Sisäministeriö
Inrikesministeriet

**7.4.2026**

**SUURELLE VALIOKUNNALLE**

Sisäministeriö kiittää mahdollisuudesta lausua asiassa U 17/2026 vp, valtioneuvoston kirjelmä eduskunnalle ehdotuksista Euroopan parlamentin ja neuvoston kyberturvallisuusasetukseksi (CSA2) ja NIS 2-muutosdirektiiviksi.

Sisäministeriö katsoo, että lähtökohtaisesti esitettyjen säädösmuutosten tavoitteet, kuten kyberturvallisuuksien kyvykkyyksien ja resilienssin lisääminen, ovat sellaisinaan kannatettavia tavoitteita.

Valtioneuvoston kannan mukaan asiaankuuluvilla viranomaisilla tulisi olla paremmat edellytykset estää, havaita ja torjua kyberturvallisuusuhkia. Näin ollen sisäministeriö pitää tärkeänä, että CSA2 ja NIS2 neuvotteluissa huomioidaan valtioneuvoston sisäisen turvallisuuden selonteon (VNS 6/2025 vp, s. 20) mukaisesti se, että lainsäädännön tulee varmistaa lainvalvontaviranomaisten pääsy tietoon kybertoimintaympäristössä ja tulee kehittää toimivaltuuksia ja työvälineitä verkossa tapahtuvien rikosten torjuntaan. Lisäksi selonteon mukaan tulee panostaa kyberuhkien havaitsemiseen ja torjuntaan sekä niihin liittyvään tiedonvaihtoon turvallisuusviranomaisten välillä.

Oikeus ja lainvalvontaviranomaisten digitaaliseen tietoon pääsyn haasteet on tunnistettu EU-tasolla pitkään, ja näihin haasteisiin vastaamiseksi on tehty paljon aloitteita EU-tasolla, kuten korkean tason asiantuntijaryhmän asettaminen vuonna 2023, kyseisen ryhmän loppuraportti suosituksineen vuonna 2024[1] ja komission vuoden 2025 etenemissuunnitelma tietoon pääsyn haasteiden ratkaisemiseksi (COM(2025) 349 final). Usea EU-virasto on osallistunut tähän työhön, ml. ENISA. Työn tarkoituksena on ollut selvittää multilateraalisessa moniviranomaisyhteistyössä, mitä konkreettisia käytännön haasteita ja teknisiä haasteita oikeus- ja lainvalvontaviranomaiset kohtaavat pääsyssä digitaalisessa ympäristössä olevaan tietoon.

Sisäministeriö kiinnittää huomiota eduskuntaselvitykseen (E 26/2024 vp), jonka mukaan ”Suomi pitää tärkeänä, että tunnistettaviin ongelmiin on tärkeä etsiä EU-tason ratkaisuja sen tietoon pääsemiseksi tarkkaan rajatuissa tapauksissa. Ratkaisujen tavoitteena tulisi olla rikosten ennalta estäminen, paljastaminen ja selvittäminen sekä syyteharkintaan saattaminen ja yleisen turvallisuuden vahvistaminen, ja niissä on huomioitava täysimääräisesti EU:n perusoikeuskirjasta, tietosuojalainsäädännöstä ja EU:n tuomioistuimen oikeuskäytännöstä johtuvat velvoitteet. Keskeistä on se, että ratkaisuilla varmistetaan oikeasuhtaisesti kaikkien perusoikeuksien toteutuminen.” Saman selvityksen mukaan ”Suomi pitää tärkeänä, että EU-tasolla kehitetään sellainen

[1] High-Level Group (HLG) on access to data for effective law enforcement - Migration and Home Affairs

Kirkkokatu 12, Helsinki
PL 26, 00023 Valtioneuvosto
Vaihde 0295 480 171 | kirjaamo.sm@gov.fi | www.intermin.fi

tasapainoinen, teknologianeutraali ja oikeasuhtainen lähestymistapa tietoon pääsyyn parantamiseksi, joka samanaikaisesti huomioi tarpeen turvata vahva salaus sekä viranomaisten laissa tarkkarajaisesti määritelty mahdollisuus yksittäistapauksissa päästä salattuihin tietoihin ja sähköiseen aineistoon". Näitä huomioita vasten sisäministeriö pitää erittäin tärkeänä sitä, että jatkoneuvotteluissa lainvalvontaviranomaisten digitaaliseen tietoon pääsyn tarpeet tehtäviensä suorittamiseksi tulevat huomioon otetuksi.

Sisäministeriö pitää valitettavana, että komission toteuttamassa vaikutustenarvioinnissa ei ole juurikaan arvioitu lainsäädäntöpaketin vaikutuksia lainvalvontaviranomaisten toimintaan. Myöskään kyberturvallisuusasetusehdotuksen resitaaleista ei käy ilmi, että asetuksessa olisi huomioitu lainvalvontaviranomaisten digitaaliseen tietoon pääsyn tarpeet tai viimeaikaisen teknologisen kehityksen vaikutus viranomaisten pääsyssä tietoon.

Sisäministeriö kiinnittää huomiota ehdotetun sääntelyn sertifiointia koskeviin toimiin. Jatkoneuvotteluissa tulisi varmistaa, että myös lainvalvontaviranomaiset on nimetty niiksi viranomaisiksi, jotka ovat kehittämässä sertifiointimääritelmiä. Lainvalvontaviranomaisten tarpeiden huomioiminen etukäteisesti olisi turvattava. Tämän huomioiminen olisi linjassa eduskuntaselvityksen (E 26/2024 vp) kanssa, jossa todetaan, että "Suomi pitää tärkeänä lainvalvontaviranomaisten osallistumista standardointikomiteoiden ja työryhmien työhön, jotta lainvalvontaviranomaisten tarpeet tulevat huomioitua tuotekehittelyssä ja suunnittelussa etukäteisesti. Tässä yhteydessä Suomi pitää tärkeänä selvittää mahdollisia teknisiä ratkaisuja ja juridisia velvoitteita palvelujen kehittämiseksi siten, että ne mahdollistavat viranomaisen reaaliaikaiseen tietoon pääsyä."

Sisäministeriö kiinnittää vielä huomiota haavoittuvuustiedon hallintaa koskeviin suunnitelmiin asetusehdotuksen haavoittuvuuksien hallintapalveluista koskevassa 16 artiklassa ja katsoo, että jatkoneuvotteluissa on tarve arvioida, tulisiko tietojen luovuttamisesta myös Europolille säätää nimenomaisesti. Samoin sisäministeriö kiinnittää huomiota U-kirjeen sivulla 13 mainittuun NIS2 muutosehdotukseen koskien poikkeamista ilmoittamisvelvoitetta. Lainvalvontaviranomaisten rooli jää esityksessä tältä osin epäselväksi ja sitäkin tulisi jatkoneuvotteluissa tarkentaa.

Johanna Puiro
Johtava asiantuntija
Poliisiosasto