

Oikeudesta kameravalvonnan tallenteisiin – empiirinen tarkastelu kansallisen ja EU:n oikeuden soveltamisesta

HAKUSANAT: asiakirjajulkisuus, henkilötieto, tarkastusoikeus, kameravalvonta, tallenne

1. Johdanto

Alkuvuodesta 2021 kameravalvonta ja julkisuusperiaatteen kytkökset demokratiaan nousivat otsikoihin entisen pääministeri Juha Sipilän epäiltyä pahoinpitelyä koskevien tallenteiden luovuttamisen yhteydessä. Eduskunnan turvallisuusjohtaja oli näyttänyt toimittajalle tallenteen tietokoneen näytöltä, josta se oli kännykän kameraa käyttäen kuvattu. Näin hankittu video oli julkaistu uutisverkkosivuilla.

Kameravalvonta on yleistynyt huomattavasti viime vuosikymmeninä. Tuhan-siin työpaikkoihin kohdistuneen tutkimuksen¹ mukaan se oli käytössä kahdessa kolmasosassa työpaikoista jo vuonna 2011. Kameravalvonta on juurtunut yhteiskuntaamme tavaksi, jolla on ilmeisiä etuja vaarojen ollessa vähemmän ilmeisiä. Valvonnan lisääntyminen on tapahtunut kontekstissa, jossa ihmisten kuvien tallentaminen on yhä tavanomaisempaa.²

Oikeudellisesti kameravalvonta on vain vähän ja välillisesti säännelty kysymys.³ Sääntely on käytännössä rikoslain (39/1889) ja yksityisyyden suojaan kuuluvien säännösten ohjaamaa. Erottelu julkisen ja yksityisen kameravalvonnan välillä on olennainen oikeudellisen sääntelyn kontekstin kannalta. Tässä artikkelissa keskitymme viranomaisten toiminnan julkisuudesta annetun lain (621/1999, JulkL) soveltamisalaan kuuluviin viranomaisiin ja näihin rinnastet-

* *Kari Telaranta*, tradenomi (ylempi AMK), väitöskirjatutkija, Tampereen yliopisto; *Riku Neuvonen*, OTT, viestintäoikeuden dosentti, julkisoikeuden yliopistonlehtori, Tampereen yliopisto.

1. Tero Mamiä – Anne Alvesalo-Kuusi – Anna Kuokkanen – Simo Virtanen, Työn elektroninen valvonta Suomessa. Tutkimuksen loppuraportti 6/2011. Työterveyslaitos, s. 40 ja 71. Saatavilla osoitteessa <https://urn.fi/URN:NBN:fi-fe201707207739>.

2. Benjamin Goold – Ian Loader – Angélica Thumala, The Banality of Security: The Curious Case of Surveillance Cameras. *British Journal of Criminology* 53(6), 2013, s. 977–996, 993.

3. Kameravalvonnan kehityksestä osana yksityisyyden suojaa Riku Neuvonen, Yksityisyyden suoja Suomessa. *Lakimiesliiton Kustannus* 2014, s. 85–87.

taviin julkista valtaa käyttäviin tahoihin⁴ sekä Euroopan unionin virastoihin. Lisäksi keskiössä on julkisilla paikoilla, kuten katualueilla, tapahtuva kamera-valvonta. Tallentavasta kameravalvonnasta muodostuu henkilötietoja, joiden käyttöön sovelletaan tietosuojalainsäädäntöä.⁵ Julkisuuslain tarkoittamien organisaatioiden kameratallenteet ovat viranomaisen asiakirjoja. Tähän viittaamme käsitteellä julkinen kameravalvonta.⁶

Tämän artikkelin tarkoituksena on tarkastella ensi sijassa julkisen kameravalvonnan oikeudellista sääntelyä toisaalta julkisina asiakirjoina ja toisaalta henkilötietoina. Käsittelemme tilanteita, joissa joku haluaa tutustua julkishallinnon tallenteisiin tai haluaa käyttää henkilötietoihinsa kohdistuvaa tarkastusoikeuttaan. Pyrimme vastaamaan tässä artikkelissa kahteen kysymykseen. Ensiksi millainen harkintavalta on tallenteiden luovuttamisesta päättävällä viranomaisella? Toiseksi voiko harkintavallan käyttöä analysoimalla pyrkiä systematisoimaan tallenteiden oikeustilaa?

Artikkelin lähestyminen kameravalvontaan tapahtuu vaihteittain. Aluksi selvitämme, mitä tarkoitetaan kameravalvonnalla ja siihen liittyvillä tallenteilla ja miten ne sijoittuvat oikeudelliseen sääntelykehikkoon. Analysoimme harkintavallan rajat tallenteiden luovuttamistilanteissa. Tämän jälkeen esittelemme käytännön testin, miten viranomaiset tätä harkintavaltaa käyttävät.

Soveltamiskäytäntöön kohdistuva analyysi toteutettiin suppeana empiirisenä tarkasteluna, jonka tavoitteena oli selvittää, miten asiakirjajulkisuutta ja omien tietojen tarkastusoikeutta koskevaa normistoa tulkitaan eri viranomaisissa. Siten esimerkiksi asianosaisjulkisuus (JulkL 11 §) ja tiedonsaanti tutkimuskäyttöön (JulkL 28 §) on rajattu tarkastelun ulkopuolelle. Lopuksi vastaamme kysymykseen siitä, onko viranomaisten soveltamiskäytännön perusteella pääteltävissä yleisempää linjaa tallenteiden luovuttamisesta.⁷

4. Julkisuuslain soveltamisalasta Tomi Voutilainen, *Oikeus tietoon: Informaatio-oikeuden perusteet*. Edita 2012, s. 94–103.

5. Tämän lisäksi on jonkinlaisia erityistapauksia ja esimerkiksi Tietosuojalautakunnan päätöksen 2/932/2011 perusteella Google sai käsitellä tietoja karttapalvelua varten määrääjän, kunhan henkilöitä tai ajoneuvoja ei voinut tunnistaa.

6. Julkinen tarkoittaa tässä yhteydessä julkisen vallan kiinteistöjä ja alueita. Angloamerikkalaisessa käytännössä julkinen on avointa ja yksityinen käsittää myös yksityisten omistamat kiinteistöt, kun taas Euroopassa yksityisesti omistettu tila voi olla julkista tai puolijulkista. Beatrice von Silva-Tarouca Larsen, *Setting the Watch: Privacy and the Ethics of CCTV Surveillance*. Hart Publishing 2011, s. 14–16.

7. Ks. Kaijus Ervasti, Lakimies, oikeus, yhteiskunta: Oikeus yhteiskunnallisena käytäntönä. Edita 2017, s. 16–17.

2. Kameravalvonnan sääntely

2.1 Kameravalvonnan käsite

Kamera- tai videovalvontajärjestelmä on järjestelmä, joka kuvaa valvottavaa kohdetta ja mahdollistaa tapahtumien valvonnan ja niiden tallentamisen.⁸ Sen keskeisiä komponentteja ovat kamera-, tallennus- ja tarkkailulaitteet ohjelmistoinen sekä muut laitteet, jotka ovat tiedon siirron ja ohjauksen kannalta tarpeellisia.⁹ Euroopan tietosuojaneuvosto (EDPB) on käyttänyt käsitettä videolaite, joka sisältää yleiskielen kannalta ajatuksen myös tallentamisesta.

Kameravalvontaa käytetään tuottamaan jatkuvaa kuvallista informaatiota halutuilta alueilta. Sen avulla pyritään estämään mahdollisia ongelmia ja selvittämään niitä jälkikäteen. Kameravalvontaa voidaan hyödyntää myös esimerkiksi joukkotapahtumissa häiriötilanteiden ennakoinnissa, alkavan tulipalon havaitsemisessa sekä tilannejohtamisessa.¹⁰

Kameravalvontaa voidaan hyödyntää kahdella tavalla, reaaliaikaisesti ja jälkikäteisesti. Reaaliaikaisen tarkkailun tavoitteena on ennaltaehkäistä epätoivottuja tapahtumia. Jälkikäteen tallenteita tutkimalla voidaan selvittää erilaisten tapahtumien kulkua. Niiden käyttö ei rajoitu pelkästään turvallisuuteen, vaan niitä voidaan käyttää myös esimerkiksi toiminnan kehittämiseen¹¹ tai yleishyödylliseen tarkoitukseen.¹² Yleishyödyllisiä tarkoituksia on esimerkiksi kelikamerat ja luontokamerat, kuten Norppalive.¹³

Nykyisessä digitaalisessa tekniikassa kuvakenno koostuu pikseleistä eli kuvapisteistä, joiden määrä kertoo kuvan tarkkuuden. Kameroiden lisäksi valvontajärjestelmä koostuu yleensä tallentimesta sekä tallentimen ja kameroiden välisistä tietoliikenneyhteyksistä.¹⁴ Järjestelmään voi liittää myös esimerkiksi mikrofoneja ja analytiikkatoimintoja kuten hahmontunnistuksen, kävijälaskennan tai lämpö- ja savupatsaiden tunnistuksen.¹⁵

8. Teknologiakeskeisestä lähestymistavasta Anthony C. Caputo, *Digital Video Surveillance and Security*. Butterworth-Heinemann 2014, s. 49–60.

9. Kimmo Arenius – Veijo Kauppi – Roger Lehtonen – Aku Pänkäläinen – Petri Käyhkö – Pekka Sallinen – Patrik Westerlund – Kim Kattilakoski – Jukka Siivonen – Mats Lindeqvist – Jouni Virta – Veli-Matti Luukkanen – Reijo Hovinen, *Kameravalvontaopas*. Turva-alan yrittäjät ry 2020, s. 10. Saatavilla osoitteessa <https://turva-alanyrittajat.fi/kameravalvontaopas>.

10. *Ibid.*, s. 7–8.

11. *Ibid.*, s. 9–10.

12. Potentiaalisista käyttökohteista laajemmin J. K. Petersen – Pamela Taylor, *Handbook of Surveillance Technologies*. Taylor & Francis 2012, s. 475–477.

13. Norppaliven avulla pystyi seuraamaan hylkeitä niiden luonnollisessa ympäristössä häiritsemättä niitä. Ks. <https://wwf.fi/luontolive/norppalive/>.

14. Arenius et al. 2020, s. 16–19.

15. Ks. *ibid.*, s. 28–35.

Turvajärjestelmien paljastumisen kannalta olennaista on, että kameratallenteista voidaan päätellä järjestelmän tekninen suorituskyky. Sitä on esimerkiksi kameran sijainti, sen erottelukyky, kuvan pakkaustaso ja kameran kyky kuvata hämärässä. Kameran ja sen teknisten ominaisuuksien päätyminen ulkopuolisille voi vaarantaa valvonnan tarkoituksen.

2.2. Kameravalvonnan yleiset reunaehdot

Suomessa kameravalvonnasta ei ole erityislakia, toisin kuin esimerkiksi Ruotsissa¹⁶, jossa viranomaisten harjoittama kameravalvonta vaatii pääsääntöisesti luvan. Suomen tilanteen arvioinnissa konteksteja ovat alueellinen eli mitä kamera kuvaa, toimijakeskeinen eli kuka on vastuussa valvonnasta ja tiedollinen eli syntyykö siitä henkilötietoja. Alueellisen, toimijakeskeisen ja tiedollisen näkökulman muodostama kolmio on olennainen sääntelyn normatiivisen ulottuvuuden kannalta.

Tiedollisesta näkökulmasta keskeinen on EU:n yleisen tietosuoja-asetuksen (2016/679, GDPR) 5 artiklan 1 kohdan alakohdan c (5.1.c) tietojen minimointiperiaate, jonka mukaan henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään. Käytännössä tämä tarkoittaa sitä, että kameravalvontaa voidaan käyttää niissä tilanteissa, joissa yksityisyyttä vähemmän loukkaavaa keinoa ei ole käytettävissä¹⁷ ja tällöinkin valvonnan tekniset ratkaisut ja niiden käyttötavat pitää valita niin, että sillä loukataan mahdollisimman vähän yksityisyyttä. Käytännössä tämä voi tarkoittaa sitä, että vaihtoehtoiset keinot, kuten vartiointi, eivät olisi käytännössä toteutettavissa niiden edellyttämien ylivoimaisten taloudellisten panostusten takia.

2.3. Kameravalvonnan tallenteet henkilötietoina

Henkilötietojen käsittelyn kannalta keskeisimpinä säännöksiä ovat tietosuojalaki (1050/2018, TSL) ja GDPR. Ne koskevat viranomaisten lisäksi myös yksityisiä.¹⁸

16. Kamerabevakningslag (2018:1200).

17. Julkiset organisaatiot ovat työnantajia, joten niihin sovelletaan lakia yksityisyyden suojasta työelämässä (759/2004). Sen 17 §:n 1 momentin mukaan ennen kameravalvonnan käyttöön ottamista on selvitettävä työntekijöiden yksityisyyteen vähemmän puuttuvien muiden keinojen käyttömahdollisuudet, ja että työntekijän yksityisyyteen ei puututa enempää kuin on välttämättöntä toimenpiteiden tarkoituksen saavuttamiseksi.

18. Eräät osakokonaisuudet on rajattu pois näiden soveltamisalalta. GDPR:ää ei sovelleta yksityishenkilöön, joka käsittelee henkilötietoja yksinomaan henkilökohtaista tai kotitaloutta koskevassa toiminnassa. Rikosasioiden tietosuojasta säädetään erikseen rikosasioiden tieto-

Arvioitaessa henkilötietojen sääntelyn suhdetta valvontakameratallenteisiin keskeistä on se, onko tallenteella henkilötietoja ja toisaalta se, käsitelläänkö niitä.

Henkilötieto on mikä tahansa tunnistettavissa olevaan luonnolliseen henkilöön liittyvä tieto. Henkilö on tunnistettavissa, jos hänet voidaan suoraan tai epäsuorasti tunnistaa esimerkiksi nimen, henkilötunnuksen, sijaintitiedon, verkotunnistietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.¹⁹ EDPB:n mukaan²⁰ (tallentava) kameravalvonta kerää ja säilyttää kuvallista tai audiovisuaalista tietoa kaikista valvottuun tilaan tulevista ihmisistä, jotka voidaan tunnistaa.

Seuraavaksi arvioidaan, *käsitelläänkö* tallenteissa olevia henkilötietoja. Käsitelyllä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti (GDPR 4.2 artikla). Asetuksen mukaan²¹ tällaista käsittelyä on tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaus, muuttaminen, hakeminen, kyseleminen, käyttö, luovuttaminen, levittäminen tai saataville asettaminen, yhteensovittaminen, yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen. Kuten asetustekstistä ilmenee, jo henkilötietojen tallentaminen ja tallenteiden säilyttäminen itsessään on henkilötietojen käsittelyä. Tietosuojavaltuutetun mukaan tallenteiden säilytysajalla ei ole merkitystä henkilötiedon käsitteen kannalta.²² Toisaalta myös ei-tallentava kameravalvonta, jota seuraa esimerkiksi vartija, täyttää asetuksen määritelmän henkilötiedosta ja sen käsittelystä.²³

Unionin tuomioistuimen tapauksessa C-345/17 oli kyse kumotun henkilötietodirektiivin (95/46/EY) tulkinnasta. Poliiseja oli videoitu poliisiasemalla kuulustelutilanteessa ja kyseinen video oli julkaistu internetissä. Poliisit olivat tapauksessa nähtävissä ja kuultavissa, joten tallenteet olivat henkilötietoja. Toisessa tapauksessa C-212/13 tuomioistuin totesi, että kotiin asennettu myös julkista

suojadirektiivissä 2016/680. EU:n toimielimiä koskee lisäksi asetus 2018/1725 luonnollisten henkilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.

19. GDPR 4.1 artikla.

20. EU:n tietosuojatyöryhmän (EDPB 2019) ohjeet 3/2019 henkilötietojen käsittelystä videolaitteilla (29.1.2020), s. 7. Saatavilla osoitteessa <https://tietosuoja.fi/euroopan-tietosuojaneuvoston-ohjeet>.

21. Luettelo ei liene tyhjentävä, sillä asetuksessa se alkaa sanalla ”kuten” (”such as”).

22. Tietosuojavaltuutetun toimisto 2022. Usein kysyttyä kameravalvonnasta. Saatavilla osoitteessa <https://tietosuoja.fi/usein-kysyttya-kameravalvonta> (noudettu 27.1.2022).

23. Myös näitä koskee tietojen minimoinnin periaatteet ja käsittelyn kohteena olevan oikeudet soveltuvin osin, kuten oikeus tietoon siitä kuka näitä tietoja käsittelee ja miksi.

tilaa kuvaava valvontajärjestelmä, joka luo henkilöstä kuvatallenteen ja tallentaa ne kovalevyille on automaattista henkilötietojen käsittelyä.²⁴

Henkilötietojen käsittely on sallittua vain ennalta määritellyissä tarkoituksissa (GDPR 6.1 artikla). Kameravalvonnan kohdalla oikeutusperuste voi olla esimerkiksi julkisen vallan käyttäminen tai yleistä etua koskevan tehtävän suorittaminen (alakohta e) tai rekisterinpitäjän oikeutettu etu (alakohta f). Kansallisesti on lisäksi säädetty (TSL 4.1 §:n 2 kohta), että alakohdan e mukainen käsittely on sallittua, jos se on tarpeen ja oikeasuhtaista viranomaisen toiminnassa yleisen edun mukaisen tehtävän suorittamiseksi.²⁵

TSL:n säännöksen tarkoituksena on mahdollistaa viranomaisten tekemä henkilötietojen käsittely silloin, kun oikeutta käsittelyyn ei voida suoraan johtaa viranomaista koskevasta tehtävä- ja toimivaltasäännöksestä eikä mahdollisesta yksityiskohtaisemmasta erityissääntelystä.²⁶ Tästä lieenee kyse silloin, kun viranomainen esimerkiksi omaa toimintaa turvatakseen on ottanut käyttöön tallentavan kameravalvonnan.

Yleisen edun edistämistehtävän lisäksi käsittelyperuste voi olla rekisterinpitäjän (tai kolmannen osapuolen) oikeutettu etu.²⁷ Viranomainen ei voi vedota käsittelyperusteena 6.1 artiklan alakohtaan f (oikeutettu etu), sillä 6.1 artikla rajaa viranomaisten tehtäviensä yhteydessä suorittaman tietojenkäsittelyn alakohdan f soveltamisalan ulkopuolelle. Näin ollen julkinen kameravalvonta on lähtökohteisesti oltava perusteltavissa yleisellä edulla (alakohta e) ja vastaavasti yksityinen kameravalvonta oikeutetulla edulla (alakohta f).²⁸ Julkinen tai yksityinen taho ei

24. Tapauksessa oli kiistaa siitä, sisältyykö tällainen henkilötietojen käsittely GDPR 2.2.c artiklan mukaisen kotitalouspoikkeuksen piiriin. Kun järjestelmällä samalla valvottiin myös julkista tilaa, se ei tuomion mukaan ollut yksinomaan henkilökohtaista tai kotitaloutta koskevaa, vaikka järjestelmä olikin asennettu kotitaloon omaisuuden, terveyden ja hengen suojaamiseksi. Ks. myös Cornelia Beatrice Gabriela, *The Video Surveillance Matter in the Case-law of the European Court of Justice*. *Lex et scientia*, 27(2) 2020, s. 32–40, 33–36.

25. Yksityisoikeudellinen yhteisö ei voi vedota käsittelyperusteena 6.1 artiklan e alakohtaan, vaikka se hoitaisikin julkisia hallintotehtäviä. HE 9/2018 vp EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi, s. 80. Tästä poikkeuksena TSL 4 §:n 1, 3 ja 4 kohtien mukainen käsittely (henkilön asema, tehtävät ja niiden hoito, tutkimus tai tilastointi ja arkistointi).

26. HE 9/2018 vp, s. 79.

27. EDPB:n mukaan periaatteessa kaikki 6.1 artiklan mukaiset lainmukaiset perusteet voivat tulla kyseeseen videovalvontatietojen käsittelyn oikeusperusteena. Sen mukaan 6.1.c artiklaa (lakisääteinen velvoite) sovelletaan, jos kansallisessa lainsäädännössä säädetään velvollisuudesta suorittaa videovalvontaa. Harvinaisissa tapauksissa rekisterinpitäjä voi käyttää 6.1.a artiklaa (suostumus) käsittelyn oikeusperusteena. EDPB:n mukaan todennäköisimmin käytettävät säännökset ovat oikeutettu etu ja yleinen etu. EDPB 2019, s. 9.

28. Ei ole päivänselvää, että viranomainen ei voisi vedota oikeutettuun etuun käsittelyperusteena. Kapeasti tulkittuna viranomaisten asianmukaista hallinnointia ja toimintaa varten suoritettava tietojenkäsittely ei olisi ”tietojenkäsittelyä, jota viranomaiset suorittavat tehtäviensä yhteydessä”. EU:n tietosuojatyöryhmän (EDPB 2014) lausunto 6/2014 direktiivin 95/46/EY 7 artiklan mukaisesta rekisterinpitäjän oikeutetun intressin käsitteestä (9.4.2014), s. 24. Saatavilla osoitteessa <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/>

voi perustella valvontaa pelkästään kiinteistön omistajan ja vuokralaisen välisellä sopimuksella.²⁹

Tietosuojalain perusteluissa todetaan yleisen edun käsittelyperusteesta, että viranomaisen on arvioitava, voidaanko kyseessä olevaa henkilötietojen käsittelyä pitää oikeasuhtaisena käsittelyn tarkoitukset huomioon ottaen. Arvioinnissa on huomioitava GDPR 5 artiklan henkilötietojen käsittelyä koskevat periaatteet, kuten tietojen minimoinnin periaate. Rekisterinpitäjän olisi myös arvioitava käsittelyn oikeasuhtaisuutta suhteessa rekisteröidyn etuihin ja perusoikeuksiin.³⁰ Yleisen edun perustetta sovellettaessa lapset tulee huomioida erityisesti.³¹ Yleisen edun perusteella oikeutetussa kameravalvonnassa on punnittava rekisteröityjen etuja ja haettua yleistä etua, samoin kuin oikeutetun edun perusteen punnintatilanteissa. Kyseessä on niin sanottu tasapainotesti.³² Se pitää tehdä perusteesta riippumatta.

GDPR 15.1 artiklan mukaan rekisteröidyllä on oikeus saada vahvistus siitä, käsitelläänkö häntä koskevia tietoja sekä tiedot muun muassa käsittelyn tarkoituksesta, tietoryhmistä, tietojen säilytysajoista ja tietojen vastaanottajista. Rekisteröidyllä on oikeus päästä häntä itseään koskeviin henkilötietoihin ja saada kaikki tietojen alkuperästä käytettävissä olevat tiedot. Rekisteröidyllä on paitsi oikeus saada ne tallenteet, joissa hän itse esiintyy, myös tieto siitä miten nämä tallenteet on hankittu. Tämä voisi sisältää esimerkiksi tiedon kameran sijainnista ja mahdollisesti myös kameran teknisiä tietoja.

EDPB:n³³ mukaan, jos tallenteella on ulkopuolisia henkilöitä, tallennetta ei pitäisi luovuttaa ilman että sitä muokataan niin, että ulkopuolisia henkilöitä ei

wp217_fi.pdf. Samassa lausunnossa (s. 24) EDPB esittää tilojen videovalvonnan turvallisuus-syistä sisältyvän laajaan tulkintaan yleistä etua koskevasta tehtävästä.

29. Apulaistietosuojavaltuutetun ratkaisussa 4.6.2021 (Dnro 4900/182/18) rekisterinpitäjä vetosi asuinrakennuksen kulunvalvontajärjestelmän osalta myös GDPR 6.1.b artiklaan, jonka mukaan käsittely on sallittua sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena. Apulaistietosuojavaltuutettu totesi, että vuokrasopimuksella sovitaan vuokrasuhteen ehdoista ja luovutetaan käyttöoikeus. ”Päämäärän saavuttamiseen ei liity tarpeellisuutta osana henkilötietojen käsittely sähkölukkojärjestelmän kautta ja tietojen kerääminen vuokralaisen kulkemisesta kotitalossaan. Lisäksi voidaan todeta, että silloin, kun on olemassa vähemmän yksityisyyden suojaan puuttuvia vaihtoehtoja, henkilötietojen käsittelyä ei voida katsoa tarpeelliseksi sopimuksen täytäntöönpanoa varten.” Kulunvalvonta ei ollut tarpeellista sopimuksen täytäntöönpanemiseksi, eivätkä edellytykset käsitellä henkilötietoja 6.1.b artiklan käsittelyperusteen nojalla täyttyneet. Siten myöskään kameravalvontaa ei ole lähtökohtaisesti mahdollista perustella pelkästään kiinteistön omistajan ja vuokralaisen välisellä sopimuksella.

30. HE 9/2018 vp, s. 79.

31. Ibid., s. 79–80.

32. Ks. Tietosuojavaltuutetun toimisto 2022. Rekisterinpitäjän oikeutettu etu. Saatavilla osoitteessa <https://tietosuoja.fi/rekisterinpitajan-oikeutettu-etu> (noudeutu 27.1.2022). Myös EU:n tietosuojatyöryhmä on käsitellyt tasapainotestiä. Ks. EDPB 2014, s. 25–52. Tässä artikkelissa ei mennä tämän syvemmin tasapainotestiin.

33. EDPB 2019, s. 23.

voi tunnistaa, mutta velvollisuutta tähän ei ole. Ulkopuolisten henkilöiden suojaamista ei ohjeen mukaan voi kuitenkaan käyttää ”tekosyynä” tietojen luovuttamatta jättämiselle. Saman ohjeen mukaan tieto valvonnan kattavuudesta ei näytä olevan salassapitointressinä kovin korkealla. Ohjeen mukaan rekisterinpitäjän olisi ilmoitettava täsmällisesti valvottu alue, jotta mahdollisesti kuvatuksi tullut voi arvioida, onko hänen henkilötietojaan mahdollisesti talletettu.³⁴

2.4 Kameravalvonnan tallenteet viranomaisen asiakirjoina

Perustuslain 12 §:n 2 momentin mukaan viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei lailla toisin säädetä. Jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta. Tallenteella tarkoitetaan sisältöä, joka on luettavissa, kuunneltavissa tai muutoin ymmärrettävissä vain teknisin apuvälinein.³⁵ Julkisuuslain (621/1999, JulkL) 5.1 § niputtaa samaan asiakirjan käsitteeseen kirjalliset ja kuvalliset esitykset sekä muut viestit.

Arvioitaessa sitä, onko viranomaisen hallussa oleva tallenne *asiakirja* eli julkisuuslain soveltamisalaan kuuluva, on ensinnä arvioitava, onko se kirjallinen tai kuvallinen esitys. Toisekseen on arvioitava sitä, onko se viranomaisen *hallussa*. Asiakirja on viranomaisen hallussa, jos se on viranomaisen palveluksessa olevan laatima tai se on toimitettu viranomaiselle asian käsittelyä varten tai muutoin toimialaan tai tehtäviin liittyen.³⁶

*Mäenpää*³⁷ jakaa julkisuuslain soveltamisalan ulkopuolelle kokonaan tai osittain jäävät asiakirjat kahteen kokonaisuuteen, joista toinen on ns. *ei-asiakirjat* (JulkL 5.3 §). Näiden yhteys julkisen vallan käyttöön on niin välillistä ja merkitykseltään vähäistä, että julkisuuslain soveltaminen niihin ei ole perusteltua. Toisen kokonaisuuden muodostaa viranomaisen sisäistä työskentelyä varten laaditut asiakirjat (JulkL 5.4 §), joihin julkisuuslakia sovelletaan vain rajoitetusti.

Tapauksessa KHO 2016:207 oli kiistaa siitä, ovatko pelastuslaitoksen palo-paikalta ottamat valokuvat sisäistä koulutusta varten hankittuja ei-asiakirjoja, vai sovellettiinko niihin julkisuuslakia. Ratkaisussaan KHO totesi, että sisäistä käyttöä varten hankituille asiakirjoille tyypillistä on se, että ne eivät välittömästi liity suoritettavaan virkatehtävään vaan tukevat viranomaisen oman toiminnan järjestämistä. Asiakirjan julkisuusasema ei ole myöskään riippuvainen siitä, onko se liitetty arkistoon vai ei (KHO 2016:117). Viranomaisen suorittaessa

34. Ibid., s. 23–24.

35. HE 309/1993 vp perustuslakien perusoikeussäännösten muuttamisesta, s. 58.

36. Myös toimeksiannon perusteella laaditut asiakirjat ovat viranomaisen asiakirjoja (JulkL 5.2 §). Tästä voi olla kyse esimerkiksi silloin, kun kameravalvonnan toteutuksesta ja tallenteiden ylläpidosta vastaa kolmas osapuoli, kuten vartioimisliike.

37. Olli Mäenpää, *Julkisuusperiaate*. Talentum 2016, s. 59–60.

lakisäateistä tehtävää, sen yhteydessä muodostuvat kuva- ja äänitallenteet ovat viranomaisen asiakirjoja.³⁸

Tapauksessa T-436/09 unionin yleinen tuomioistuin otti kantaa kameravalvonnan tallenteiden asemaan asiakirjoina. Kuvaruudulla näkyvät valvontakameran kuvat eivät ole asiakirjoja, jos ne pysyvät teknisellä laitteella tallentumatta mihinkään vain hetken. Kuitenkin valvontakameraan liitetty tallennuslaite muodostaa tallenteen, joka on ”kiistatta” mahdollisen tutkimuspyynnön kohteena oleva asiakirja. Tapauksessa kyse oli laitteesta, joka tallentaa kuvat automaattisesti viimeisten 30 vuorokauden ajalta, Tilanne ei muutu, vaikka yli 30 vuorokautta vanhat kuvat poistetaan järjestelmästä ja korvataan uusimmilla kuvilla.³⁹

Julkisuuslain perusteluiden mukaan asiakirja on viranomaisen hallussa, kun se on fyysisesti viranomaisen toimipaikassa tai viranomaisessa toimivalla paikasta riippumatta. Esimerkiksi tallenne saattaa fyysisesti sijaita palveluyrityksen tiloissa. Se on kuitenkin viranomaisen määrättävissä, ja viranomainen voi käyttää sitä joko tietoliikenneyhteyksien avulla tai siten, että palveluyritys tulostaa tai muutoin tuottaa tiedostosta aineistoa viranomaisen käyttöön.⁴⁰ Olennaista on, onko tallenne viranomaisen määräysvallassa.

Tallenne voi olla kokonaan tai osittain salassa pidettävä. Salassapidon perusteista on säädetty JulkL 24 §:ssä. Tyypillisesti videovalvonnan tallenteiden salassapitoperuste on perusteltu 24.1 §:n 7 kohdalla, jonka mukaan henkilöiden, rakennusten, laitosten, rakennelmien sekä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat ja niiden toteuttamiseen vaikuttavat asiakirjat on pidettävä salassa, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna turvajärjestelyjen tarkoituksen toteutumista. Ilmeisyyden arviointi on tallenteen luovuttamisesta päättävän viranomaisen harkintavallassa.⁴¹

Kuopion hallinto-oikeuden tapauksessa Dnro 12/0154/2 3.4.2012 oli kysymys esitutkintapöytäkirjan liitteenä olleesta cd-levystä. Tallenne sisälsi valvontakameran kuvaa putkatilojen käytävältä. Poliisilaitos oli kieltäytynyt antamasta tallennetta, koska se sisälsi poliisin tilojen turvallisuuteen liittyvää tietoa ja teknistä tietoa. Hallinto-oikeus totesi, että tallenteessa näkyy putkatilojen ovia, mutta esimerkiksi niiden lukitusjärjestelmästä ei ole tehtävissä tarkkoja havaintoja. Tallenteesta ei ollut saatavissa lisätietoa turvajärjestelyistä verrattuna siihen, mitä julkisen esitutkintapöytäkirjan perusteella on saatavissa. Hallinto-oikeus arvioi, että tieto oli joka tapauksessa laadultaan yleisesti tiedossa olevaa ja niin vähäistä, ettei sillä ole merkitystä poliisin turvajärjestelyjen kannalta.

38. Kari Telaranta, Ovatko viranomaisen ottamat valokuvat julkisia asiakirjoja? *Defensor Legis* 3/2017, s. 459–465, 465.

39. Tuomion kohdat 126–127.

40. HE 30/1998 vp laiksi viranomaisten toiminnan julkisuudesta ja siihen liittyviksi laeiksi, s. 55.

41. Samalla on huomioitava, että viranomaisen päätöksellä voidaan kieltää liikkuminen tietyillä paikoilla, jolloin oikeudeton alueelle tunkeutuminen tulee rangaistavaksi RL 24:3 säännöksen mukaan julkisrauhan rikkomisena, tästä enemmän Neuvonen 2014, s. 126–128.

Tallenteiden salassapitoa voi yrittää perustella myös muilla kuin turvajärjestelyillä. Edellä mainitussa tapauksessa poliisilaitos perusteli luovuttamatta jättämistä myös sillä, että tallenteen antaminen loukkaisi julkisuuslain 24.1 §:n 26 kohdan tarkoittamalla tavalla poliisien yksityiselämää. Poliisin kulkeminen virantoimituksessa putkatielojen käytävällä ei ollut lainkohdassa tarkoitettu, yksityiselämään liittyvä, arkaluonteinen tieto.⁴²

Tapauksessa KHO 2021:27 oli kyse pahoinpitelytapauksen esitutkintapöytäkirjan liitteenä olevasta videosta, joka oli kuvattu teollisuushallin valvontakameralla. Poliisilaitos kieltäytyi luovuttamasta tietoja, koska rikoksen asianosaisten ovat tunnistettavissa tallenteelta ja rikoksen tekotapa on selvästi nähtävissä. Lisäksi tallenteella näkyy ulkopuolisia henkilöitä sekä asianosaisten ja rikoksesta epäillyn käyttäytymiseen sekä ilmeisiin liittyviä yksityiskohtia. Tallenne ylitti poliisilaitoksen arvion mukaan tarkkuudellaan sen, mitä oli pääteltävissä julkiseksi tulleista asiakirjoista.

KHO:n mukaan tallenteesta välittyy henkilöiden yksityiselämään liittyvää informaatiota. KHO nojautui lainvalmisteluaineistoon,⁴³ jonka mukaan henkilön yksityiselämään liittyvät arkaluonteiset seikat ja rikoksen uhria koskevat tiedot voivat olla salassa pidettäviä. KHO totesi, että vaikka tallenteilla on useiden henkilöiden yksityiselämään liittyvää tietoa, tämä tieto ei ole arkaluonteista ja tallenteet eivät siten olleet salassa pidettäviä.

Edellä mainittujen oikeustapausten valossa voidaan todeta, että lähtökohtaisesti ihmisten näkyminen tallenteella ei vielä loukkaa heidän yksityisyyttään.⁴⁴ Paljastuvan tiedon täytyy olla arkaluonteista. Mikäli henkilö näkyy esimerkiksi kadulle suunnatun tai virastossa olevan valvontakameran tallenteessa, tieto itsessään ei ole arkaluonteinen. Vaikka tallenteella näkyisi rikos, kuten pahoinpitely, myöskään se ei vielä lähtökohtaisesti ole salassa pidettävä arkaluonteinen tieto. Tiedon paljastumisesta tulisi aiheutua haittaa.

Tallenteisiin liittyvä julkisuus on EU-oikeuden kontekstissa erilainen. EU:n perusoikeuskirjan 42 artiklaa konkretisoivan Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi annetun asetuksen ((EY) N:o 1049/2001, Julka)⁴⁵ mukaan jokaisella unionin kansalaisella sekä jokaisella luonnollisella henkilöllä, joka asuu jossain jäsenvaltiossa, sekä jokaisella oikeushenkilöllä, jolla on sääntömääräinen kotipaikka jossain jäsenvaltiossa,

42. Ikään kuin varmuuden vuoksi hallinto-oikeus totesi myös, että tallenne ei sisällä sellaista tietoa, joka oikeuttaisi salaamisen julkisuuslain 24.1 §:n 32 kohdan perusteella.

43. HE 30/1998 vp ja HE 222/2010 vp esitutkinta- ja pakkokeinolainsäädännön uudistamiseksi.

44. Huomioitavaa on vielä, että kuinka henkilöt näkyvät. Vuonna 2012 syyttäjä teki syyttämättä jättämispäätöksen tapauksessa, jossa henkilöä epäiltiin kotietsintää tekevien poliisien salakatselusta valvontakameroiden avulla. Neuvonen 2014, s. 134–135.

45. Asetuksen synnystä ja valmisteluun liittyvistä jännitteistä, ks. Joni Heliskoski – Päivi Leino, *Darkness at the Break of Noon: The Case Law on Regulation No. 1049/2001 on Access to Documents*. *Common Market Law Review* (43) 2006, s. 735–781.

on oikeus tutustua EU:n toimielinten hallussa oleviin asiakirjoihin (2 artikla). Asetuksen mukaan asiakirjalla tarkoitetaan mitä tahansa tallennetta, eli paperille tulostettua tai sähköisessä muodossa tallennettua tekstiä taikka ääni- tai kuvatallennetta tai audiovisuaalista tallennetta, joka koskee toimielimen vastuualueeseen kuuluvia politiikkoja, toimintaa ja päätöksiä (3 artikla). Sisäiseenkin käyttöön laaditut asiakirjat tulee asetuksen mukaan esittää.

Asiakirjan määritelmä on siis EU:n asetuksessa vastaava kuin julkisuuslaissa lukuun ottamatta sitä seikkaa, että asetuksessa ei määritellä *ei-asiakirjaa*. Myös luovuttamisesta kieltäytymisen perusteet ovat hieman toisistaan poikkeavia.⁴⁶ Näitä ovat ehdottoman suojaintressin salassapitoperusteet, jotka on määritelty asetuksen 4 artiklan 1 kohdassa,⁴⁷ joita ovat muun muassa yleistä turvallisuutta koskevan yleisen edun suojaaminen sekä yksityiselämän, yksilön koskemattomuuden sekä erityisesti henkilötietojen suojaaminen. Poiketen muista salassapitoperusteista, edes *ylivoimainen yleinen etu* ei oikeuta luovuttamaan ehdottoman suojaintressin alaisia tietoja.

Edellä mainitusta huolimatta, vaikka tallenteelle tallentunut tieto olisi salassa pidettävää, sen esittäminen tai luovuttaminen voi olla silti sallittua harvinaisissa tärkeään yleiseen etuun liittyvissä tilanteissa. EIT:n Guja vastaan Moldova -tapauksessa viranomaisen palveluksessa oleva luovutti salassa pidettäviä tietoja medialle. Yleisön tarve informaation saamiseen voi olla niin voimakas, että se syrjäyttää salassapitovelvollisuuden. Kyse on paljastuksesta aiheutuvan haitan ja julkisen tarpeen tietojen paljastamiseen välisestä punninnasta. Tärkeää on, että on toimittu vilpittömässä mielessä, uskottu tietojen olevan tosia ja pidetty niiden paljastamista julkisen edun mukaisena.⁴⁸

Yhteenvetona Suomen viranomaisten ja EU:n toimielinten hallussa oleviin kameravalvonnan tallenteisiin soveltuu lähtökohtaisesti sekä julkisuus että tutustumisoikeus.⁴⁹

46. Riku Neuvonen, Oikeus julkiseen tietoon. Kauppakamari 2017, s. 46–49.

47. Lehtonen et al. ovat luonnehtineet sääntelyä samantapaiseksi kuin julkisuuslain tarkoittama vahinkoedellytyksinen salassapito-olettamaan perustuva salassapito, josta on kyse silloin, kun tietoja salataan turvajärjestelyitä koskevan JulkL kohdan perusteella. Lasse Lehtonen – Maija Häll – Sampo Brander, Euroopan unionin asiakirjojen salassapito yleisen edun perusteella. Lakimies 2/2007, s. 208–227, 211.

48. Guja v. Moldova 12.2.2008. Hakemus nro 14277/04. Euroopan ihmisoikeustuomioistuin. Riku Neuvonen on purkanut Guja-tapauksen perusteella muodostuvia kriteereitä pilliinpuhaltajien sananvapaudelle. Ks. Riku Neuvonen, Pilliinpuhaltajien asema Suomessa, s. 246–247 teoksessa Päivi Korpisaari (toim.), Viestinnän muuttuva sääntely. Viestintäoikeuden vuosikirja 2016. Helsingin yliopisto, s. 241–254.

49. Samanlaisia oikeuksia on turvattu myös Euroopan neuvoston yleissopimuksessa viranomaisten asiakirjojen julkisuudesta, joka on ratifioitu Suomessa blankettilailla (16/2015). Yleissopimus kattaa myös julkista valtaa käyttävät yksityiset.

3. Tietopyynnöt kameravalvonnan tallenteista

Artikkelin empiiristä osuutta varten toinen kirjoittajista kävi kävelemässä eri virastojen valvontakameroiden edessä. Käynnin yhteydessä otettiin ylös kamerasijainti sekä ajankohta, jolloin kameraan on taltioitunut kirjoittajan henkilötietoja. Tämän jälkeen ensin pyydettiin luovuttamaan tallenne yhden minuutin ajalta. Tässä vaiheessa ei vielä paljastettu, että tietojen pyytäjä todennäköisesti näkyy tallenteella. Tarkoituksena oli selvittää viranomaisen tulkintalinja tallenteesta yleisöjulkisena asiakirjana, jota pyydetäessä ei tarvitse perustella pyyntöään eikä todistaa henkilöllisyyttään (JulKL 13.1 §).⁵⁰ Viranomaisen vastauksesta kirjattiin ylös mahdollisen kieltäytymisen syy sekä perusteet. Muutamassa tapauksessa keskustelua jatkettiin kieltäytymisen perusteiden syventämiseksi.

Kaikki viranomaiset kieltäytyivät luovuttamasta tietoja JulKL tai JulKA nojalla. Pääosin perusteena oli JulKL 24 §:n 1 momentin 7 kohta.⁵¹ Lisäksi eräät täydensivät perusteluitaan viittaamalla muuhun lainsäädäntöön. EU:n virastojen kohdalla kieltäytymisen syy oli JulKA 4 artiklan 1 kohta.

Seuraavaksi pyydettiin kirjoittajan omien henkilötietojen tarkastusta GDPR 15 artiklan nojalla. Kahdelta viranomaiselta omien tietojen tarkastusta ei pyydetty, koska kirjoittaja ei ollut vieraillut kyseisen viranomaisen valvontakameroiden edustalla siten, että henkilötietoja olisi tallentunut järjestelmään. Koonti tietopyyntöjen tuloksista on koottu taulukkoon.

50. Myös JulKA 6.1 artikla. Vaikka kyse olikin tutkimuksellisesta tarkoituksesta, se kytkeytyy JulKL 3 §:n tarkoitukseen mahdollisuudesta valvoa julkisen vallan käyttöä, muodostaa vapaasti mielipiteensä sekä vaikuttaa julkisen vallan käyttöön. Julkisuudella on funktionsa myös kansalaisten ja viranomaisen välisen luottamuksen ylläpitämisessä, jota ilman viranomaisen on vaikea toimia. Ks. Vigjilence Abazi – Eljalill Tauschinsky, *Reasons of Control and Trust: Grounding the Public Need for Transparency in the European Union*. *Utrecht Law Review* 11(2) 2015, s. 78–90, 81–84.

51. Yksikään viranomaisista ei vastannut, että kyse olisi ”henkilörekisteristä tai muusta asiakirjasta, josta tieto voidaan luovuttaa vain tietyin edellytyksin” (JulKL 13.2 §), jolloin pyytäjän olisi ilmoitettava tietojen käyttötarkoitus, muut tietojen luovuttamisen edellytysten selvittämiseksi tarpeelliset seikat sekä tarvittaessa tiedot sitä miten tietojen suojaus on tarkoitus järjestää. ”Muut asiakirjat” viittaa lähinnä salassa pidettäviin asiakirjoihin (ks. HE 30/1998 vp, s. 70). Henkilörekisterin käsite on ongelmallisempi. Mikäli lyhyt tallenne tai kuva katsottaisiin henkilörekisteriksi, saattaisi se tarpeettomasti vaikeuttaa julkisuusperiaatteen toteuttamista. Alkuperäiseen henkilörekisterin (ks. kumottu henkilörekisterilaki 523/1999 3.1 §:n 3 kohta) määritelmään sisällynyt vaatimus henkilötietojen helposta ja taloudellisesti edullisesta löydettävyydestä täyttynee muun muassa kasvojen tunnistusalgoritmien kehittämisen myötä. Lyhyehkö tallenne tai still-kuva ei kuitenkaan täyttäne GDPR 4.6 kohdan määritelmää tietojoukosta. Ks. myös Päivi Korpisaari, *Miten henkilötietojen suoja rajoittaa paikkatietojen käyttämistä?* *Liikejuridiiikka* 1/2018, s. 40 ja myös tapaus T-436/09 asiakirjan ja tietokannan käsitteistä.

Taulukko 1: Viranomaisten vastaukset tietopyyntöihin.

Viranomainen	Luovutuspyyntö	Julkisuusperusteinen luovutus	Tarkastusperusteinen luovutus
Euroopan komissio	Parlamentin edusta	Ei, JulkA 4.1 artiklan alakohta a	Ei pyydetty
Euroopan kemikaalivirasto ECHA	Eteläpään seinusta	Ei, JulkA 4.1 artiklan alakohta b	Kyllä, paikan päällä katsottavaksi
Helsingin kaupunki	Kaupungintalon edusta	Ei, JulkL 24.1 §:n 7 kohta	Kyllä, paikan päällä luovutettavaksi
TPK	Presidentinlinna, Katajanokan kulma	Ei, JulkL 24.1 §:n 7 kohta	Ei, TSL 34.1 §:n 1 k, GDPR 23.1 artiklan c ja d alakohta
Ulkoministeriö	Ankkurikadun sivusta	Ei, JulkL 24.1 §:n 7 kohta	Ei, TSL 34.1 §:n 1 k, GDPR 23.1 artiklan d alakohta
Suojelupoliisi	Ratakadun ja Fredrikinkadun kulma	Ei, JulkL 24.1 §:n 7 ja 9 kohta	Ei pyydetty
VNK	OM henkilöstöravintolan edusta	Ei, JulkL 24.1 §:n 7 kohta + muita	Ei, TSL 34.1 §:n 1 k, GDPR 23.1 artiklan d alakohta
KKO	Eteläinen sivu	Ei, JulkL 24.1 §:n 7 kohta	Kyllä, luovutus jos todistaa henkilöllisyyden

JulkL 14.3 §:n mukaan tieto julkisesta asiakirjasta on annettava mahdollisimman pian, kuitenkin viimeistään kahden viikon kuluessa siitä, kun viranomainen on saanut asiakirjan saamista koskevan pyynnön. JulkA 7.1 artiklan mukainen määräaika on 15 työpäivää.⁵²

GDPR 12 artiklan 3 kohdan mukaan pyydetty tiedot on toimitettava ilman aiheetonta viivytystä kuukauden kuluessa pyynnön vastaanottamisesta. Määräaika voidaan tarvittaessa jatkaa enintään kahdella kuukaudella ottaen huomioon pyyntöjen monimutkaisuus ja määrä.

Kirjasimme ylös viranomaisten vastausajat. Pääsääntöisesti viranomaiset vastasivat julkisuusperusteisiin tietopyyntöihin juuri ja juuri määräaikojen puiteissa. Nopeimmat vastaukset saatiin muutamassa päivässä tietopyynnön lähettämisestä. Yhdessä tapauksessa viranomainen väitti, että tallenne ei olisi

52. JulkL 14.3 §:n nojalla määräaika voidaan esimerkiksi suuren työmäärän vuoksi pidentää kuukauteen. Vastaavasti JulkA 7 ja 8 artiklat mahdollistavat ensimmäisen ja toisen (muutoksenhaku) vaiheen pidennyksen 15 työpäivällä. Euroopan komissio päätyikin toisessa vaiheessa käyttämään tätä mahdollisuutta: ”Valitettavasti emme ole vielä pystyneet keräämään kaikkia tietoja, jotka tarvitaan pyyntönne perusteellista analysointia varten lopullisen päätöksen tekemiseksi.”

asiakirja, johon sovelletaan julkisuusasetusta. Vastauksesta tehtiin oikaisupyyntö, johon saatiin vastaus kolmen viikon kuluttua oikaisupyyntöstä. Tässä vastauksessa mainittu virhe oikaistiin.

Henkilötietojen tarkastuspyyntöön viranomaiset vastasivat nopeasti, yksi jopa samana päivänä. Enimmillään pyynnön käsittelyyn kului 5 päivää (sisältäen viikonlopun), joten pyyntöihin reagoidaan GDPR:n edellyttämällä tavalla. Sen sijaan JulkL 14.3 §:n maksimista näyttää muodostuneen vastausaika.⁵³ Muutamassa tapauksessa määräaika ylittyi enintään kahdella päivällä.

3.1. Tietopyynnot tallenteisiin viranomaisen asiakirjoina

Yhtä lukuun ottamatta kaikki viranomaiset pitivät tallenteita sellaisina, joiden luovuttaminen voi johtaa turvajärjestelyjen vaarantumiseen. Vastauksia ei pääsääntöisesti perusteltu tarkemmin, vaan perusteet olivat yleisellä tasolla, esimerkiksi ”turvajärjestelyt voivat vaarantua teknisistä syistä”. Yksi viranomainen kuitenkin tarkensi, että tallenteen antaminen paljastaisi tietoja muun muassa kameravalvotun alueen rajauksesta ja kameravalvonnan laadusta (erottelukyky ja toiminta hämärässä).

Turvajärjestelyiden vaarantumisen lisäksi viranomaiset ilmoittivat myös täydentäviä salassapitoperusteita. Suojelupoliisi ilmoitti luovuttamisen paitsi vaarantavan turvajärjestelyt, myös vaarantavan valtion turvallisuuden ja olevan vastoin erittäin tärkeää yleistä etua. Monessa tapauksessa viranomainen totesi muun ohella, että tallenteet saattavat sisältää tai sisältävät EU:n yleisen tietosuojasetuksen mukaisia henkilötietoja.

Arvioimme syyksi perusteluiden niukkuudelle sen, että asiakirjajulkisuuteen perustuvissa tietopyynnöissä tyydyimme pääsääntöisesti viranomaisen ensimmäiseen vastaukseen asiassa, jos sen arvioitiin olevan oikeudellisesti kestävällä pohjalla ja vastaavan muiden viranomaisten tulkintalinjaa. Kahdessa tapauksessa jo ensimmäisen pyynnön johdosta saimme valituskelpoisen hallintopäätöksen.⁵⁴

EU:n toimielinten vastaukset poikkesivat toisistaan. Kemikaalivirasto totesi vastauksessaan, että tallenteissa esiintyy henkilötietoja, eikä niitä siitä syystä

53. Kaksi viikkoa on verraten pitkä aika. Norjassa aikaraja on kolme päivää, viiden päivän jälkeen voi jo valittaa. Tanskassa määräaika on kaksi päivää ja maksimi kymmenen ja Islannissa määritelmä on heti, kuitenkin seitsemän päivän sisällä.

54. Tietopyynnöstä pitäisi aina antaa valituskelpoinen päätös, kuten eduskunnan oikeusasiamies on ratkaisussaan 22.3.2003 korostanut. Valituskelpoinen päätös tarkoittaa viranomaisen päätöstä valitusosoituksineen. Yksittäisen virkamiehen tai viranhaltijan vastauksesta tietopyyntöön voi pyytää viranomaisen valituskelpoisen päätöksen. Valituskelpoinen päätös voidaan toki antaa jo heti vastauksena tietopyyntöön. Neuvonen 2019, s. 101–103.

voida luovuttaa (JulkA 4.1 artiklan b alakohta).⁵⁵ EU:n komissio puolestaan totesi, että videovalvontalaitteet on asennettu ihmisten, omaisuuden ja tiedon suojaamiseksi ja siten muodostavat osan komission turvallisuusinfrastruktuuria. Tiedon luovuttaminen paljastaisi komission mukaan tämän infrastruktuurin komponentteja ja vaarantaisi siten yleisen turvallisuuden. EU:n komissio perusteli luovuttamisesta kieltäytymistä JulkA 4.1 artiklan alakohdalla a, jonka mukaan toimet eivät anna tutustuttavaksi asiakirjaa, jonka sisältämien tietojen ilmaiseminen vahingoittaisi yleistä turvallisuutta.

EU:n komission ensimmäiseen vastaukseen tehtiin uudistettu hakemus.⁵⁶ Hakemuksessa väitettiin, että komissio ei voisi vastata yleisestä turvallisuudesta parlamenttirakennuksen lähiympäristössä, sillä yleisestä turvallisuudesta ka-tualueella vastaa lain⁵⁷ nojalla Belgian poliisi.⁵⁸ Komissio ei muuttanut kantaansa, vaan totesi että sillä on laaja harkintavalta sen arvioidessa sitä, voiko asiakirjaan tutustuminen vahingoittaa yleistä etua.⁵⁹ Komissio totesi, että videotallenteen julkistaminen vaarantaisi komission henkilöstön, vierailijoiden ja suuren yleisön turvallisuuden, jota komissio piti JulkA 4.1 artiklan yleiseen turvallisuuteen kuuluvana asiana. Kysymys siitä, kenellä on toimivalta yleiseen turvallisuuteen liittyvään kameravalvontaan, oli komission mukaan merkitykseltön.

Lisäksi komissio totesi, että kameravalvonnalla on kolme tavoitetta: väärinkäytösten ehkäiseminen, havaitseminen ja dokumentointi. Väärinkäytöksiä voi komission mukaan esiintyä monissa muodoissa, joita ovat esimerkiksi väkivalta, luvaton pääsy rakennuksiin tai epäsosiaalinen käyttäytyminen kuten omaisuuden fyysinen vahingoittaminen.

Komission mukaan pyydetyn tallenteen julkistaminen voisi vakavasti vaarantaa edellä mainitut tavoitteet, sillä se paljastaisi kyseisen turvallisuusinfra-

55. Kemikaalivirasto totesi vastauksessaan, että henkilötietojen luovuttaminen voisi olla mahdollista asetuksen 2018/1725 artiklan 9 kohdan 1 alakohdan b nojalla edellyttäen, että hakija olisi perustellusti esittänyt, että tiedot on tarpeen siirtää yleistä etua koskevaa erityistä tarkoitusta varten. Tällainen tarkoitus saattaisi olla esimerkiksi tieteellinen tutkimus. Tähän ei tekemissämme tietopyynnöissä vedottu, sillä tutkimus kohdistui viranomaisten toimintaan, ei tallenteiden sisältöön.

56. JulkA 7 ja 8 artiklojen perusteella EU-toimielinten asiakirjajulkisuusasioiden käsittelyprosessi on hieman vastaavalla tavalla kaksivaiheinen, kuten julkisuuslain mukainen käsittelyprosessi (vrt. JulkL 14.3 §). JulkA 7 artiklan mukaan hakija voi viidentoista työpäivän kuluessa siitä, kun hän on vastaanottanut toimielimen vastauksen, tehdä uudistetun hakemuksen ja pyytää toimielintä tarkistamaan kantaansa. Jos uudistettu hakemus hylätään, hakija voi nostaa kanteen toimielintä vastaan tuomioistuimessa ja/tai kannella oikeusasiamiehelle EY:n perustamissopimuksen asianomaisten määräysten mukaisesti.

57. CHAPITRE III. Art 14. 5 AOUT 1992. Loi sur la fonction de police.

58. Suomessa yleisen järjestyksen ja turvallisuuden ylläpitoa on pidettävä julkisena hallintotehtävänä, josta on säädettävä lailla. Siten esimerkiksi yksityinen vartioimisliike ei voi vastaanottaa toimeksiantoa yleisen järjestyksen ja turvallisuuden ylläpitämiseksi. HE 22/2014 vp laiksi yksityisistä turvallisuuspalveluista sekä eräksi siihen liittyviksi laeiksi, s. 27.

59. Komissio viittasi unionin oikeuden tapauksiin C-266/05 (kohta 56) ja T-264/04 (kohta 40).

struktuurin osatekijöitä. Kolmannet henkilöt voisivat komission näkemyksen mukaan saada selville komission kameraverkon täsmällisen kattavuuden esimerkiksi tutkimalla, missä he näkyvät kameroissa ja missä eivät. Tämä voisi helpottaa väärinkäytöksiä, sillä yksilöt voisivat kehittää menetelmiä välttääkseen havaitsemisensa, ja häiriötapausten jälkeiset tutkimukset olisivat hyödyttömiä, koska tapahtumapaikalta ei olisi saatavilla kuvaa.⁶⁰

Komissio totesi vastauksessaan myös, että julkistetut asiakirjat tulevat koko suuren yleisön eivätkä ainoastaan pyynnön esittäjän saataville (ns. erga omnes -vaikutus). Komissio perusteli luovuttamatta jättämistä myös komission päätöksellä 2015/443.⁶¹ Henkilöiden, ajoneuvojen, tavaroiden ja laitteiden saapuminen komission tiloihin ja poistuminen niistä kirjataan fyysisen turvallisuuden varmistamiseksi. Tällainen julkisen toimielimen tavoitteleva päämäärä kuuluu komission mukaan ”yleisen turvallisuuden” käsitteen alaan riippumatta jäsenvaltion omasta toimivallasta ja siitä, kuuluvatko valvontakamerat katualueella komission toimivaltaan vai eivät.

Kaikilla tietopyynnön kohteeksi valikoituneilla viranomaisilla oli intressi olla paljastamatta videovalvontalaitteiden teknisiä yksityiskohtia, jotka voivat paljastua tallenteet luovuttamalla.⁶² Sekä EU-oikeuteen että julkisuuslakiin pohjautuva argumentaatio oli identtistä, luovuttamatta jättämisellä haluttiin suojella arvoja kuten ”kokonaisturvallisuus” ja ”omaisuuden turvallisuus”.⁶³ Turvajärjestelmään kuuluvalla kameralla on tarkoitus suojata näitä arvoja. Ainoastaan yhdessä tapauksessa vedottiin pelkästään siihen, että tallenteet luovuttamalla rikottaisiin kolmannen osapuolen (kuvassa näkyvän henkilön) oikeutta yksityisyyteen.

Luovuttamatta jättäminen kolmannen osapuolen henkilötietojen perusteella saattaa olla mahdollista EU:n toimielimille julka 4 artiklan nojalla. Vastaavaa

60. Euroopan komission päätös C(2021) 5556 final, 19.7.2021.

61. Päätöksen mukaan toimielimen on toteutettava toimenpiteitä henkilöiden, omaisuuden ja tiedon turvallisuuden varmistamiseksi.

62. Toisin kuin joidenkin muiden tallennemuotojen kohdalla, ei videotallenteen kohdalla ole helpoa toteuttaa osajulkisuutta, ks. KHO 28.9.2016 T 4078.

63. Turvallisuuteen liittyvät käsitteet voidaan nähdä epämääräisinä ja kieltäytymistä koskevien perusteluiden valossa rakentuvat ensisijaisesti viranomaisen tarpeelle suojata omaa toimintaa ja omaisuutta eriasteisilta ”hyökkäyksiltä”. Kun viranomaiset suojaavat itseään, he samalla katsovat suojaavansa laajemmin yleistä etua, jonka edistämiseksi viranomainen on olemassa. Perusteluiden valossa luovuttamatta jättäminen kytkeytyy ensi sijassa ”kovaan” turvallisuuteen (security), turvallisuuden järjestysulottuvuuteen, joka puolestaan kytkeytyy ns. yleiseen järjestykseen ja turvallisuuteen. Ks. Kari Telaranta, Turvallisuus lainsäätäjän diskursseissa 2019, s. 184–219 teoksessa Alisa Puustinen (toim.), Pelastus- ja turvallisuustutkimuksen vuosikirja 2019. Pelastusopisto. Saatavilla osoitteessa <https://www.pelastusopisto.fi/tutkimus-ja-tietopalvelut/tki-palvelut/vuosikirja/>. Kerttula on väitöskirjassaan analysoinut henkilökohtaisen turvallisuuden ja yleisen järjestyksen ja turvallisuuden suhteesta käytyä keskustelua. Ks. Timo Kerttula, Vartijat ja järjestyksenvalvojat julkisen vallan käyttäjinä. Helsingin yliopisto 2010, s. 79–85. Saatavilla osoitteessa <http://urn.fi/URN:ISBN:978-952-10-5547-8>.

mahdollisuutta ei ole julkisuuslain 24 §:n salassapitoperusteissa.⁶⁴ Erona EU-oikeuteen tallenteella olevan henkilötiedon tulee olla arkaluonteinen ollakseen salassa pidettävä.⁶⁵

3.2. Tietopyynnöt tallenteisiin henkilötietoina

Kun tarkastelun kohteena olevat virastot kieltäytyivät luovuttamasta tallenteita asiakirjajulkisuuden perusteella, seuraavaksi samoja virastoja lähestyttiin pyynnöllä saada itseään koskevista henkilötiedoista jäljennös. Kahta virastoa lukuun ottamatta kirjoittaja kävi näyttäytymässä valvontakameran edessä pitäen kädessään erityisellä kuviolla varustettua paperia. Näyttäytyminen pyrittiin järjestämään siten, että kuvassa ei näkyisi muita ihmisiä.

Yksikään virastoista ei kiistänyt kirjoittajasta otetun kuvan asemaa henkilötietona. Kolme kuudesta virastosta oli valmiita luovuttamaan tai esittämään pyydetty tallenteet. Yksi virastoista olisi tarjonnut tallenteen muistitikulle tallennettuna, jos kirjoittaja olisi vieraillut viraston nimeämässä yhteyspisteessä ja toinen tarjosi mahdollisuutta tulla tutustumaan tallenteeseen paikan päällä. Kolmas olisi halunnut vielä varmistua siitä, että tietojen pyytäjä on sama kuin tallenteella oleva henkilö, ja olisi tämän jälkeen ollut valmis luovuttamaan tallenteen.

Kolme kuudesta virastosta kieltäytyi luovuttamasta pyydettyjä tietoja. Kieltäytymistä perusteltiin muun muassa sillä, että luovuttamalla kameratallenteet, olisi tiedon saajalla pääsy viraston ja valtion turvallisuusjärjestelyihin ja mahdollisuus selvittää muun muassa mahdollisia kameravalvonnan katvealueita. Pelkästään tietoa siitä, käsitelläänkö rekisteröidyn tietoja tallenteessa, voidaan vastausten mukaan pitää riittävänä tietona esimerkiksi katvealueiden selvittämiseksi. Edelleen luovuttamisesta kieltäytymistä perusteltiin sillä, että luovuttaminen voisi vaarantaa virastoon kohdistuvat turvallisuusvaatimukset tai heikentäisi oleellisesti viraston mahdollisuutta huolehtia sen lakisääteisestä tehtävästä. Lisäksi vedottiin siihen, että luovuttaminen häittäisi rikosten ehkäisemistä tai selvittämistä.⁶⁶ Myös henkilöstön ja vierailijoiden oikeussuoja sekä turvallisuus,

64. TSL 28 §:n mukaan oikeuteen saada tieto ja muuhun henkilötietojen luovuttamiseen viranomaisen henkilörekisteristä sovelletaan, mitä viranomaisten toiminnan julkisuudesta säädetään.

65. Mikael Koillinen kiinnitti ennen GDPR:n voimaantuloa huomiota sen jännitteeseen kotimaisen julkisuusperiaattemme kanssa ja mahdollisiin EU-oikeuden etusijaperiaatteesta johtuviin ongelmiin. Lopulliseen asetukseen päätyntyn julkisuusperiaatteen huomioimisen mahdollistava 86 artikla näyttäisi vastaavan tähän huoleen. Ks. Mikael Koillinen, Oikeudesta anonyymien julkisen vallan käyttöön. Lakimies 1/2016, s. 26–52, 48–51. Ks. myös Helge Kranenborg, Access to Documents and Data Protection in the European Union: On the Public Nature of Personal Data. Common Market Law Review 45(4) 2008, s. 1079–1114.

66. Rikosten selvittämisen kannalta tallenteiden hyödyntämisessä näyttäisi olevan Paasosen ja Luomalan mukaan parantamisen varaa. Mikäli kameroiden yhtenä tarkoituksena on rikosten

omaisuuden suojaaminen ja kansainvälisten tietoturvavelvoitteiden täyttäminen mainittiin suojattavina arvoina.

Virastojen mukaan niiden omasta turvallisuudesta huolehtiminen on velvollisuus, ja tallenteiden luovuttaminen vaarantaisi näiden lakisääteisten tehtävien hoitamisen. Virastot vetosivat tältä osin vastauksissaan muun muassa lakiin kansainvälisistä tietoturvasuvelvoitteista (588/2004), lakiin tasavallan presidentin kansliasta (100/2012) sekä asetukseen asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019).

TSL:n perusteluissa todetaan,⁶⁷ että kansallisen turvallisuuden, puolustuksen, yleisen järjestyksen ja turvallisuuden vaarantuminen tai rikosten ehkäisemisen ja selvittämisen vaarantuminen on ollut peruste tiedon luovuttamisesta kieltäytymiselle myös tietosuojalakia edeltäneessä henkilötietolaissa (523/1999, 27 §). Henkilötietolain 27 §:n perusteluissa⁶⁸ viitattiin henkilötietolakia edeltäneeseen henkilörekisterilakiin (471/1987), jonka 12 §:n mukaan tarkastusoikeutta ei ollut, jos tiedon antaminen saattaisi vahingoittaa valtion turvallisuutta taikka suhteita toiseen valtioon tai kansainväliseen järjestöön, haitata rikosten ehkäisemistä tai selvittämistä taikka olla vastoin muuta erittäin tärkeää yleistä etua. Henkilötietolailla implementoidun, kumotun tietosuojadirektiivin 13 artikla ei mahdollistanut poikkeamista tärkeän yleisen edun perusteella, joten se jäi pois henkilötietolaista.⁶⁹

Yleiseen etuun liittyvien rajoitusperusteiden osalta on siis viitattu taaksepäin aina henkilörekisterilakiin saakka. Henkilörekisterilain 12 §:n yksityiskohtaisissa perusteluissa todettiin, että mainitut rajoitukset koskisivat lähinnä viranomaisten rekistereitä ja rajoitusperusteen käyttö edellyttää aina tapauskohtaista harkintaa. Näin ollen rajoituksista piti nimenomaan säätää erikseen.⁷⁰ Yleiseen etuun ja rikostorjuntaan liittyvät tarkastusoikeuden rajoitukset ovat siis alun perinkin koskeneet lähtökohtaisesti vain viranomaisten hallussa olevia henkilötietoja.

Nyt tehdyssä empiirisessä tarkastelussa kerätyt havainnot puoltavat sitä johtopäätelmää siitä, että nämä yleiseen etuun liittyvät rajoitusperusteet soveltuvat vain tietyille virastoille. Ne valtion viranomaiset, joilla oli poikkeuksellisia lakisääteisiä tehtäviä oman turvallisuutensa varmistamiseen liittyen, kytkivät omien turvajärjestelyidensä salassapidon, myös rekisteröidyltä itseltään, oman toiminnan suojaamiseen rikoksilta ja muilta hyökkäyksiltä sekä laajemmin kyseisen viranomaisen yleiseen etuun liittyvään tehtävään. Muut, valtion turvallisuuden kannalta vähemmän keskeiset virastot sen sijaan eivät vedonneet yleisen

selvittäminen, keskiöön nousee kameroiden sijoittelu sekä videokuvan laatu. Jyri Paasonen – Mikko Luomala, Kameravalvonta tutkimus- ja sääntelykohteena. Edilex 2021, s. 3. Saatavilla osoitteessa <https://www.edilex.fi/artikkelit/24627>.

67. HE 9/2018 vp, s. 119.

68. HE 96/1998 vp henkilötietolaiksi ja eräksi siihen liittyviksi laeiksi, s. 62.

69. Ibid., s. 62.

70. HE 49/1986 vp henkilörekisterilaiksi ja siihen liittyviksi laeiksi, s. 36.

järjestyksen ja turvallisuuden vaarantumiseen taikka rikosten ehkäisemisen ja selvittämisen vaarantumiseen, vaan päätyivät antamaan pyydetty tiedot.

3.3. Havainnot käsittelytoimista laadituista selosteista

Tarkastuspyynnöissä pyydettiin GDPR 30.1 artiklan edellyttämä seloste käsittelytoimista. Selosteessa on oltava muun muassa rekisterinpitäjän, hänen edustajansa ja tietosuojavastaavan nimi sekä yhteystiedot, käsittelyn tarkoitukset, kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä, kenelle henkilötietoja luovutetaan, mahdollisuuksien mukaan eri tietoryhmien poistamisen suunnitellut määräajat⁷¹ sekä mahdollisuuksien mukaan yleinen kuvaus teknisistä ja organisatorisista turvatoimista.

GDPR 37.1.a artikla edellyttää, että tietosuojavastaava on nimettävä aina kun tietojenkäsittelyä suorittaa jokin muu viranomainen tai julkishallinnon elin kuin lainkäyttötehtäviään hoitava tuomioistuin. Saman artiklan 6 kohdan mukaan tietosuojavastaava voi olla henkilöstön jäsen tai hän voi hoitaa tehtäviään palvelusopimuksen perusteella. Artiklan 7 kohdan mukaan rekisterinpitäjän tai henkilötietojen käsittelijän on julkistettava tietosuojavastaavan yhteystiedot. Ei liene mahdollista, että tietosuojavastaavana toimisi esimerkiksi viranomaisen kirjaamo tai muu vastaava yleinen yhteydenottopiste.⁷² Tiedon saaminen julkisen vallan käyttäjien nimistä kuuluu julkisuusperiaatteen ydinalueeseen.⁷³

EU:n komissiolta ei pyydetty selostetta kameravalvontaan liittyvistä käsittelytoimista. Muilta se pyydettiin ja saatiin (7 kpl). Selosteista tarkistettiin, onko niissä kerrottu kameravalvonnan tarkoitus, tietojen käsittelyperuste, tietosuojavastaava ja hänen yhteystietonsa, tietojen hankintatapa sekä säilytyksen määräajat. Pääsääntöisesti kameravalvonnan tarkoituksena oli työntekijöiden ja muiden tiloissa olevien turvallisuuden varmistaminen ja omaisuuden suojeleminen. Yhdessä selosteessa mainittiin lisäksi järjestyksen valvonta. Yhdessä selosteessa ei kerrottu lainkaan kameravalvonnan tarkoitusta.

Yhdessä tapauksessa tarkoituksena oli mahdollistaa poliisin tekninen valvonta. Selosteen mukaan tietoja ei pääsääntöisesti luovuteta, ja jos niitä luovu-

71. Kun kyseessä on henkilötiedot, joita ei ole saatu henkilöltä itseltään (kuten kameravalvonnan tallenteet), GDPR 14.2.a artikla edellyttää ilmoittamaan joko henkilötietojen säilytysajan tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit.

72. Tietosuojavastaava on ilmoitettava rekisterinpitäjän selosteessa ”tarvittaessa”, kun taas henkilötietojen käsittelijän on ilmoitettava aina tietosuojavastaavan nimi. Emme arvioineet, missä määrin GDPR soveltuu poliisin hallinnassa olevien tilojen kameravalvontaan ja missä määrin sovelletaan rikosasioiden tietosuojadirektiiviä 2016/680. Laki (1054/2018) sisältää vastaavat säännökset kuin GDPR, 38 § edellyttää nimeämään tietosuojavastaavan ja 18 § edellyttää laatimaan selosteen käsittelytoimista.

73. Koillinen 2016, s. 36.

tetaan, se tehdään ”voimassa olevan lainsäädännön velvoittamissa ja sallimissa rajoissa”. Selosteesta ei yksiselitteisesti selvinnyt, luovutetaanko henkilötietoja eteenpäin toiselle viranomaiselle (poliisi). Henkilötietojen käsittely ei ole oikeutettua muilla kuin tietosuojasetuksen 6 artiklassa mainituilla perusteilla. Siten käsittelyperuste ei lähtökohtaisesti voine olla poliisin tarve tietoihin, kun kyseessä on jokin muu viranomainen kuin poliisi.⁷⁴

Toisessa selosteessa oli kuvattu melko yksityiskohtaisesti kameroiden sijainti, valvotut alueet ja kameravalvonnan toiminta-aika. Muissa selosteissa oli todettu esimerkiksi, että tallennetaan ”laitteiden ja järjestelmien” tuottamaa tietoa, tai mainittiin valvontakamerat alueilla ja toimipisteissä tai kiinteistöt ja niiden välitön läheisyys. Yhdessä selosteessa ei kerrottu tietojen hankinnasta mitään.

Tietosuojavastaavan nimi ja yhteystiedot oli merkitty kolmeen selosteeseen. Yhdessä selosteessa oli vain titteli, toisessa vain sähköpostiosoite. Kahdesta selosteesta puuttui tietosuojavastaavan nimi ja yhteystiedot kokonaan tai tietosuojavastaavaksi oli nimetty kirjaamo tai vaihde. Tietojen säilytysaika oli pääsääntöisesti 1 kuukausi (3 kpl). Yhdellä viranomaisella säilytysajaksi oli merkitty ”enintään 1 vuosi” ja kaksi sisälsi säilytysajan osalta viittauksen toiseen asiakirjaan.⁷⁵ Eräässä selosteessa säilytysaika oli ”tietolähdekohtainen”.

Monessa selosteessa haasteena oli niiden yleisluonteisuus. Selosteelle oli usein pyritty mahduttamaan kaikki ”ydintoiminnan” ulkopuolisten rekistereiden asiat. Erityisesti kameravalvontaa varten laadituissa selosteissa henkilötietojen käsittelyn perusteeksi oli merkitty yleinen etu. Kaikenkattavissa selosteissa käsittelyperuste saattoi olla tarve rekisterinpitäjän lakisääteisen veloitteen noudattamisesta. Tallentavaa kameravalvontaa ei voi perusteella lakisääteisellä velvoitteella, ellei laissa selkeästi edellytetä, että viranomainen tekee tiloissaan teknistä valvontaa. Kahdessa selosteessa käsittelyperustetta ei ilmoitettu lainkaan.

Rekisteröidyn oikeuksien kannalta tallenteiden säilyttämisaika on omien tietojen tarkastusoikeuden toteuttamiseksi merkityksellinen, mutta yksiselitteisesti säilytysaika ilmeni vain kolmessa tapauksessa. Tarkastelun perusteella ongelmia oli tietosuojavastaavien nimeämisessä. Yhteystietoja ei kerrottu kolmessa tapauksessa seitsemästä. Selosteiden perusteella myös kameravalvonnan lainmukaisuus herättää epäilyjä, sillä sen oikeutus tulee aina kyetä palauttamaan GDPR 6 artiklan mukaiseen lainmukaiseen käsittelyperusteeseen.

74. Ks. Apulaistietosuojavaltuutettu 4.6.2021 Dnro 4900/182/18. Tapauksessa apulaistietosuojavaltuutettu totesi, että rekisterinpitäjän tulee myös kiinnittää huomiota siihen, ettei se perustelee henkilötietojen käsittelyä poliisin tarpeella.

75. Mainitut asiakirjat olivat ”tiedonohjaussuunnitelma” ja ”arkistonmuodostussuunnitelma”.

4. Pohdinta

Viranomaisten tulkinnan perusteella valvontakameroiden tallenteet eivät ole kaikille luovutettavia julkisia asiakirjoja. Päätösten perustelujen mukaan viranomaiset haluavat turvata, että kameravalvonta osana teknisiä turvallisuusjärjestelyitä ei vaarannu. Mikäli tallenteet olisivat julkisia, kuka tahansa voisi pyytää kameroiden tallenteet ja päätellä niistä turvajärjestelyiden kannalta keskeisiä tietoja.

Yksittäisen kameran suorituskykytietojen paljastuminen ei välttämättä ole turvajärjestelmien kokonaisuuden kannalta merkittävää. Kameran teknisiä yksityiskohtia voi tallenteen lisäksi olla pääteltävissä myös muutoin, esimerkiksi tarkastelemalla kameraa ulkoisesti. Yksittäisen kameran merkitys voi olla muutoinkin vähäinen esimerkiksi siitä syystä, että useat kamerat kuvaavat samaa tilaa. Este tallenteen luovuttamiselle ei saa olla täysin hypoteettinen, vaan turvajärjestelmien vaarantumisen on oltava kohtuullisesti ennakoitavissa.⁷⁶

Joskus intressi, kuten yleinen etu tallenteiden luovuttamiselle voi olla salassapitoa suurempi. Salassapito ei ole ehdoton. Yksittäisen tallenteen luovuttamisen kannalta merkitystä on sillä, kuinka merkittävä turvajärjestelyiden vaarantumisen luovuttamisesta seuraa. Tallenne tulisi luovuttaa, jos se viranomaisen mukaan ei vaaranna turvajärjestelyitä. Arvioinnissa viranomaisen on syytä punnita niitä intressejä, jotka puoltavat tallenteen luovuttamista suhteessa luovuttamisesta mahdollisesti aiheutuvaan haittaan.

Toisaalta turvajärjestelyiden arvo suojattavana intressinä ei voi olla rajaton. Turvajärjestelyt tulisi muutoinkin suunnitella ja toteuttaa uudestaan sellaisen tilanteen jälkeen, jossa turvajärjestelyitä koskevia tietoja on vuotanut tai niitä on jouduttu luovuttamaan. Siten punninnassa voi olla kyse siitä, mikä on turvajärjestelyiden tilapäisen vaarantumisen ennakoitavissa oleva vaikutusaika ja vaarantumisen vakavuuden aste ja siitä, paljonko turvajärjestelyiden uudelleen-toteutus tulee maksamaan. Luovuttaminen voi olla perusteltavissa esimerkiksi tärkeällä yleisellä edulla, vaikka turvajärjestelyiden arvioitaisiinkin vaarantuvan.

Viranomaisten tulkintalinja on yhtenäinen, kun on kyse julkisuusperusteisesta tallenteiden luovuttamisesta satunnaiselle luovutusta pyytävälle ilman luovuttamista puoltavia intressejä. Samalla olemme havainneet, että näiden tietopyyntöjen vastausajan maksimista on tullut käytännössä vastausaika. Viranomaisten tulkinnat erkaantuvat, kun kyse on tietojen luovuttamisesta henkilötietojen tarkastusoikeuden perusteella.

Tietopyynnön perusteella eräät viranomaiset kieltäytyivät luovuttamasta henkilötietoja. Kieltäytymistä viranomaiset perustelivat kyseisten viranomaisten yleiseen etuun liittyvällä tehtävällä, ja viranomaisen lakisääteisellä velvolli-

76. Ks. Yhteisöjen tuomioistuimen suuren jaoston tuomio yhdistetyissä asioissa C-39/05 ja C-52/05, kohta 43.

suudella suojata omaa toimintaansa. Tämä voi olla hyväksyttävää, jos kyse on erittäin tärkeästä yleisestä edusta kuten valtion jatkuvuudesta (kokonaisturvallisuudesta).⁷⁷ Taustalla on sama tarve suojata turvajärjestelmiä kuin lähestyttäessä tallenteita asiakirjajulkisuuden kautta.

Empiirisessä tarkastelussa mukana ollut EU-virasto kieltäytyi luovuttamasta tallennetta perustellen salaamista tallenteessa esiintyvän ulkopuolisen henkilötiedoilla ja päätyi vastaavasti tietojen esittämisen kannalle, kun kävi ilmi, että henkilötiedot ovat tallenteen pyytäjän.

Yksityisyyden suojan kannalta olennaista on, että esimerkiksi tapauksessa KHO 2021:27 kyse oli jokseenkin arkaluonteisista videotallenteista, mutta ei kuitenkaan niin arkaluonteisista, että salassapitokynnys ylittyisi. KHO arvioi, että tallenteiden sisältö huomioon ottaen oli syytä olettaa, että tiedon antamisen niistä muutoin kuin viranomaisen luona nähtäväksi voisi johtaa eräiden tallenteilla esiintyvien henkilöiden yksityisyyden suojan loukkaamiseen.

Esitutinnan tai tuomioistuinprosessin yhteydessä talletetuista äänistä ja kuvista tieto voidaan antaa vain luovuttamalla tallenne viranomaisen luona nähtäväksi, jos tallenteen sisältö huomioon ottaen on syytä olettaa, että tiedon antaminen muulla tavoin voisi johtaa tallenteessa esiintyvän henkilön yksityisyyden suojan loukkaamiseen.⁷⁸ Esitutkintalain perusteluiden⁷⁹ mukaan tarkoituksena on se, että kukaan ei voisi saada tallenteesta kopiota, vaikka sen sisältämät tiedot olisivat julkisia. Keskeistä on viranomaisen kontrolli siitä, että tallenne ei päädy henkilön haltuun.

Kameravalvonnan tallenteissa on kyse eri intressien välisestä punninnasta ja niiden saattamisesta keskenään tasapainoon.⁸⁰ Rekisterinpitäjän etujen vastapainona on oikeus valvoa julkishallinnon toimintaa ja yksilön mahdollisuus vaikuttaa omien tietojensa käyttöön. Oikeus omaan dataan ja sen hallintaan voidaankin nähdä digitaalisen ajan ihmisoikeutena.⁸¹

77. Kokonaisturvallisuuden käsitteeseen sisältyy muun muassa valtion johtaminen, kansainvälinen toiminta, Suomen puolustuskyky ja sisäinen turvallisuus. Valtioneuvoston periaatepäätös kokonaisturvallisuudesta 5.12.2012, s. 7. Saatavilla osoitteessa <https://valtioneuvosto.fi/documents/10184/1210166/periaatepaatos-kokonaisturvallisuudesta.pdf>.

78. Esitutkintalaki (805/2011) 7 §:n 2 momentti. Vastaava säännös on oikeudenkäyntien julkisuudesta yleisissä tuomioistuimissa annetun lain (370/2007) 13 §:n 2 momentissa.

79. HE 222/2010 vp, s. 233.

80. Perustuslakivaliokunta on painottanut, että yksityiselämän ja henkilötietojen suojalla ei ole etusijaa muihin perusoikeuksiin nähden, vaan ne tulee suhteuttaa muihin perus- ja ihmisoikeuksiin sekä muihin painaviin yhteiskunnallisiin intresseihin, kuten yleiseen turvallisuuteen. Perustuslakivaliokunnan lausunto hallintovaliokunnalle esityksestä EU:n yleistä tietosuojaa-asetusta täydentäväksi lainsäädännöksi PeVL 14/2018 vp, s. 8.

81. Ks. Antti Poikola – Kai Kuikkaniemi – Ossi Kuittinen – Harri Honko – Aleksi Knuutila, MyData: johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen. Liikenne- ja viestintäministeriö 2018. Saatavilla osoitteessa <http://urn.fi/URN:ISBN:978-952-243-554-5>.

Kameravalvontaan julkisella paikalla liittyy henkilötietojen suojan ohella muitakin individualistisia suojeleuintressejä.⁸² Hirsch kytkee yksityisyyden anonymitteettiin, jossa ihminen voi olettaa pysyvänsä tunnistamattomana julkisellakin paikalla ja olematta erityisen tarkkailun alla. Se voi vaarantua kameravalvonnan avulla tapahtuvan toiminnan tarkkailun johdosta. Kohdennetun, vaikeasti haavaitavan seurannan kohteeksi joutuminen voi olla häiritsevää, vaikka ei tekisikään mitään väärää.⁸³

Larsenin mukaan yksilön kontrolli omiin tietoihin on sitä tärkeämpää, mitä henkilökohtaisesti merkityksellisemmistä asioista on kyse ja mitä enemmän ulkopuolinen puuttuminen voi vaikuttaa yksilön identiteettiin.⁸⁴ Yksityisyyden suojan tarve voi olla riippuvainen siitä informaatiosta, jota kuvattalenteelta on saatavissa esimerkiksi tilanteen intiimiydestä.⁸⁵ Suutelevat henkilöt tai autossa nenäänsä kaivava henkilö saattavat odottaa suurempaa yksityisyyttä, kuin yksin kävelevä, ”massaan sulautuva” henkilö.⁸⁶

Nämä eri intressit tulisivatkin parhaiten huomioiduksi siten, että tiedot olisivat nähtävissä rekisterinpitäjän luona. Tällöin rekisterinpitäjällä säilyisi mahdollisuus valvoa, että tallenteiden kopioita ei päädy ulkopuolisten haltuun. Eduskunnan turvallisuusjohtajan pyrkimys näyttäisikin olleen tämä.⁸⁷ Siitä huo-

82. Toisaalta yksityisyydellä voi olla myös yhteisöllisyyttä tukeva funktio, jolloin yksilön suojelelkoituu myös yhteisön hyväksi. Ymmärryksen lisääminen sen yhteisöllisestä merkityksestä voioi parantaa sen asemaa suhteessa turvallisuuteen, jolle yksityisyydellä on tapana jäädä alisteiseksi. Ks. Susanna Lindroos-Hovioheimo, Henkilötietojen suoja EU-oikeudessa: yksityisyyttä yksilön kustannuksella. Lakimies 1/2018, s. 52–75. Hän lähestyy EU:n yksityisyysskehitystä immuni-saation käsitteen avulla.

83. Laajaan yksityisyyssäilytykseen voi kytkeä yksilön mahdollisuudet vaikuttaa siihen, miten hän näyttäytyy maailmassa ja kenen odotuksiin tai uteliaisuuteen hänen täytyy vastata. Hirsch kytkee valvonnan myös sanan- ja kokoontumisvapauteen, joiden toteuttamiseen valvonnalla voi olla negatiivinen vaikutus. Hänen mukaansa myös tallenteiden leviämisen laajuus on merkityksellistä yksityisyyden kannalta – on eri asia, päätyykö tallenne muutaman virkamiehen katsottavaksi vaiko televisiolähetukseen. Andrew von Hirsch, The Ethics of Public Television Surveillance, s. 61–65 teoksessa Andreas von Hirsch – David Garland – Alison Wakefield. Ethical and Social Perspectives on Situational Crime Prevention. Hart Publishing 2004, s. 59–76.

84. Larsen 2011, s. 17. Larsen syventää Hirschin ajatuksia ja jakaa yksityisyyden julkisilla paikoilla neljään normatiiviseen ulottuvuuteen (s. 22–30) ja pohtii kasvokkain kohtaamisen ja kamera-valvonnan kautta valvotuksi tuleminen merkityseroja yksityisyyden kannalta (s. 60–61).

85. Ks. Hirsch 2004, s. 63 ja Larsen 2011 s. 17 ja s. 157–158.

86. Ulkopuolisen voi olla vaikeaa päätellä, millaista yksityisyyden suoja henkilö odottaa. Yksinkin kuvassa näkyvään henkilöön saattaa esimerkiksi kohdistua sosiaalisia odotuksia siitä, että hänen pitäisikin olla jossain muualla kuin kyseisessä paikassa kyseisenä hetkenä. Oma kysymyksensä on se, voiko tällaisilla subjektiivisilla odotuksilla olla oikeudellista suoja. Lindroos-Hovioheimo (2018, s. 64) esittää yksilölähtöiselle näkökulmalle vaihtoehdoksi yksilön persoonan suojaamista yleisten normien perusteella, jolloin yksilöllä itsellään ei ole valtaa päättää, missä hänen yksityisyytensä rajat kulkevat.

87. Tallenteen luovuttamista sen pelkän esittämisen sijaan puoltavia näkökulmia voidaan tunnistaa. Ks. Telaranta Kari, Eduskunnan kameratallenteiden esittäminen edisti julkisuusperiaatetta ja turvasi demokratiaa. Perustuslakiblogi. Suomen valtiosääntöoikeudellinen seura 2021. Saata-

limatta tallenne päättyi julkisuuteen toimittajan kuvattua sen näytöltä kännykkä-kamerallaan. Toisaalta esimerkiksi valvontakameran resoluutiota ei voi päätellä tällaisesta kopiosta.⁸⁸ Julkisuuteen jo päätyneen tallenteen osalta ei luovuttamiselle pitäisi olla samanlaisia esteitä, ellei salassapito perustu useampaan seikkaan. Turvajärjestelmät ovat ainakin jo tulleet sen osalta julkisiksi.

Viranomaisella on harkintavalta siitä, missä, milloin ja missä muodossa tallenteet luovutetaan tai esitetään. Siten tallenteiden esittäminen viranomaisessa toteuttaa paremmin tarkastusoikeuden ja asiakirjajulkisuuden tavoitteita kuin kategorinen kieltäytyminen. Tällöin salassa pidettävä osa, eli kameravalvonnan tekniset yksityiskohdat, eivät tule laajemmin tietoon (ks. JulkL 10 §, osittaisjulkisuus).

Mikäli turvajärjestelyille aiheutuva haitta on vähäinen tai olematon,⁸⁹ tallenteet voidaan myös luovuttaa. Luovuttaminen voi sisältää riskin ulkopuolisten henkilötietojen päättymisestä laajempaan levitykseen, jolloin luovutettaessa tulisi harkita ulkopuolisten henkilöiden henkilötietojen suojaamista esimerkiksi sumentamalla.⁹⁰ Rajatapauksissa viranomainen voi kysyä lisätietoja (JulkL 13.2 §) – mikäli tietopyynnön perusteena on esimerkiksi tallenteella näkyvä mielenkiintoinen luonnonilmiö, tallennetta voi rajata kyseiseen ilmiöön ennen sen luovuttamista.

GDPR 9 artiklan 1 kohdan mukaan rotuun tai etniseen alkuperään, poliittisiin mielipiteisiin, uskonnolliseen tai filosofiseen vakaumukseen, ammattiliiton jäsenyyteen, terveyteen tai seksuaaliseen käyttäytymiseen ja suuntautumiseen liittyvien tietojen käsittely on kielletty. Sama koskee geneettisiä tai biometrisia tietoja henkilön yksiselitteistä tunnistamista varten. Myös lasten henkilötietoja on pyrittävä suojaamaan.⁹¹ Vastaavasti JulkL 24.1 §:n mukaan muun muassa henkilön terveydentila, vammaisuus, seksuaalinen käyttäytyminen tai suuntautuminen tai hänen henkilökohtaiset olonsa ovat salassa pidettäviä. Siten mikäli kuvataallenteelta on pääteltävissä tällaisia tunnistettavissa olevan ulkopuolisen arkaluonteisia tietoja, niiden sumentaminen luovuttamisen yhteydessä on tarpeen. Muilta osin GDPR 86 artikla mahdollistaa henkilötietojen julkisuusperusteisen luovuttamisen.

villa osoitteessa <https://perustuslakiblogi.wordpress.com/2021/03/02/kari-telaranta-eduskunnan-kameratallenteiden-esittaminen-edisti-julkisuusperiaatetta-ja-turvasi-demokratiaa/>.

88. Eduskunnan julkisuuslinjauksista myös KHO 20.12.2016 T 5423.

89. JulkL 17 §:n mukaan tietojen saamista ei saa rajoittaa enempää kuin suojattavan edun vuoksi on tarpeellista.

90. GDPR resitaalin 68 mukaan ”jos tietyssä henkilötietoja sisältävässä tietojoukossa tiedot koskevat useampia kuin yhtä rekisteröityä, oikeus vastaanottaa henkilötietoja ei saisi rajoittaa toisten rekisteröityjen tämän asetuksen mukaisia oikeuksia ja vapauksia”. Arkaluonteisuudesta riippuen tällaisia tietoja voi olla tarpeen sumentaa siinäkin tapauksessa, että tiedot esitetään luovuttamisen sijasta.

91. GDPR resitaali 38.

Viranomaisilla on parantamisen varaa, kun on kyse kameravalvonnan lainmukaisuudesta. Osa tietosuojaselosteista oli vaikeasti löydettävissä tai ei huomioinut kameravalvontaa lainkaan. Myöskään kameravalvonnan perusteltavuutta ei ilmeisesti ole aina arvioitu tasapainotestillä. Olisikin suositeltavaa laatia oma selosteensa, joka on saatavissa viranomaisen verkkosivuilta. Siinä tulisi kertoa paitsi tietosuojavastaavan yhteystiedot, myös tietojen käsittelyperuste ja tallenteiden säilytysaika.

Tallenteen esittämisestä tai luovuttamisesta päättämisen ohella tärkeä kysymys on se, pitäisikö tallennetta tai sen kuvannutta kameraa olla ylipäätään olemassa.⁹² Kameravalvonnan lisääntyminen ja siihen liittyvän avoimuuden puuttuminen myös siellä, missä se ei välttämättä ole perusteltua,⁹³ on kytkettävissä yliturvallistamiseen.⁹⁴ Siinä jokin määritellään turvallisuusarvoksi tarkoituksessa saada tarpeettoman korkea etusija suhteessa muihin intresseihin ja siten esimerkiksi lisää toimivaltuuksia, resursseja tai mahdollisuuksia poiketa säännöistä.⁹⁵

92. Larsenin (2011, s. 186) mukaan ihmiset eivät arvosta anonymiteettiään kovin korkealle, ja ovat valmiita vaihtamaan sen perusteettomiin lupauksiin parantuvasta turvallisuudesta. Toisaalta on osoitettu, että yksilöiden arvostus omaa yksityisyyttään kohtaan ja yksilöiden käyttäytyminen sen suojaamiseksi eivät kohtaa. Ilmiötä kutsutaan yksityisyyssparadoksiksi. Ks. Pamela Wisniewski – Xinru Page, *Privacy Theories and Frameworks*, s. 19 teoksessa Bart P. Knijnenburg – Xinru Page – Pamela Wisniewski – Heather Richter Lipford – Nicholas Proferes – Jennifer Romano, *Modern Socio-Technical Perspectives on Privacy*. Springer 2022, s. 15–41. Saatavilla osoitteessa <https://doi.org/10.1007/978-3-030-82786-1>. Vrt. oikeudellinen yksityisyyssparadoksi, Lindroos-Hovinheimo 2018, s. 62.

93. Vastausta kysymykseen, mitä on laitton kameravalvonta julkisella paikalla, on vaikeaa antaa. Kauppi pitää ongelmana rikosnimikettä ”salakatselu”, sillä salakatseluun voi syyllystä, vaikka se olisi täysin avointa ja siitä olisi ilmoitettu kyltein. Hän esittääkin, että rikoslain salakatselua koskeva rikosnimike muutettaisiin paremmin vastaamaan tekoa, jota on pidettävä rikosoikeudellisesti moitittavana – nimike voisi hänen mukaansa olla laitton kuvaaminen tai laitton katselu. Konsta Kauppi, *Kameravalvonta, yksityisyyden suoja ja rikosoikeus*. Pro gradu -tutkielma, Helsingin yliopisto 2020, s. 115. Saatavilla osoitteessa www.edilex.fi/opinnaytetyot/21259. Salakatselusta ja sen valmistelun kriminalisoimisesta Riku Neuvonen, *Viestintä- ja informaatio-oikeuden perusteet*. Kauppakamari 2019, s. 241–243.

94. Turvallistamisesta Barry Buzan – Ole Wæver – Jaap de Wilde, *Security: A New Framework for Analysis*. Lynne Rienner Publishers 1998, s. 21–48. Yliturvallistamisesta Juha Mäkinen – Laura Puumala, *Eettisiä näkökulmia maanpuolustuksen ja yhteiskunnallisen turvallisuuden dilemmoihin ja paradokseihin*. Tiede ja Ase (79) 2021, s. 32–63, 40–43. Saatavilla osoitteessa <https://journal.fi/ta/article/view/113763>.

95. Turvallistamisesta huumausainerikoksissa Niklas Vainio, *Viestinnän yksityisyyden suojan turvallisuusperusteinen rajoittaminen perustuslakivaliokunnan käytännössä*. Lakimies 6/2017, s. 813–837, 820. Kansallisen turvallisuuden ja terrorismin keinotekoisesta linkityksestä rahanpesuun ja sen potentiaalisista haitoista kansallisille rikosoikeusdoktriineille Tatu Hyttinen – Salla Heinikoski, *Justification of supranational criminal law – Analysis of collective securitization in the EU-level harmonization of money laundering provisions*. Maastricht Journal of European and Comparative Law 26(6) 2019, s. 815–832 ja Kauppi 2020, s. 112–113. Erivapauksien turvallisuusperusteisesta legitimoinnista hallituksen esityksissä Telaranta 2019, erit. s. 198.

Access to CCTV footage: An empirical study of national and EU law

KARI TELARANTA, Master of Business Administration, Doctoral Researcher, Tampere University; RIKU NEUVONEN, LL.D., Senior Lecturer of Public Law, Tampere University

The authors look into the status of recorded CCTV footage in both European Union and Finnish national public organisations both as personal data and as public documents. They outline the legal framework for the confidentiality of and access to such footage. They then dive deeper by empirically examining the application practices of the authorities, so as to systematise the legal status of the footage and the margin of discretion of the authorities.

In assessing whether to grant access to CCTV footage, an authority should balance the interests in favour of granting access and the potential risk of undermining security arrangements. An authority has discretion to decide where, when and in what form the footage is released or access granted to it. Compared to public release, granting access by way of showing the footage at the premises of the authority may cause less disadvantage. This would achieve the best balance between competing interests.