Tietosuojavaltuutetun toimisto

Ylitarkastaja Heikki Partanen

HE 9/2018 vp

13.3.2018

Eduskunnan lakivaliokunta ja perustuslakivaliokunta

Muistio HE:stä koskien EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi erityisesti ehdotuksista, jotka liittyvät hallinnollisiin sakkoihin ja rikosoikeudellisiin seuraamuksiin

Kun arvioidaan henkilötietojen suojaa koskevien säännösten rikkomisen seuraamuksia tietosuoja-asetuksen (lyh. TSA) mukaan, on perusteltua tarkastella seuraamusjärjestelmää kokonaisuutena, joka kattaa valvontaviranomaisen TSA 58 artiklan 2 kohdassa tarkoitetut korjaavat toimivaltuudet ja viime kädessä TSA 83 artiklassa tarkoitetut hallinnollisen sakot sekä TSA 84 artiklassa tarkoitetut ennen kaikkea rikosoikeudelliset seuraamukset. TSA:n johdanto-osan 149 kohdan mukaan jäsenvaltiot voivat vahvistaa tämän asetuksen rikkomiseen sekä tämän asetuksen mukaisesti ja siinä asetuissa rajoissa annettujen kansallisten sääntöjen rikkomiseen sovellettavia rikosoikeudellisia seuraamuksia koskevat säännöt ottaen kuitenkin huomioon kaksoisrangaistavuuden kielto.

Seuraavassa esitellään ensin henkilötietolain mukainen seuraamusjärjestelmä ja tämän hetkisen seuraamusjärjestelmän painopisteen eli rikosoikeudelliseen vastuuseen ja kehittymiseen vaikuttaneet säännökset. Sen jälkeen arvioidaan TSA:n 83 artiklan 7 kohtaan perustuvaa ehdotusta ja sen perusteluita siitä, ettei hallinnolliset sakot tulisi miltään osin sovellettavaksi viranomaistoiminnassa tapahtuvan henkilötietojen käsittelyn osalta. Kolmanneksi tarkastellaan seuraamusjärjestelmän painopisteen muuttamista rikosoikeudellisesta vastuusta hallinnollisiin seuraamusmaksuihin. Viimeisenä arvioidaan muutettavaksi ehdotettua rikoslain 38 luvun 9 §:n tunnusmerkistöä ja ehdotetaan korvaavia rikostunnusmerkistöjä.

1. Seuraamusjärjestelmä henkilötietolain ja rikoslain mukaan

Henkilötietolain mukainen seuraamusjärjestelmä perustuu lain 44 §:ssä tarkoitettuihin tietosuojalautakunnan määräyksiin, joilla kielletään lainvastainen käsittely, velvoitetaan oikaisemaan laiminlyönti, määrätään rekisteritoiminta lopetettavaksi taikka peruutetaan tietosuojalautakunnan myöntämä lupa. Tietosuojavaltuutetun toimivalta on lain 40 §:n perusteella rajoitettu siihen, että hänen on pyrittävä ohjein ja neuvoin siihen, ettei lainvastaista menettelyä jatketa tai uusita. Lisäksi hän voi tarvittaessa saattaa asian tietosuojalautakunnan käsiteltäväksi tai ilmoitettava asia syytteeseen panoa varten (käytännössä tutkintapyyntö esitutkinnan suorittamiseksi). Ainoa taloudellinen seuraus on mahdollinen em. tietosuojalautakunnan määräysten

tehosteeksi annettu ja määrätty uhkasakko, jota ei voi pitää rangaistuksen luonteisena seuraamuksena vaan annetun määräyksen noudattamisen tehosteena.

Kun tietosuojavaltuutettu on vuosittain vienyt tietosuojalautakunnan käsiteltäväksi muutamia määräysasioita eikä juurikaan ole itse tehnyt tutkintapyyntöjä esitutkinnan aloittamiseksi, on henkilötietojen suojan rikosoikeudellinen seurausjärjestelmä kehittynyt lähinnä rekisterinpitäjien ja asianomistajien tekemien tutkintapyyntöjen ja esitutkinnassa muuten ilmi tulleista epäilyttävien henkilötietojen käsittelytapauksien kautta.

Tietosuojaviranomaisen panos rikosoikeudellisen seuraamusjärjestelmän kehittymisessä on liittynyt rikoslain 38 luvun 10 §:n 3 momentissa tarkoitettuun lausunto- ja kuulemismenettelyyn. Tämän menettelyn tarkoituksena on henkilötietojen suojaan liittyvän oikeudellisen asiantuntemuksen hyödyntäminen tämän tyyppisissä data- ja informaatiorikosvastuun tapauksissa. Olennaista on myös se, että lausunto- ja kuulemismenettely ei koske vain henkilötietolain vastaista tekoa tai laiminlyöntiä vaan se koskee rikoslain 38 luvun muitakin tunnusmerkistöjä, jolla on katsottu olevan merkitystä henkilötietojen suojan näkökulmasta. Näitä tunnusmerkistöjä ovat henkilörekisteririkoksen lisäksi salassapitorikokset, henkilötietoihin kohdistuvat tietomurrot datarikoksina sekä viestintäsalaisuuden loukkaukset. Lisäksi viranomaistoiminnassa lain vastaista henkilötietojen käsittelyä on arvioitu virkavelvollisuuden rikkomisena (ks. KKO 2014:86).

2. Ei hallinnollisia sakkoja viranomaisille – ehdotuksen perusteluista (s.56 – 57)

Hallituksen esityksessä ehdotetaan, että Suomi käyttäisi tietosuoja-asetuksen 83 artiklan 7 kohdasta ilmenevää kansallista liikkumavaraa siten, ettei hallinnollisia sakkoja voitaisiin miltään osin määrätä viranomaisille ja itsenäisille julkisoikeudellisille laitoksille. Ehdotusta on perusteltu sillä, että tällainen viranomaiseen kohdistuva rangaistusluonteinen hallinnollinen seuraamus olisi **nykyisen oikeusjärjestyksen kannalta vieras menettely**, joka edellyttäisi eräänlaista järjestelmämuutosta. Tällainen vieraus ei sellaisenaan ole ollut peruste hylätä tai vastustaa asetuksen valmistelussa tällaisia seuraamuksia kansallisen oikeusjärjestelmän kannalta vieraina[1] ja siten rajoitusta nimenomaan viranomaisten osalta perustellaan sillä, ettei tällaista ”järjestelmämuutosta” ole tässä yhteydessä ehditty valmistelemaan.

Toinen perustelu liittyy näkemykseen siitä, ettei seuraamusmaksulla olisi vastaavanlaista vaikutusta kuin yksityissektorilla ottaen huomioon toiminnan budjettisidonnaisuuden. Tällä ilmeisesti tarkoitetaan sitä, että taloudelliset sanktiot ovat vaikutuksiltaan selkeämpiä taloudellista voittoa tavoittelevassa toiminnassa ja tuntuvampia seuraamusmaksujen enimmäismäärät huomioon ottaen. Tämä ei mielestäni kuitenkaan poista tietosuoja-asetuksen perusteena olevan **riskiperusteisen lähestymistavan ytimessä olevaa viime kädessä taloudellista punnintaa** – suojaustoimet edellyttävät usein taloudellista panostusta tai korkeariskisestä käsittelystä pidättäytymistä, jos riittävään suojaukseen ei ole varoja. Julkishallinnon budjettitaloudessa taloudelli-

[1] Kuten Tanskassa ja Virossa tietosuoja-asetuksen johdanto-osan 151 kappaleen mukaan

set sanktiot kannustaisivat oikeasuhtaisen riskiperusteisen lähestymistavan käyttöönottoon, jotta rajalliset resurssit tulisivat kohdennetuiksi myös henkilötietojen suojan näkökulmasta tehokkaasti.

Kolmanneksi perusteeksi esitetään, ettei hallinnollista seuraamusmaksua olisi tässä vaiheessa tarpeellista ulottaa koskemaan viranomaisten henkilötietojen käsittelyä nimenomaan sillä perusteella, että viranomaisia sitoo hallinnon laillisuusvaatimus ja viranomaisen on noudatettava hallinnon yleislakeja. Tietosuoja-asetuksen yhteydessä kansallisen erityissääntelyn liikkumavara on kaventunut lähinnä täydentämään ja yhteensovittamaan tietosuoja-asetusta kansalliseen oikeusjärjestelmään. Toisaalta hallitusten esitystä valmistellut työryhmä teetti selvityksen kansallisista erityissäännöksistä, joita löytyi lähes 800. Näiden säännösten läpikäynti voi johtaa erityissääntelyn purkamiseen tarpeettomina tai liian jäykkinä taikka vain niiden syrjäytymiseen EU-oikeuden etusijaperiaatteen nojalla ja tietosuoja-asetuksen suoraan soveltamiseen. Kun tietosuoja-asetus perustuu riskiperusteiseen tietosuojaperiaatteiden soveltamiseen, jättää ja tuleekin jättää rekisterinpitäjälle sellaista liikkumavaraa, mitä ei voida välttämättä saavuttaa perinteisillä perustuslakivaliokunnan tulkintakäytännön mukaisella yksityiskohtaisella käsittelyä tai rekisterinpitoa koskevalla sääntelyllä. Tietosuoja-asetuksessa lainmukaisuuden vaatimus kattaa lähinnä käsittelyperustetta koskevat asetuksen 6.1 artiklan vaatimukset ja näin ollen lainmukaisuusvaatimus ei tulisi kattamaan kaikkia TSA 5.1 tarkoitettuja tietosuojaperiaatteita siten, kun TSA 25 artiklassa (sisäänrakennettu ja oletusarvoinen tietosuoja) edellytetään. **Olennaista on se, että lainsäätäjä ei voi yksityiskohtaisesti ratkaista henkilötietojen käsittelyyn liittyviä riskejä vaan vastuu on rekisterinpitäjällä**, joka viime kädessä määrää henkilötietojen käsittelyn keinoista ja tarkoituksista ja siten vastaa riskiperusteisen lähestymistavan toteuttamisesta.

Neljäntenä perusteluna esitetään se, että viranomaisen henkilötietojen käsittelyä koskee myös rikosoikeudellinen virkavastuu ja vahingonkorvausvastuu. Virkarikosvastuu johtaa usein yksittäisen virkamiehen menettelyn arviointiin, jolloin ei tavoiteta viranomaisorganisaatiota rekisterinpitäjänä, jonka on vastuussa asetuksen mukaisesta riskiperusteisesta lähestymistavasta. Tämä edellyttää organisoitua riskihallintaa, jossa riskiarvioinnin perusteella nimenomaan rekisterinpitäjäorganisaatio tekee päätöksiä tietoisesti käsittelyyn liittyvistä riskeistä ja niihin nähden riittävistä suojaustoimista. Se, että yksittäinen virkamies on virkavastuussa mahdollisesta jo ennen viranhoitoaan organisaatiossa tehdyistä ratkaisuista tai käytännöistä, ei vaikuta oikeudenmukaiselta seuraamusjärjestelmältä **vaan moite tulisi voida kohdentaa viranomaisorganisaatioon rekisterinpitäjänä**, joka on TSA:n mukaan ensisijaisesti vastuussa henkilötietojen käsittelystä.

Ehdotuksen merkittävin peruste liittynee seuraamusjärjestelmän muutokseen, jonka toimivuudesta ja oikeudellisesta ennakoitavuudesta ei ole kansallisia kokemuksia. Ehdotuksen mukaan pääosin rikosperusteisesta seuraamusjärjestelmästä siirrytään hallinnollisten seuraamusmaksuihin perustuvaan järjestelmään. Kyse ei ole pelkästään ehdotuksen 25 §:ssä säädetyistä seuraamusmaksun vanhentumisesta tai sen perinnän järjestämisestä vaan siitä, miten asetuksen mukainen valvontaviranomainen voi ja kykenee selvittämään epäiltyjä rikkomistapauksia ja mitä ovat ne oikeusturvavaatimukset, joita seuraamusmaksumenettelyn tulisi täyttää. Kun oikeudellinen epävarmuus

hallinnollisten seuraamusmaksujen käytännöistä ja maksuista on suuri, on luonnollista, että tällainen rekisterinpitäjään kohdistuva riski halutaan minimoida tietosuoja-asetuksen sallimin keinoin. **Tämä ei kuitenkaan poista tätä oikeudellista epävarmuutta, jota tällainen uusi tai ”nykyisen oikeusjärjestyksen kannalta vieras menettely” aiheuttaa niille, joihin hallinnollista seuraamusmaksua sovelletaan**. Ratkaisu ei ole myöskään tasapuolinen esimerkiksi toimialoilla, joilla julkishallinto ja yksityiset palvelun tarjoajat toimivat rinnakkain tai kilpailutilanteessa esim. sote-uudistuksen myötä. Kun TSA 83 artiklan mukaan hallinnollisia sakkoja olisi mahdollista määrätä rekisterinpitäjälle ja henkilötietojen käsittelijälle, jää hallituksen esityksessä myös epäselväksi se, voisiko hallinnollisia sakkoja määrätä henkilötietojen käsittelijälle, joka käsittelee henkilötietoja rekisterinpitäjänä toimivan viranomaisen lukuun.

3. Seuraamusjärjestelmän muuttaminen rikosperusteisesta hallinnollisiin seuraamusmaksuihin perustuvaksi

Hallituksen esityksen lähtökohtana on siirtyminen mahdollisimman kattavasti seuraamusmaksuihin perustuvaan järjestelmä. Sivulla 56 todetaan, että rikosoikeudellisista seuraamuksista säädettäisiin kansallisesti ainoastaan siltä osin kuin se on tarpeellista ja siltä osin kuin yleisen tietosuoja-asetuksen VIII luvun mukaiset seuraamukset eivät tule sovellettaviksi. Tämä merkitsee seuraamusjärjestelmän melko täydellistä muutosta, jonka perusteluita ei hallituksen esityksessä kovin yksityiskohtaisesti ilmaista. Keskeisenä perusteena näyttäisi olevan TSA:n puhtaaksi viljelty tulkinta, jota on perusteltu ne bis in idem -periaatteella eli kaksoisrangaistavuuden kiellolla, jota käsitellään sivuilla 44-45. Kyse on siitä, että kun on olemassa erilaisia rangaistuksen luonteisia seuraamuksia lainvastaisesta menettelystä, ei samasta teosta voida määrätä kahta rangaistuksen luonteisten seuraamusta. Tämä periaate ohjaa ensivaiheessa valvontaviranomaisen harkintaa siinä vaiheessa, kun päätetään siitä, mikä seuraamus olisi kussakin tilanteessa tehokkain, oikeasuhtaisin ja varottavin eikä se sellaisenaan edellytä pelkästään hallinnollisiin sakkoihin perustuvaa seuraamusjärjestelmää.

Valittuun linjaukseen voi vaikuttaa myös rikosoikeuden ns. ultima ratio -periaate, jolle on annettu erilaisia tulkintoja[2]. Lahti pitää mahdollisena kompromissiratkaisuna sitä, että rikosoikeudellinen seuraamusjärjestelmä ja hallinnollinen sanktiojärjestelmä toimivat rinnakkaisesti edellyttäen, että niiden tarkoituksen- ja oikeudenmukaisuutta on koordinoitu ottaen myös ne bis in idem -periaate huomioiden (mt.s. 110). Usein käytetty soveltamistilanne on verotuksen hallinnolliset seuraamusmaksut ja niiden suhde verorikoksiin, mutta harvoin nämä soveltamistilanteet johtavat edes vaatimuksiin verorikosten dekriminalisoinnista. Tällöin rikosoikeuden ultima ratio -periaate on ymmärretty täydentävänä periaatteena törkeiden tai muuten hallinnollisten seuraamusmaksujen ulottumattomissa olevien tekojen seuraamuksina ja voidaan puhua sekajärjestelmästä, jossa hallinnolliset ja rikosoikeudelliset seuraamukset ovat ainakin joltain osin päällekkäisiä. Selkeänä poikkeuksena voidaan pitää kilpailulainsäädäntöä, jossa vuonna 1992 (480/1992) säädettiin kilpailurikkomismaksusta ja kilpailurajoitusrikos dekriminalisoitiin.

[2] Lahti Raimo: Rikosoikeuden ultima ratio -periaatteesta ja hallintosanktioiden asemasta. www.edilex.fi/artikkelit/11711

Perustuslakivaliokunta on asiallisesti rinnastanut rangaistuksen luonteisen taloudellisen seuraamuksen rikosoikeudelliseen seuraamukseen. Vaikka perustuslain 8 §:n rikosoikeudellinen laillisuusperiaate ei sellaisenaan ole katsottu kohdistuvan hallinnollisten seuraamusten sääntelyyn, on hallinnollisen seuraamusten yleisistä perusteista säädettävä perustuslain 2 §:n 3 momentin edellyttämällä tavalla, koska sen määräämiseen sisältyy julkisen vallan käyttöä. Laissa on valiokunnan vakiintuneen käytännön mukaan täsmällisesti ja selkeästi säädettävä maksuvelvollisuuden ja maksun suuruuden perusteista. Lisäksi valiokunta on pitänyt tärkeänä varmistaa, että säännökset täyttävät sanktioiden oikeasuhteisuuteen liittyvät vaatimukset (PeVL 28/2014 vp).

Koillisen[3] mukaan hallinnollisten seuraamusmaksujenkin osalta on vaikea irrottautua laillisuusvaatimuksen ennakoitavuutta edellyttävistä tarkkuuden ja täsmällisyyden vaatimuksista ja hän piti ilmeisenä, että TSA:n seuraamussääntelyn toteuttamistapa ei kohtaa perustuslakivaliokunnan käytännön luomia odotuksia, vaikka muodollisesti ei olekaan kyse blankosääntelystä. Yksityiskohtaisessa tarkastelussa Koillinen otti esille muun muassa seuraamusmaksun perusteena TSA 83.4 kohdan a) alakohdan, jossa viitataan TSA 25 artiklan sisäänrakennettuun ja oletusarvoiseen tietosuojaan. Tarkasteltuaan tietosuoja-asetuksen hallinnollista seuraamusjärjestelmää konstitutionaalisten vaatimusten (laillisuus-, suhteellisuus- ja syyllisyysperiaatteet) kannalta, Koillinen päätyi siihen, että näiden vaatimusten suojaamisessa asetuksen soveltamiskäytännöille jää merkittävä rooli.

Tämä tarkoittaa muun muassa sitä, että esimerkiksi TSA 25 artiklan rikkominen edellyttää riskiperusteisen lähestymistavan mukaisesti sallitun ja kielletyn riskinoton tunnistamista. Tässä arvioinnissa voitaneen tai tulisi jopa hyödyntää rikosoikeudellisen huolimattomuuden arviointiin kehitettyjä käsitteitä ja käytäntöjä[4]. Tällöin olennaisena edellytyksenä voidaan pitää hyvien tai riittävien sekä jatkuvasti ajan tasalla olevien käsittelykäytäntöjen aikaansaamista, joiden perusteella voitaisiin riskinperusteisen lähestymistavan laiminlyöntejä tai puutteita arvioida ja päätyä hallinnollisiin seuraamusmaksuihin. Tällaisten hyväksyttyjen käsittely- ja suojauskäytäntöjen puute on merkittävästi rajoittanut henkilörekisteririkokseen nykyisinkin sisältyvän rekisterinpitäjän rikosoikeudellisen (törkeän) huolimattomuuden arviointia. Tällaiset yleisesti saatavilla olevat hyvät käytännöt ja niiden hyväksymismekanismit loisivat myös seuraamusjärjestelmältä edellytettyä ennakoitavuutta.

Tietosuoja-asetuksen mukaan valvontaviranomaisen tehtävänä on osallistua hyvien käytäntöjen muodostamiseen (esim. hyväksymällä vakiosopimusehtoja ja vahvistamalla käytännesääntöjä sekä myöntämällä sertifikaatteja ja hyväksyä sertifiointikriteereitä) ja siten valvontaviranomainen osallistuu ja vaikuttaa seuraamusmaksujen määräytymisperusteisiin. Kyse ei ole viranomaiselle delegoidusta säädösvallasta vaan EU-oikeudessa paljon käytetystä standardioikeustyyppisestä sääntelystä. Kun valvontaviranomainen on myös toimivaltainen määräämään näiden hyväksyttyjen käytäntöjen vastaisesta menettelystä tai laiminlyönnistä hallinnollisia seuraamusmaksuja, olisi hallituksen esityksessä tullut kiinnittää huomiota tällaiseen valvontavi-

[3] Koillinen Mikael: Hallinnolliset seuraamukset tietosuojan sanktiomekanismina. DL 4/2016 s. 578
[4] Nuutila Ari-Matti: Rikosoikeudellinen huolimattomuus. 1996

ranomaisen toiminnan olennaiseen muutokseen nykyiseen verrattuna. Tällaiset viranomaistoiminnan muutokset ovat huomattavia ja poikkeavat olennaisesti siitä, mikä rooli valvontaviranomaiselle on nykyisen lainsäädännön myötä muodostunut. Kun koko seuraamusjärjestelmän tehokkuus ja oikeussuhteisuus perustuvat valvontaviranomaisiin toimintaan, olisi tällaisen viranomaistoiminnan kehittäminen edellyttäminen lainvalmistelussa määrätietoisempaa kuin nyt ehdotettu tietosuojalautakuntaa viittaava asiantuntijalautakunta ja eduskunnan oikeusasiamieheen viittaava apulaistietosuojavaltuutettu. Jos käytetään kilpailuoikeudellista seuraamusjärjestelmää esimerkkinä, on valvontaviranomaisen toimintaan kehitetty vuodesta 1992 alkaen niin tutkintatoimien ja toimivaltuuksien (esim. kilpailulain 37 §:n tiedonsaantioikeus luottamuksellisen viestinnän sisällöstä). Tässä mielessä olemme hallinnollisten tietosuojaoikeudellisten seuraamusmaksujen osalta nollapisteessä ja tällaisen seuraamusjärjestelmän kehittäminen, ottaen myös huomioon perustuslain sille asettamat laillisuus-, suhteellisuus- ja syyllisyysperiaatteet, tulee kestämään vuosia, ellei vuosikymmeniä.

Tällaisessa tilanteessa ei mielestäni ole perusteltua muuttaa nykyistä rikosoikeudellista seuraamusjärjestelmää kategorisesti hallinnollisiin seuraamusmaksuihin perustuvaksi ennen kuin hallinnollisista seuraamusmaksuista on saatu kokemuksia. Yhtenä koetinkivenä voidaan pitää TSA 33 artiklassa tarkoitettu henkilötietojen tietoturvaloukkauksista tehtäviä ilmoituksia, joiden tarkoituksena ei ole niinkään rangaistusluonteisten seuraamusmaksujen määrääminen vaan tällaisten tapahtumien aiheuttamien vahinkojen rajoittaminen, torjunta ja korjaaminen. Tästä syystä ehdotan seuraavassa erityistä rekisterinpitäjän rikostunnusmerkistöä niiden tapausten varalle, joissa hallinnolliset seuraamusmaksut eivät tule kyseeseen tai ne eivät ole yksittäisessä tapauksessa tehokkaita, oikeasuhteisia ja varottavia. Kun ehdotukset liittyvät hallituksen esityksessä tarkoitettuun uuteen tietosuojarikos -tunnusmerkistöön, arvioin ensin mainittua tunnusmerkistöä.

4. Ehdotetusta tietosuojarikos -tunnusmerkistöstä

Hallituksen esityksessä ehdotetaan nykyisen henkilörekisteririkoksen (rikoslain 38 luvun 9 §) korvaamista seuraavalla **tietosuojarikoksen** tunnusmerkistöllä:

Joka muutoin kuin Euroopan parlamentin ja neuvoston luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetussa asetuksessa (EU) 2016/679 (yleinen tietosuoja-asetus) tarkoitettuna rekisterinpitäjänä tai henkilötietojen käsittelijänä tahallaan tai törkeästä huolimattomuudesta hankkii henkilötietoja niiden käyttötarkoituksen kanssa yhteensopimattomalla tavalla, luovuttaa henkilötietoja tai siirtää henkilötietoja vastoin
1) yleisen tietosuoja-asetuksen,
2) tietosuojalain (/),
3) henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (/) tai
4) henkilötietojen käsittelyä koskevan muun lain
henkilötietojen käyttötarkoitussidonnaisuutta, luovuttamista tai siirtämistä koskevaa säännöstä ja siten loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa tai olennaista haittaa, on tuomittava tietosuojarikoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Tietosuojarikoksesta tuomitaan myös se, joka tahallaan tai törkeästä huolimattomuudesta toimii vastoin sitä, mitä 1 momentin 1—4 kohdassa tarkoitetussa säädöksessä säädetään henkilötietojen käsittelyn turvallisuudesta.

Perustuslain 8 §:n rikosoikeudellista laillisuusperiaatteen on vakiintuneesti katsottu sisältävän vaatimuksen sääntelyn täsmällisyydestä ja tarkkarajaisuudesta. Rikoksen tunnusmerkistö on ilmaistava laissa riittävällä täsmällisyydellä siten, että säännöksen sanamuodon perusteella on kohtuudella ennakoitavissa, onko jonkin toiminta tai laiminlyönti rangaistavaa (esim. PeVL 37/2016).

Tunnusmerkistön 1. momentti

Ehdotettu tunnusmerkistö rakentuu edelleenkin viittauksin henkilötietojen suojaa koskeviin erityissäännöksiin. Tunnusmerkistön 1 momentti on kirjoitettu siten, että siihen voi syyllistyä henkilö, joka ei ole TSA:ssa tarkoitettu rekisterinpitäjä tai henkilötietojen käsittelijä. Rekisterinpitäjillä ja henkilötietojen käsittelijöillä tarkoitettaneen TSA:n 4 artiklan 7 kohdan rekisterinpitäjää ja 8 kohdan henkilötietojen käsittelijää.

Kun tekijäpiiri on määritelty siten, että se koskee henkilöitä, joihin ei sovelleta TSA:n rekisterinpitäjän tai henkilötietojen käsittelijän vastuuta koskevia säännöksiä, joudutaan vaikeuksiin tai osittain mahdottomuuksiin muiden tunnusmerkistön muodostavien kriteerien osalta. Tällaisia kriteereitä ovat johdantolauseen teonkuvaukset ”hankkii henkilötietoja niiden käyttötarkoituksen kanssa yhteensopimattomalla tavalla”, ”luovuttaa tai siirtää henkilötietoja vastoin” mainittuja aineellisoikeudellisia säännöksiä. Käyttötarkoituksella ja yhteensopimattomuudella tarkoitettaneen keskeistä henkilötietojen suojan periaatetta, joka on ilmaistu TSA:n 5.1 artiklan b) alakohdassa. Yksityiskohtaisemmin tästä periaatteesta tai yhteensopivuusarvioinnista säädetään TSA 6.4 artiklassa. Säännökset velvoittavat nimenomaan rekisterinpitäjää, jolla on lisäksi TSA 25.2 ja 32 artikloiden mukaiset velvollisuudet suojata henkilötietoja asiattomalta pääsyltä ja käyttötarkoituksen vastaiselta käsittelyltä. Kun nämä aineellisoikeudelliset säännökset velvoittavat ensisijaisesti rekisterinpitäjää (käyttötarkoitussidonnaisuuden periaate ja kolmansiin maihin siirtoa koskevat vaatimukset), **näyttäisi säännökseltä putoavan aineellisoikeudellinen velvoittavuus, joihin tämän tyyppiset erikoisrikosoikeudelliset tunnusmerkit perustuvat**, kun tekijöinä voi olla vain muita kuin rekisterinpitäjiä tai heidän lukuun käsitteleviä henkilöitä. Jos ulkopuolinen on saanut oikeudettomasti henkilötietoja esim. tietomurron seurauksena, ei häntä voi koskea alkuperäisen rekisterinpitäjän käyttötarkoitus vaan häntä olisi arvioitava uutena rekisterinpitäjänä, joka on ryhtynyt määräämään henkilötietojen käsittelyn tarkoituksista ja keinoista (rekisterinpitäjän tunnusmerkit) ja hänellä tulisi olla TSA:n edellyttämä laillinen käsittelyperuste, jota ei lähtökohtaisesti voi olla jos hän on omavaltaisesti ryhtynyt käsittelemään henkilötietoja omissa tai muuten rekisterinpitäjän kannalta vieraissa tarkoituksissa (esim. asiakastietojen ottaminen mukaan siirtyessään kilpailijan palvelukseen) tai tietoja on hankittu muuten lainvastaisesti, tuntemattomiin tai laittomiin tarkoituksiin (kuten identiteettivarkaus). Lisäksi perinteiset luovutussäännökset koskevat nimenomaan rekisterinpitäjiä, ei yksittäisiä työntekijöitä, joiden osalta luovutustyyppisten tekotapojen rikosvastuu perustuu salassapitorikoksiin.

Perusteluiden mukaan tunnusmerkistön tarkoituksena on säätää rangaistavaksi uteliaisuudesta tapahtuva henkilötietojen käsittely ilman käsittelyyn oikeuttavaa perustetta ns. urkintatilanteet. Tällä on tarkoitettu tietojärjestelmän sinänsä oikeutetun käyttäjän muussa kuin työtehtävissä, useimmiten uteliaisuutta, tapahtuvaa tiedon hankintaa. Tällöin ei ole kyse tietomurrosta, koska tekijä käyttää sinänsä itselleen kuuluvia tunnuksia, vaan tapauksia on arvioitu henkilörekisteririkoksen tunnusmerkistöön sisältyvän tekotavan eli käyttötarkoituksena vastaisena käsittelynä, johon yksittäinen käyttäjä on sitoutunut saadessaan käyttöoikeudet henkilötiedolliseen tietojärjestelmään.

Ottaen huomioon perusteluissa erityisesti täsmennetty rangaistavan käytöksen kohdeala, olisi kyse lähinnä TSA:n 4 artiklan 10 kohdassa tarkoitetusta henkilöstä, joka ei siis ole kolmas osapuoli eikä rekisterinpitäjä tai käsittelijä vaan **henkilö, jolla on oikeus käsitteellä henkilötietoja suoraan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena**. TSA:n yksityiskohtaiset säännökset, jotka liittyvät tällaisiin henkilöihin löytyvät TSA 32.4 ja 29 artiklasta, joissa edellytetään rekisterinpitäjän varmistamaan, että tällaiset henkilöt (yksittäiset käyttäjät) käsittelevät henkilötietoja ainoastaan rekisterinpitäjän ohjeiden mukaan. Näiltä osin rangaistavuus jäisi rekisterinpitäjän ohjeiden varaan, mikä jättäisi rangaistavan käytöksen alan avoimeksi ja edellyttäisi rekisterinpitäjän toimenpiteitä, minkä ei voi katsoa täyttävän rikosoikeudellisen laillisuusperiaatteen vaatimuksia.

Tunnusmerkistön 1. momentti sisältää lisäksi voimassa olevan henkilörekisteririkoksen tunnusmerkistöön sisältyvän vaikutusarvioinnin. Kun TSA:ssa suojattavana oikeushyvänä ei enää ole yksityisyyden suoja vaan laajemmin tunnistettavissa olevan henkilön oikeudet ja vapaukset, olisi perusteltua muuttaa tätä vaikutusarviointia vastaavasti, jollei sitä sitten pidetä tarpeettomana. Näiltä osin keskeinen oikeustapaus on KKO 1998:85, jossa loukkausta arvioitiin seuraavasti: ”Henkilörekisterissä olevien henkilötietojen luovuttaminen vastoin rekisteröidyn suostumusta muuhun käyttötarkoitukseen kuin siihen, mihin tiedot oli rekisteröity, on tyypillisesti yksityisyyden suojan perustavoitteiden vastaista. Tällöin loukataan rekisteröidyn henkilön oikeutta tietää ja päättää itseään koskevien tietojen käytöstä.”

Tunnusmerkistön 2. momentti

Toisin kuin 1. momentissa tässä tunnusmerkistössä tekijänä voi olla rekisterinpitäjä tai käsittelijä, jolloin vastuu kohdistuu tahoihin, joita mainitut erityissäännökset koskevat Sinänsä säännöksessä ei poissuljeta muitakaan, mutta käytännössä käsittelyn turvallisuutta koskevilla säännöksillä tarkoitetaan kuitenkin esim. TSA:n 32 artiklaa, joka koskee ensisijaisesti rekisterinpitäjää ja käsittelijää. Kun TSA:n 32 artikla perustuu asetuksessa omaksuttuun riskiperusteiseen voi kyse olla tällaisen arvioinnin laiminlyönnistä tai puutteista taikka riittävien suojaustoimien toteuttamisen puutteista. Jossain tilanteessa nämä puutteet voivat johtaa TSA 33 artiklan edellyttämään tietoturvaloukkausilmoituksiin, jolloin tulisi ottaa huomioon myös itsekriminointisuojaa koskevat periaatteet, jotka voivat johtaa siihen, että seuraamusjärjestelmä painottuu niissä tapauksissa hallinnollisiin sanktioihin.

Näiltä osin voimassaolevat tunnusmerkistöt sisältävät kahden tyyppisiä tietoturvaan ja henkilötietojen suojaukseen liittyviä tekotapoja. Ensinnäkin kyse voi olla henkilötietolain 32 §:ssä tarkoitetun suojauksen laiminlyönnistä henkilörekisteririkoksena, joka edellyttää törkeää huolimattomuutta ja seurausarvioinnin mukaista loukkausta. Kyseessä on selvästi rekisterinpitäjään kohdistuva rangaistusuhka. Toinen voimassaolevista tunnusmerkistöistä on henkilörekisteririkkomuksen tunnusmerkistö henkilötietolain 48 §:n 2 momentin 3 kohdassa eli rikkoo henkilötietojen suojaamisesta ja henkilörekisterin hävittämisestä annettuja säännöksiä, jossa voi olla tekijänä niin rekisterinpitäjä kuin käyttöoikeuden saanut käyttäjä. Tässä tunnusmerkistössä ei edellytetä suojattavien oikeushyvien loukkausta vaan niiden vaarantaminen riittää.

5. Ehdotukset korvaaviksi tunnusmerkistöiksi

Kun arvioidaan rikosoikeudellisten seuraamuksia hallinnollisia sakkoja täydentävinä seuraamuksina, on täsmennettävä tällaisten seuraamusten käyttöalaa. Yhtenä tavallaan riskiperusteinä näkökulmana voidaan pitää laittoman käsittelyn riskilähdetyyppistä jaottelua tekijätahojen mukaan. Kuten edellä on ilmennyt, näitä tahoja on useimmiten kolmenlaisia eli 1) rekisterinpitäjä tai henkilötietojen käsittelijä 2) edellä mainittujen tahojen alaisuudessa henkilötietoja käsittelevät (käyttäjät) sekä 3) muut kuin edellä mainitut tahot eli ulkopuoliset.

Olennaista on myös hahmottaa rikoslain 38 luvun data-, viestintä- ja informaatiorikosten kokonaisuus ja tällaisten informaatiorikosten asema tässä kokonaisuudessa. Esimerkiksi tietomurto on nykyään yleinen datarikos, jolla suojataan tietojärjestelmiä ulkopuolista tunkeutumista vastaan. Alunperinhän tietomurto oli vain henkilörekisteriin tunkeutumista koskeva tunnusmerkistö henkilörekisterilain (471/1987) 45 §:ssä tarkoitettu henkilörekisteriintunkeutumisen tunnusmerkistö, joka muutettiin vuonna 1995 yleisempää muotoon. Joka tapauksessa tietomurto suojaa myös henkilötiedollisia tietojärjestelmiä edellä tarkoitetun 3) kohdan tekijöiltä eli ulkopuolisilta kunhan tietojärjestelmä on jotenkin suojattu siten, että tekijä on tullut murtaa tietojärjestelmän suojaus. Vuonna 2015 (368/2015) tunnusmerkistöä jonkin verran lievennettiin siten, että tietomurto kattaa tiedonhankinnan tietojärjestelmään tunkeutumatta esim. käyttämällä tietojärjestelmän haavoittuvuutta tai muuten vilpillisin keinoin.

Jos tietomurron seurauksena on saatu henkilötietoja ja niitä on ryhdytty käsittelemään omissa tai muissa kuin rekisterinpitäjän hyväksymissä tarkoituksissa, voidaan tekijän katsoa ryhtyneen rekisterinpitäjäksi (määrää käsittelyn tarkoitukset ja keinot) ja tällainen oikeudeton ryhtyminen henkilötietojen käsittelyyn tulisi säätää rangaistavaksi. Rikoslain 38 luvun yhteydessä tämä rangaistusuhka täydentää tietomurto, joka täyttyy jo silloin kuin tietojärjestelmään tunkeudutaan tai tietoja hankitaan. Tämä olisi olennaista tällaisten data- ja informaatiorikosten tutkinnan ja torjunnan näkökulmasta ottaen huomioon myös rikoslain 34 luvun 9 a ja 9 b §:ien vaarantamisrikokset sekä henkilötietojen käyttö muiden rikosten välineinä kuten petokset ja identiteettivarkaus -tyyppiset teot.

Olen ehdotuksessa eriyttänyt rekisterinpitäjän ja käyttäjän teonkuvaukset toisistaan siten, että ensin on lähinnä tahalliset rekisterinpitäjärikokset ja sen jälkeen rekisterinpitäjän rikosoikeudellinen huolimattomuus ja lopuksi käyttäjää koskevat oikeudettoman käsittelyn ja suojauksen rikkomisen tai laiminlyönnin tunnusmerkistöehdotukset.

Tässä yhteydessä on korostettava, että kaikki jäljempänä ehdotetut tunnusmerkistöt sisältyvät voimassaolevien henkilörekisteririkoksen (RL 38:9 §) ja – rikkomuksen (henkilötietolaki 48 §:n 2 momentti) tunnusmerkistöihin. Hallituksen esitykseen sisältyvät tunnusmerkistöt vastaavat jäljempänä ehdotetuista tunnusmerkistöistä henkilötietojen urkintaa (4) ja henkilötietojen suojan laiminlyöntiä (3) ja siten **hallituksen esitys sisältää merkittävän henkilötietojen suojaan koskevan dekriminalisoinnin.** Ehdotukset eivät kuitenkaan ole yhtä laajoja kuin voimassaolevat tunnusmerkistöt vaan niihin on pyritty poimimaan keskeiset ja myös käytännössä sovelletut tekotavat.

5.1. Rekisterinpitäjän rikokset

1. Tietosuojarikos

Se, joka ryhtyy käsittelemään henkilötietoja ilman asetuksen 6.1 artiklan tai asetuksessa tarkoitetun EU:n tai kansallisen lain perustetta tai 9 tai 10 artiklan vastaisesti saatuaan tai hankittuaan henkilötiedot muualta kuin henkilöltä itseltään tai henkilöltä erehdyttämällä henkilöä käsittelyn tarkoituksesta ja laajuudesta, on tuomittava tietosuojarikoksesta sakkoon tai enintään kahdeksi vuodeksi vankeuteen.

Tunnusmerkistö selventäisi nykyiseen henkilörekisteririkoksen tunnusmerkistöön sisältyvää oikeudetonta rekisterinpitäjäksi ryhtymistä. Rekisterinpitäjäksi ryhtymisen tunnusmerkit liittyvät siihen, ettei henkilötietoja käsitellä enää rekisterinpitäjän lukuun (käsittelijä) tai alaisuudessa (käyttäjä) vaan niitä ryhdytään käsittelemään omissa tai muuten rekisterinpitäjän käyttötarkoituksiin nähden vieraissa ja yhteensopimattomissa tarkoituksissa. Suhteessa jäljempänä esitettävään henkilötietojen urkinta -rikokseen kyse olisi laajamittaisemmasta käsittelystä tai ainakin olosuhteista, joissa voidaan katsoa käyttäjän tai ulkopuolisen ryhtyneen määräämään käsittelyn tarkoituksista ja keinoista. Rangaistavina esitekoina voisivat olla salakatselu ja/tai -kuuntelu, viestintäsalaisuuden loukkaus ja tietomurto sekä vaaran aiheuttaminen tietojenkäsittelylle (erityisesti vakoiluohjelmat). Vuonna 2015 muutettiin viestintäsalaisuuden loukkauksen tunnusmerkistöä siten, että yksittäiseen tietokoneen (päätelaitteen) kohdistuva tiedonhankinta (päätelaitevakoilu) voisi täyttää viestintäsalaisuuden loukkauksen tunnusmerkistön (tiedonhankinta ns. tietojärjestelmän sisäisestä luottamuksellisesta datan siirrosta).

Tämän osalta seuraamusarviointia ei enää edellytettäisi vaan riittävää olisi TSA:n 5.1 a) kohdan laillisuusperiaatteen ja sitä täsmentävän 6.1 artiklan vastainen käsittelyyn ryhtyminen. Tilanteissa, jossa rekisterinpitäjä on oikeudettomasti menettänyt henkilötietoihin määräysvallan, kyse olisi sitä, että henkilötietojen suoja voitaisiin näissä tilanteissa ymmärtää myös kollektiivisena oikeutena. Kun rekisterinpitäjä on menettänyt määräysvallan käsittelemiinsä henkilötietoihin, tarkoittaa lähtökohtaisesti sitä, ettei myöhempi käsittely ole kyseessä oleville henkilöille ennakoitavissa eikä heidän tiedolliset oikeudet toteudu. Tällainen tunnusmerkistö on tarpeen myös tilanteissa, joissa rekisterinpitäjän tekee TSA 33 artiklassa tarkoitetun tietoturvaloukkausilmoituksen ja oikeudettoman käsittelyn keskeyttämiseksi tai lopettamiseksi tarvittaisiin poliisin turvaamistoimenpiteitä tai pakkokeinoja. Tunnusmerkistö olisi myös tarpeen tilanteissa, joissa asiakirjapohjaisia henkilötietoja saadaan julkisuuslain perusteella ja niitä ryhdytään käsittelemään TSA:n tarkoittamalla tavalla ilman laillista oikeutta (esim. rikostuomiot).

2. Törkeä tietosuojarikos

Jos tekijä ryhtyy oikeudettomasti käsittelemään asetuksen 9.1 artiklassa tai 10 artiklassa tarkoitettuja erityisiä henkilötietoryhmiä tarkoituksena saattaa tai teko on omiaan saattamaan henkilö vainon tai syrjinnän taikka muun ihmisarvoa loukkaavan menettelyn kohteeksi ja tekoa voidaan pitää kokonaisuutena arvostellen törkeänä, on rikoksentekijä tuomittava törkeästä tietosuojarikoksesta sakkoon tai vankeuteen enintään kolmeksi vuodeksi.

Ehdotuksessa on kriteeriksi otettu erityistä suojaa edellyttävät tietotyypit, jotka ilmaistaan 9.1. ja 10 artikloissa. Kvalifioitu tekotapa tulisi kyseeseen silloin kuin tällaisia tietoja käsitellään tarkoituksena henkilöiden vapauksien ja oikeuksien loukkaaminen. Loukkauksina voi tulla kyseeseen rikoslain uusi vainoamissäännökseen (RL 25: 7 a) tai syrjintää (RL 11:11). Muu ihmisarvoa loukkaava menettely liittyisi muun muassa yleiseen halveksuntaan. Tämän tunnusmerkistön voisi täyttää rikostuomioita julkaiseva Facebook -sivusto, jonka tarkoituksena on saattaa tai on omiaan saattamaan tunnistetut rikoksentekijät vainon tai syrjinnän taikka yleisen halveksunnan kohteeksi. Näiltä osin kyse olisi oikeusvaltiollisesta periaatteesta, jonka mukaan rikoksesta määrätyt seuraamukset on oltava laissa säädettyjä. Kokonaisarvioinnissa voisi ottaa huomioon henkilötietojen levittämisen tehokkuuden ja toiminnalle haettu julkisuus.

3. Henkilötietojen suojan laiminlyönti

Joka tahallaan tai huolimattomuudesta laiminlyö huolehtia henkilötietojen asetuksen 5.1 b) ja f) alakohdissa tarkoitettujen tietosuojaperiaatteiden riittävästä ja ajanmukaisesta toteuttamisesta, on tuomittava henkilötietojen suojauksen laiminlyönnistä sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Henkilötietojen suojan laiminlyönnistä tuomitaan myös se, joka siirtää henkilötietoja kolmansiin maihin vastoin asetuksen 44-49 artikloja.

Laillisessa henkilötietojen käsittelyssä ei voida useinkaan puhua tahallisuudesta vaan eri asteisesta huolimattomuudesta, kun henkilötietojen käsittely on johtanut kiellettyihin seurauksiin (esim. tiedot päätyneet ulkopuolisille). Kuten edellä todettiin nykyinen rikosoikeudellisen vastuu alaraja eli törkeä huolimattomuus on ollut usein vaikeasti osoitettavissa (vrt. tuottamuksellinen virkasalaisuuden rikkominen) ja edellyttäisi jatkossakin hyväksyttävien suojauskäytäntöjen vastaista menettelyä.

Se, mihin asetuksen 5 artiklan periaatteista rikosoikeudellinen huolimattomuusvastuu voisi parhaiten soveltua tehosteeksi olisi käyttötarkoituksen määrittelyn laiminlyönti. Mikäli käyttötarkoitusta ei ole määritelty, ei monia muitakaan henkilötietojen käsittelyn reunaehtoja voida soveltaa ja toteuttaa. Toinen soveltuva käyttökohde olisi 5.1 f) alakohdassa mainittu eheyden ja luottamuksellisuuden periaate, joka ilmenee oikeussäännön tasolla erityisesti 32 artiklassa.

5.2 Käyttäjän rikokset

4. Henkilötietojen urkinta

Se, joka hankkii tietojärjestelmään saamiensa käyttöoikeuksiensa avulla henkilötietoja, joihin hänellä ei ole käyttöoikeuksiensa perusteella oikeutta, on tuomittava henkilötietojen urkinnasta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Henkilötietojen urkinnasta tuomitaan myös se, joka on syöttänyt tietojärjestelmää tai erehdyttänyt sen rekisterinpitäjää antamalla virheellisen tai harhaanjohtavan tiedon tiedonsaantiperusteistaan ja saanut siten oikeudettomasti henkilötietoja.

Käyttäjärikoksilla tarkoitan sinänsä laillisen tietojärjestelmän luvallisen käyttäjän laittomia käsittelytekoja. Ensimmäinen tekotapa liittyy rekisterinpitäjän palveluksessa saatujen käyttöoikeuksien väärinkäyttöön, kun käyttöoikeuksia ei voi ennakolta yksityiskohtaisesti määritellä. Tämä koskee myös ns. teknisen käyttöyhteyden avulla muualta hankittuja tietoja. Toisen momentin tekotapa liittyy tiedonsaantitilanteisiin, joissa tietojärjestelmään ei anneta jatkuvaa käyttöoikeutta vaan kyse on kyselykohtaisista tiedonantokäytännöistä, joissa tiedonantaminen edellyttää käyttötarkoituksen selvittämistä (esim. luottotietorekisteri). Tämä jälkimmäinen tekotapa jäisi laillisen käyttäjän laittoman käsittelyn ja tietomurron väliin ja siten selventäisi nykyistä oikeustilaa, jossa rekisterinpitäjän erehdyttäminen ei sisälly tunnusmerkistöön.

Käyttäjän oikeudeton tiedonhankinta voi liittyä salassa pidettävän tiedon hyväksikäyttöön tai paljastamiseen, jolloin tällaisen tiedonhankinnan voi katsoa sisältyvän salassapitorikokseen. Kun tietojärjestelmiin liittyvänä salassapitointressinä voi olla muukin kuin luonnollisen henkilön oikeudet ja vapaudet kuten viranomaistoiminnan tehokkuuden turvaaminen kuten esitutkintasalaisuus, on tällaisia oikeudellisia intressejä loukkaavaa tiedonhankintaa arvioitu virkavelvollisuuden rikkomisena (esim. poliisimies käyttäjänä hakee itseensä epäiltynä kohdistuvan ilmoituksen poliisiasiantietojärjestelmästä).

5. Henkilötietojen suojauksesta ja hävittämisestä annettujen määräysten rikkominen

Joka tahallaan tai huolimattomuudesta rikkoo henkilötietojen suojauksesta ja hävittämisestä annettuja määräyksiä tai rekisterinpitäjän käyttöön ottamia standardeja henkilötietojen suojauksesta ja hävittämisestä, on tuomittava henkilötietojen suojausmääräysten rikkomisesta sakkoon.

Tämä tunnusmerkistö koskisi käyttäjää ja vastaisi osittain henkilötietolain 48 §:n 2 momentin 3 kohdassa tarkoitettua henkilörekisteririkkomusta ja kattaisi nykyistä selkeämmin huolimattoman hävittämisen tapaukset (kaatopaikkatapaukset), joihin salassapitorikos ei sovellu, koska niissä tarkoituksena on ollut henkilötietojen hävittäminen eikä niinkään salassapitorikostyyppiset tekotavat eli paljastaminen tai hyväksikäyttö.

Rangaistusasteikkoja ehdotan nostettavaksi tasolle, johon tietoverkkorikosdirektiivin perusteella vuonna 2015 nostettiin muita rikoslain 38 luvun tunnusmerkistöjä. Samalla olisi mielestäni nostettava salassapitorikoksen rangaistusasteikkoa, koska sitä pidetään perinteisesti moitittavampana kuin pelkäksi urkinnaksi jäänyttä tiedonhankintaa.

Rangaistusasteikon nosto vaikuttaa suoraan syyteoikeuden vanhentumiseen (kahdesta viiteen vuoteen), mitä voi pitää perusteltuna, kun urkintatekoja usein selvitetään ensin rekisterinpitäjän toimesta. Lisäksi tulisi arvioida sitä, voidaanko urkintatapaukset hoitaa muuten kuin saattamalla tapaukset esitutkintaan.

Lisäksi on mainittava, että tämän tyyppisiä tekoja on pidetty vahingonkorvauslain 5 luvun 6 §:n tarkoittamina loukkauksina, joiden perusteella tuomioistuimet ovat määränneet kärsimyskorvauksia.

6. Tietosuojaviranomaisen kuuleminen (rikoslain 38 luvun 10 §:n 3 momentti)

Lisäksi esitän, että tietosuojaviranomaisen kuulemissäännöstä täydennettäisiin edellä mainituilla tunnusmerkistöillä ja muutettaisiin nykyaikaisempaan muotoon siten, että kuuleminen ei tulisi kyseeseen vain niissä tapauksissa, joissa päädytään syytteen nostamiseen vaan myös tapauksissa, joissa syyteharkinta päätetään muilla tavoilla. Siten ehdotan säännöksen kohdan ”syytteen nostamista” korvaamista ”syyteharkinnan päättämistä”.