Sisäministeriö Perusmuistio EU/805/2025-SM-4

Simonen Katariina 20.11.2025

Etenemissuunnitelma – lainvalvontaviranomaisten laillinenja tosiasiallinen pääsy dataan, tiedonanto

Kokous
-

Eduskuntatunnus

-

Käsittelyvaihe ja jatkokäsittelyn aikataulu

Komissio antoi tiedonannon etenemissuunnitelmaksi lainvalvontaviranomaisten laillinen ja tosiasiallinenpääsy dataan 24.6.2025 [COM(2025) 349 final]. Komissio antoi tiedonannon osana Euroopan unioninsisäisen turvallisuuden strategian (ProtectEU) täytäntöönpanoa (kts. E 39/2025 vp).

Tiedonannossa komissio esittelee toimenpiteitä ja välineitä, joilla pyritään turvaamaan lainvalvontaviranomaistenlainmukainen ja tehokas tietoon pääsy digitaalisessa ympäristössä. Etenemissuunnitelma perustuu korkean tason asiantuntijaryhmän (*High-Level Group on access to data for law enforcement*)15.11.2024 antamaan loppuraporttiin. Komission etenemissuunnitelma sisältää suosituksia kuudessa erikokonaisuudessa, joita ovat: tietojen säilyttäminen, todistusaineiston rajat ylittävä hankinta, digitaalinen rikostutkinta, tiedon luettavuuden varmistaminen, teknologian ja lainmukaisen tietoon pääsyn yhteensovittaminen(standardointi) sekä todistusaineiston tehokas ja lainmukainen analyysi (tekoäly).

EU-tasolla lainmukaisen tietoon pääsyn edistämistä koskevia toimia on alettu edistää jo vuoden 2025aikana. Komissio on muun muassa käynnistänyt tässä tarkoituksessa tietojen säilytysvelvollisuutta koskevan vaikutustenarvioinnin ja asettanut salauksen teknologiatiekartan laatimista varten asiantuntijaryhmän.

Tällä E-kirjeellä annetaan komission lainvalvontaviranomaisten lainmukaista ja tehokasta tietoon pääsyä koskevan tiedonannon sisällöstä tieto eduskunnalle sekä muodostetaan kantoja, joilla voidaan ennakollisesti vaikuttaa EU-tasolla valmisteltaviin kokonaisuuksiin. Asiakokonaisuuteen liittyviä kantoja on muodostettu aiemmin eduskuntaselvityksissä E 26/2024 vp ja E 39/2025 vp.

Suomen kanta

Valtioneuvoston sisäisen turvallisuuden selonteon (VNS 6/2025 vp) lainsäädännön ja toimivaltuuksien yhtenä toimenpiteenä on varmistaa lainvalvontaviranomaisten pääsy tietoon kybertoimintaympäristössä ja kehittää toimivaltuuksia ja työvälineitä verkossa tapahtuvien rikosten torjuntaan.

Digitaalisen todistusaineiston saatavuuden varmistaminen

Suomi pitää haastavana nykytilannetta, jossa tietojen säilytysvelvollisuutta koskevan lainsäädännön sisältö vaihtelee eri jäsenvaltioissa merkittävällä tavalla niin säilytysvelvollisten, säilytettävien tietoluokkien sekä säilytysmääräaikojen osalta. Pirstaloitunut sääntely aiheuttaa oikeudellista epävarmuutta niin tietoja pyytävien viranomaisten kuin tietoja säilyttävien yritystenkin näkökulmasta. Suomen näkemyksen mukaan pirstaloitunut sääntelyympäristö hankaloittaa lainvalvontaviranomaisten toimintamahdollisuuksia ja näin ollen edesauttaa rikollisten toimintamahdollisuuksia.

Suomi pitää hyvänä komission aikomusta laatia vaikutustenarviointi säilytysvelvollisuutta koskevasta sääntelystä ja että tietopohjaa kartutetaan sidosryhmäkuulemisilla. Suomi muodostaa yksityiskohtaisemmin kantansa EU-tason velvoittavaan sääntelyyn komission vaikutusarvioinnin sekä mahdollisen lainsäädäntöehdotuksen perusteella. Suomi pitää tärkeänä, että vaikutusarvioinnissa huomioidaan viranomaisten tarpeiden lisäksi täysimääräisesti vaikutukset palveluiden käyttäjien ja rikosten uhrien perusoikeuksiin, kuten yksityiselämän ja henkilötietojen suojaan, oikeuteen elämään ja koskemattomuuteen, puolustautumisoikeuksiin ja tehokkaisiin oikeussuojakeinoihin sekä vaikutukset julkisen hallinnon käyttämien tieto- ja viestintäpalveluiden tieto- ja kyberturvallisuuteen. Suomi pitäisi asianmukaisena, että komissio tarkastelisi myös mahdollisen sääntelyn vaikutuksia sisämarkkinoiden toimintaan.

Suomi pitää tärkeänä, että vaikutusarvioinnissa käsitellään sääntelyn soveltumista sellaiseen palveluntarjoajien joukkoon, joiden osalta EU-tasoinen sääntely on välttämätöntä. Suomi pitää hyvänä, että komissio arvioi pääasiassa lainsäädäntötoimia, jotka kohdistuvat eurooppalaisen sähköisen viestinnän säännöstön soveltamisalaan kuuluville palveluntarjoajille. Suomi suhtautuu myönteisesti sellaisiin lainsäädäntötoimiin, joilla tuodaan nykytilaan verrattuna lisäarvoa rikostorjunnan kannalta ja samalla varmistetaan kansalaisten perusoikeuksien toteutuminen. Siten tarkastelussa tulisi keskittyä erityisesti useassa EU-jäsenmaassa toimiviin palveluntarjoajiin. Suomi pitää tärkeänä, että viestinnän sisältötietojen säilyttäminen on rajattu tarkastelun ulkopuolelle.

Suomi pitää tärkeänä, että mahdollinen sääntely on oikeasuhtaista ja puuttuminen luottauksellisen viestinnän suojaan, yksityiselämään ja henkilötietojen suojaan rajoittuu välttämättömään. Mahdollisen sääntelyn tulee huomioida EU:n perusoikeuskirjasta, tietosuojalainsäädännöstä ja EU:n tuomioistuimen oikeuskäytännöstä johtuvat velvoitteet samalla tunnustaen tarve kehittää lainsäädäntöä, joka vastaa verkkomaailman kehityksestä johtuviin tarpeisiin. Suomi pitää tärkeänä, että mahdollisessa sääntelyehdotuksessa varmistetaan sellainen tietojen säilytysaika, jota voidaan pitää välttämättömänä tehokkaan rikostutkinnan ja rikostorjunnan turvaamiseksi ja rikosvastuuseen saattamiseksi.

Suomi suhtautuu erittäin kriittisesti vakavan rikollisuuden tason määrittelyyn EU-tasolla.

Suomi pitää tärkeänä, että mahdollisen sääntelyn tulisi jättää riittävästi kansallista liikkumavaraa jäsenvaltioiden järjestelmien erityispiirteiden tarkoituksenmukaisen huomioon ottamisen mahdollistamiseksi.

Suomi pitää tärkeänä, että mahdollinen sääntely koskee tietojen säilyttämistä tehokkaan rikostutkinnan, rikostorjunnan ja rikosoikeudellisen vastuun toteuttamisen varmistamiseksi. Erityisesti Suomi kiinnittää huomiota siihen, että sääntelyn ei tule koskea kansallisen turvallisuuden varmistamiseksi säilytettäviä tietoja. Kansallisen turvallisuuden osalta toimivalta kuuluu jäsenmaille. Sääntelyinstrumentissa tulee myös mahdollistaa säilyttämis- ja luovuttamisvelvollisuudesta säätäminen kansallisessa lainsäädännössä kansallisen turvallisuuden suojaamiseksi.

Todistusaineiston hankkiminen eri järjestelmistä ja lainkäyttöalueilta

Suomi korostaa, että lainmukainen rajat ylittävä tietoihin pääsy on tärkeää. Tietoon pääsyn varmistamisessa tulee ottaa huomioon digitaalisen ympäristön jatkuva kehitys.

Suomi pitää tärkeänä rajat ylittävää yhteistyötä EU-tasolla todisteiden hankkimiseksi. Sen sijaan EU-sääntelyllä ei tule rajoittaa vapaata todistelua ja vapaata todistusharkintaa oikeudenkäynneissä (ks. myös E 57/2023 vp).

Digitaalinen rikostutkinta

Suomi pitää tärkeänä, että digitaalisen rikostutkinnan kyvykkyyksiä ja yhteistyötä kehitetään EU-tasolla. Tässä työssä on tärkeää hyödyntää täysimääräisesti EU-virastojen tarjoama tuki.

Todisteiden luettavuuden varmistaminen: datan salauksen purkaminen

Suomi kannattaa asiantuntijaryhmän asettamista salausta koskevan teknologiatiekartan laatimiseksi nopeassa aikataulussa. Suomi pitää tärkeänä, että tasapainoisia, perus- ja ihmisoikeuksia kunnioittavia lähestymistapoja etsitään laajassa yhteistyössä. Suomi pitää tärkeänä, että asiantuntijaryhmä tunnistaa teknologisia ratkaisuja, jotka mahdollistavat laissa tarkkarajaisesti määritellyissä yksittäistapauksissa lainvalvontaviranomaisten pääsyn salattuihin tietoihin ja samalla turvaavat vahvaa salausta sekä kyberturvallisuuden korkean tason.

Suomi pitää myös tärkeänä sitä, että tulevaisuuden teknologisten ratkaisujen tulee mahdollistaa vain tarkkarajaisesti määritellyissä yksittäistapauksissa lainvalvontaviranomaisten pääsy salattuihin tietoihin.

Suomi toistaa näkemyksenään, ettei esitetä toimenpiteitä, joilla heikennetään viestintä- ja tietojärjestelmien turvallisuutta tai jotka johtaisivat viestinnän salauksen käytön kieltämiseen, rajoittamiseen tai sen tarkoituksen kiertämiseen. Suomi huomioi, että tämä ei kuitenkaan poissulje teknologisen kehityksen tai muiden järjestelyjen mahdollistamaa tuomioistuimen luvalla yksittäistapauksissa tapahtuvaa lainvalvontaviranomaisten pääsyä salattuun tietoon.

Teknologian ja laillisen saatavuuden yhteensovittaminen: standardointi

Suomi pitää tärkeänä, että lainmukaisen tietoon pääsyn mahdollistavat standardointiratkaisut toteutetaan selkeiden standardien pohjalta, joita kehitetään kaikkien sidosryhmien yhteistyössä. Suomi pitää tässä yhteydessä tärkeänä, että EU-tasolla kehitetään yhteisiä standardeja, joilla voidaan mahdollistaa tietoon pääsy tilanteissa, joissa lainmukaiset edellytykset sille täyttyvät.

Todistusaineiston tehokas ja laillinen analysointi: tekoäly

Suomi kannattaa EU tason yhteistyön tiivistämistä tekoälyn hyödyntämiseksi rikostorjunnassa liittyen tekoälyn kehitystyöhön, testaukseen ja käyttöönottoon. On tärkeää, että tekoälyn käyttöön rikosten tutkinnassa ja torjunnassa luodaan hyväksyttyjä käytänteitä, huomioiden EU:n tekoäly- ja tietosuojalainsäädäntö

Pääasiallinen sisältö

Komission etenemissuunnitelman mukaan lähes kaikilla vakavan ja järjestäytyneen rikollisuuden muodoilla on digitaalinen jalanjälki. Europol vahvistaa tämän vuoden 2025 vakavan ja järjestäytyneen rikollisuuden uhka-arviossaan (SOCTA). Nykyisin noin 85 prosenttia rikostutkinnoista perustuukin sähköiseen todistusaineistoon. Palveluntarjoajille osoitetut tietopyynnöt ovat kolminkertaistuneet vuosien 2017 ja 2022 välillä ja tietojen tarve on kasvava.

Etenemissuunnitelmassa todetaan, että vaikka viime aikoina on saatu merkittäviä esimerkkejä siitä, että lainvalvonta - ja oikeusviranomaiset ovat onnistuneet puuttuman rikollisten viestintäverkkoihin, monet tutkinnat viivästyvät tai epäonnistuvat, koska digitaalista todistusaineistoa ei ole saatavilla oikea-aikaisesti. Kriittisiä rikostodisteita jää saamatta esimerkiksi siksi, että palveluntarjoajat poistavat ne muutaman päivän kuluessa henkilötietojen ja yksityisyyden suojaa koskevien velvoitteidensa tai liiketoimintaan liittyvien tarpeidensa vuoksi, tai siksi että todisteita ei voida hankkia lainkäyttöalueiden välisten lainvalintaa koskevien ristiriitojen vuoksi tai koska tieto ei ole luettavassa muodossa datan salauksen vuoksi, tai tietoja 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 jäsenmaiden oikeudellisen kehyksen kanssa.

Komission etenemissuunnitelmassa edellytetään lailliselta dataan pääsyltä tasapainoa eri intressien välillä. Laillisen pääsyn on oltava välttämätöntä ja oikeasuhtaista, sen on kunnioitettava perusoikeuksia ja varmistettava yksityiselämän ja henkilötietojen asianmukainen suoja ja kyberturvallisuus. Laillisen pääsyn on perustuttava selkeisiin, tarkkoihin ja helposti käytettävissä oleviin sääntöihin, sen on kuuluttava riippumattomien valvontamekanismien piiriin ja sen yhteydessä on tarjottava tehokkaita oikeussuojakeinoja henkilöille, joihin dataan pääsy voi vaikuttaa.

Komission etenemissuunnitelma sisältää suosituksia kuudessa eri kokonaisuudessa, jotka esitellään lyhyesti alla.

I) Digitaalisen todistusaineiston saatavuuden varmistaminen: datan säilyttäminen

Viestintään liittyvä muu kuin sisältötieto (esimerkiksi tilaaja- ja sijaintitieto, päivämäärä, kellonaika, kesto, lähettäjä, vastaanottaja, viestin koko) on 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.

Korkean tason asiantuntijaryhmä suositteli datan säilyttämistä koskevan yhdenmukaistetun EU:n kehyksen luomista sen varmistamiseksi, että rikosten tutkinnassa ja rikoksiin liittyvissä syytetoimissa on tarvittava digitaalinen todistusaineisto käytettävissä.

Sähköisten viestintäpalveluiden tarjoajat voivat säilyttää viestintään liittyviä tietoja vain niin kauan kuin se on sallittua EU:n yksityisyyden suojaa ja tietosuojaa koskevan lainsäädännön mukaisesti. Viestintäpalveluntarjoajat voidaan kuitenkin lakisääteisesti velvoittaa säilyttämään näitä tietoja rikostutkintojen varmistamiseksi. Unionin tuomioistuin kumosi vuonna 2014 tietojen säilyttämistä koskevan direktiivin unionin oikeuden vastaisena, minkä jälkeen tietojen säilyttämisvelvollisuutta koskevasta lainsäädännöstä on tullut hajanaista ja epätasaista. Jäsenvaltioiden kansalliset lainsäädännöt eroavat toisistaan.

Etenemissuunnitelman mukaan komissio toteuttaa seuraavat keskeiset toimet:

- komissio laatii vuonna 2025 vaikutustenarvioinnin datan säilyttämistä koskevien EU:n sääntöjen päivittämiseksi tarpeen mukaan;

- Europolia ja Eurojustia kehotetaan tehostamaan yhteistyötä sähköisten viestintäpalvelujen tarjoajien kanssa;

- Europolia ja Eurojustia kehotetaan kehittämään yhteistyössä yksityisen sektorin kanssa luettelo datasta, jota sähköisten viestintäpalvelujen tarjoajat käsittelevät liiketoimintatarkoituksiin.

II) Todisteiden hankkiminen eri järjestelmistä ja lainkäyttöalueilta

Lainmukainen ja reaaliaikainen pääsy viestintätietoihin on olennainen tekijä rikollisten pysäyttämiseksi verkossa ja sen ulkopuolella. Korkean tason asiantuntijaryhmä totesi, että laillisen tietojenhankinnan tehokkuus on heikentynyt huomattavasti, kun viestinnässä on siirrytty perinteisistä puheluista ja tekstiviesteistä avoimen internetin kautta jaettaviin (ns. over-the-top eli OTT) viestintäpalveluihin, joita tarjotaan sovellusten avulla. Tänä päivänä noin 97 % kaikista matkapuhelinviesteistä lähetetään viestintäsovellusten kautta, kun taas perinteisiä teksti- ja multimediaviestejä on vain noin kolme prosenttia viesteistä. Korkean tason asiantuntijaryhmä totesi myös, että vuodesta 2020 lähtien useat rikollisryhmät ovat päättäneet siirtyä takaisin tavallisiin läpisalattuihin OTT-viestintäpalveluihin joissakin merkittävissä rikollisten käyttämissä viestintäverkoissa esiintyneiden häiriöiden vuoksi. Tilannetta vaikeuttaa se, että kansalliset säännöt, joilla asetetaan laillista tietojen sieppausta koskevia velvoitteita, ovat EU:ssa hajanaisia.

Etenemissuunnitelman mukaan komissio aikoo ehdottaa muun muassa seuraavia toimia tilanteen parantamiseksi:

- komissio ehdottaa toimia, joilla parannetaan laillista tietojenhankintaa koskevien rajat ylittävien pyyntöjen tehokkuutta olemassa olevilla välineillä, muun muassa arvioimalla tarvetta vahvistaa edelleen eurooppalaista tutkintamääräystä (EIO);

- komissio kartoittaa toimia, joilla luodaan tasapuoliset toimintaedellytykset kaikentyyppisille viestintäpalvelujen tarjoajille laillista tietojenhankintaa koskevien velvoitteiden täytäntöönpanossa;

- komissio määrittää tehokkaimman tavan puuttua yhteistyöhaluttomia viestintäpalvelujen tarjoajia koskevaan ongelmaan;

- komissio tukee suojattuun tietojenvaihtoon tarkoitettujen valmiuksien käyttöönottoa jäsenvaltioiden, Europolin ja muiden turvallisuusvirastojen välillä.

III) Digitaalinen rikostutkinta

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

Komissio esittää etenemissuunnitelmassa useita toimia, joilla pyritään parantamaan lainvalvontaviranomaisten digitaalisen rikostutkinnan kyvykkyyksiä haltuun otettujen laitteiden tutkinnassa. Komissio aikoo Europolin tuella:

- koordinoida digitaalisen rikostutkinnan yhteisten teknisten ratkaisujen tutkimusta, kehittämistä ja käyttöönottoa ja ylläpitoa koskevaa puute- ja tarveanalyysia;

- tukea edelleen teknisten ratkaisujen kehittämistä digitaalista rikostutkintaa varten asianmukaisten rahoitus- ja koordinaatiomekanismien avulla;

- tukea jäsenvaltioita ja niiden hankintaviranomaisia pilottivaiheesta alkaen niiden toteuttaessa digitaalisen rikostutkinnan välineiden lisenssien yhteishankintoja.

Tämän lisäksi komissio pyytää etenemissuunnitelmassa jäsenvaltioita osallistumaan digitaalisen rikostutkinnan välineiden kehittämiseen, validointiin ja käyttöönottoon. Tähän teemaan liittyy myös Europolin kehittäminen digitaalisen operatiivisen asiantuntemuksen osaamiskeskukseksi sekä komission tuki CEPOLin koulutustyölle.

IV) Todisteiden luettavuuden varmistaminen: datan salauksen purkaminen

Salaus ja muut kyberturvallisuustoimenpiteet ovat tärkeitä tietojärjestelmien suojaamisessa vakoilulta ja häiriöiltä sekä viestinnän, yksityiselämän ja henkilötietojen suojaamisessa. Noin 60 - 80 % viestintäsovelluksista on päästä päähän salattuja, mukaan lukien yleisimmät palveluntarjoajat, kuten WhatsApp, Messenger, Signal ja iMessage, kun taas tekstiviestien ja perinteisten puheluiden käyttö on merkittävästi vähenemässä.

Korkean tason ryhmä korosti, että jäsenvaltioilla on vain vähän asiantuntemusta ja valmiuksia laitteella olevan datan salauksen purkamiseen. Onnistumisasteissa on merkittäviä eroja vaihdellen jäsenvaltioissa 15 - 20 prosentista yli 66 %:iin. Haasteita on monia, kuten se, että salauksen purkamisessa käytettävät laitteet ovat kalliita ja pitkälle erikoistuneita, ja ne kuluttavat paljon resursseja. Useimmat lainvalvontaviranomaiset käyttävät kaupallisia ratkaisuja, joilla on vaikeuksia pysyä teknologisen kehityksen mukana, ja korkeat lisenssikustannukset vähentävät merkittävästi käyttöoikeudet saaneiden käyttäjien määrää. EU:n ulkopuolella kehitetyt kaupalliset ratkaisut eivät välttämättä vastaa EU:n viranomaisten tarpeita tai digitaalisen rikostutkinnan standardeja. Viranomaiset eivät voi päästä edes tehokkaimpien salauksenpurkualustojen avulla tietyntyyppisiin nykyaikaisiin laitteisiin tallennettuun dataan, joka on suojattu kryptosuorittimilla tai vahvoilla salausalgoritmeilla ja monimutkaisilla salasanoilla. Kvanttiturvallisten salausratkaisujen käyttöönotto ja kvanttiavaimen jakamisen kehittäminen ovat ratkaisevan tärkeitä datan turvaamiseksi uudella kvanttiaikakaudella. Tämä vaikeuttaa kuitenkin laillista pääsyä digitaaliseen todistusaineistoon tulevina vuosina, ja lainvalvontaviranomaisten on tehtävä investointeja pysyäkseen mukana teknologian nopeassa kehityksessä.

Etenemissuunnitelman mukana komissio:

- laatii salausta koskevan teknologisen etenemissuunnitelman;

- tukee uusien salauksenpurkuvalmiuksien tutkimusta ja kehittämistä, jotta Europolille voidaan tarjota seuraavan sukupolven salauksenpurkuvalmiudet.

V) Teknologian ja laillisen saatavuuden yhteensovittaminen

Standardit ovat välttämättömiä digitaalisessa viestinnässä. Ne ovat pääasiassa teollisuuden toimijoiden kehittämiä, ja ne takaavat teknologian tarjoajien kehittämien järjestelmien ja laitteiden yhteen toimivuuden ja edistävät teknologioiden yhdenmukaisuutta oikeudellisten velvoitteiden kanssa (ml. lainvalvontaviranomaisten laillinen tietoon pääsy).

Etenemissuunnitelman mukaan komissio:

- kehittää ja virtaviivaistaa tiiviissä yhteistyössä Europolin kanssa standardointitoimia, jotka koskevat tiedon laillista saatavuutta ja joita tuetaan asianmukaisilla hallintomekanismeilla;

- kannustaa jäsenvaltioita osoittamaan riittävät resurssit sen varmistamiseksi, että turvallisuusalan toimijat osallistuvat lainmukaista tietoon pääsyä koskeviin asiaankuuluviin standardointifoorumeihin.

VI) Todistusaineiston tehokas ja lainmukainen analysointi: tekoäly

Komission tiedonannossa viitataan Europolin ja Eurojustin arvioon, jonka mukaan yhtä useammat tutkintatoimet sisältävät erittäin suuria datamääriä, jolloin analysoitava tietomäärä voi olla ylivoimainen ja johtaa käsittelyaikojen pidentymiseen ja tallennuskapasiteettiin liittyviin ongelmiin. Jäsenvaltioilta puuttuu usein mekanismit ja infrastruktuuri, joita tarvitaan suurten tietomäärien siirtämiseksi muihin jäsenvaltioihin ja Europoliin.

Etenemissuunnitelman mukaan komissio:

- edistää 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 tekoälyasetuksen mukaisesti;

- kartoittaa lainvalvontaviranomaisten ja muiden sidosryhmien tarpeita;

- tukee selkeiden ohjeiden laatimista tekoälyn käytöstä lainvalvonnassa;

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

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

Tiedonanto ei ole oikeudellisesti sitova, eikä sillä ole oikeusperustaa.

Käsittely Euroopan parlamentissa

-

Kansallinen valmistelu

Oikeus- ja sisäasioiden EU 7 -jaoston ja viestintäjaoston EU19 kirjallinen menettely 13. - 17.11.2025

Eduskuntakäsittely

-

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

-

Taloudelliset vaikutukset

Etenemissuunnitelma lainvalvontaviranomaisten laillisesta ja tosiasiallinen pääsystä dataan on EU:n komission tiedonanto, eikä se aiheuta suoria taloudellisia vaikutuksia. Taloudellisiin vaikutuksiin otetaan kantaa erikseen tiedonannossa esiteltyjen toimien pohjalta mahdollisesti annettavien lainsäädäntöaloitteiden käsittelyn yhteydessä.

Muut asian käsittelyyn vaikuttavat tekijät

E 39/2025 vp – Komission tiedonanto EU:n sisäisen turvallisuuden strategiasta ”ProtectEU”

E 26/2024 vp – Lainvalvontaviranomaisten lainmukainen tietoon pääsy digitaalisessa ympäristössä eli ns. Going Dark -aloite

Asiakirjat

COM(2025) 349 final

Laatijan ja muiden käsittelijöiden yhteystiedot

Katariina Simonen SM
Hannele Taavila SM
Johanna Puiro SM
Joni Korpinen OM
Amanda Mäkelä OM
Pauliina Penttilä LVM
Anne Lamminmäki VNK

VAHVA-tunnus

EU/805/2025

Liitteet -

Viite -