19.7.2017

EOAK/6148/2016

Ratkaisija: Apulaisoikeusasiamiehen sijainen Pasi Pölönen

Esittelijä: Tarkastaja Peter Fagerholm

Viite**:** 1.12.2016 vireille tullut kantelu

SALASSA PIDETTÄVÄN TIETOAINEISTON LÄHETTÄMINEN SÄHKÖPOSTITSE

1 KANTELU

Kantelija arvosteli --- poliisilaitoksen menettelyä esitutkintapöytäkirjan lähettämistavassa. Kantelija kertoo pyytäneensä, että hänen tilaamansa esitutkintapöytäkirja tulisi lähettää hänelle sähköpostitse. Se lähetettiin hänelle kuitenkin postitse. Hän kysyi, mihin perustuen pöytäkirjaa ei voitu lähettää hänelle sähköpostitse.

2 SELVITYS

Kantelun johdosta hankittiin poliisilaitoksen selvitys ja lausunto. Asiassa hankittiin myös Poliisihallituksen lausunto.

2.1
Selvitykset ja lausunnot

Tutkintasihteeri --- mukaan hän ei ollut kuullut tai lukenut mistään, että pöytäkirjat saisi lähettää sähköpostitse. Hän kertoo keskustelleensa pöytäkirjan lähettämistavasta rikoskomisario --- kanssa. Rikoskomisario A oli ohjeistanut, että kantelijan pyytämä pöytäkirja tulee lähettää hänelle postitse. Tutkintasihteerin selvityksen perusteella poliisilaitoksen eri toimipisteiden välillä oli ainakin tapahtumahetkellä erilaiset käytännöt pöytäkirjojen lähettämistavoissa.

Rikoskomisario A:n mukaan hän ei muista kantelijan tapausta. Hän kertoo kuitenkin lukuisia kertoja antaneensa tutkintasihteerille ohjeen lähettää pöytäkirjat postitse. Tämä johtui komisario A:n mukaan lähinnä teknisistä syistä, koska toimiston skannauskoneen syöttölaite oli epäkunnossa. Hän toteaa kuitenkin, että tavoitteena on palvella asiakkaita jatkossa ensisijaisesti sähköisesti.

Rikosylikomisario --- mukaan kantelijan pyytämässä pöytäkirjassa oli salassa pidettävää aineistoa. Viitaten poliisihallinnon määräyksiin Rikosylikomisario toteaa, että pöytäkirja olisi silti voitu lähettää kantelijalle sähköpostitse poliisihallinnon hyväksymän salausohjelman kautta.

Rikosylikomisarion mukaan --- pääpoliisiasemalla otettiin syksyllä 2016 käyttöön esitutkintapöytäkirjojen lähettäminen salatussa sähköpostissa. Vuoden 2017 tammikuussa rikostutkintasektorin ohjausryhmän kokouksessa ohjeistettiin kaikkien poliisiasemien tutkintayksiköitä siitä, että tarvittaessa esitutkintapöytäkirjat voidaan lähettää salatussa

sähköpostissa. Hän toteaa, että Tutkintasihteerin olisi tullut lähettää pöytäkirja kantelijalle salatussa sähköpostissa. Näin toteaa myös poliisilaitos omassa lausunnossaan.

Poliisihallitus on lausunnossaan seikkaperäisesti käsitellyt muun muassa asiakirjapyyntöihin liittyvää lainsäädäntöä sekä Poliisihallituksen ohjeistusta ja menettelytapoja liittyen salassa pidettävien asiakirjojen lähettämiseen.

Poliisihallitus toteaa, että poliisin salassa pidettävien tietoaineistojen käsittelyä koskevan ohjeen (POL-2015-3101) kohdan 3.7 mukaan suojaustasoille IV ja III kuuluvaa tietoaineistoa voidaan periaatteessa toimittaa hallinnon ulkopuoliselle asiakkaalle sähköisessä muodossa sähköpostin välityksellä asianmukaisesti salattuna. Aineiston tulee olla salattu suojaustasolle hyväksytyllä menetelmällä (salausohjelmisto). Poliisihallinnossa noudatetaan Poliisihallituksen mukaan Viestintäviraston asiaa koskevaa ohjeistusta ja käytössä on Viestintäviraston hyväksymät salausohjelmistot kullekin suojaustasolle. Poliisilla tällä hetkellä käytössä olevat, tässä tapauksessa kyseeseen tulevat salausohjelmistot ovat Poliisihallituksen mukaan Deltagon (suojaustasolle IV) ja KiloCrypt (suojaustasolle III). Poliisihallinnossa käytössä oleva Deltagon-salausohjelmisto on Poliisihallituksen mukaan tietoturvallinen tapa välittää tietoa salattuna poliisihallinnon ja ulkoisten toimijoiden välillä aina suojaustasolle IV asti. Palvelu on automaattisesti käytössä kaikilla poliisin sähköpostia käyttävillä.

Suojaustason III asiakirjoihin Deltagon-salaus ei Poliisihallituksen mukaan kuitenkaan enää riitä, joten suojaustason III asiakirjoja ei voida lähettää Deltagon -ohjelmiston välityksellä. Tällä hetkellä poliisihallinnossa ainoa sallittu tapa lähettää sähköisesti suojaustason III asiakirjoja on lähettää salassa pidettävä aineisto Kilocrypt-ohjelmiston välityksellä. Kilocrypt-salauksen käyttö edellyttää samanlaista Kilocrypt-ohjelmaa sekä asiakirjan lähettävältä että vastaanottavalta taholta. KiloCrypt-ohjelma ei ole julkisessa jaossa oleva ohjelmisto. Näin ollen suojaustason III asiakirjojen lähettäminen poliisihallinnon ja Tuve-verkon ulkopuolelle sähköpostitse on Poliisihallituksen mukaan tällä hetkellä käytännössä mahdotonta.

Poliisihallitukselle osoitetussa lausuntopyynnössä on erikseen pyydetty ottamaan kantaa myös asiakkaan tunnistautumiseen salassa pidettäviä tietoja luovuttaessa.

Poliisihallitus toteaa, että annettaessa tietoja salassa pidettävistä asiakirjoista on varmistauduttava pyytäjän henkilöllisyydestä. Asiaa säännellään laissa sähköisestä asioinnista viranomaistoiminnassa (534/2016). Lain 18 §:n 2 momentin mukaan asianosaisen tai tämän edustajan on tunnistauduttava asiakirjaa noutaessaan. Tunnistautumisessa on tällöin käytettävä tunnistautumistekniikkaa, joka on tietoturvallinen ja todisteellinen.

Poliisihallituksen käsityksen mukaan henkilön osoitetietojen (mukaan lukien sähköpostiosoite) oikeellisuuden varmistamisesta ei ole erillisiä säännöksiä tai ohjeita, vaan asiaa tulee arvioida lähinnä viranomaisen yleisen huolellisuusvelvoitteen näkökulmasta. Deltagon-ohjelman turvaominaisuutena on kuitenkin se, että ohjelma antaa avata salatun sähköpostin vain siitä sähköpostiosoitteesta käsin, johon viesti on lähetetty.

Poliisihallitus toteaa, että poliisi käyttää asiassa tapauskohtaista harkintaa. Lähtökohtana on kuitenkin se, että mikäli asiakkaalle luovutetaan salassa pidettävää aineistoa, henkilön identiteetti tulisi varmistaa aukottomasti. Käytännössä, kun kyse on asiakkaan omassa intressissä tapahtuvasta tietojen suojaamisesta, poliisi luottaa melko pitkälti asiakkaan itse ilmoittamien yhteystietojen oikeellisuuteen. Poliisihallituksen mukaan asianmukaisena menettelytapana voitaisiin pitää esimerkiksi sitä, että henkilökohtaisesti tavattu ja tunnistettu henkilö ilmoittaa tietyn sähköpostiosoitteen omaksi yhteystiedokseen.

Viitaten asiakirjojen salassapitoperusteihin Poliisihallitus toteaa, että niiden perimmäinen tarkoitus on suojata asiakkaan yksityisyyttä ja häntä koskevia arkaluonteisia tietoja sivullisilta. Toisaalta Poliisihallitus toteaa myös, että salassa pidettävän aineiston luokittelun oikeellisuuteen tulee kiinnittää erityistä huomiota, jotta yhtäältä vältyttäisiin yliluokittelusta johtuvilta asiakirjojen käsittelylle aiheutuvilta hankaluuksilta ja jotta toisaalta asiakirjojen sisältämä tieto tulisi kuitenkin aina asianmukaisesti suojatuksi.

Lausuntonaan Poliisihallitus katsoo, vastoin poliisilaitoksen näkemystä, ettei kantelijalle olisi voitu lähettää esitutkintapöytäkirjaa sähköpostitse edes salattuna, koska se sisälsi suojaustason III tietoaineistoa. Suojaustason III tietoaineistoa ei voida tietoturvallisesti välittää hallinnon ulkopuolelle poliisihallinnossa yleisesti käytössä olevan Deltagon-ohjelmiston kautta. Tämän suojaustason tietoaineiston lähettämiseen soveltuva, poliisihallinnon käytössä oleva salausohjelma KiloCrypt ei ole yleisesti ulkopuolisten asiakkaiden saatavilla. Näin ollen Poliisihallituksen mukaan esitutkintapöytäkirjaa ei olisi voitu lähettää kantelijalle sähköpostitse.

Poliisihallitus toteaa, että poliisilaitoksen on syytä arvioida uudelleen esitutkintapöytäkirjan toimittamista koskevaa ohjeistustaan. Poliisihallitus kertoo tästä syystä lähettäneensä lausuntonsa tiedoksi myös poliisilaitokselle.

3 RATKAISU

3.1
Oikeusohjeita
Poliisihallinnossa, kuten yleensä koko julkishallinnossa, käsitellään paljon sekä julkista että salassa pidettävä tietoa. Viranomaisille on lainsäädännössä asetettu lukuisia tietoturvavelvoitteita ja velvoitteita henkilötietojen suojaamiseen. Tietoturvallisuus perustuu viranomaisten toiminnan julkisuudesta annettuun lakiin (jäljempänä julkisuuslaki) sekä lukuisiin muihin lakeihin. Julkisuuslain tarkoituksena on muun muassa toteuttaa avoimuutta ja hyvää tiedonhallintatapaa viranomaisten toiminnassa.

Julkisuuslain 18 §:n mukaan viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä.

Henkilötietolain 32 §:n 1 momentin mukaan rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta.

Myös julkisuuslaki kiinnittää huomiota henkilötietojen suojaan sähköisessä muodossa olevien asiakirjojen luovuttamisesta puhuttaessa. Julkisuuslain 16 §:n 3 momentin mukaan viranomaisen henkilörekisteristä saa antaa henkilötietoja sisältävän kopion tai tulosteen tai sen tiedot sähköisessä muodossa, jollei laissa ole toisin erikseen säädetty, jos luovutuksensaajalla on henkilötietojen suojaa koskevien säännösten mukaan oikeus tallettaa ja käyttää sellaisia henkilötietoja.

Sähköisestä asioinnista viranomaistoiminnassa annetun lain 19 §:ssä säädetään tavallisesta sähköisestä tiedoksiannosta. Säännöksen mukaan muu kuin 18 §:ssä tarkoitettu asiakirja [lain mukaan postitse saantitodistusta vastaan toimitettava tai muuten todisteellisesti toimitettava asiakirja] voidaan antaa tiedoksi asianomaiselle sähköisenä viestinä hänen suostumuksellaan. Jos kuitenkin asianomaisen yksityisyyden suojaaminen, muu erityinen suojan tai suojelun tarve taikka oikeuksien turvaaminen sitä edellyttää, asiakirjan tiedoksiantoon on sovellettava, mitä 18 §:ssä tai tiedoksiannosta muutoin säädetään. Viitatun 18 §:n 2 momentin mukaan asianosaisen tai tämän edustajan on tunnistauduttava asiakirjaa noutaessaan. Tunnistautumisessa on tällöin käytettävä tunnistautumistekniikkaa, joka on tietoturvallinen ja todisteellinen (lainmuutoksella 534/2016 momentista poistettiin siinä ollut viittaus vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa tarkoitettuun tunnistusvälineeseen ja laatuvarmenteeseen).

Vahvasta sähköisestä tunnistamisesta ja sähköisistä luottamuspalveluista annetussa laissa säädetään sähköisen tunnistamisen järjestelmälle asetettavista vaatimuksista. Julkishallinnon kaikissa palveluissa ei ole toistaiseksi käyttömahdollisuutta vahvalle sähköiselle tunnistautumiselle. Vahvassa sähköisessä tunnistautumisessa käytetään tunnistusvälineenä pankkien verkkopankkitunnuksia, Väestörekisterikeskuksen kansalaisvarmenteita tai teleyritysten mobiilivarmenteita.

Tietoturvallisuudesta valtionhallinnossa annetun valtioneuvoston asetuksen 19 §:n 3 momentin mukaan valtionhallinnon viranomainen voi sallia, että suojaustasoon III kuuluva asiakirja siirretään viranomaisen tietoverkossa, jonka käyttö on rajoitettu, jos viranomainen on varmistanut, että tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät tavanomaisesti sovellettavan korotetun tietoturvallisuuden tason vaatimukset. Sama koskee suojaustasoon IV kuuluvien valtakunnalliseen henkilörekisteriin talletettujen arkaluonteisten henkilötietojen tai biometristen tunnistetietojen siirtämistä tietoverkossa. Suojaustasoon IV kuuluvan muun asiakirjan saa siirtää valtionhallinnon viranomaisen päättämällä tavalla.

Tietosuojavaltuutetun (esim. Dnro 1475/41/2009) mukaan käsiteltäessä henkilörekisteriin kuuluvia henkilötietoja automaattisen tietojenkäsittelyn avulla, esimerkiksi lähettämällä sähköpostitse henkilötietoja, tulee henkilötietolaissa mainitut huolellisuus- ja suojaamisvelvoitteet ottaa riittävällä tavalla huomioon. Arkaluontoisia tai lain mukaan salassa pidettäviä henkilötietoja ei tulisi lähettää suojaamattomassa sähköpostiyhteydessä. Tietosuojavaltuutettu on katsonut, että rekisterinpitäjä ei voi poiketa henkilötietojen suojaamisvelvollisuudestaan edes rekisteröidyn suostumuksella.

3.2
Asian arviointia

Tietojen saaminen viranomaisten asiakirjoista nykyaikana tyypillisesti käytettävillä tavoilla ja välineillä on julkisuusperiaatteen kannalta perusteltua. Esitutkintapöytäkirjoja tilataan poliisilta käsitykseni mukaan enenevissä määrin juuri sähköpostitse. Kuitenkin, kuten edellä mainituista säännöksistä ilmenee, salassa pidettävän asiakirjan sähköpostitse toimittamista rajoittavat erilaiset tietoturvaan, henkilön tunnistamiseen ja henkilötietojen suojaan liittyvät tekijät. Näiden rajoittavien tekijöiden taustalla on julkisuusperiaatteen kanssa yhteen sovitettavia muita perusoikeuksia kuten tarve suojella yksityiselämää.

Viranomaisten lähettäessä salassa pidettävää tietoaineistoa sähköpostitse hallinnon ulkopuoliseen verkkoon on yhtäältä kysymys siitä, miten tietoaineisto voidaan lähettää tietoturvallisesti siten, ettei siihen ulkopuolinen pääse käsiksi. Tätä varten on, kuten

Poliisihallituksen lausunnosta ja ohjeesta ilmenee, olemassa Viestintäviraston eri aineistojen suojaustasoille hyväksymät salausohjelmat. Käytettävissäni olevan aineiston perusteella minulla ei ole aihetta epäillä kyseisten Poliisihallituksen mainitsemien salausohjelmien teknisiä vaatimuksia ja/tai soveltuvuutta käytettäväksi kyseisiin tarkoituksiin. Viittaan tältä osin siis Poliisihallituksen lausuntoon.

Asiassa on kyse paitsi sähköpostin salauksesta myös siitä, miten voidaan luotettavasti varmistaa, että vastaanottaja on se, joka hän väittää olevansa (asiakkaan tunnistaminen). Esimerkiksi lähetettäessä salassa pidettäviä mutta asianosaisjulkisia tietoja sähköpostitse tulee olla varmaa, että viesti lähetetään vain sellaiselle henkilölle, jolla on oikeus tiedon saantiin. Ellei asiakasta ja/tai hänen yhteystietojaan voida luotettavalla tavalla tunnistaa, on mahdollista, että salassa pidettävää tietoa tai henkilötietoja tulee lähetetyksi sellaiselle henkilölle, jolla ei ole lakiin perustuvaa oikeutta kyseeseen tulevan tiedon saamiseen.

Henkilön tunnistamisessa Poliisihallitus on ilmoittanut poliisihallinnossa käytettävän tapauskohtaista harkintaa. Lähtökohtana se pitää, että henkilön identiteetti tulisi varmistaa aukottomasti, mikäli hänelle luovutetaan salassa pidettävää aineistoa. Tämä voi Poliisihallituksen mukaan tarkoittaa henkilökohtaista tapaamista, jonka yhteydessä henkilö ilmoittaa yhteystietonsa. Totean, että tunnistamisen tavoista ei ole säädetty laissa tai muissa oikeusnormeissa kattavasti tai yksityiskohtaisesti. Käsitykseni mukaan asiakkaan tunnistaminen yksin sähköpostiviestin tai puhelinsoiton perusteella voi kuitenkin olla ongelmallista.

Asiassa on kyse myös salassa pidettävän tietoaineiston luokittelun oikeellisuudesta, kuten Poliisihallitus lausunnossaan aiheellisesti korostaa. Kuten Poliisihallitus toteaa, tietoaineisto tulee suojata asianmukaisesti. Mikäli kuitenkin tapahtuu Poliisihallituksen mainitsemaa ”yliluokittelua”, voi tämä vaikeuttaa tai jopa kokonaan estää tietoaineiston lähettämistä sähköpostitse. Erityisesti koska julkishallinnon asiakkaat käyttävät enenevissä määrin viranomaisten sähköisiä palveluja ja suosivat sähköpostin käyttöä tavanomaisen postin sijaan, tulee asiantila nähdäkseni huomioida ja asiakirjojen luokittelu eri suojaustasoihin tehdä tarkasti ja mahdollisimman yhdenmukaisin kriteerein.

Selvyyden vuoksi totean vielä, että asiakirjan turvallisuusluokittelu (esimerkiksi suojaustasolle III tai IV) ei itsessään tarkoita päätöstä asiakirjojen tai sen sisältämien tietojen julkisuudesta tai salassapidosta. Puhuttu luokittelu perustuu asetustasoiseen säädökseen eikä voi ohittaa perustuslaissa ja lakitasolla säädettyä julkisuusperiaatetta. Viranomaisen asiakirjan julkisuus ratkaistaan julkisuuslain tai julkisuudesta erikseen annettujen muiden lakien perusteella.

3.3
Kannanotto Tämän asian arvioinnissa yhdyn pitkälti Poliisihallituksen lausunnossaan esittämään. --- poliisilaitos on lähettänyt salassa pidettävää tietoaineistoa sisältävän esitutkintapöytäkirjan kantelijalle postitse. Menettely on ollut asianmukainen eikä se anna minulle aihetta toimenpiteisiin.

Totean, että poliisilaitoksella näyttää kuitenkin olleen virheellinen käsitys salassa pidettävän tietoaineiston lähettämistavasta kyseisen suojaustason (III) osalta. Poliisihallitus on korjannut poliisilaitoksen virheellisen käsityksen toimittamalla sille jäljennöksen lausunnostaan.

4
Toimenpiteet

Käsillä olevan yksittäisen asian selvitetty tila huomioon ottaen pidän riittävänä toimenpiteenä kiinnittää --- poliisilaitoksen huomiota edellä esittämiini käsityksiin ja Poliisihallituksen lausunnossa esitettyyn.

Pyydän --- poliisilaitosta ilmoittamaan 29.9.2017 mennessä, mihin toimenpiteisiin se on mahdollisesti ryhtynyt Poliisihallituksen lausunnon johdosta.

Edellä lausutussa tarkoituksessa lähetän jäljennöksen tästä päätöksestäni --- poliisilaitokselle.

Lähetän jäljennöksen päätöksestäni myös Poliisihallitukselle tiedoksi. Koska asialla on nähdäkseni yleisempää merkitystä, pyydän, että Poliisihallitus saattaa päätökseni kaikkien poliisiyksiköiden tietoon.