäsenvaltioita kannustetaan toteuttamaan rajat ylittäviä laillista tietojen sieppausta koskevia toimenpiteitä, jotka perustuvat olemassa oleviin mekanismeihin, kuten eurooppalaiseen tutkintamääräykseen sekä kahden- ja monenvälisiin sopimuksiin.**

## III. Todisteiden hakeminen tutkintatoimissa takavarikoiduista laitteista: digitaalinen rikostutkinta

Rikostutkintatoimien suorittamiseksi lainvalvonta- ja oikeusviranomaisten on voitava käyttää, kerätä, analysoida ja säilyttää elektronisiin laitteisiin tallennettua digitaalista todistusaineistoa. Digitaalisen todistusaineiston avulla voidaan esimerkiksi tunnistaa järjestäytyneiden rikollisryhmien jäseniä tai sulkea pois epäiltyjä henkilöitä.[27]

Korkean tason työryhmä tarkasteli useita haasteita, jotka haittaavat tutustumista digitaaliseen todistusaineistoon. Kansallisilla viranomaisilla on vakava puute digitaalisessa rikostutkinnassa tarvittavista resursseista ja valmiuksista. Niillä on vaikeuksia kehittää jatkuvasti uusia taitoja ja välineitä pysyäkseen uuden teknologian (esimerkiksi uudentyyppisten laitteiden ja käyttöjärjestelmien, esineiden internetin ja pilvipalvelujen) vauhdissa. Jäsenvaltioiden välistä

[27] Erään korkean tason työryhmässä käsitellyn tapauksen yhteydessä suoritettiin laiteanalyysi, jonka avulla todistettiin, ettei epäilty ollut osallisena murhassa. Korkean tason työryhmän loppuraportti, s. 12.

rajat ylittävää yhteistyötä haittaa vertailukelpoisten valmiuksien puute sekä se, ettei ole olemassa mekanismeja digitaalisen rikostutkinnan asiantuntijoiden taitojen ja asiantuntemuksen tunnustamiseksi. Nykyiset kaupalliset ratkaisut vanhentuvat nopeasti. Ne ovat myös liian kalliita, ja usein ne kehitetään EU:n ulkopuolella. Lisäksi ne saattavat soveltua huonosti jäsenvaltioiden viranomaisten tarpeisiin tai ne eivät välttämättä täytä EU:n digitaalisen rikostutkinnan vastuuvelvollisuusvaatimuksia tai muita oikeudellisia vaatimuksia.

Tästä syystä korkean tason työryhmä suositteli, että hankkeille myönnettäisiin kohdennettua rahoitusta sekä digitaalisen rikostutkinnan välineiden tutkimukseen ja kehittämiseen että niiden käyttöönottoon, jotta voitaisiin vahvistaa EU:n lainvalvontaviranomaisten kykyä suorittaa digitaalista rikostutkintaa takavarikoitujen laitteiden avulla. Korkean tason työryhmä suhtautui myönteisesti komission jatkuviin pyrkimyksiin tukea näitä toimia ja myöntää rahoitusta tietyistä EU:n välineistä (Horisontti Eurooppa, Digitaalinen Eurooppa -ohjelma ja sisäisen turvallisuuden rahasto) sekä EU:n seuraavan pitkän aikavälin talousarvion (monivuotisen rahoituskehyksen) vastaavista välineistä.

Vastauksena näihin suosituksiin[28] **komissio aikoo koordinoida Europolin tuella puute- ja tarveanalyysia, jossa käsitellään digitaalisen rikostutkinnan yhteisten teknisten ratkaisujen tutkimusta, kehittämistä, käyttöönottoa ja ylläpitoa.**

Resurssien käyttö on maksimoitava luomalla synergioita digitaalisen rikostutkinnan hankkeiden välille muun muassa yhdistämällä jäsenvaltioiden ohjelmista rahoitetut hankkeet olemassa oleviin mekanismeihin tai verkostoihin. Tässä yhteydessä olisi rahoitettava julkisen ja yksityisen sektorin kumppanuuksia, jotta voidaan tarjota täysin testattuja ja käyttövalmiita ohjelmistotyökaluja ilman lisenssikustannuksia.[29]

OLAF on hallinnollisten tutkimusten suorittamista koskevan toimeksiantonsa puitteissa hankkinut merkittävää kokemusta digitaalisen rikostutkinnan prosesseista ja välineistä, ja se voi auttaa jäsenvaltioiden viranomaisia vahvistamaan valmiuksiaan unionin petostentorjuntaohjelman kautta.

**Europolin ohjelmistotyökalupakki** on turvallinen verkkoalusta, joka on yksinomaan lainvalvontaviranomaisten käytettävissä ja jonka avulla jaetaan Europolin, Euroopan lainvalvontaviranomaisten ja tiedeyhteisön kehittämiä ilmaisia ja ei-kaupallisia ohjelmistoja. Kansalliset tutkintaviranomaiset ovat käyttäneet ohjelmistotyökalupakin työkaluja laajasti tukemaan vakavien ja järjestäytyneiden rikosten, muun muassa ihmiskaupan, kyberrikollisuuden ja verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan, tutkintaa. Tämän ohjelmistotyökalupakin olisi edelleen oltava ensisijainen jakelukanava EU:n hankkeissa kehitetyille digitaalisille tutkintavälineille. Jäsenvaltioita kannustetaan jakamaan olemassa olevissa mekanismeissa tai verkostoissa digitaalisessa rikostutkinnassa käytettäviä avoimen lähdekoodin välineitä, joita on kehitetty kansallisella tasolla. **Europol voi edelleen kehittää ja edistää ohjelmistotyökalupakkiaan**, jotta EU:n lainvalvontaviranomaisille

[28] Suositusjoukko 1, korkean tason työryhmän loppuraportti.

[29] Esimerkiksi Euroopan kyberrikollisuuden vastaisen teknologian kehittämisyhdistys (EACTDA) (www.eactda.eu) toimittaa EU:n lainvalvontaviranomaisille täysin testattuja ja käyttövalmiita ohjelmistotyökaluja ilman lisenssikustannuksia sekä käyttöoikeuden ohjelmistotyökalujen lähdekoodiin. Tähän mennessä valmistuneiden kahdeksan välineen lisäksi EACTDA kehittää 16:ta muuta digitaalista tutkintavälinettä, jotka on määrä toimittaa vuoden 2025 puoliväliin mennessä.

voidaan tarjota luotettavia, turvallisia, maksuttomia, helposti asennettavia ja skaalautuvia tutkintavälineitä.

Komissio tukee myös **jäsenvaltioiden lainvalvontaviranomaisten innovatiivisten ratkaisujen käyttöönottoa olemassa olevien mekanismien, kuten EMPACTin[30], kautta ja sisäisen turvallisuuden rahaston tätä koskevien ehdotuspyyntöjen avulla**.

Korkean tason työryhmä korosti, että **digitaalisen rikostutkinnan välineiden lisenssit** ovat kalliita ja joskus kohtuuttomia joillekin lainvalvontaviranomaisille. Digitaalisen rikostutkinnan välineet voivat tuottaa tietoa muodossa, joka ei ole yhteensopiva jatkokäsittelyssä käytettävien järjestelmien kanssa. Lisäksi luottamus on olennaisen tärkeää digitaalisessa rikostutkinnassa, eikä siinä käytettävien välineiden siksi pitäisi olla ”mustia laatikoita” (eli välineitä, jotka käsittelevät tietoja ilman, että luotetut viranomaiset pystyvät tarkastamaan, miten ne toimivat). Digitaalisen rikostutkinnan välineiden jakamista olisi tuettava arviointijärjestelmillä ja tarvittaessa sertifioimalla kaupallisia välineitä EU:n tasolla, jotta varmistetaan, että ne vastaavat luotettavuusvaatimuksia ja rikostutkimusstandardeja aiheuttamatta kohtuutonta rasitetta. Tukea olisi annettava myös käyttämällä yhteisiä hankintajärjestelmiä, joilla varmistetaan yhteistyö operatiivisten yksiköiden ja hankintaviranomaisten yhteyspisteiden välillä.[31]

Tästä syystä **komissio tukee jäsenvaltioiden operatiivisia yksiköitä ja hankintaviranomaisia pilottivaiheesta alkaen niiden toteuttaessa digitaalisen rikostutkinnan välineiden lisenssien yhteishankintoja.**

***Keskeiset toimet***

**Komissio aikoo Europolin tuella**

- **koordinoida digitaalisen rikostutkinnan yhteisten teknisten ratkaisujen tutkimusta, kehittämistä, käyttöönottoa ja ylläpitoa koskevaa puute- ja tarveanalyysia ennen vuoden 2026 toista neljännestä**

- **tukea edelleen teknisten ratkaisujen kehittämistä digitaalista rikostutkintaa varten asianmukaisten rahoitus- ja koordinointimekanismien avulla**

- **tukea jäsenvaltioita ja hankintaviranomaisia pilottivaiheesta alkaen niiden toteuttaessa digitaalisen rikostutkinnan välineiden lisenssien yhteishankintoja (ennen vuoden 2027 toista neljännestä).**

**Europolia kehotetaan kehittämään ja edistämään edelleen ohjelmistotyökalupakkiaan, jotta lainvalvontaviranomaiset saavat käyttöönsä ei-kaupallisia digitaalisia välineitä (vuoden 2025 kolmannesta neljänneksestä alkaen).**

**Jäsenvaltioita kehotetaan osallistumaan digitaalisen rikostutkinnan välineiden kehittämiseen, validointiin ja käyttöönottoon sekä tukemaan ja ohjaamaan tätä työtä.**

[30] Euroopan monialainen rikosuhkien torjuntafoorumi EMPACT on EU:n jäsenvaltioiden turvallisuusaloite, jonka puitteissa määritellään ja priorisoidaan järjestäytyneen ja vakavan kansainvälisen rikollisuuden aiheuttamia uhkia ja puututaan niihin.

[31] Tämän on perustuttava iProcureNet-hankkeeseen (www.iprocurenet.eu/), joka on rahoitettu EU:n tutkimuksen ja innovoinnin puiteohjelmasta ja jossa on kehitetty menetelmä turvallisuusalan yhteishankintoja varten, sekä jäsenvaltioiden hankintaviranomaisten verkostoon.

EU:n lainvalvontakoulutusvirasto (CEPOL) tarjoaa digitaaliseen rikostutkintaan osallistuville tutkijoille koulutusta muun muassa mobiililaitteiden ja reaaliaikaisen tiedon tutkinnasta. Korkean tason työryhmän suosituksen[32] mukaisesti **komission olisi tuettava jatkossakin koulutusmateriaalien ja -resurssien luomista** sellaisten olemassa olevien mekanismien kautta, joihin toimijat ja tiedeyhteisö osallistuvat[33]. Lisäksi CEPOLin ja jäsenvaltioiden olisi **asetettava etusijalle digitaalisen rikostutkinnan koulutuksen tarjonta.**

Korkean tason työryhmä korosti myös, että EU:n tasolla voitaisiin luoda sertifiointijärjestelmä digitaalisen rikostutkinnan asiantuntijoille. Tällaisella järjestelmällä varmistettaisiin digitaalisen rikostutkintatyön laatu, parannettaisiin oikeudenkäyntien avoimuutta ja lisättäisiin lainvalvontaviranomaisten välistä luottamusta yli rajojen.

Korkean tason työryhmän suositusten[34] mukaisesti CEPOL **voisi tukea alan toimijoita ja tiedeyhteisöä ja hyödyntää kaikkia olemassa olevia verkostoja ja mekanismeja[35] luotaessa EU:n tason sertifiointijärjestelmä digitaalisen rikostutkinnan asiantuntijoille**.

***Keskeiset toimet***

**<u>Komissio</u> aikoo**

- **tukea edelleen koulutusmateriaalien ja -resurssien luomista.**

**<u>CEPOLia ja jäsenvaltioita</u> kannustetaan**

- **asettamaan etusijalle digitaalisen rikostutkinnan koulutuksen tarjonta (vuoden 2025 kolmannesta neljänneksestä alkaen)**
- **tukemaan digitaalisen rikostutkinnan asiantuntijoille tarkoitetun sertifiointijärjestelmän kehittämistä ja täytäntöönpanoa EU:n tasolla (valmisteltava vuoden 2026 ensimmäisen neljänneksen ja vuoden 2028 viimeisen neljänneksen välillä).**

Korkean tason työryhmä antoi suosituksia, joiden mukaan olisi helpotettava ratkaisujen ja digitaalisen rikostutkinnan välineiden jakamista jäsenvaltioiden välillä luottamuksen ilmapiirissä.[36] Vastauksena suosituksiin **<u>Europolin tulisi kehittää edelleen rooliaan EU:n digitaalisen operatiivisen asiantuntemuksen osaamiskeskuksena digitaalisen rikostutkinnan alalla</u>**. Tähän voisi sisältyä SIRIUS-hankkeen[37] kaltaisen hankkeen perustaminen helpottamaan tiedon, asiantuntemuksen, teknisten ratkaisujen, digitaalisen rikostutkinnan välineiden ja parhaiden käytäntöjen jakamista luottamuksen ilmapiirissä. Europolin olisi myös tehostettava koordinointitehtävänsä hoitamista luotaessa digitaalista rikostutkintaa koskevaa tietämystä EU:n tasolla viime vuosina kehitettyjen mekanismien

[32] Suositusjoukko 3, korkean tason työryhmän loppuraportti.

[33] Esimerkiksi Euroopan kyberrikollisuuden tutkinnan koulutusryhmä-ECTEG (www.ecteg.eu) on järjestö, joka tekee tiivistä yhteistyötä Europolin ja CEPOLin kanssa ja jonka tavoitteena on tarjota lainvalvontaviranomaisille ilmaisia koulutusresursseja digitaalisen tutkinnan alalla. Sitä rahoitetaan tällä hetkellä EU:n sisäisen turvallisuuden rahastosta.

[34] Suositusjoukko 3, korkean tason työryhmän loppuraportti.

[35] Erityisesti EKTEG.

[36] Suositusjoukko 1, korkean tason työryhmän loppuraportti.

[37] Europolin ja Eurojustin johtamalla SIRIUS-hankkeella tuetaan EU:n lainvalvonta- ja oikeusviranomaisia helpottamalla verkkopalvelujen tarjoajien tallentaman sähköisen todistusaineiston tehokasta saatavuutta yli rajojen. Hankkeessa tarjotaan käytännön työkaluja, koulutusta ja resursseja yli 9 000 toimijalle sekä edistetään verkkopalvelujen tarjoajien välistä yhteistyötä ja tiedon jakamista kansainvälisten tapahtumien ja kumppanuuksien avulla.

pohjalta.[38] Europol voi aloittaa osan näistä toimista nykyisen toimeksiantonsa puitteissa. Europol tarvitsee kuitenkin vahvistettua toimeksiantoa ja lisäresursseja, jotta se voi kehittää näitä toimia kaikilta osin ja vastata jäsenvaltioiden operatiivisiin tarpeisiin.

**Komissio ehdottaa Europolin toimeksiannon kunnianhimoista tarkistamista** Euroopan komission vuosien 2024–2029 poliittisissa suuntaviivoissa ja eurooppalaisessa sisäisen turvallisuuden strategiassa esitetyn sitoumuksen mukaisesti. Tätä varten komissio tarkastelee tiiviissä yhteistyössä jäsenvaltioiden kanssa, miten voitaisiin vahvistaa Europolin teknistä asiantuntemusta ja valmiuksia tukea kansallisia lainvalvontaviranomaisia digitaalisessa ympäristössä. Tässä työssä on ratkaisevan tärkeää tehostaa digitaalista rikostutkintaa koskevia Europolin valmiuksia vahvistamalla sen toimeksiantoa ja tarjoamalla sille lisäresursseja.

Korkean tason työryhmä suositteli, että asiantuntijoiden tiedonsaantia parannettaisiin erityisten mekanismien avulla ja että asiantuntijat tekisivät yhteistyötä digitaalisen rikostutkinnan välineiden tuottajien ja kehittäjien kanssa.[39] Vuodesta 2026 alkaen **Europolin olisi edistettävä omien resurssiensa avulla asiaankuuluvien kansallisten viranomaisten ja asiantuntijoiden välistä yhteistyötä, jotta voidaan helpottaa julkisen ja yksityisen sektorin välistä yhteistyötä digitaalisen rikostutkinnan alalla**. Sen olisi tuettava jäsenvaltioita digitaalisten välineiden ja yhteisten menettelyjen kehittämisessä muun muassa vahvistamalla yhteisiä tietomuotoja digitaalista rikostutkintaa varten.[40]

***Keskeiset toimet***

**Europolia kehotetaan**

- **kehittymään digitaalisen operatiivisen asiantuntemuksen osaamiskeskukseksi digitaalisen rikostutkinnan alalla ja vahvistamaan rooliaan tämän alan tietämyksen luomisen koordinoinnissa EU:n tasolla (vuodesta 2026 alkaen)**

- **helpottamaan lainvalvontaviranomaisten ja yksityisten tahojen, myös palveluntarjoajien, välistä yhteistyötä digitaalisen rikostutkinnan alalla ja edistämään yhteisten tietomuotojen vahvistamista digitaalista rikostutkintaa varten (vuodesta 2026 alkaen).**

## IV. Todisteiden luettavuuden varmistaminen: datan salauksen purkaminen

Salaus ja muut kyberturvallisuustoimenpiteet ovat tärkeitä tietojärjestelmien suojaamisessa vakoilulta ja häiriöiltä sekä viestinnän, yksityisyyden ja henkilötietojen suojaamisessa. Noin 60–80 prosenttia viestintäsovelluksista on läpisalattuja, mukaan lukien yleisimmät palveluntarjoajat, kuten WhatsApp, Messenger, Signal ja iMessage, ja tekstiviestien ja perinteisten puheluiden käyttö vähenee merkittävästi kaikkialla maailmassa.[41]

[38] Erityisyhteisöt Europolin asiantuntijafoorumissa (https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts); rikostutkinnan asiantuntijoiden foorumi (https://www.europol.europa.eu/publications-events/events/forensic-experts-forum-2024-conference); Europolin teollisuus- ja tutkimuspäivät (https://www.europol.europa.eu/publications-events/events/europol-industry-and-research-days-2025).

[39] Suositusjoukko 1, korkean tason työryhmän loppuraportti.

[40] Näitä toimia olisi tuettava asianmukaisesta EU:n rahoituslähteestä (tutkimus- tai kehitysohjelmat suunniteltujen järjestelmien valmiustason mukaan).

[41] Mainittu prosenttiosuus koskee läpisalausta viestien lähetyksen aikana.

Korkean tason työryhmä painotti, että tämä kehitys vaikuttaa lainvalvonta- ja oikeusviranomaisten kykyyn kerätä todisteita rikostutkinta- ja syytetoimien aikana, koska laillisesta viestien sieppauksesta tulee enimmäkseen mahdotonta. Korkean tason työryhmä korosti, että jäsenvaltioilla on vain vähän asiantuntemusta ja valmiuksia lepäävän datan salauksen purkamiseen ja että onnistumisaste vaihtelee merkittävästi: joissakin jäsenvaltioissa se on 15–20 prosenttia, toisissa yli 66 prosenttia.

Salauksen purkamisessa käytettävät laitteet ovat kalliita ja pitkälle erikoistuneita, ja ne kuluttavat paljon resursseja. Useimmat lainvalvontaviranomaisten digitaalisen rikostutkinnan osastot käyttävät kaupallisia ratkaisuja laitteilla olevien tietojen saamiseksi. Kaupalliset ratkaisut eivät pysy teknologian kehityksen tahdissa, vaan ne vanhentuvat nopeasti, ja korkeat lisenssikustannukset vähentävät merkittävästi käyttöoikeudet saaneiden käyttäjien määrää. Lisäksi näitä ratkaisuja kehitetään usein EU:n ulkopuolella, minkä vuoksi ne eivät välttämättä vastaa EU:n viranomaisten tarpeita tai digitaalisen rikostutkinnan standardeja. Tämän seurauksena niitä käytetään menestyksekkäästi vain hyvin harvoissa tutkintatoimissa.

Näiden välineiden käytöllä on muitakin haittapuolia. Viranomaiset hyödyntävät tutkintatoimissaan usein haavoittuvuuksia päästäkseen käsiksi salauksen purkuun tarkoitettuihin avaimiin. Tämä voi joissakin tapauksissa aiheuttaa jännitteitä suhteessa kyberturvallisuuden oletusarvoista varmistamista koskevaan politiikkatavoitteeseen. Lisäksi salattuun dataan pääsy on yhä vaikeampaa. Korkean tason työryhmä totesi, että viranomaiset eivät voi päästä edes tehokkaimpien salauksenpurkualustojen avulla tietyntyyppisiin nykyaikaisiin laitteisiin tallennettuun dataan, joka on suojattu kryptosuorittimilla tai vahvoilla salausalgoritmeilla ja monimutkaisilla salasanoilla.

**Kvanttiturvallisen salauksen** kehittäminen ja käyttöönotto on välttämätöntä datan suojaamiseksi tulevilta kvanttitietokoneiden hyökkäyksiltä, jotka tekisivät arkaluonteisesta viestinnästä, rahoitusliiketoimista ja valtionsalaisuuksista alttiita salauksen purkamiselle ja datan hyödyntämiselle. Kuten **kvanttiturvalliseen salaukseen** siirtymisen koordinoidusta toteutussuunnitelmasta annetussa komission suosituksessa[42] ja eurooppalaisessa sisäisen turvallisuuden strategiassa (ProtectEU) todetaan, kvanttiturvallisten salausratkaisujen käyttöönotto ja kvanttiavaimen jakamisen kehittäminen ovat ratkaisevan tärkeitä datan turvaamiseksi uudella kvanttiaikakaudella. Kuten Europol korostaa, tämä vaikeuttaa kuitenkin laillista pääsyä digitaaliseen todistusaineistoon tulevina vuosina, ja lainvalvontaviranomaisten on tehtävä investointeja pysyäkseen mukana teknologian nopeassa kehityksessä.[43]

Korkean tason työryhmä[44] suositteli laatimaan teknologisen etenemissuunnitelman, jolla toteutetaan kohdennettu ja sisäänrakennetulla tavalla laillinen pääsy dataan tarpeen mukaan samalla kun varmistetaan vankka turvallisuus ja kyberturvallisuus noudattaen kaikilta osin oikeudellisia velvoitteita, jotka koskevat laillista pääsyä dataan. Vastauksena tähän **komissio antaa asiantuntijaryhmälle tehtäväksi tukea salausta koskevan teknologisen etenemissuunnitelman laatimista.** Asiantuntijaryhmä määrittää ja arvioi teknisiä ratkaisuja, joiden avulla lainvalvontaviranomaiset voisivat käyttää salattua dataa laillisesti varmistaen kyberturvallisuuden ja kunnioittaen perusoikeuksia. Ryhmään kuuluu lainvalvonnan, kyberturvallisuuden, salauksen, viestintäteknologian, standardoinnin ja perusoikeuksien

[42] Suositus kvanttiturvalliseen salaukseen siirtymisen koordinoidusta toteutussuunnitelmasta.
[43] The Second Quantum Revolution:the impact of quantum computing and quantum technologies on law enforcement | Europol.
[44] Suositusjoukko 10, korkean tason työryhmän loppuraportti.

asiantuntijoita. Työtä tuetaan teknologisten tutkimusten avulla ja osoittamalla konseptin toimivuus. Työn tarkoituksena on määrittää

- **välineitä, joita lainvalvontaviranomaiset tarvitsevat tällä hetkellä ja tulevaisuudessa** voidakseen löytää, hakea ja analysoida salattua dataa laillisesti; näiden välineiden on helpotettava digitaalista rikostutkintaa, salauksen purkamista, etänä suoritettavaa tiedonkeruuta ja rikosten analysointia
- **teknologioita, joilla varmistetaan, että tulevat tieto- ja viestintäteknologiat**, kuten kuudennen sukupolven matkaviestinverkot (6G) ja kvanttiturvallinen salaus, eivät vaaranna lainvalvontaviranomaisten kykyä saada tietoja laillisesti, samalla kun varmistetaan perusoikeuksien noudattaminen ja kyberturvallisuus.

Jos välineitä ei tällä hetkellä ole, teknologisen etenemissuunnitelman odotetaan sisältävän suosituksia niiden kehittämisestä ja siitä, miten voidaan sekä varmistaa yhteensopivuus EU:n oikeudellisen kehyksen kanssa että taata kyberturvallisuus. Teknologisen etenemissuunnitelman tulokset voivat myös luoda pohjan erityistoimille, joilla edistetään standardointiin sovellettavaa koordinoitua toimintamallia.

Europolin salauksenpurkualusta on osoittautunut erittäin hyödylliseksi tärkeiden rikostapausten, muun muassa Sky ECC-[45] ja EncroChat-tapausten, käsittelyssä. Tarvitaan tehostettuja salauksenpurkuvalmiuksia, joita edistetään myös tekoälyyn ja suurteholaskentaan tehtävillä lisäinvestoinneilla, jotta voidaan varmistaa, että lainvalvontaviranomaisilla on valmiudet purkaa yhä monimutkaisempia salausalgoritmeja.

Korkean tason työryhmä suositteli[46] rahoituksen lisäämistä datan saatavuutta koskevan innovoinnin tukemiseksi. Vastauksena suositukseen **komissio tukee uusien salauksenpurkuvalmiuksien tutkimusta ja kehittämistä** sen varmistamiseksi, että Europolilla on vuoden 2030 jälkeen hyvät valmiudet tukea jäsenvaltioita ottaen huomioon uuden teknologian kehitys ja pitkälle kehittynyt alan tutkimus. Aloitteen yhteydessä voitaisiin lisätä rahoitusta, jolla tuetaan salauksen purkamista koskevaa tutkimusta sekä välineiden kehittämistä ja täytäntöönpanoa jäsenvaltioissa. Jäsenvaltiot osallistuvat tiiviisti aloitteeseen ja tuovat esiin erityisvaatimuksensa sekä pyrkivät parantamaan valmiuksiaan, taitojaan ja teknisiä resurssejaan hyödyntämällä EU:n tasolla suunniteltua teknologiaa ja mahdollisesti harkitsemalla yhteisiä hankintoja.

***Keskeiset toimet***

**Komissio aikoo**

- **laatia salausta koskevan teknologisen etenemissuunnitelman (vuoden 2026 toisella neljänneksellä)**
- **tukea uusien salauksenpurkuvalmiuksien tutkimusta ja kehittämistä, jotta Europolille voidaan tarjota seuraavan sukupolven salauksenpurkuvalmiudet (vuodesta 2030 alkaen).**

[45] New major interventions to block encrypted communications of criminal networks |Europol.
[46] Suositusjoukko 10, korkean tason työryhmän loppuraportti.

## V. Teknologian ja laillisen saatavuuden yhteensovittaminen: standardointi

Standardit ovat digitaalisessa viestinnässä olennaisia. Ne ovat useiden toimijoiden, pääasiassa teollisuuden toimijoiden, kehittämiä, ja ne takaavat teknologian tarjoajien kehittämien järjestelmien ja laitteiden yhteentoimivuuden ja edistävät teknologioiden yhdenmukaisuutta oikeudellisten velvoitteiden kanssa, myös niiden velvoitteiden, jotka koskevat lainvalvontaviranomaisten laillista pääsyä dataan. Euroopan telealan standardointilaitos (ETSI) on kehittänyt useita tietojen laillista sieppausta ja paljastamista koskevia standardeja. Standardoinnissa on kuitenkin puutteita, kuten viidennen sukupolven matkaviestinverkkojen (5G) kohdalla, sillä niiden kehittämisessä laillista pääsyä dataan ei ole otettu asianmukaisesti huomioon. Tämä on estänyt lainvalvonta- ja oikeusviranomaisia saamasta tarvittavaa todistusaineistoa rikollisten tunnistamiseksi ja saattamiseksi oikeuden eteen.[47]

Korkean tason työryhmä suositteli, että järjestelmien laillista käyttöä koskevien ratkaisujen suunnittelussa noudatettaisiin varovaista toimintatapaa, mikä tarkoittaa, ettei teollisuutta pitäisi vaatia integroimaan järjestelmiä, jotka todennäköisesti heikentävät salausta yleisesti tai järjestelmällisesti palvelun kaikkien käyttäjien osalta. Laillinen pääsy dataan on rajoitettava kohdennetusti ja tapauskohtaisesti tiettyihin viestintätilanteisiin.

Yleisesti ottaen kaikki ratkaisut olisi pantava täytäntöön sellaisten selkeiden standardien pohjalta, joiden kehittämisessä otetaan huomioon kaikilta sidosryhmiltä, muun muassa teollisuuden edustajilta, tietosuojan, yksityisyyden suojan ja kyberturvallisuuden asiantuntijoilta ja lainvalvonta-alan toimijoilta, saatu palaute. Salausta käsiteltäessä on kuitenkin noudatettava varovaisuutta, kuten korkean tason työryhmä korostaa. Teknologisessa etenemissuunnitelmassa määritettyjen ratkaisujen pohjalta suunnitellaan erityistoimenpiteitä, joilla edistetään standardointiin sovellettavaa koordinoitua toimintamallia.

Standardoinnissa olisi otettava huomioon sovellettavat oikeudelliset vaatimukset, ja sen olisi perustuttava arvioituihin ratkaisuihin. Standardoinnin on varmistettava, ettei laillinen pääsy dataan ole ristiriidassa sovellettavien kyberturvallisuusstandardien, kuten kyberresilienssisäädöksen nojalla laadittujen standardien tai NIS2-direktiivin täytäntöönpanoa tukevien standardien, kanssa eikä muutoinkaan heikennä tuotteiden ja palvelujen turvallisuutta.

Korkean tason työryhmän suositusten[48] mukaisesti **komissio kehittää ja virtaviivaistaa sisäisen turvallisuuden standardointiin sovellettavaa EU:n toimintamallia kiinnittäen erityistä huomiota digitaaliseen rikostutkintaan sekä tietojen lailliseen paljastamiseen ja sieppaamiseen.** Toimintamalli perustuu jatkuvaan toimintaympäristöä koskevaan analyysiin, jonka lainvalvonta-alan toimijat tekevät erityisesti Europolin johtaman sisäisen turvallisuuden standardointia käsittelevän eurooppalaisen työryhmän yhteydessä. Tällä toimella myös lisätään työryhmän resursseja ja laajennetaan sen vastuualuetta sekä lisätään yhteistyötä muiden standardointialoitteiden kanssa erityisesti tekoälyn ja digitaalisen rikostutkinnan alalla. Tavoitteena on varmistaa, että turvallisuusnäkökohdat sisällytetään standardointipolitiikkaan. Lisäksi aloitteessa kehitetään ja järjestetään turvallisuusalan standardointia koskevaa koulutusta ja annetaan sisäisen turvallisuuden rahaston kautta rahoitustukea asiaankuuluviin standardointifoorumeihin osallistuville asiantuntijoille. Aloitteeseen sisällytetään myös asiaankuuluvia hallintomekanismeja.

[47] Ks. First report on Encryption from the EU Innovation Hub on Internal Security, 11.6.2024.
[48] Suositusjoukko 10, korkean tason työryhmän loppuraportti.

***Keskeiset toimet***

- **<u>Komissio</u> kehittää ja virtaviivaistaa tiiviissä yhteistyössä Europolin kanssa standardointitoimia, jotka koskevat datan laillista saatavuutta ja joita tuetaan sopivilla hallintomekanismeilla (vuoden 2025 toisen neljänneksen ja vuoden 2027 toisen neljänneksen välillä).**

- **<u>Jäsenvaltioita</u> kannustetaan osoittamaan riittävästi resursseja sen varmistamiseksi, että turvallisuusalan toimijat osallistuvat asiaankuuluviin datan laillista saatavuutta käsitteleviin standardointifoorumeihin.**

## VI. <u>Todistusaineiston tehokas ja laillinen analysointi: tekoäly</u>

Europol ja Eurojust totesivat hiljattain, että yhä useammat tutkintatoimet sisältävät erittäin suuria datamääriä.[49] Tyypillisessä lasten seksuaalista hyväksikäyttöä koskevassa tapauksessa tutkintatoimissa on usein analysoitava 1–3 teratavua dataa, joka voi sisältää 1–10 miljoonaa kuvaa ja tuhansia tunteja videomateriaalia.[50] Vuonna 2023 Europolin Large File Exchange -sovelluksen (LFE) kautta vaihdettiin 1 553 822 suurta tiedostoa.[51] EncroChat-tapauksessa siepattiin yli 115 miljoonaa järjestäytyneestä rikollisuudesta epäiltyjen välillä käytyä keskustelua. Seuraavina kuukausina Europol ja lainvalvontaviranomaiset pystyivät kehittyneiden analyysitekniikoiden ja -välineiden, muun muassa koneoppimisen, avulla tunnistamaan toimintamalleja, yhteyksiä ja hotspot-alueita, mikä johti 6 558 epäillyn pidättämiseen. Alankomaiden ja Ranskan viranomaiset jakoivat nämä tiedot EU:n jäsenvaltioissa ja kolmansissa maissa toimivien kollegoidensa kanssa, minkä ansiosta pelkästään Yhdistyneessä kuningaskunnassa estettiin yli 200 suunniteltua murhaa.[52]

Tutkintatoimien aikana käsiteltävän datan määrä kasvaa jatkuvasti, minkä vuoksi datan tallentaminen, hallinta ja tehokas analysointi on vaikeaa ilman merkittävää asiantuntemusta, laskentaresursseja ja erikoistyökaluja. Europol ja Eurojust vahvistivat, että datan määrä voi olla tutkijoille ylivoimainen, ja se voi pidentää käsittelyaikoja ja aiheuttaa tallennuskapasiteettiin liittyviä ongelmia. Lisäksi jäsenvaltioilla ei useinkaan ole tarvittavia mekanismeja ja infrastruktuuria suurten datamäärien siirtämiseksi muihin jäsenvaltioihin ja Europolille.

Lainvalvontaviranomaisten on siksi välttämätöntä käyttää tekoälyä voidakseen ehkäistä, havaita ja tutkia rikoksia ja suojella yhteiskuntiamme digitaalisella aikakaudella. Tekoälypohjaiset ratkaisut voivat suorittaa yksinkertaisia tehtäviä, kuten tehdä konekäännöksiä tai muuntaa puhetta tekstiksi, tai monimutkaisempia tehtäviä, kuten suodattaa dataa, korreloida todisteita valtavasta datamäärästä tai torjua tekoälyn haitallista käyttöä. Lainvalvontaviranomaisten käyttöön tarkoitettujen tekoälypohjaisten välineiden on oltava tarkkoja ja läpinäkyviä sekä täysin tekoälyä, tietosuojaa ja yksityisyyttä koskevan EU:n oikeudellisen kehyksen mukaisia, jotta voidaan varmistaa luotettavat ja eettiset datavetoiset

[49] Common Challenges in Cybercrime, 2024, Europolin ja Eurojustin katsaus.
[50] Europolin järjestäytynyttä verkkorikollisuutta koskeva uhka-arvio (IOCTA).
[51] Europolin konsolidoitu vuotuinen toimintakertomus 2023.
[52] Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée. Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized | Europol. EncroChat.

tutkintatoimet. Tekoäly ja suurteholaskenta ovat ensiarvoisen tärkeitä, jotta voidaan päästä salattuihin tietoihin sekä tukea tutkintatoimia ja rikosteknisiä analyyseja.

**Komissio edistää tekoälyratkaisujen kehittämistä ja käyttöönottoa** korkean tason työryhmän suositusten mukaisesti, sillä suosituksissa kehotetaan lisäämään rahoitusta tekoälypohjaisten data-analyysivälineiden tutkimukseen ja kehittämiseen ja asettamaan selkeät tulostavoitteet[53]. Tässä yhteydessä kohdennetaan investointeja keskeisten valmiuksien kehittämiseen, muun muassa ratkaisuihin, joiden avulla tunnistetaan tutkintavihjeitä erittäin suurista datamääristä täysin tietosuoja- ja yksityisyysperiaatteita noudattaen, tai kryptovaluuttatransaktioiden jäljittämisen parantamiseen. Myös tekoälyvälineiden koulutus-, testaus- ja arviointimahdollisuuksia voitaisiin hyödyntää tekoälyn sääntelyn testiympäristössä tekoälysäädöksen[54] mukaisesti toimivaltaisten valvontaviranomaisten tuella ja ohjauksessa. Lisäksi tekoälytehtaat ja tulevat gigatehtaat voisivat tukea tekoälypohjaisten välineiden ja palvelujen kehittämistä lainvalvontatarkoituksiin. Komission olisi helpotettava näitä toimia analysoimalla sidosryhmien, kuten Europolin innovaatiolaboratorion ja EU:n oikeus- ja sisäasioiden virastojen sisäisen turvallisuuden innovaatiokeskuksen, tarpeita.

Jäsenvaltiot voivat saada käyttöönsä tarvittavat valmiudet vähäisin kustannuksin tai ilmaiseksi ja varmistaa yhteensopivuuden tekoälysäädöksen vaatimusten kanssa. Tekoälyn osalta on ratkaisevan tärkeää omaksua kattava toimintamalli, johon sisältyy muun muassa standardoitujen tietomuotojen luominen tietojenvaihtoa varten ja tällaisten järjestelmien käyttöä koskevien ohjeiden laatiminen tekoälysäädöksen ja sovellettavan EU:n tietosuojalainsäädännön mukaisesti. Tätä toimea voitaisiin tukea myöntämällä rahoitusta sisäisen turvallisuuden rahastosta, Digitaalinen Eurooppa -ohjelmasta ja Horisontti Eurooppa -ohjelmasta. Toimeen kuuluu Europolin ja EMPACT-foorumin tukeminen, jotta varmistetaan asianmukainen yhteensovittaminen operatiivisten tarpeiden kanssa ja edistetään käyttöönottoa ja valtavirtaistamista alan toimijoiden keskuudessa.

***Keskeiset toimet***

**Komissio aikoo**

- **edistää uusien tekoälyratkaisujen luomista ja käyttöönottoa sekä parantaa nykyisiä digitaalisten todisteiden suodattamisessa ja analysoinnissa käytettäviä tekoälyratkaisuja muun muassa hyödyntämällä tekoälyn sääntelyn testiympäristöjä kattavasti ratkaisujen kehittämisessä, testaamisessa ja arvioinnissa tekoälysäädöksen mukaisesti (vuosina 2025–2028)**

- **käydä vuoropuhelua lainvalvontaviranomaisten ja muiden sidosryhmien kanssa kartoittaakseen niiden tarpeita Europolin innovaatiolaboratorion ja EU:n oikeus- ja sisäasioiden virastojen keskuksen työn pohjalta**

- **tukea selkeiden ohjeiden laatimista tekoälyn käytöstä lainvalvonnassa**

- **tukea pilottihankkeita, joiden tarkoituksena on kehittää ja kouluttaa oikeudellisesti ja teknisesti luotettavia tekoälyratkaisuja digitaalista rikostutkintaa, data-analyysia ja muita lainvalvontaviranomaisten käyttöön tarkoitettuja tutkintavälineitä varten.**

[53] Suositus 4, korkean tason työryhmän suositukset.
[54] Ks. tekoälysäädöksen 57 artikla.