Eduskunnan hallintovaliokunta

Suojelupoliisin lausunto hallituksen esityksestä eduskunnalle laeiksi sähköisen viestinnän palveluista annetun lain, henkilötietojen käsittelystä Puolustusvoimissa annetun lain 29 §:n ja henkilötietojen käsittelystä poliisitoimessa annetun lain 22 §:n muuttamisesta (HE 243/2022 vp).

Eduskunnan hallintovaliokunta on pyytänyt Suojelupoliisin lausuntoa otsikossa mainitusta asiasta. Suojelupoliisi lausuu kunnioittavasti seuraavaa:

Suojelupoliisi pitää ehdotettuja lainsäädännön muutosesityksiä perusteltuina ja erittäin tarpeellisina, sillä esitys parantaisi olennaisesti yhteiskunnan edellytyksiä torjua yhteiskunnan elintärkeisiin toimintoihin kohdistuvia vakavimpia kyberuhkia.

Esitys ei loisi viranomaisille uusia tehtäviä tai toimivaltuuksia, vaan se mahdollistaa olemassa olevien vastuiden ja velvoitteiden mahdollisimman tehokkaan toteuttamisen tavalla, jota nykysääntely ei kaikilta osin tue.

Esitys korjaa tiedonsaantiongelman vakavimmissa tietoturvaloukkaustilanteissa

Yhteiskunnan toiminta perustuu entistä enemmän digitaalisiin järjestelmiin samaan aikaan, kun geopoliittinen tilanne on entistä jännitteisempi. Yhteiskuntamme toiminta voidaan lamauttaa verkon yli ilman, että tekijä astuu fyysisesti Suomen maaperälle. Silti nykyinen sääntely asettaa esteitä viranomaisten keskinäiselle tiedonkululle, jolloin yhteiskunnan elintärkeisiin toimintoihin kohdistuvia nopeasti kärjistyviä uhkia ei voida torjua tehokkaasti.

Sähköisen viestinnän palveluista annettuun lakiin esitetty uusi 319 a § korjaisi tietojen vaihdossa tunnistetun keskeisen ongelman: kaikki toimivaltaiset viranomaiset eivät saa ajoissa tietoa vakavasta tietoturvaloukkauksesta, jolloin ne eivät voi käynnistää toimenpiteitä yhteiskunnan ja sen jäsenten suojaamiseksi.

Vakavassa tietoturvaloukkaustilanteessa tarvitaan kolme rinnakkaista prosessia yhteiskunnan eri etujen turvaamiseksi:

1. Tekninen tietoturvaprosessi, jonka tavoitteena on pysäyttää tekninen poikkeama, estää jatkovahinko tietojärjestelmässä sekä palauttaa kohdejärjestelmä turvalliseen tilaan. Tietoturvaprosessissa myös pyritään estämään saman kaltainen poikkeama muissa kohteissa.

Pelkkä tekninen selvitys ei kuitenkaan riitä torjumaan tahallista uhkaa, eikä estämään sen toistumista. Tarvitaan myös:

2. Rikosprosessi, jonka tavoitteena on rajata rikosvahinko, selvittää tapahtuman tosiasiat rikosoikeuden näkökulmasta, ja kohdistaa tekijään rikosseuraamus.
3. Kansallisen turvallisuuden suojaamisen prosessi, jonka tavoitteena on estää jatkovahinko kansalliselle turvallisuudelle sekä selvittää tosiseikat ulko- ja

turvallisuuspoliittisen päätöksenteon tueksi, jotta Suomi voi reagoida asianmukaisella tavalla.

Kukin prosesseista on aikakriittinen, ja niillä kaikilla on vahingon rajaamisessa ja yhteiskunnan toipumisessa oma tehtävänsä, jota toinen prosessi ei voi korvata. Eri toimivaltuuksin hankitun tietojen jakaminen muille viranomaisille muihin turvallisuustehtäviin on havaittu erittäin hankalaksi, vaikka se olisi nopeassa tilanteessa välttämätöntä yhteiskunnan suojaamiseksi, ja vaikka muilla viranomaisilla olisi oikeus tiedon käsittelemiseen, jos sen vain haltuunsa saisivat.

Tietoturvaprosessissa on tehokkaimmat tiedonsaantioikeudet, koska tiedon käyttöala on puhtaasti teknisen poikkeaman selvittäminen ja siitä toipuminen. Sen sijaan kahteen muuhun prosessiin liittyy akuutin uhkan pysäyttämisen lisäksi seuraamusmenettelyn valmistelu ja seuraamuksesta päättäminen. Rikosprosessissa poliisi suorittaa akuutin rikostorjunnan lisäksi esitutkinnan syyttäjälle ja syyttäjä edelleen valmistelee asian tuomioistuimen ratkaistavaksi. Kansallisen turvallisuuden suojaamiseen liittyy akuutin uhkan torjunnan lisäksi ulko- ja turvallisuuspoliittisen päätöksenteon valmistelu, jossa ensivaiheen vastuuviranomainen on joko Suojelupoliisi tai sotilastiedustelu riippuen tietojärjestelmästä, joka on joutunut ulkovallan vihamielisen vaikuttamisen kohteeksi. Kummassakin selvitysprosessissa tarvitaan nopeasti teknistä tunnistetietoa tekijän jäljittämiseksi, koska verkossa jälki katoaa nopeasti.

Vaihdettava tieto voi olla viestinnän tietoa tai henkilötietoa

Vaihdettavat tiedot voivat olla teknisesti luonteeltaan viestinnän tietoja, sillä hyökkäystarkoituksessa lähetetty liikenne on usein naamioitu harmittomaksi viestinnäksi, jotta sitä ei tunnistettaisi. Olisi kuitenkin varsin poikkeuksellista, että luovutettava data sisältäisi sivullisten viestintää, sillä esitys rajaa luovutuksen vain vastaanottavan viranomaisen tehtävän kannalta välttämättömään tietoon, ja esitys jättää luovuttavalle viranomaiselle luovutukseen harkintavaltaa.

Erikoistutkija Sari Kajantie