Artikkeli

VERTAISARVIOITU
KOLLEGIALT GRANSKAD
PEER-REVIEWED
www.tsv.fi/tunnus

Riskinäkemykset ja turvakäytännöt suomalaisten tutkivien toimittajien työssä

Tutkivaa journalismia pidetään riskipitoisena journalismin lajina, ja sen harjoittajiin kohdistuu erityisiä turvallisuus- ja tietoturvauhkia. Näiden uhkien luonne ja vakavuus vaihtelevat kuitenkin merkittävästi kontekstista toiseen. Tyypillisesti journalistit pyrkivät huomioimaan nämä riskit ja varautumaan niihin omalla toiminnallaan. Tämä tutkimusartikkeli tarkastelee suomalaisten tutkivien journalistien näkemyksiä työhön liittyvistä riskitekijöistä ja kartoittaa heidän työssään soveltamia turvakäytäntöjä. Lisäksi artikkeli tarkastelee sitä, miten journalistit arvioivat turvakäytäntöjen tarvetta erilaisissa tilanteissa, millaiset tekijät hankaloittavat turvakäytäntöjen soveltamista työssä sekä mitä kautta tutkivat toimittajat ovat saaneet tietoa ja oppia turvallisuutta ja tietoturvaa koskevissa asioissa. Tutkimusaineisto koostuu 12 tutkivan journalistin teemahaastatteluista ja journalistien ennen haastattelua täyttämistä esitietokyselyistä. Aineiston analyysi osoittaa, että tutkivien journalistien huolenaiheet liittyvät Suomessa erityisesti lähteiden suojeluun. Journalistit käyttävät merkittävää itsenäistä harkintavaltaa soveltamiensa turvakäytäntöjen suhteen ja perustavat yleensä harkintansa tapauskohtaisesti tekemiinsä riskiarvioihin. Turvakäytäntöjen opiskelu ja osaamisen ylläpito jäävät tyypillisesti journalistien oman aktiivisuuden varaan, mutta tietoa ja apua jaetaan kollegiaalisesti tutkivien toimittajien ammattikunnan sisällä.

AVAINSANAT: Journalismi (professio), tutkiva journalismi, turvallisuus, tietoturva, turvakäytännöt

Journalismi on globaalisti riskialtis professio, jonka harjoittajiin kohdistuu monenlaisia uhkia (esim. RSF 2023). Uhkatekijöiden vakavuus ja luonne vaihtelevat kuitenkin merkittävästi valtiosta ja kontekstista toiseen (emt.). Journalismin lajeista tutkivaa journalismia pidetään erityisen riskialttiina (esim. Parker 2015, 121; Waisbord 2022, 1949), ja sen harjoittamisen on myös Suomessa havaittu altistavan toimittajia painostuksen, häirinnän ja uhkailun kaltaisille ilmiöille (Hiltunen, Suuronen ja Pöyhtäri 2024; Hiltunen 2022, 104–105).

Tutkivassa journalismissa toimittajat oma-aloitteisesti selvittävät ja tuovat julki yhteiskunnallisesti merkittävää tietoa ja epäkohtia (Kuutti 1995; Cancela ym. 2021). Usein he myös pyr-

https://doi.org/10.23983/mv.141474

kivät osoittamaan epäkohdista vastuussa olevia tahoja (Kuutti 1995; Cancela ym. 2021). Tutkiva journalismi toteuttaa voimallisesti journalismin demokraattista tehtävää yhteiskunnallisen vallankäytön valvojana ja kriittisenä tarkastelijana (Karadimitriou ym. 2022), mikä johtaa herkästi jännitteisiin ja konflikteihin poliittista ja taloudellista valtaa käyttävien tahojen kanssa (esim. Bennett ja Serrin 2005). Nykyisessä mediaympäristössä tätä tendenssiä voimistavat yhteiskunnan medioitumiseen liittyvät trendit, jotka ovat saaneet yhä suuremman osan yhteiskunnallisista toimijoista panostamaan aktiiviseen maineenhallintaan ja imagonrakennukseen (Hiltunen 2022). Näiden pyrkimysten ja kriittisen journalismin välillä vallitsee yhteensovittamaton jännite, joka heijastuu erilaisten vaikutusyritysten kautta journalistien työhön yhä useammin myös Suomessa (emt.).

Suomi sijoittuu muiden Pohjoismaiden kanssa kärkipäähän lehdistönvapautta ja journalistien turvallisuutta kartoittavissa vertailuissa (RSF 2023; Freedom House 2023). Tästä huolimatta esimerkiksi journalismista viholliskuvia luovan puhetavan yleistyminen (esim. HS 2023), häirintä- ja uhkailukampanjat (esim. PTY 2023), kokemukset kasvaneesta väkivallan uhasta, pelko ulkovaltojen vaikutus- ja painostuspyrkimyksistä sekä journalisteihin kohdistuneet oikeudenkäynnit (esim. SJL 2021) ovat herättäneet ammattikunnassa kasvavaa huolta. Lisäksi digitaalinen ympäristö on tuonut mukanaan esimerkiksi verkkovakoilun (esim. Halminen 2016) ja tietomurtojen (esim. Strömberg 2023) kaltaisia uusia uhkakuvia. Datajournalismin työkäytäntöjen yleistyminen on myös nostanut esiin erityiskysymyksiä liittyen esimerkiksi laajojen digitaalisten tietoaineistojen käsittelyyn, säilyttämiseen ja tietoturvaan (Uskali ja Kuutti 2016, 60, 170–172). Muutosten voi perustellusti ajatella vaikuttavan erityisesti tutkiviin journalisteihin, sillä he tyypillisesti harjoittavat pitkäjänteistä omaa tiedonhankinta- ja tutkimustyötä, käsittelevät ja analysoivat arkaluontoisia tietoja ja aineistoja sekä hyödyntävät laajasti nimettömiä lähteitä ja tietovuotoja (esim. Crete-Nishihata ym. 2020).

Edellä mainituista syistä on perusteltua selvittää, millaisia riskejä suomalaiset tutkivat journalistit näkevät työhönsä liittyvän ja miten he pyrkivät varautumaan näihin uhkiin ja torjumaan niitä. Lisäksi artikkelissa kartoitetaan, miten journalistit ovat oppineet itsensä ja tietojensa suojaamisessa käyttämiään turvakäytäntöjä sekä millaiset tekijät hankaloittavat näiden käytäntöjen soveltamista toimittajan työssä. Tutkimuksen tuloksia voidaan hyödyntää journalistien kouluttamisessa sekä tiedotusvälineissä tutkivan journalismin konkreettisten tukitoimien suunnittelussa.

Tutkimus on osa kansainvälistä hanketta, jossa aihetta tarkastellaan samanaikaisesti kolmessa Euroopan maassa: Suomessa, Virossa ja Tšekissä. Tämä tarjoaa mahdollisuuden riskinäkemysten ja turvakäytäntöjen vertailemiseen myös maiden välillä (ks. Urbániková ym. 2024). Tässä tutkimusartikkelissa analysoin tuloksia Suomen osalta. Analyysi perustuu 12 suomalaisen tutkivan journalistin teemahaastatteluihin sekä journalistien ennen haastattelua täyttämiin esitietolomakkeisiin.

Tutkiva journalismi, turvallisuus, tietoturva ja turvakäytännöt

Tutkiva journalismi on käsitteenä hankalasti määriteltävä, eikä sen sisällöstä vallitse yksimielisyyttä ammatinharjoittajien piirissä tai tutkimuskentällä (esim. Cancela ym. 2021, 880–882;

Kuutti 1995, 54–58). Kilpailevat määritelmät ovat painottaneet erilaisia tutkivan journalismin elementtejä ja lähtökohtia, kuten tavanomaisesta journalismista poikkeavaa epistemologiaa (Bjerknes 2022), asennetta ja menetelmiä (Kuutti 1995, 37), journalistien poikkeuksellista omaa aktiivisuutta ja motivaatiota (Cancela ym. 2021, 880), keskittymistä piilotettujen tai unohdettujen asioiden julkituomiseen (Hunter 2011, 8–12) tai tutkivan journalismin normatiivista roolia yhteiskunnallisen hyväksyttävyyden rajojen tuottamisessa ja ylläpitämisessä (Ettema ja Glasser 1998).

Suomalaista tutkivaa journalismia käsittelevässä väitöskirjassaan Heikki Kuutti (1995, 55–58) pitää tutkivan journalismin tunnusmerkkeinä sen perustumista toimituksen omaan tutkimustyöhön ja kohdistumista yhteiskunnallisesti merkittävään tietoon, joka on luonteeltaan salattua tai jollekin taholle kiusallista. Tuotetun tiedon yhteiskunnallisen merkittävyyden vaatimus toistuu useissa tutkivan journalismin määrittelyissä (ks. esim. Cancela 2021, 880–883). Tarkoituksena on erottaa tutkiva journalismi ”tirkistelyjournalismista”, jossa tutkimusten kohteena on esimerkiksi julkisuuden henkilöiden yksityiselämä (Kuutti 1995, 56). Toisaalta ajatusta tiedon salatusta tai kiusallisesta luonteesta tutkivan journalismin edellytyksenä on haastettu korostamalla, miten tärkeää roolia journalistiset tutkimukset ovat näytelleet vaiettujen tai sivuutettujen yhteiskunnallisten ongelmien esiin nostamisessa (Karadimitriou ym. 2022, 105). Datajournalismin puolella on puolestaan käyty keskustelua siitä, voiko toimittajien avoimesta datasta tai sen yhdistelmistä tekemiä uusia löydöksiä pitää tutkivana journalismina (Uskali ja Kuutti 2016, 142–148).

Tarkkarajaisen ja ulossulkevan määrittelyn sijaan voikin olla hedelmällisempää hahmottaa ”tutkivuus” eräänlaisena journalismin ominaisuutena ja jatkumona (Cancela ym. 2021; ks. myös Kuutti 1995, 56–58). Tällöin on mahdollista tarkastella, missä määrin tietty journalistinen juttu ja sen tuotantoprosessi sisältävät erilaisia tutkivaan journalismiin liitettyjä elementtejä ja millä tavoin ne toteuttavat tähän journalismin lajiin yhdistettyjä määreitä ja ihanteita (Cancela ym. 2021; Bjerknes 2022).

Suomessa tutkiva journalismi oli pitkään harvinaista, ja sitä harjoittivat yksittäiset, aiheesta kiinnostuneet toimittajat (Arolainen 2000, 114). Tutkiva suuntaus ja tutkivat toimitukset vakiintuivat osaksi suomalaista journalismia vasta 1990-luvulla, ja Tutkivan journalismin yhdistys perustettiin Suomeen vuonna 1992 (emt.). Erityisesti 2010-luvulta eteenpäin myös tutkivan datajournalismin muodot ovat saaneet jalansijaa suomalaisissa tiedotusvälineissä (Uskali ja Kuutti 2016, 70–77). Tutkivan journalismin pullonkaulana ovat kuitenkin toimitusten resurssit, ja tutkivan työn edellytysten onkin arvioitu heikentyneen Suomessa 2000-luvun aikana (Ala-Fossi ym. 2021, 188–189). Suomalaista tutkivaa journalismia ja sen työkäytäntöjä tutkittiin erityisen aktiivisesti vuosituhannen vaihteen tienoilla (esim. Kuutti 1995; 2001; 2003). Kuitenkin 2010-luvulta eteenpäin tutkivaa journalismia on käsitelty tutkimuksissa lähinnä opinnäytetasolla (esim. Kokkonen 2023; Laitinen 2017; Mustikainen 2014; Heino 2013), joskin tutkivaa datajournalismia on tarkasteltu osana laajempaa datajournalismitutkimusta (ks. Uskali ja Kuutti 2015; 2016).

Aikaisemmin kuvaamieni määrittelyvaikeuksien takia sovelsin tässä tutkimuksessa haastateltavien valintakriteereinä sekä omaa suomalaisen journalismin kentän tuntemustani että journalistien itsemäärittelyjä. Kaikki haastateltavat olivat journalisteja, joiden tutkija on katsonut harjoittavan tutkivaa journalismia ja jotka itse määrittelevät itsensä tutkiviksi toimittajiksi.

Jokaiselta haastateltavalta kysyttiin tutkivaksi toimittajaksi identifioitumisesta haastattelun aluksi. Haastateltavien joukko vastasi journalismin kentällä vallitsevaa ymmärrystä siitä, ketkä lasketaan tutkivan journalismin harjoittajiksi.

On kuitenkin syytä huomioida, että Suomessa vain erittäin rajallinen joukko journalisteja pystyy keskittymään yksinomaan tutkivaan journalismiin, ja he työskentelevät lähinnä suurimmissa tiedotusvälineissä (ks. Ala-Fossi ym. 2021, 188–189). Näkökulmien moninaisuuden takaamiseksi otin siis mukaan myös sellaisia työsuhteisia ja freelancer-toimittajia, jotka harjoittavat tutkivaa journalismia aiheiden ja mahdollisuuksien niin salliessa, mutta tekevät myös muun tyyppistä journalismia. Tällaiset toimittajat itse usein korostivat tutkivan asenteen ja menetelmien heijastuvan myös heidän muussa journalistisessa työssään.

Toimittajan *turvallisuuden* määrittelen suojaksi fyysiseltä väkivallalta ja häirinnältä sekä näiden uhkalta. Turvallisuus kattaa myös journalistin henkilökohtaisen ja työnantajan omaisuuden suojan vaurioittamiselta tai tuhoamiselta. Lisäksi se ulottuu journalistin työyhteisöön ja läheisiin. Näin ollen tutkimuksessa kartoitettavat turvallisuusriskit kattavat henkilökohtaisesti koetut uhkatilanteet, mutta myös esimerkiksi työyhteisöön, toimitiloihin sekä kotiin ja perheeseen kohdistuvat uhat.

Tietoturvalla tarkoitan viestinnän ja eri muodossa olevien tallennettujen tietojen yksityisyyttä ja koskemattomuutta (ks. Tsui ja Lee 2021). Määritelmä kattaa digitaalisessa muodossa olevat tiedot ja sähköisen viestinnän mutta myös fyysiset formaatit, kuten paperidokumentit ja käsin kirjoitetut muistiinpanot sekä tallennuslaitteet, kuten nauhurit ja kamerat. Lähtökohtaisesti kaikki tieto, joka ei ole vain muistinvaraista, on tallennettuna jonkinlaiseen fyysiseen tai digitaaliseen muotoon. Tietoturva kytkeytyy journalismin kontekstissa olennaisesti lähdesuojan takaamiseen. Lähdesuojasta ja oikeudesta anonyymiin ilmaisuun säädetään Suomessa sananvapauslaissa (Finlex 2023). Tavoitteena on varmistaa, että kansalaiset uskaltavat tuoda journalismin välityksellä yhteiskunnallisia epäkohtia julki ilman pelkoa negatiivisista sanktioista (ks. myös McGregor ym. 2016, 418).

Turvakäytännöt ovat toimia, välineitä tai toimintatapoja, joiden tarkoituksena on edistää journalistien turvallisuutta ja/tai tietoturvaa (ks. Crete-Nishihata ym. 2020). Nämä voivat olla proaktiivisia tai reaktiivisia ja sijoittua työprosessin eri vaiheisiin. Journalistit voivat esimerkiksi salata henkilötietonsa oma-aloitteisesti jo ennen riskialttiiksi arvioidun juttuprosessin aloittamista ja käydä kryptattua sähköpostiviestintää lähteiden kanssa prosessin aikana. Julkaisun jälkeen he voivat hävittää kaiken juttuun liittyvän aineiston reaktiona pyrkimyksiin selvittää siteerattuja nimettömiä lähteitä. Kaikkien näiden toimien, toimintatapojen ja välineiden tarkoitus on ehkäistä ja minimoida lähteisiin, journalistiseen prosessiin ja journalistiin itseensä kohdistuvia turvallisuus- ja tietoturvauhkia.

Suoranaisesti turvallisuuteen ja tietoturvaan kohdistuvien uhkatekijöiden lisäksi tarkastelen tässä artikkelissa myös muun tyyppisiä tutkivien journalistien työssään tunnistamia riskejä. Näistä näkyvimmin aineistossa korostuivat riski toimittajaan kohdistetuista oikeusjutuista ja/tai vahingonkorvausvaatimuksista sekä työn henkisestä kuormituksesta johtuva uupumisen riski.

Teoreettinen viitekehys: Mentaaliset mallit ja turvakulttuurit

Koska ajantasaista tutkimusta tutkivaan journalismiin liittyvistä riskeistä Suomessa tai muissa Pohjoismaissa on erittäin niukasti, lähtökohtani on empiirinen ja eksploratiivinen. Tutkimuksen teoreettisena viitekehyksenä toimivat *mentaaliset mallit* (Tsui ja Lee 2021; McGregor ja Watkins 2016) ja *turvakulttuurit* (Crete-Nishihata ym. 2020; Karlsson ym. 2015). Tämän tutkimuksen kontekstissa mentaaliset mallit ovat journalistien yksilöllisiä käsityksiä työhön liittyvistä riskeistä ja uhista, niiden merkityksestä ja todennäköisyydestä sekä turvakäytäntöjen tarpeesta (ks. Tsui ja Lee 2021). Nämä sisäistetyt mallit ohjaavat journalistien käyttäytymistä ja uhkiin varautumista siitä huolimatta, että ne eivät välttämättä ole täysin linjassa todellisuuden kanssa (McGregor ja Watkins 2016).

Mentaaliset mallit ovat keskeinen tekijä laajempien turvakulttuurien muotoutumisessa. Turvakulttuurin kaksi muuta elementtiä ovat jaetut turvallisuuteen liittyvät arvot ja yhteiset toimintamallit (Crete-Nishihata ym. 2020; Karlsson ym. 2015). Turvakulttuurit ovat luonteeltaan kollektiivisia ja muotoutuvat ja leviävät sosiaalisesti (emt.). Niillä on merkittävä ohjaava vaikutus turvakäytäntöjen soveltamiseen. Turvakulttuureita on yleensä tutkittu erilaisissa organisaatioissa, jossa niiden muotoutumiseen liittyy monien tekijöiden yhteisvaikutusta sekä eri professioiden keskinäistä neuvottelua ja kamppailua (Ramachandran ym. 2013; Crete-Nishihata ym. 2020, 1069, 1072; McGregor ym. 2016). Turvakulttuureita voidaan kuitenkin tarkastella myös saman profession harjoittajien keskuudessa, ja suorittaa vertailuja professioiden välillä (Ramachandran ym. 2013).

Aikaisemmat tutkimukset useissa eri maissa ovat tarkastelleet sekä journalistien tapaa arvioida riskejä ja uhkia että kartoittaneet tekijöitä ja mekanismeja, jotka vaikuttavat turvakäytäntöjen omaksumiseen ja käyttöönottoon journalismissa. Masashi Crete-Nishihata, Joshua Oliver, Christopher Parsons, Dawn Walker, Lokman Tsui ja Ronald Deibert (2020, 1078–1080) erottavat neljä ulottuvuutta, joiden kautta he erittelevät journalistien työssään kohtaamia uhkia. Ensimmäinen on uhan tyyppi, eli onko kyseessä esimerkiksi fyysisen väkivallan vai luottamuksellisten tietojen vuotamisen uhka. Toisen ulottuvuuden muodostaa se, onko kysymys realisoituneesta vai vasta potentiaalisesta uhasta. Kolmas ulottuvuus on se, mihin tai kehen uhka kohdistuu: journalistiin itseensä, koko tiedotusvälineeseen vai esimerkiksi lähteeseen. Neljän ulottuvuus koskee uhan aiheuttajaa, eli sitä onko kyse esimerkiksi yksityishenkilöstä, yrityksestä, viranomaisesta tai tiedustelupalvelusta.

Susan McGregor ja Elizabeth Watkins (2016) sekä Crete-Nishihata kollegoineen (2020) havaitsivat, että journalistit tekivät päätöksiä tietoturvaan liittyvien turvakäytäntöjen tarpeellisuudesta sen perusteella, arvioivatko he käsitellyn aiheen ”arkaluontoiseksi”. Erityisen tietoturvasta huolehtimisen ajateltiin kuuluvan lähinnä niihin tapauksiin, joissa työ oli omiaan herättämään vaikutusvaltaisten tahojen, kuten valtiollisten toimijoiden, mielenkiinnon. Journalistit eivät useinkaan kokeneet tietoturvakysymyksiä tai aineiston suojaamista merkityksellisiksi, mikäli kyse ei ollut heidän arvionsa mukaan erityisen ”arkaluontoisista” aineistoista tai lähteistä.

Jennifer Henrichsen (2022) havaitsi, että yhdysvaltalaisissa tiedotusvälineissä digitaalisten turvakäytäntöjen omaksumista jarruttaa kolme keskeistä tekijää: turvallisuuden ja tietoturvan hahmottaminen yksilöllisenä ongelmana kollektiivisen vastuun sijaan, johdon ja päätöksen-

tekijöiden vastahankaisuus muutosten tekemiseen sekä kokemukset siitä, että turvakäytännöt hidastavat ja vaikeuttavat journalistisen työn tekemistä. Organisaatiotasolla muutoksia ajavat systemaattisen suunnittelun sijaan useimmiten turvallisuusteemasta kiinnostuneet ja uhkiin vakavasti suhtautuvat yksilöt, jotka levittävät tietoisuutta ja osaamista eteenpäin organisaatiossa sekä toimivat välittäjinä esimerkiksi IT-osaston, ylemmän johdon ja journalistien välillä tietoturva-asioissa (emt., 1838–1841). Työnkuvansa takia tutkivat journalistit saattoivat usein toimia tällaisessa roolissa (emt., 1839). Toisaalta lisääntyvät tekniset osaamisvaatimukset saattoivat johtaa siihen, että tietoturvaan liittyvät asiat ”ulkoistettiin” yhä suuremmalta osin IT-ammattilaisille, eikä niiden osaamisen nähty olevan keskeistä journalisteille itselleen (emt., 1837).

Susan McGregor, Polina Charters, Tobin Holliday ja Franziska Roesner (2015) havaitsivat useita selittäviä tekijöitä sille, miksi digitaalista tietoturvaa lisäävät käytännöt ja ohjelmistot eivät päädy journalistien päivittäiseen käyttöön. Ne voidaan esimerkiksi kokea liian monimutkaiseksi tai niiden nähdään hidastavan työprosesseja sekä hankaloittavan erityisesti kanssakäymistä lähteiden kanssa (emt., 408–409). Lisäksi riittämätön koulutus tai vaikeudet saada teknistä tukea omasta organisaatiosta voivat rajoittaa näiden käyttöönottoa (emt., 408). Yleisin syy käyttämättömyyteen kuitenkin oli, ettei niitä mielletty tarpeellisiksi oman riskiarvion perusteella, eli omaa työtä ei pidetty erityisen ”arkaluontoisena” (ks. myös McGregor ja Watson 2016; Crete-Nishihata ym. 2020, 1077–1078).

Tämän artikkelin tulokset havainnollistavat, millaisia yhtäläisyyksiä ja eroja tutkivan journalismin riskeihin liittyvissä mentaalisissa malleissa voidaan havaita haastateltujen journalistien välillä ja miten nämä riskimallit sekä käsitykset turvakäytäntöjen hyödyllisyydestä näkyvät journalistien toiminnassa. Hyödynnän turvakulttuureihin tukeutuvia selitysmalleja tarkastellessani sitä, millaisia haasteita ja ongelmia tutkivat journalistit ovat kohdanneet turvakäytäntöjen soveltamisessa sekä sitä, miten journalistit ovat oppineet ja omaksuneet turvakäytäntöjä. Arvioin myös, hahmottuuko tutkimusaineistosta suomalaisen tutkivan journalismin profession sisäistä, jaettua turvakulttuuria.

Aineisto ja menetelmä

Tässä artikkelissa vastataan seuraaviin tutkimuskysymyksiin:

1. Millaisia turvallisuus- ja tietoturvariskejä sekä muita riskitekijöitä suomalaiset tutkivat journalistit näkevät työhönsä liittyvän?

2. Miten suomalaiset tutkivat journalistit pyrkivät työssään huomiomaan ja ehkäisemään turvallisuus- ja tietoturvariskejä?

3. Mitä kautta suomalaiset tutkivat journalistit ovat saaneet tietoa ja oppia turvakäytännöistä, ja millaisia haasteita he ovat kohdanneet turvakäytäntöjen käyttöönotossa ja soveltamisessa?

Tutkimukseen osallistuneet 12 suomalaista tutkivaa journalistia valikoitiin kriittisten tapausten otannalla eli valitsemalla perusjoukosta osallistujia, jotka todennäköisimmin pystyvät tarjoamaan tutkimusaiheen näkökulmasta käyttökelpoista tietoa (Patton 1990, 174–176). Moninaisten näkökulmien tavoittamiseksi otoksen koostumuksessa huomioitiin myös edustavuus, joten siihen pyrittiin valitsemaan eri-ikäisiä ja eri sukupuolia edustavia journalisteja, jotka työskentelevät erilaisissa tiedotusvälineissä, erilaisissa työsuhteissa ja erikoistuivat eri aihealueisiin.

Koska tutkimuksessa paljastuu yksityiskohtia journalistien ja näiden työnantajien turvallisuus- ja tietoturvajärjestelyistä, osallistujille luvattiin anonymiteetti. Tästä syystä taustatietoja tarjotaan artikkelissa vain rajoitetusti, suoria haastattelulainauksia on muutettu yleiskielisemmäksi ja osaa tiedoista on hämärretty tunnistamisen ehkäisemiseksi. Otin potentiaalisiin osallistujiin yhteyttä sähköpostitse. Ennen osallistumispäätöstä osanottajat saivat nähtäväkseen tietosuojailmoituksen ja suostumuslomakkeen tietoisen suostumuksen varmistamiseksi.

Osanottajien keski-ikä oli 44 vuotta, ja yhtä lukuun ottamatta kaikki osallistujat työskentelivät tavoittavuudeltaan valtakunnallisessa mediassa. Osallistujajoukosta 10 työskenteli toimittajana ja kaksi muunlaisissa työtehtävissä. Haastatelluista journalisteista valtaosa (9) oli vakituisessa työsuhteessa ja kolme harjoitti journalismia freelancereina tai vapaata toimittajuutta ja määräaikaisia työsuhteita yhdistäen. Kaikilla osanottajilla oli yliopisto- tai ammattikorkeakoulututkinto, ja seitsemän oli opiskellut pääaineenaan journalismia tai viestintää. Taulukko 1 havainnollistaa osanottajajoukon keskeisiä ominaisuuksia:

Taulukko 1. Osallistujajoukon keskeiset ominaisuudet (n=12)

Sukupuoli	n	Pääasiallinen työnantaja	n	Kokemus alalta	n
Nainen	6	Sanomalehti	5	Yli 15 vuotta	5
Mies	6	Yleisradio	3	11–15 vuotta	4
		Aikakauslehti	3	6–10 vuotta	3
		Itsenäinen verkkolehti tai -sivusto	1		

Tutkimuksen teemahaastattelut tehtiin 5.5.–9.6.2023, ja niiden keskipituus oli 59 minuuttia. Haastatteluista kahdeksan tehtiin kasvokkain ja neljä videoyhteyden välityksellä. Haastattelut nauhoitettiin ja litteroitiin sanatarkasti. Ennen teemahaastattelua osallistujia pyydettiin täyttämään sähköinen esitietolomake (liite 1), jolla kerättiin osallistujan perustiedot ja kartoitettiin turvakäytäntöjen tuntemusta sekä niiden soveltamista työn osana.

Teemahaastattelurunko (liite 2) keskittyi kolmeen teemaan: kokemuksiin ja näkemyksiin tutkivaan journalismiin liittyvistä riskeistä, työssä sovellettuihin turvakäytäntöihin ja niihin vaikuttaviin tekijöihin sekä turvakäytäntöjen oppimiseen ja omaksumiseen. Lisäksi haastatteluissa hyödynnettiin vastaajakohtaisesti esitietolomakkeen tuottamaa tietoa. Näin oli mahdollista kartoittaa, millaisissa tilanteissa osallistujat olivat soveltaneet tiettyjä turvakäytäntöjä ja miten he perustelivat niiden tarpeellisuutta tai tarpeettomuutta erilaisissa tapauksissa. Osal-

listujille tarjottiin myös mahdollisuus olla tutkijaan yhteydessä jälkikäteen ja tehdä lisäyksiä tai täsmennyksiä haastatteluihinsa.

Aineiston analyysimenetelmänä käytin laadullista sisällönanalyysiä ja induktiivista sovellettua teema-analyysiä (Guest ym. 2012). Analysoin aineiston tietokoneavusteisesti ATLAS.ti 23 -ohjelmalla käyttäen kahta erilaista koodausstrategiaa. Ensimmäisellä kierroksella harjoitin rakennekoodausta, jota ohjasivat esittämäni tutkimuskysymykset (Saldaña 2013, 84–87). Esimerkiksi tarkastellessani toimittajien näkemyksiä työhön liittyvistä riskeistä koodasin tällä koodilla kaikki haastattelujen osat, joissa käsiteltiin erilaisia riskitekijöitä. Myöhemmässä vaiheessa tuotin kategorioiden sisälle induktiivisesti hierarkkisen alakoodirakenteen. Esimerkiksi riskitekijöiden osalta erotin alakoodeilla ”tietoturvariskit”, ”turvallisuusriskit” ja ”muut riskit”, ja tietoturvariskien alakategoriana ”digitaaliset” ja ”analogiset” tietoturvariskit jne. Rakennekoodaus toimii aineiston esikäsittelynä ja luettelointina, mikä mahdollistaa empiirisiin tutkimuskysymyksiin vastaamisen sekä luo pohjan tarkempien laadullisten analyysien tekemiselle (Namey ym. 2008, 141).

Toisella koodauskierroksella sovelsin temaattista koodaus- ja analyysistrategiaa (Saldaña 2013, 209–213), jossa pyrin yhtäläisyyksien, erojen ja ristiriitaisuuksien analyysin avulla tunnistamaan aineistosta laajempia rakenteita ja teemoja (Guest ym. 2012). Tarkastelin esimerkiksi sitä, millaisia yhtäläisyyksiä ja eroja riskinäkemyksissä ilmeni sekä sitä, millaisia selityksiä ja perusteluja journalistit itse antoivat näkemyksilleen ja toiminnalleen. Tätä kautta oli mahdollista päästä kiinni riskeihin ja turvakäytäntöihin liittyviin mentaalisiin malleihin ja analysoida niiden yhtymäkohtia ja eroavaisuuksia koko osallistujajoukon tasolla. Kuvaan seuraavissa tulosluvuissa näistä elementeistä syntyvää kokonaiskuvaa ja vastaan esittämiini tutkimuskysymyksiin.

Lähteiden suojelu journalistien ensisijaisena huolena

Ensimmäinen tutkimuskysymykseni koski riskeihin liittyviä mentaalisia malleja eli sitä, millaisia turvallisuusuhkia, tietoturvauhkia ja muun tyyppisiä uhkia suomalaiset tutkivat journalistit näkivät työhönsä kohdistuvan. Tulokset osoittavat, että suomalaisten tutkivien journalistien uhka-arvioissa korostuu riski luottamuksellisten lähteiden paljastumisesta. Journalisteihin itseensä kohdistuvat turvallisuusuhat koettiin harvinaisiksi, joten lähteiden paljastuminen kohosi haastateltujen keskuudessa tyypillisesti ensisijaiseksi huoleksi (ks. myös McGregor ym. 2016, 423). Tämä korostaa myös lähteiden luottamuksen ja anonymiteetin säilyttämisen keskeistä merkitystä tutkivan journalismin harjoittamisessa (Kuutti 1995, 120–123). Toisaalta erilaisten tietoturva- ja turvallisuusriskien koettiin lisääntyneen nykyisessä viestintäympäristössä, minkä osaltaan nähtiin kasvattavan myös tutkivan työn kuormitukseen liittyvää uupumisen riskiä. Tarkastelen seuraavaksi journalistien riskinäkemyksiä ja niiden keskeisiä yhtäläisyyksiä ja eroja riskityyppi kerrallaan, aloittaen turvallisuusuhista ja edeten siitä tietoturvauhkien kautta muihin uhkatyyppeihin.

Haastatellut kokivat, ettei tutkivan journalismin harjoittamiseen Suomessa liity tyypillisesti merkittäviä fyysisiä uhkia. Vertailukohdaksi haastateltavat nostivat usein valtioita, joissa tutkivat toimittajat joutuvat jatkuvasti huomioimaan esimerkiksi väkivallan ja vangitsemisen uhan.

Näihin verrattuna työn Suomessa koettiin olevan hyvin turvallista. Poikkeuksen muodostivat tapaukset, joissa tutkivan työn nimenomaisena kohteena olivat rikolliset, järjestäytynyt rikollisuus, terrorismi ja/tai ääriliikkeet. Tällaisissa tapauksissa yksittäisen toimittajaan kohdistuvaa fyysistä uhkaa pidettiin mahdollisena, ja se pyrittiin yleensä huomioimaan jo ennakolta juttuja suunnitellessa.

Toiseksi erityisuhaksi koettiin tilanteet, joissa jotkin toimijat pyrkivät tarkoituksellisesti lietsomaan toimittajaan kohdistuvaa häirintää ja uhkaa sekä osallistamaan muita henkilöitä näihin kampanjoihin. Tällaiset tilanteet sijoittuivat tyypillisesti verkkoympäristöön, ja niihin yhdistyi usein myös pyrkimys mustamaalaamiseen ja henkilökohtaisten tietojen julkiseen levittämiseen (ks. myös Hiltunen 2022, 128–30). Vaikka nämä kampanjat olivat haastateltavien mukaan pysyneet sanallisella ja/tai lievän häirinnän tasolla, he näkivät toiminnan johtavan pahimmillaan potentiaalisiin fyysisiin uhkiin, kuten yksi haastateltava kuvasi:

> Näitä kuvia ja yhteystietoja se tykitti sinne [– –] ja samalla kirjoitti kaikkia viestejä, jossa mustamaalasi ja haukku mua ja yllytti ihmisiä hyökkäämään mun kimppuun ja käyttämään niitä yhteystietoja kaikin mahdollisin keinoin mun piinaamiseen [– –] Se oli kyllä karmeaa aikaa. (H2)

Lisäksi osa haastatelluista koki journalistien ammattikuntaan kohdistuvien fyysisten riskitekijöiden yleisesti kasvaneen yhteiskunnallisen polarisaation ja lisääntyneen julkisen vihamielisyyden takia. Tämän nähtiin kasvattavan erityisesti impulsiivisen väkivallan uhkaa (ks. myös Hiltunen 2022, 110, 131–135). Vaikka riski ei kytkeytynytkään erityisesti tutkivan journalismin harjoittamiseen, ammattikunnan näkyvinä edustajina tutkivat toimittajat olivat kehityssuunnasta huolissaan, kuten käy ilmi alla olevasta lainauksesta:

> [– –] ehkä tää että miten toimittajiin viime vuosina ollaan myös Suomessa käyty fyysisesti kiinni erilaisissa esimerkiksi mielenosoituksissa. [– –] se kynnys tulee koko ajan mun mielestä matalammaksi [– –] Ja varsinkin kun on yhteiskunnallinen ilmapiiri, missä medioita tai toimittajia vastaan lietsotaan, niin kyllähän se avaa kaikenlaisia mahdollisuuksia [– –] (H4)

Koska haastatellut journalistit kuitenkin pitivät Suomen tilannetta yleisesti turvallisena, he kertoivat tyypillisesti uskaltavansa tavata uusia ja tuntemattomia lähteitä verrattain vapaasti ja harjoittaa tiedonhankintaa ilman erityisiä turvallisuushuolia. Vain yksi haastateltu ilmoitti joutuneensa Suomessa potentiaalisesti uhkaavaan tilanteeseen uransa aikana tiedonhankinnan ja haastateltavien tapaamisen yhteydessä.

Tietoturvariskeistä journalistit nostivat uhkatekijöinä esiin *tietomurrot ja haittaohjelmat*, *digitaaliset jäljet*, *laitteisiin liittyvät riskit* sekä *henkilöriskit*. Haastateltujen journalistien mukaan digitaalisiin tietoturvauhkiin oli toden teolla herätty useimmissa mediataloissa vasta viimeisen reilun kymmenen vuoden aikana. Muutoksen taustalla nähtiin useita tekijöitä. Julkisuudessa näkyvästi esillä olleet tietomurrot sekä tietojenkalastelu- ja verkkohyökkäykset ovat lisänneet tietoisuutta riskien vakavuudesta. EU:n yleinen tietosuoja-asetus on tuonut uusia velvollisuuksia kaikille dataa säilyttäville ja käyttäville toimijoille ja pakottanut ne kiinnittämään huomiota

tietojen suojaamiseen. *Helsingin Sanomien* Viestikoekeskus-uutisointia seuranneet tapahtumat osoittivat, että myös Suomen viranomaiset ovat valmiita takavarikoimaan ja tutkimaan journalistien työvälineitä päästäkseen tietovuotajien jäljille. Viimeisimpänä Venäjän hyökkäyssodan Ukrainaan ja kiristyneen kansainvälisen tilanteen koettiin lisänneen tietomurtoihin, tiedusteluun ja vakoiluun liittyviä uhkakuvia.

Haastateltavat nostivat esiin myös huolen siitä, miten toimituksissa tapahtuneet muutokset lisäävät potentiaalisia haavoittuvuuksia. Verkottuneiden tietojärjestelmien, kuten sisäverkkojen ja sähköisten toimitusjärjestelmien myötä hyökkääjälle voi riittää, että yksi käyttäjistä erehtyy antamaan tunnuksensa kalasteluhyökkäyksessä tai asentamaan haittaohjelman verkossa olevalle laitteelleen. Tämä muuttaa tietoturvan luonnetta kollektiivisempaan suuntaan (ks. myös Henrichsen 2022, 1833–84). Vaikka itse toimisi huolellisesti, muiden käyttäjien toiminta saattaa vaarantaa myös oman tietoturvan (emt.).

Digitaaliset ympäristöt ja sähköinen viestintä aiheuttavat uudentyyppisiä riskejä myös yhteydenpitoon lähteiden kanssa. Lähes jokainen sähköinen viestinnän tapa jättää jälkeensä digitaalisia jälkiä, joiden avulla voidaan pyrkiä selvittämään viestinnän sisältöä tai tietoja siitä, keihin ja milloin henkilö on ollut yhteydessä. Myös tietojen ottaminen ulos järjestelmistä saattaa jättää merkinnän digitaaliseen rekisteriin, tai dokumentteihin voi tulostua niiden vuotajan paljastavia tietoja. Juttujen kohteet, kuten viranomaiset, yritykset ja organisaatiot voivat koettaa selvittää journalisteille tietoja antaneita henkilöitä näiden jälkien avulla. Näin yksi haastateltava valotti sähköiseen viestintään liittyviä riskejä:

> Mä tiedän, että [– –] munkin juttujeni lähteitä yritetty [jutun kohteena olleessa organisaatiossa] sisäisesti selvittää, sähköpostien metatietoja ja muita, ihan sähköpostien sisältöjäkin varmaan tutkimalla. (H3)

Selkeä ero riskitekijöihin liittyvissä mentaalisissa malleissa näkyi siinä, pitivätkö journalistit mahdollisena, että kotimaiset tai ulkomaiset viranomaiset ja/tai tiedustelupalvelut pyrkisivät seuraamaan heidän viestintäänsä tai urkkimaan heidän digitaalisessa muodossa olevia tietojaan. Osa piti tätä realistisena ja uskoi että erilaisilla turvakäytännöillä voidaan lähinnä hankaloittaa tai hidastaa valtiollisten toimijoiden pyrkimyksiä, muttei lopulta estää niitä kokonaan (ks. myös Bradshaw 2017, 344). Toiset taas ajattelivat, että journalisteja seurataan enemmän julkaistujen juttujen ja muiden avointen lähteiden avulla eikä urkinta varsinaisesti ulotu journalistien tietoihin tai yhteydenpitoon.

Työvälineisiin liitetyt *laiteriskit* jakautuvat kolmeen erilliseen uhkakuvaan: vakoiluun laitteen kautta, laitteen joutumiseen tutkinnan kohteeksi ja laitteen varastamiseen tai hukkaamiseen. Erityisen riskialttiiksi työvälineeksi haastatellut journalistit arvioivat matkapuhelimen. Tyypillisesti se on aina mukana, sisältää pääsyn sähköpostiin, pikaviestimiin sekä muihin sovelluksiin, ja sitä käytetään usein yhteydenpitoon lähteiden kanssa. Matkapuhelinta pidettiin erityisen alttiina kaikille kolmelle yllä mainituille laiteriskille. Yksi haastatelluista kuvasi matkapuhelimeen liittyviä riskejä ulkomailla tapahtuneen esimerkin kautta:

> Me ollaan koko ajan tehty duunii sillä ajatuksella, että tää [matkapuhelin] on turvallinen viestintäväline. Mutta [– –] Meksikossa oli [– –] satoja toimittajia ja ihmisoikeusjuristeja joiden kännykässä oli Pegasus-virusohjelma. Ne oli kaapannu ne. Kyllä se huolestuttaa tosi paljon. Jos me ajatellaan, et miten paljon sovelluksia me nyt käytetään muutenkin puhelimessa, et siinä on koko elämä. Silloinhan jos semmonen tapahtuu, niin sillon ei edes ne tavallisesti turvalliset tavat enää toimi. (H1)

Toisen potentiaalisen laiteriskin muodostivat aineiston perusteella nauhureiden kaltaiset tallennuslaitteet, jotka eivät useinkaan teknisesti mahdollista tallennusten suojaamista tai kryptaamista. Näin ollen laitteen takavarikoiminen tai varastaminen tietäisi suoraa pääsyä siihen tallennettuun materiaaliin.

Myös tilanteissa, joissa tietoturvasta on huolehdittu teknisellä tasolla, jäljelle jäävät edelleen *henkilöriskit*. Huolimattomuus tai tahallisen toiminta saattoivat vaarantaa luottamukselliset tiedot. Haastatellut tutkivat journalistit näkivät huolellisuuden ja lähdesuojan ylläpitämisen äärimmäisen velvoittavina turvallisuuteen liittyvinä vaatimuksina ja kokivat toisinaan paineita siitä, olivatko he varmasti tehneet riittäviä toimia lähteidensä suojelemiseksi. Tästä syystä osallistujat ilmaisivat turhautumistaan tapauksissa, joissa kokivat, etteivät muut organisaation jäsenet noudattaneet samanlaista huolellisuutta ja ottaneet tätä velvollisuutta riittävän vakavasti. Nämä tilanteet nostivat siis pintaan koettuja eroja organisaatioiden eri osien välisissä turvakulttuureissa, kuten alla olevassa lainauksessa, joka havainnollistaa toimittajan ja ylempään johtoon kuuluvan henkilön eriäviä toimintatapoja ja suhtautumista lähteiden anonymiteettiin:

> [– –] silleen räikeitä tapauksia että [– –] vaikka pomoportaassa oleva tyyppi, toimittaja on sille uskoutunut jostakin että tällainen lähde mulla on, niin sitten se saattaa puhuu siitä avoimesti toimituksen käytävällä ja ei pidä sitä salaisuutta, mikä taas on sille toimittajalle ihan kauhea tilanne. Että täällä nämä kaikki kollegatkin kuulee, ja et se voi olla jonkun jutun kohdalla jo aivan liian paljon että edes toimituksen toiset jäsenet tietää mitään. [– –] Olen kuullut sellaisia asioita ja itse todistanut sellaisia tilanteita [– –] ehkä vähän olisi aiheen pelotella ihmisiä siitä, että ihmisillä on oikeasti paljon pelissä silloin kun ne luottaa teihin ja teidän instituutioonne. (H6)

Vielä huolimattomuutta tai ajattelemattomuutta vaikeammaksi hallittavaksi koettiin riski siitä, että toimitusorganisaatioon kuuluvat henkilöt vuotaisivat luottamuksellista tietoa tahallisesti ulospäin. Nykyisen toimitusympäristön, jossa esimerkiksi muistiinpanot, sisäinen viestintä ja toimitusjärjestelmässä olevat keskeneräiset jutut saattavat olla sisäisesti näkyvissä suurelle joukolle ihmisiä, koettiin lisäävän tähän liittyviä uhkakuvia. Organisaation sisäinen luottamus nähtiin siis erittäin merkittäväksi tekijäksi tutkivan journalismin tietoturvan ja lähdesuojan näkökulmasta.

Henkilöriskit ulottuvat välillisesti myös lähteiden toimintaan. Vaikka journalisti olisi huolehtinut teknisestä suojaamisesta ja tietojen alkuperän hämärtämisestä, lähteet saattoivat omalla toiminnallaan paljastaa itsensä. Journalistit kokivat lähteiden suojaamisen kuuluvan periaatteellisella tasolla heidän vastuulleen, mutta pystyivät vaikuttamaan lähteiden omaan toimintaan käytännössä vain rajoitetusti, kuten yksi haastateltavista alla kuvaa:

> Vaikka sä itse noudattaisit tiukkaa protokollaa miten sä toimit, niin sun lähteet ei välttämättä toimikaan samalla tavalla. [– –] sikäli se voi mennä omaan piikkiin, että olen joskus kokenut, että en ole ehkä tarpeeksi osannut ohjeistaa itse sitä lähdettä, riittävällä tavalla. Vaikka olisin ohjeistanut, mutta en ole välttämättä riittävän painokkaasti osannut tuoda sitä esille. [– –] Toki aina toisen ihmisen toimintaan ei pysty vaikuttamaan, se on rajallista. (H12)

Journalisteihin kohdistuvat *oikeusuhat ja vahingonkorvausvaatimukset* muodostivat työhön ylimääräisen uhka- ja kuormitustekijän. Oikeusprosesseihin joutuminen vei aikaa ja resursseja muulta työltä. Muutama haastatelluista koki, että poliisin into tutkia journalistien työstä tehtyjä rikosilmoituksia oli kasvanut myös niissä tapauksissa, joissa on päällisin puoli selvää, ettei ilmoitukselle ole todellisia perusteita. Oikeusuhat ovat erityisen hankalia freelancereiden näkökulmasta. Jos työnantajat eivät osallistu prosessin aiheuttamiin kuluihin tai korvaa niihin kuluvaa aikaa, freelancer on pitkälti omillaan. Suurimman ongelman muodosti kuitenkin prosessien hitaus. Käynnissä olevat oikeusprosessit koettiin aina jossain määrin kuluttaviksi, ja pahimmillaan ne venyivät useiden vuosien mittaisiksi, kuten haastateltava alla kuvaa:

> Oma tuntumani on, että poliisi lähtee helpommin tutkimaan rikosilmoituksia jotka on tehty toimittajista tai niiden lähteistä. [– –] nimettömät lähteet kertovat kokemuksistaan ja poliisi on raahannut niitä kuulusteluun. Kyllä se on kylmä suihku sille lähdesuojalle. [– –] Ja sitten juttujen tutkinta on kestänyt [– –], mikä on tosi kuormittavaa ja raskasta toimittajille. [– –] Onhan se ihan hyvä, et kaikki hoidetaan prosessina niin kuin pitäisi. Mutta prosessit on vaan niin perseellään, kun resursseja ei poliisilla ole. Sitten joku perustutkinta kestää kaksi vuotta. (H3)

Yleisimmäksi uhkatekijäksi nähtiin kuitenkin työn aiheuttama henkinen kuormitus ja siitä johtuva *uupumisen riski*. Haastatellut pitivät tutkivan journalismin erityispiirteenä, että sitä harjoittaessa päädytään usein jännitteiseen suhteeseen sekä konflikteihin juttujen lähteiden ja kohteiden kanssa. Tutkivassa journalismissa hyödynnetään tyypillisesti myös lähdesuojaa ja luottamuksellisia tai salassa pidettäviä tietoja muita journalismin lajeja useammin, ja projektit saattavat kestää pitkään sekä olla työmäärältään valtavan suuria. Kaikkien näiden tekijöiden katsottiin lisäävän työn kuormittavuutta. Haastattelukatkelma alla havainnollistaa tätä:

> En itsekään ole ollut huolestunut omasta fyysisestä turvallisuudesta. [– –] ne isoimmat riskit kohdistuukin siihen henkiseen turvallisuuteen [– –] että miten kestää sen työn tuomat rasitukset omassa elämässään. Koska nämä toimitukselliset projektit on usein sellaisia, että ei niitä oikein voi jättää sinne työpaikalle, vaan kyllä ne seuraa mielessä myös kotiin. Että miten se toimittajan henkinen kantti pysyy [– –] että miten pystytään huolehtimaan omista henkisistä resursseista niissä ristipaineissa, joita tutkivan journalismin projekteissakin tulee. (H7)

Tähän liittyen uutena huolenaiheena nykyisessä viestintäympäristössä esiin nostettiin myös journalisteihin kohdistuvat julkiset häirintä- ja mustamaalauskampanjat, joita juttujen kohteet ja/tai erilaiset intressiryhmät pyrkivät tietoisesti käynnistämään ja lietsomaan. Osa haastatelluista journalisteista koki pelkästään uhan näiden kohteeksi joutumisesta aiheuttavan jänni-

tettä tiettyjen aihepiirien ja henkilöiden käsittelyyn, ja niitä kokeneet kuvailivat kampanjoiden tuottavan työhön ylimääräistä henkistä kuormitusta. Tällaisten kampanjoiden eskaloituminen saattaa johtaa myös fyysisiin turvallisuusuhkiin (Holton ym. 2023, 865–866).

Tutkivassa työssä saatettiin myös kohdata myös raskaita aiheita ja kohtaloita sekä järkyttävää materiaalia. Osa haastelluista koki, että henkiseen jaksamiseen liittyvien riskien tiedostaminen ja käsittely on alalla monella tavoin lapsen kengissä. Esimerkiksi avointa keskustelua työn tunnepuoleen kohdistamista vaatimuksista tai ”debriefing”-kulttuuria pidettiin varsin harvinaisina, ja tähän toivottiin laajempaa kulttuurista muutosta. Haastattelulainaus alla havainnollistaa näitä toiveita:

> [– –] toimittajan tunnetyö, tunteiden käsittely, stressin tason käsittely, se on ehkä sellainen asia, mitä suomalaisessa työkulttuurissa yleensäkään ei ole riittävästi mietitty. [– –] tutkivista toimittajista on sellainen aika vanhanaikainen käsitys, että pitäisi olla kova luu ja pitäisi kestää kaikki, mutta eihän se todellakaan niin mene. Et pitäisi olla paljon parempia puhumaan auki asiat, jotka tuntuu ikäviltä. Et saattaa olla tosi traagisia tarinoita, kohtaloita mitkä koskettaa syvästi, tai just sitä et miltä tuntuu, jos joku soittaa sulle keskellä yötä ja huutaa, että ootpas sä huora. Niin kuin tällaisia asioita, et siihen meidän pitäisi olla paljon avoimempia ja myös parempia puhumaan siitä, et miten se vaikuttaa. (H8)

Yksilöllinen harkinta korostuu turvakäytännöissä

Toinen tutkimuskysymykseni tarkastelee sitä, miten tutkivat journalistit pyrkivät työssään huomiomaan erilaiset riskitekijät ja varautumaan niihin. Tulokset osoittavat, että tutkivat journalistit käyttävät itse merkittävää harkintavaltaa turvakäytäntöjen suhteen. Vain harvoilla työantajilla oli turvallisuuteen tai tietoturvaan liittyviä yhteisiä ohjeistuksia tai linjauksia, ja nekin keskittyivät yleensä esimerkiksi perustietoturvaan tai muihin yleisempiin asioihin. Laaja yksilöllinen harkintavalta heijastaa journalistien suurta autonomiaa omien työkäytäntöjensä suhteen moniin muihin ammattikuntiin verrattuna (ks. myös McGregor ym. 2016, 429; Crete-Nishihata ym. 2020, 1072). Tutkivien journalistien yksilölliset mentaaliset mallit riskeistä ja näkemykset erilaisten turvakäytäntöjen tarpeellisuudesta ja tehokkuudesta ovat siis avainasemassa, kun halutaan ymmärtää turvakäytäntöjen hyödyntämistä. Oma merkityksensä on myös organisaatioiden turvakulttuureilla sekä niiden turvallisuudelle ja turvakäytännöille antamalla painoarvolla.

Fyysisten uhkien vähäinen rooli journalistien riskikäsityksissä näkyy siinä, että turvallisuuden takaamiseen tähtäävät toimet olivat harvinaisia. Yhdelläkään haastatellulla ei ollut käytössä esimerkiksi kotihälytysjärjestelmää, kannettavaa hälytyspainiketta tai itsepuolustusvälineitä. Yksi osallistujista ilmoitti vaihtelevansa säännöllisesti käyttämiään kulkureittejä turvallisuussyistä ja vieneensä häneen kohdistuneen uhkauksen viranomaisten tietoon. Pääosin tutkimukseen haastatellut journalistit kokivat, että heillä ei työnkuvansa takia ollut tarvetta fyysisille turvakäytännöille ja että niiden antama potentiaalinen turvallisuushyöty olisi marginaalista verrattuna niistä aiheutuvaan käytännön vaivaan. Nekin harvat, joilla fyysisiä turvakäytäntöjä oli aktiivikäytössä, eivät perustelleet niitä akuutilla tarpeella vaan lähinnä korostivat käytäntöjen luonnetta varotoimina ja turvallisuudentunteen tuojina, kuten lainaus alla kuvaa:

> [– –] ne on varotoimia ja ne on myös omaa henkistä turvallisuutta, eli kun tietää, että ne on käytössä, niin kokee olonsa turvatummaksi kuin silloin, jos ne ei ole käytössä. Vaikka ne ei tulisi koskaan käyttöön konkreettisesti, ne kuitenkin voi tuoda tiettyä mielenrauhaa. (H5)

Haastateltavat kertoivat vain harvoin tekevänsä riskiarvioita fyysisistä tapaamisista uusien lähteiden kanssa, ja silloinkin kun niitä tehtiin, ne olivat luonteeltaan ylimalkaisia. Tiedonhankinnassa erilaisia fyysisiä turvakäytäntöjä otettiin käyttöön ainoastaan erittäin harvinaisissa poikkeustapauksissa, ja silloinkin suojaustoimet olivat verrattain kevyitä. Ne koostuivat lähinnä journalistin omasta ennakkoarvioinnista ja esihenkilöiden informoimisesta. Yksi haastateltavista kuvasi erääseen tapaukseen liittynyttä ennakkovarautumista näin:

> Oli silleen hommat mietitty valmiiksi. Yhteystietoja niille henkilöille, joiden kanssa mä siellä asioin, että pystyy olemaan niihinkin nopeasti yhteydessä. [– –] Tommosta hiihtolenkkitasoa kun lähetään Lappiin hiihtämään, että kerrotaan mitä reittejä ollaan menossa ja minne ja mihin mennessä pitäisi kuulua takaisin. Ei mitään sen kummallisempaa. Mutta kuitenkin, eka kerta että millään juttukeikalla tolla tavalla nimenomaan turvallisuussyistä [– –] (H3)

Omien tietojen jakamisen välttäminen ja/tai piilottaminen olivat kuitenkin yleisiä varotoimia haastateltujen keskuudessa. Yhtä lukuun ottamatta kaikki osallistujat (11) ilmoittivat, että he olivat rajoittaneet ulkopuolisten pääsyä sosiaalisen median profiileihinsa ja välttivät tietoisesti henkilökohtaisten tietojen, kuten omien ja perheenjäsentensä kuvien, jakamista. Puolet osanottajista (6) oli myös ohjeistanut lähipiiriään toimimaan vastaavalla tavalla. Neljä oli tehnyt tietojenluovutuskiellon, ja kahdella oli voimassa turvakielto. Tietojen jakamisen välttämistä tai niiden piilottamista pidettiin ensisijaisesti proaktiivisena toimena, jolla pyrittiin välttämään itseen tai lähipiiriin kohdistuvaa häirintää tai uhkaa. Kun henkilökohtaisia tietoja ei ole suoraan saatavilla, heikommin motivoituneiden toimijoiden arveltiin luopuvan aikeistaan tai siirtyvän helpompiin kohteisiin.

Tietoturvariskien ja niihin varautumisen osalta haastatteluissa korostui erityisesti tapauskohtainen harkinta. Tietoturvaa koskevissa riskiarvioissa huomioitiin esimerkiksi jutun aihe, lähteenä käytettävien tietojen luonne, lähteiden rooli ja asema sekä potentiaaliset ”vastapuolet” sekä näiden oletetut mahdollisuudet ja kompetenssi tietojen ja lähteiden urkkimiseen. Riskiarvioinnissa hyödynnetään siis hyvin samanlaisia ulottuvuuksia kuin Masashi Crete-Nishihata, Joshua Oliver, Christopher Parsons, Dawn Walker, Lokman Tsui ja Ronald Deibert (2020, 1078–1080) erittelivät tutkimuksessaan. Haastattelemani journalistit mielsivät perusteellisemmat digitaaliset tietoturvatoimet usein tarpeellisiksi vasta tilanteissa, joissa vastapuolella ajateltiin olevan valtiotason toimijoita tai muuten tietoteknisesti erityisen kyvykkäitä tahoja.

Myös digitaaliset jäljet nähtiin lähdesuojan näkökulmasta keskeiseksi tietoturvariskiksi. Näin ollen tutkivat journalistit pyrkivät suosimaan välineitä ja ratkaisuja, joilla jälkiä yhteydenpidosta syntyy mahdollisimman vähän ja jotka tekevät niiden selvittämisestä tavanomaista vaikeampaa. Jälkiä voitiin myös tarkoituksellisesti hämärtää jälkikäteen. Erityisen haastavana pidettiin ensikontakteja lähteisiin. Jos lähde ottaa yhteyttä tai tähän joudutaan olemaan yhteydessä esimerkiksi työsähköpostin tai työpuhelimen välityksellä, jälki yhteydenotosta on jo syntynyt. Lähteitä kontaktoidessa pyrittiin siis ensisijaisesti suosimaan henkilökohtaisia

puhelinnumeroita ja sähköposteja, jotta digitaaliset jalanjäljet eivät olisi esimerkiksi mahdollisen työnantajan helposti jäljitettävissä. Vähänkään arkaluonteisimmissa asioissa toimittajat ilmoittivat ehdottavansa lähteilleen siirtymistä joko salatun Signal-pikaviestimen tai salauksen sisältävän sähköpostin käyttöön. Signal ja muut salatut pikaviestimet ovat osittain korvanneet salattuja sähköposteja journalistien työvälineinä, ja haastatelluista journalisteista kaikki paitsi yksi (11) ilmoittivat käyttävänsä näitä viestimiä säännöllisesti työssään. Toimittajat saattoivat hyödyntää yhteydenpidossa myös prepaid-liittymillä varustettuja puhelimia, jotka eivät olleet yhdistettävissä heihin tai heidän työnantajaansa. Jos digitaaliset jäljet haluttiin minimoida, voitiin pyrkiä rajoittamaan kaikkea sähköistä yhteydenpitoa tai käyttää sitä ainoastaan tapaamisten sopimiseen. Varsinaisten asioiden käsittely säästettiin kasvokkaisiin kohtaamisiin. Vaihtoehtoisesti myös koko yhteydenpito voitiin hoitaa välikäsien kautta.

Lähtökohtaisesti journalistit näkivät olevansa itse päävastuussa yhteydenpidon luottamuksellisuuden takaamisesta. Koska heillä oli tietoturvamenetelmien käyttöön lähteiltä usein puuttuvaa osaamista ja rutiinia, journalistit kokivat yleensä omaksi velvollisuudekseen ehdottaa siirtymistä turvallisempiin viestintäkanaviin ja opastaa lähteitä näiden käytössä. Tietoturvallisempien kanavien käytöllä nähtiin olevan myös performatiivinen funktio, joka osoittaa lähteelle, että journalisti ottaa lähdesuojaan ja tietoturvaan liittyvät riskit vakavasti. Tämän koettiin edistävän keskinäistä luottamusta ja sitä, että lähteet uskalsivat puhua asioista vapaammin. Lainaus alla havainnollistaa sekä journalistien kokemaa vastuuta että turvakäytäntöjen performatiivista roolia:

> [– –] mä ajattelen kuitenkin että meillä toimittajilla on päävastuu tietoturvallisuudesta sen takia, koska eihän lähteet voi olla eksperttejä ja asiantuntijoita niissä tapauksissa. Niin esimerkiksi Signal, niin käytän tosi matalalla kynnyksellä myös sen takia, että mä haluan ehkä näyttää sille lähteelle, että mä otan tämän asian nyt vakavasti [– –] Että se ehkä luo sitä luotettavuutta myös sillä tavalla. (H4)

Tietojen säilytystä ja käsittelyä koskevia turvatoimia suunniteltaessa arvioitiin erityisesti tiedon luonnetta ja tahoja, joilla olisi intressi päästä tietoon ja/tai selvittää sen vuotaja sekä näiden tahojen käytettävissä olevia keinoja. Moni haasteltavista täsmensi, että kyse oli vain harvoin tiedoista, jotka olivat virallisesti salattuja tai liikesalaisuuksia. Tyypillisemmin kyse oli esimerkiksi yrityksen tai organisaation sisäisistä tiedoista tai materiaaleista, joiden välittäminen ulospäin rikkoi potentiaalisesti työntekijän tai viranhaltijan lojaliteettivelvoitetta.

Luottamuksellisten tietojen säilyttämisen tavat vaihtelivat merkittävästi osallistujien välillä. Osa säilytti tietoja oman tietokoneensa kovalevyllä, osa pilvipalvelussa. Toisilla oli arkaluonteisten tietojen säilyttämistä varten erillisiä kryptattuja kovalevyjä tai salasanasuojattuja muistitikkuja sekä ”kylmiä” tietokoneita, joita ei kytketty ollenkaan internetiin tai sisäverkkoihin. Jos tietoon koettiin kohdistuvan merkittäviä digitaalisia uhkia, niitä voitiin säilyttää vain paperisina salaisessa paikassa ja/tai lukkojen takana. Tietoja voitiin pyrkiä myös anonymisoimaan esimerkiksi korvaamalla lähteiden nimiä ja muuta tunnistetietoa peitenimillä. Erittäin riskialttiiksi koetuissa tapauksissa hyödynnettiin useita turvakäytäntöjä samanaikaisesti. Aineisto voitiin varastoida esimerkiksi kryptatulle kovalevylle verkosta irti olevassa tietokoneessa, jota sitten säilytettiin lukitussa tilassa. Lähtökohtaisesti turvakäytäntöjen valikoimasta siis poimit-

tiin tai omaksuttiin toimintatapoja tietoturvan takaamiseksi sillä perusteella, millaisia uhkia ja toimijoita vastaan journalistit ajattelivat todennäköisimmin suojautuvansa (ks. myös Crete-Nishihata ym. 2020, 1078–1080). Haastattelulainaus alla havainnollistaa, miten uhka-arviot ja turvakäytännöt esiintyivät pohdinnoissa rinnakkain:

> [– –] on yksi asia että tutkii jotain henkilöitä tai instituutioita, mutta sitten on eri asia et jos sä alat tutkimaan valtiota, puolustusvoimia, tai sitten kaiken näkevää Googlea, jolla on tosi hyvät tietenkin mahdollisuudet varmaan urkkia tietoa [– –] Niin jos tekisi jotain sellaista tutkivaa juttua, niin sitten pitäisi varmaan miettiä aika tarkasti että miten sitä tehdään, että se tieto ei vuoda. (H4)

Laiteriskien minimoimiseksi tutkivien journalistien käytössä oleviin tietokoneisiin ja matkapuhelimiin sovellettiin toisinaan poikkeavia ja järeämpiä tietoturvaratkaisuja. Journalistit saattoivat myös tietoisesti olla itse asentamatta esimerkiksi pääsyä sähköpostiinsa tai vastaaviin ohjelmistoihin matkapuhelimeensa. Tietyissä tapauksissa voitiin myös sopia, että lähteitä tavatessa tekniset laitteet jätetään kokonaan pois tai suljetaan tapaamistilan ulkopuolelle keskustelun ajaksi. Myös näin toimimisella oli performatiivinen funktionsa. Se havainnollistaa konkreettisesti, ettei journalisti tallenna tapaamista teknisesti millään tavalla, vaan keskittyy asiaan täysin ja on pelkästään paperisten muistiinpanojen ja/tai oman muistinsa varassa.

Journalistien arviot kollektiivisen tietoturvan edistämiseen tähtäävistä käytännöistä omassa organisaatiossaan vaihtelivat. Osa haastatelluista koki, että näihin riskeihin on alettu suhtautua vakavasti. Konkreettisesti tämä näkyi esimerkiksi koko henkilöstölle suunnattuina tietoturvakoulutuksina, kaikkien käytössä olevien laitteiden varustamisella turvalaitteilla- ja ohjelmistoilla ja siinä, että kaikki organisaation jäsenet pakotetaan teknisesti käyttämään tiettyjä turvatoimia, kuten kaksivaiheista tunnistautumista. Tähän nähtiin yhdistyvän myös pyrkimys siirtää tietoturvaan liittyvää ajattelua yksilöiden omasta harkinnasta kokonaisuuden hallintaan (vrt. Henrichsen 2022, 1833–34). Näitä toimia pidettiin yleisesti hyvänä tapana lisätä tietoturvaa työyhteisön tasolla, kuten alla oleva lainaus kuvaa:

> [– –] se on ikään kuin integroitu jo siihen toimintaympäristöön, mikä on tietysti hyvä. Et ei erikseen tarvitse sitten niin kuin kouluttaa, vaan pakotetaan. Kyse on siitä, että pakotetaan ihmiset tekemään asiat vaikeammin ja hitaammin kuin aikaisemmin, mikä liittyy tietoturvaan. [– –] velvollisuus huolehtia siitä tietoturvasta, niin koskee ihan kaikkia. (H7)

Toisissa työyhteisöissä ja erityisesti freelancereiden kohdalla tietoturvasta huolehtimisen koettiin usein jäävän enemmän yksilöiden vastuulle ja näiden oman aktiivisuuden varaan. Tällöin myös yksilökohtaiset erot osaamisessa ja kiinnostuksessa korostuvat, kuten haastateltava alla kuvaa:

> [– –] se tekninen ennakoiminen, se on aika paljon toimittajista itse kiinni, että ei ne kyllä yleensä ole niin kiinnostuneita siitä [– –] Joko on tai sitten ei ole. [– –] että pitäisi luoda sellaisia käytäntöjä, et näin me toimitaan, et näin meillä tehdään, koska– – Että se ei olisi toimittajan omasta tahdostaan kiinni. (H8)

Moni haastatelluista piti henkilöriskeihin varautumista erityisen haasteellisena. Tämä korosti organisaation turvakulttuurin ja sisäisen luottamuksen merkitystä. Vaikka omat esihenkilöt ja tutkivat kollegat ymmärtäisivät työn luonteen ja lähdesuojan vaatimukset, jutun sisällöstä tietävien henkilöiden piiri laajenee väkisin siinä vaiheessa, kun mukaan tulee esimerkiksi editoreiden, graafikoiden, kuvittajien, kuvaajien ja verkkotuottajien kaltaisia toimijoita. Kun juttu viedään sähköiseen toimitusjärjestelmään, se voi näkyä sadoille ihmisille, joista osa saattaa työskennellä esimerkiksi saman konsernin muissa välineissä. Yli puolet vastaajista (7) ilmoitti, että on joskus syöttänyt arkaluontoiset jutut toimitusjärjestelmään vasta viimeisellä mahdollisella hetkellä näiden riskien pienentämiseksi.

Opit turvakäytännöistä leviävät ammattikunnan sisällä

Kolmas tutkimuskysymykseni keskittyi siihen, mitä kautta journalistit saavat tietoa ja oppia turvakäytännöistä sekä millaisia haasteita niiden käyttöönotossa ja soveltamisessa kohdataan. Tulokset osoittavat, että turvakäytäntöjen opiskelu on Suomessa pitkälti tutkivien journalistien oman aktiivisuuden varassa, eikä näitä tyypillisesti opita muodollisen koulutuksen kautta ammattiin opiskeltaessa. Yleisimmät tavat oppia turvakäytännöistä olivat kollegat, itseopiskelu ja/tai järjestöjen koulutukset. Vain yksi haastatelluista oli saanut fyysiseen turvallisuuteen liittyvää koulutusta, ja seitsemän ilmoitti osallistuneensa digitaalisen tietoturvan koulutukseen uransa aikana. Tietoturvakoulutusten tarjoajina korostuivat järjestöt, kuten Tutkivan journalismin yhdistys, Suomen Journalistiliitto ja ulkomaiset tutkivan journalismin yhdistykset. Journalistien työnantajat tarjosivat koulutusta tietoturva- tai turvallisuusaiheista vain harvoin, ja tällaiset koulutukset keskittyivät tyypillisesti yleisempään organisaation tietoturvaan, kuten kalasteluyritysten ja haittaohjelmien torjumiseen.

Tutkivaan journalismiin liittyvän tietoturvan erityistarpeisiin vastaaminen oli yleensä toimitusten ja IT-osastojen ”harrastuneiden yksilöiden” varassa. Journalistit kertoivat kääntyvänsä näiden henkilöiden puoleen, kun tarvitsivat tietoturvaratkaisuihin liittyvää tietoa tai osaamista. Tämä vastaa Jennifer Henrichsenin (2022, 1838–41) havaintoja turvallisuustematiikasta kiinnostuneiden yksilöiden keskeisestä roolista: nämä henkilöt toimivat osaamisen jakajina sekä välittäjinä eri osastojen välillä ja vaikuttavat toiminnallaan turvakulttuurin muotoutumiseen journalististen organisaatioiden sisällä.

Turvakäytäntöihin liittyvinä haasteina ja ongelmina haastateltavat nostivat esille *ajan tasalla pysymiseen*, *teknisen haastavuuden*, *turvakäytäntöjen työhön aiheuttaman kitkan* sekä *tutkivan työn erityistarpeiden huomioimisen organisaation turvakulttuurissa*. *Itsensä ajan tasalla pitämisen* hankaluus kytkeytyi tutkivan journalismin tarpeisiin räätälöidyn säännöllisen koulutuksen harvinaisuuteen. Erityisesti digitaalisen tietoturvan kentän koettiin olevan jatkuvassa muutostilassa, ja edellyttävän jatkuvaa seuraamista ja omien tietotaitojen ylläpitämistä. Esimerkiksi tietoturvallisina pidetyt ohjelmistot saattoivat yllättäen osoittautua haavoittuvaisiksi tai haittaohjelmat alkaa levitä uusilla tavoilla. Moni haastatelluista koki, ettei heidän organisaationsa tietoturvassa välttämättä huomioida tutkivien journalistien erityistarpeita eikä tällaisen osaamisen ylläpitoa harjoiteta systemaattisesti. Hektisessä työympäristössä osaamisesta huolehtimisen koettiin siis jäävän usein journalistien omalle vastuulle. Riskinä on, että ajanpuutteen takia tietoturvakäytäntöjen päivittäminen jää tekemättä ja niiden antama suoja heikkenee.

Erityisen haastavaa ajan tasalla pysyminen oli freelancereille, jotka tyypillisesti joutuvat huolehtimaan näistä usein ilman organisaation tukea ja omalla ajallaan. Haastattelulainaus alla havainnollistaa tällaisessa asemassa työtään tekevän journalistin pohdintaa aiheesta:

> [– –] koko ajan pitäisi kyetä ylläpitämään omaa osaamistaan ja siihen ei varsinaisesti ole minkäänlaisia resursseja toimitusten sisällä. Ja silloin kun tekee freelancerina, niin siinä on aika yksin ja se vie paljon työaikaa. Tietysti perusjutut on helppo ottaa haltuun. [– –] mutta kyllähän välineet ja asiat kehittyy koko ajan. Se, että pitää itseään koko ajan tasalla, vaatii työtä. Jos saa [palkan] siitä ajasta, kun kirjoittaa niitä juttuja, ja työaikaa ei varsinaisesti voi käyttää siihen, että kouluttaa itseään, niin se jää helposti tekemättä. (H5)

Teknisen haastavuuden osalta journalistit hahmottivat kaksijakoista kehitystä. Koska digitaalisten tietoturvauhkien koettiin yleisesti lisääntyneen, journalistien osaamistarpeisiin heijastui kasvaneita vaatimuksia. Tilanteissa, joissa journalistien viestintään tai tietoihin katsottiin kohdistuvan erityinen uhka, apua jouduttiin usein hakemaan muilta tahoilta. Suuremmissa mediataloissa tällaista apua tarjosivat esimerkiksi IT-osastot. Turvakäytännöt eivät siis näissä tapauksissa olleet enää pelkästään journalistien omissa käsissä, vaan teknistä osaamista tarvittiin tähän erikoistuneilta toimijoilta (ks. myös Henrichsen 2022, 1837).

Toisaalta Signalin kaltaiset helppokäyttöiset ja salatut pikaviestimet ovat samanaikaisesti vähentäneet journalisteilta ja lähteiltä vaadittavaa teknisen osaamisen tarvetta ja tehneet salatusta viestinnästä helpompaa ja saavutettavampaa. Tämän koettiin yleisesti vähentäneen kynnystä salatun viestinnän käyttöön lähteiden kanssa. Tätä pidettiin lähtökohtaisesti erittäin myönteisenä kehityksenä, sillä lähteiden halukkuus ja osaaminen salattujen viestintäkeinojen käyttöön ovat aikaisemmin muodostaneet merkittävän esteen niiden laajamittaiselle käytölle (ks. myös Henrichsen 2022, 1836; McGregor ym. 2015, 403–404). Yksi haastatelluista journalisteista kuvasi tätä muutosta näin:

> Signal on muuttanut tätä pelikenttää tosi hyväksi. Koska siellä voi puhua, siellä voi soittaa, siellä voi järjestää ryhmäpuheluita, sinne voi ladata tiedostoja ym. [– –] Aikaisemmin piti olla julkisia avaimia ja salattuja avaimia ja niiden avainten kanssa piti leikkiä, se oli vaikeeta. Signal on kyllä muuttanut tätä ympäristöä tosi paljon parempaan suuntaan, että siitä on tullut käyttäjäystävällisempi. (H7)

Merkittävänä haasteena pidettiin kuitenkin *turvakäytännöstä koituvaa ylimääräistä vaivaa*. Monet turvakäytännöistä hankaloittivat ja hidastivat asioiden tekemistä (ks. myös Henrichsen 2022, 1834–37; McGregor ym. 2015, 408–409). Koska niukat resurssit muodostavat jatkuvan haasteen tutkivassa työssä, tutkivat journalistit joutuivat hakemaan tasapainoa riittävien turvakäytäntöjen ja toisaalta työn sujuvuuden välillä. Tämä kytkeytyi olennaisesti journalistien omiin arvioihin siitä, millaisia uhkia he näkevät työhönsä kohdistuvan. Kuitenkin myös yleisessä turvakäytäntöihin liittyvässä ajattelutavassa oli havaittavissa eroja. Osa haastatelluista koki, että tiettyjen käytäntöjen noudattaminen kokoaikaisesti auttoi integroimaan ne omiin työrutiineihin ja edisti näin kokonaisturvallisuutta. Haastattelulainaus alla havainnollistaa tällaista toimintatapaa ja ajattelua sen takana:

> [– –] jos [– –] aina vaihtaisin, että tietyissä tilanteissa vasta alan käyttää sitä turvallisempaa välinettä, niin sitten se jää todennäköisemmin tekemättä, koska ihminen on perusluonteeltaan laiska, ainakin itse olen. On helpompaa käyttää koko ajan sellaista. (H5)

Toiset taas ottivat erilaisia turvakäytäntöjä käyttöön lähtökohtaisesti aina vain tarpeen mukaan ja tapauskohtaisesti tekemänsä riskiarvion perusteella. Nämä tarpeet saattoivat muuttua myös juttuprosessin aikana, jos journalistin haltuun päätyi esimerkiksi salassa pidettäviä dokumentteja tai jutun riskiprofiili muuttui merkittävästi.

Ajattelutapojen erot tulivat esiin myös suhtautumisessa siihen, pitäisikö toimituksissa ja tiedotusvälineissä laatia ja soveltaa yhteisiä linjauksia esimerkiksi luottamuksellisten tietojen säilyttämisestä tai lähteiden kanssa toimimisesta. Osa koki, että kaikkien noudattamat yhteiset käytännöt voisivat yleisesti parantaa kokonaistietoturvaa ja selkeyttää käytäntöjä. Osa puolestaan näki, että nämä kysymykset olivat ajankohtaisia lähinnä harvoille tutkiville toimittajille, jotka osaavat ottaa ne riittävästi huomioon jo nykyisellään. Näin ollen niiden standardoiminen ei välttämättä toisi merkittävää lisäarvoa vaan voisi tarpeettomasti hankaloittaa nykyisellään hyvin toimivia prosesseja. Tällöin korostettiin usein sitä, että lähtökohtaisesti journalistit keräävät tietoa aina julkaistavaksi, ja salassa pidettävät tai luottamukselliset tiedot ovat journalistisessa työssä poikkeuksia.

Työyhteisön ja työnantajien osalta turvakäytäntöjen soveltamisen haasteena korostuivat organisaatioiden turvakulttuurit ja niistä kumpuava *ymmärrys tutkivan journalismin tarpeista*. Tämä konkretisoitui kysymykseen siitä, ymmärretäänkö tietyssä organisaatiossa tutkivaan journalismiin liittyviä erityistarpeita ja -huolia (ks. myös Henrichsen 2022, 1834–37). Esimerkiksi pilvipalvelujen, digitaalisten yhteistyöalustojen, koneellisten litterointipalvelujen ja automaattisen puhelujen tallennuksen kaltaiset työkalut saattoivat helpottaa merkittävästi journalistista työtä, mutta tutkivan journalismin näkökulmasta niihin nähtiin sisältyvän piileviä tietoturvariskejä. Näin ollen näiden pakottamista ylhäältä päin kaikkien organisaation jäsenten käyttöön ei välttämättä pidetty hyvänä asiana. Myös IT-osastot katsoivat toisinaan tietoturvaa niin vahvasti organisaationäkökulmasta, että poikkeusluvista tutkivien toimittajien kaipaamien erityisohjelmistojen asentamiseen tai toimenpiteiden tekemiseen työnantajan välineisiin jouduttiin vääntämään niiden kanssa. Jos lähdesuoja sekä turvallisuus- ja tietoturvauhat otettiin välineessä vakavasti, niihin liittyviin asioihin oltiin valmiimpia kiinnittämään huomiota ja sijoittamaan resursseja organisaatiotasolla. Jos taas näihin suhtauduttiin välinpitämättömästi tai vähättelevästi, muutosten läpi ajamiseksi saattoi joutua taistelemaan ymmärtämättömyyttä tai jopa aktiivista vastustusta vastaan.

Loppupäätelmät

Tässä artikkelissa on tarkasteltu suomalaisten tutkivien journalistien näkemyksiä työhön liittyvistä turvallisuus- ja tietoturvariskeistä sekä sitä, millaisin toimin ja tavoin journalistit pyrkivät vähentämään ja ehkäisemään näitä riskejä. Lisäksi artikkeli analysoi sitä, mistä journalistit ovat saaneet tietoa ja oppia turvakäytännöistä ja millaisia kysymyksiä ja hankaluuksia liittyy niiden soveltamiseen työn osana. Analyysin perusteella suomalaisten tutkivien journalistien

keskuudessa hahmottuu muutamia jaetun turvakulttuurin piirteitä. Niistä keskeisin on lähteiden suojelu keskeisenä arvona (ks. myös Tsui ja Lee 2021, 1327–28; Crete-Nishihata ym. 2020, 1077; McGregor ym. 2016, 422–423; Kuutti 1995, 120–123). Lähteisiin kohdistuvat riskit korostuivat, koska journalisteihin itseensä kohdistuvat suorat uhat arvioitiin Suomessa harvinaisiksi, ja ne koskettivat vain pientä osaa tutkivaa työtä harjoittavista toimittajista. Viranomaisten halu koetella lähdesuojaa sekä erilaisten toimijoiden into pyrkiä selvittämään toimittajille puhuneita henkilöitä tulkittiin konkreettisiksi osoituksiksi siitä, ettei Suomessakaan ole tässä asiassa varaa sinisilmäisyyteen tai varomattomuuteen.

Tulokset myös osoittavat, että suomalaiset tutkivat journalistit käyttävät hyvin itsenäistä harkintavaltaa siinä, millaisia turvakäytäntöjä he soveltavat erilaisissa tapauksissa (ks. myös McGregor ym. 2016, 429; Crete-Nishihata ym. 2020, 1072). Harkinnan pohjana toimivat mentaaliset mallit todennäköisistä riskeistä ja erilaisten turvakäytäntöjen tehosta niiden torjumiseksi. Koska erilaisten turvakäytäntöjen opetteluun ja käyttöönottoon kuluu aikaa ja resursseja, ja niiden koetaan usein hankaloittavan ja hidastavan journalistista työtä, journalistit pyrkivät työekonomian nimissä välttämään riskeihin nähden ”liian järeitä” turvakäytäntöjä (ks. myös Henrichsen 2022, 1835–1837; McGregor ym. 2016, 429–430). Keskeiset riskiarvioihin vaikuttavat tekijät ovat jutun aihe ja sen koettu ”arkaluontoisuus”, lähteiden rooli ja asema sekä näkemys potentiaalisista ”vastapuolista”, joilla olisi intressi urkkia jutun lähteitä ja/tai pyrkiä tavalla tai toisella vaikuttamaan sen julkaisemiseen (ks. myös Crete-Nishihata ym. 2020, 1078). ”Vastapuolien” yhteydessä journalistit arvioivat sitä, millaisia resursseja, keinoja ja osaamista niillä ajateltiin olevan ja millaisten ”pelisääntöjen” mukaan niiden uskottiin toimivan näissä tilanteissa. Omia turvakäytäntöjä mukautettiin tarvittaessa tämän tapauskohtaisen harkinnan pohjalta.

Vaikka suomalaisten tutkivien journalistien mentaalisissa riskimalleissa oli paljon yhteneväisyyttä, keskeisenä erona nousivat esiin arviot viranomaisten ja tiedustelupalvelujen journalisteihin sekä näiden viestintään ja laitteisiin kohdistamasta vakoilusta. Osa haastateltavista piti tällaista seuraamista ja urkintaa hyvinkin mahdollisena myös Suomen oloissa, kun taas osa uskoi sen tapahtuvan lähinnä vain jälkikäteisesti julkaistuja juttuja seuraamalla.

Vastakkaisena uudempana trendinä journalistien omaan harkintaan perustuvalle yksilölliselle turvakäytäntöjen soveltamiselle näyttäytyivät organisaatioiden yleistyvät pyrkimykset kollektiivisen tietoturvan ja turvallisuuden parantamiseen (ks. myös Henrichsen 2022, 1833–84.). Kaikilta käyttäjiltä saatettiin esimerkiksi alkaa edellyttää kaksivaiheisen tunnistautumisen ja VPN-yhteyksien käyttöä, ja yhtenevät tietoturvaratkaisut saatettiin ulottaa kaikkiin työnantajan journalisteille tarjoamiin työvälineisiin. Näissä toimissa aktiivinen toimija on yksilön sijaan organisaatio, ja logiikka on päinvastainen kuin journalistien omissa suojautumistoimissa: arvioita ei tehty henkilö- ja tapauskohtaisesti vaan samat käytänteet pakotettiin ylhäältä päin kaikille organisaation jäsenille (ks. myös McGregor ym. 2016). Tämä mukailee näkemystä nykyaikaisten digitaalisten uhkien kollektiivisesta luonteesta: heikko lenkki tietoturvassa saattaa myös paremmin suojautuneet vaaraan. Toisaalta organisaatiot saattoivat myös tehdä keskitettyjä päätöksiä esimerkiksi digitaalisista työskentelyalustoista tai muista teknisistä ratkaisuista tavalla, joka ei huomioinut tutkivan työn erityistarpeita (ks. myös McGregor ym. 2016, 425). Organisaatiotason toimet osaltaan kasvattivat eroja sekä työsuhteisten ja freelancereiden että suurten ja pienten organisaatioiden toimittajien välillä: freelancereilla ja pienten organisaatioiden journalisteilla on laajempi autonomia päättää omista turvakäytännöistään ja ratkaisuis-

taan, mutta samanaikaisesti niistä huolehtiminen jää enemmän heidän omalle vastuulleen, eikä heillä ole käytössään yhtä laajaa institutionaalista tukea ja samanlaisia resursseja kuin suurten organisaatioiden työsuhteisilla toimittajilla (Crete-Nishihata ym. 2020, 1080–81; Tsui ja Lee 2021, 1328–29).

Tutkimus osoittaa, että erityisiin tutkivan journalismin turvakäytäntöihin liittyvä osaamisen hankkiminen ja ylläpitäminen on tyypillisesti journalistien oman aktiivisuuden ja kiinnostuksen varassa. Tämä korostaa esimerkiksi teknisestä osaamisesta syntyviä eroja tietoturvassa. Tietotekniikkaa paremmin hallitsevat journalistit pystyvät omaksumaan ja ottamaan teknisiä välineitä ja turvakäytäntöjä käyttöön vaivattomammin kuin heidän tekniikkaa heikommin tuntevat kollegansa. Toisaalta aineistossa näkyy vahvasti kollegiaalisuus ja tiedon jakaminen. Vinkkejä turvakäytäntöjen soveltamiseen saadaan omilta kollegoilta työn ohessa, ja apua voidaan pyytää muilta alalla olevilta. Myös järjestöjen koulutustoiminta on vahvasti kollegiaalista, ja kouluttajina toimivat usein toiset tutkivat journalistit. Suomalaisen tutkivan journalismin turvakulttuurin yhteisiä toimintamalleja rakennetaan siis osaltaan kollegiaalisen tietojen jakamisen välityksellä.

Vaikka tämä tutkimus keskittyi tarkastelemaan tutkivien journalistien työssään soveltamia käytäntöjä turvallisuuden ja tietoturvan näkökulmasta, on syytä huomioida, että monet tässä tutkimuksessa turvakäytännöiksi nimetyistä toimista ovat todellisuudessa monikäyttöisiä. Niiden soveltamisella voidaan tavoitella samanaikaisesti hyvin erilaisia vaikutuksia ja hyötyjä (ks. McGregor ym. 2015, 407). Aineisto havainnollistaa esimerkiksi turvakäytäntöjen performatiivista funktiota sekä journalisteille itselleen että näiden lähteille. Suojaamalla itsensä journalisti kokee, että voi paremmin luottaa lähdesuojan ja tietoturvan pitävyyteen sekä edistää omaa mielenrauhaansa ja turvallisuudentunnettaan. Lähteille turvakäytäntöjen soveltaminen toimii konkreettisena osoituksena siitä, että journalisti ottaa lähdesuojan vaatimukset vakavasti, mikä voi edistää keskinäisen luottamuksen muodostumista (ks. myös Tsui ja Lee 2021, 1327; McGregor ym. 2015, 407). Monien turvakäytäntöjen koettiin olevan perusteltuja myös journalismin työprosessien näkökulmasta. Esimerkiksi lähteiden tapaaminen usean henkilön voimin lisää osaltaan turvallisuutta, mutta se miellettiin ensisijaisesti hyödylliseksi työn sujuvuudelle ja lopputulokselle. Työparin läsnäolo tapaamisissa mahdollistaa tietojen arvioinnin ja kysymysten esittämisen kahden henkilön voimin, eikä tapaamisten sisältöä tarvitse jälkikäteen referoida erikseen työparin toiselle osapuolelle. Näin ollen turvallisuus oli usein vain yksi lisäperuste sille, että tutkivat journalistit olivat päätyneet soveltamaan tällaisia käytäntöjä työssään.

Kiitokset

Haluan kiittää kaikkia tutkimukseen osallistuneita journalisteja heidän ajastaan ja luottamuksestaan. Lisäksi kiitän yliopistotutkija Esa Reunasta Tampereen yliopistosta käsikirjoituksen kommentoinnista.

Rahoitus

Tutkimus on tehty Suomen Akatemian rahoittaman Communication Rights in the Age of Digital Disruption (CORDI) -tutkimuskonsortion taloudellisella tuella.

Kirjallisuus

Ala-Fossi, Marko: John Grönvall, Kari Karppinen ja Hannu Nieminen. 2021. "Finland: Sustaining professional norms with fewer journalists and declining resources." Teoksessa *The Media for Democracy Monitor 2021: How Leading News Media Survive Digital Transformation (Vol. 1)*, toimittaneet Josef Trappel ja Tales Tomaz, 153–196. Göteborg: Nordicom. https://doi.org/10.48335/9789188855404-4

Arolainen, Teuvo. 2000. "Tutkivan journalismin vuosikymmen." *Media & viestintä* 23 (1): 114–127.

Bennett, Lance ja William Serrin. 2005. "The Watchdog Role." Teoksessa *The Press* toimittaneet Geneva Overholser ja Kathleen Jamieson, 395–405. Oxford: Oxford University Press.

Bjerknes, Fredrik. 2022. "Inventive Factfinders: Investigative Journalism as Professional Self-representation, Marker of Identity and Boundary Work." *Journalism Practice 16* (6): 1037–1056. https://doi.org/10.1080/17512786.2020.1845780

Bradshaw, Paul. 2017 "Chilling Effect: Regional journalists' source protection and information security practice in the wake of the Snowden and Regulation of Investigatory Powers Act (RIPA) revelations." *Digital Journalism* 5 (3): 334–352. https://doi.org/10.1080/21670811.2016.1251329

Cancela, Pauline, David Gerber ja Annik Dubied. 2021. "'To Me, It's Normal Journalism' Professional Perceptions of Investigative Journalism and Evaluations of Personal Commitment." *Journalism Practice* 15 (6): 878–893. https://doi.org/10.1080/17512786.2021.1876525

Crete-Nishihata, Masashi, Joshua Oliver, Christopher Parsons, Dawn Walker, Lokman Tsui ja Ronald Deibert. 2020. "The Information Security Cultures of Journalism." *Digital Journalism* 8 (8): 1068–1091. https://doi.org/10.1080/21670811.2020.1777882

Ettema James ja Theodore Glasser. 1998. *Custodians of Conscience: Investigative Journalism and Public Virtue*. New York: Columbia University Press.

Finlex. 2023. Laki sananvapauden käyttämisestä joukkoviestinnässä. Viitattu 10.10.2023. https://www.finlex.fi/fi/laki/ajantasa/2003/20030460

Freedom House. 2023. Freedom in the World: Country Scores. Viitattu 10.10.2023. https://freedomhouse.org/countries/freedom-world/scores

Guest, Greg, Kathleen MacQueen ja Emily Namey. 2012. *Applied Thematic Analysis*. Los Angeles: SAGE.

Halminen, Laura. 2016. Mediayhtiö Sanoma verkkovakoiluyrityksen kohteena – ei näyttöä onnistumisesta. *Helsingin Sanomat* 5.5.2016. https://www.hs.fi/kotimaa/art-2000002903807.html

Heino, Jatta. 2013. *Vallan vahtikoira vai arkistojen urkkija? Tutkivan journalismin työmenetelmät sanomalehdessä*. Opinnäytetyö, Kemi-Tornion ammattikorkeakoulu.

Henrichsen, Jennifer. 2022. "Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the 'Security Champion." *Journalism Practice* 16 (9): 1829–1848. https://doi.org/10.1080/17512786.2021.1927802

Helsingin Sanomat (HS). 2023. Media ei ole kansan vihollinen. 15. elokuuta. Viitattu 12.10.2023. https://www.hs.fi/paakirjoitukset/art-2000009782952.html

Hiltunen, Ilmari. 2022. *External Interference in Finnish Professional Journalism*. Väitöskirja, Tampereen yliopisto.

Hiltunen, Ilmari; Aleksi Suuronen ja Reeta Pöyhtäri. 2024. "Harassed for Their Job: Exploring Factors That Render Journalists Prone to Harassment and Intimidation". *Journalism Studies*. Tulossa.

Holton, Avery, Valérie; Bélair-Gagnon, Diana Bossio ja Logan Molyneux. 2023. "'Not Their Fault, but Their Problem': Organizational Responses to the Online Harassment of Journalists." *Journalism Practice* 17 (4): 859–874.

Hunter, Mark. 2011. *Story-Based Inquiry: A Manual for Investigative Journalists*. Paris: UNESCO.

Karadimitriou, Achilleas; Torbjörn von Krogh; Christian Ruggiero; Cecilia Biancalana, Mauro Bomba ja Wai Han Lo. 2022. "Investigative journalism and the watchdog role of news media: Between acute challenges and exceptional counterbalances." Teoksessa *Success and failure in news media performance: Comparative analysis in the Media for Democracy Monitor 2021*, toimittaneet Josef Trappel ja Tales Tomaz, 101–125. Göteborg: Nordicom. https://doi.org/10.48335/9789188855589-5

Karlsson, Fredrik, Joachim Åstrom ja Martin Karlsson. 2015. "Information Security Culture State of the Art Review between 2000 and 2013." *Information and Computer Security* 23 (3): 246–285.

Kokkonen, Saara-Miira. 2023. *"Intoa olisi, mutta sillä ei elä": millaisia haasteita toimittajat kohtaavat tutkivan journalismin parissa tänä päivänä?"*. Opinnäytetyö, Turun ammattikorkeakoulu.

Kuutti, Heikki. 1995. *Tutkiva journalismi: Journalistinen suuntaus ja suomalaisen journalismin tutkivuus*. Väitöskirja, Jyväskylän yliopisto.

Kuutti, Heikki. 2001. *Tutkittu juttu: Johdatus tutkivaan journalismiin*. Jyväskylä: Atena.

Kuutti, Heikki. 2003. *Tutkivan journalismin lisääminen: Toimituskäytäntö ja journalistikoulutus*. Jyväskylä: Mediainstituutti.

Laitinen, Minja. 2017. *MOT - mikä oli tutkittava: tietolähteet tutkivassa journalismissa*. Pro gradu -tutkielma, Tampereen yliopisto.

McGregor, Susan, Polina Charters, Tobin Holliday ja Franziska, Roesner. 2015. "Investigating the Computer Security Practices and Needs of Journalists." *Proceedings of the 24th USENIX Security Symposium*, 399–414. https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-mcgregor.pdf

McGregor, Susan ja Elizabeth Watkins. 2016. "'Security by Obscurity': Journalists' Mental Models of Information Security". *The Official Research Journal of ISOJ* 6 (1). https://isoj.org/research/security-by-obscurity-journalists-mental-models-of-information-security/

McGregor, Susan, Franziska Roesner ja Kelly Caine. 2016. "Individual versus Organizational Computer Security and Privacy Concerns in Journalism". *Proceedings on Privacy Enhancing Technologies Symposium* 4: 418–435. https://doi.org/10.1515/popets-2016-0048

Mustikainen, Tuomas. 2014. *Juttuaiheena talousrikos: toimittajien tiedonhankinta pitkäkestoisessa talousrikosprosessissa*. Pro gradu -tutkielma, Jyväskylän yliopisto.

Namey, Emily, Greg Guest, Lucy Thairu ja Laura Johnson. 2008. Data reduction techniques for large qualitative data sets. Teoksessa *Handbook for team-based qualitative research*, toimittaneet Greg Guest ja Kathleen MacQueen, 137–61. Lanham: AltaMira Press.

Parker, Kelsey. 2015. *Aggression Against Journalists: Understanding Occupational Intimidation of Journalists Using Comparisons with Sexual Harassment*. Väitöskirja, University of Tulsa.

Patton, Michael. 1990. *Qualitative Evaluation and Research Methods*. Beverly Hills, CA: SAGE.

Päätoimittajien Yhdistys (PTY). 2023. PTY vetoaa: journalistien työrauhaa puolustettava. Viitattu 10.10.2023. https://www.paatoimittajat.fi/uutiset/pty-vetoaa-journalistien-tyorauhaa-puolustettava/

Ramachandran, Sriraman, Chino Rao, Tim Goles ja Gurpreet Dhillon. 2013. "Variations in Information Security Cultures across Professions: A Qualitative Study." *Communications of the Association for Information Systems* 33. https://doi.org/10.17705/1CAIS.03311

Reporters Without Borders (RSF). 2023. World Press Freedom Index. Viitattu 10.10.2023. https://rsf.org/en/index

Saldaña, Johnny. 2013. *The Coding Manual for Qualitative Researchers*. Los Angeles: SAGE.

Strömberg, Jari. 2022. STT varoitti entisiä ja nykyisiä työntekijöitään sähköpostilla: tietomurron tekijät saivat ehkä haltuunsa henkilötunnuksia ja osoitteita. *Yle Uutiset* 15.8.2022. https://yle.fi/a/3-12577406

Suomen Journalistiliitto (SJL). 2021. Journalistiliitto: Toimittajien vankeusuhka äärimmäisen vakava asia. Viitattu 10.10.2023. https://journalistiliitto.fi/fi/journalistiliitto-toimittajien-vankeusuhka-aarimmaisen-vakava-asia/

Tsui, Lokman ja Francis Lee. 2021. "How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom." *Journalism* 22 (6): 1317–1339. https://doi.org/10.1177/14648849198494 18

Uskali, Turo ja Heikki Kuutti. 2015. "Models and Streams of Data Journalism." *The Journal of Media Innovations* 2 (1): 77–88.

Uskali, Turo ja Heikki Kuutti. 2016. *Datajournalismin työkäytännöt*. Tampere: Vastapaino.

Urbániková, Marína; Ilmari Hiltunen ja Signe Ivask. 2024. Navigating Safety in 'Safe' Countries: A Cross-Country Analysis of Investigative Journalists' Safety and Security Practices. Käsikirjoitus arvioitavana.

Waisbord, Silvio. 2022. "Can Journalists Be Safe in a Violent World?" *Journalism Practice* 16 (9): 1948–1954. https://doi.org/10.1080/17512786.2022.2098524

Liite 1: Tutkimuksen esitietolomake

A. Turvakäytännöt ja tietoturva I

1. Mitä seuraavista toimista olet ainakin kerran journalistisen työurasi aikana käyttänyt itsesi, läheistesi, lähteidesi, viestintäsi ja/tai datasi turvaamiseksi? (Vastausvaihtoehdot: Kyllä/Ei)

A. Tietoturva ja yksityisyyden suoja digitaalisissa ympäristöissä

- Yksityisyysasetusten tiukentaminen sosiaalisen median tileilläsi (esim. rajoitukset siihen, kuka pääsee näkemään profiilisi, tiukempien yksityisyysasetusten asettaminen sovelluksiin ja peleihin, rajoitukset siihen, kuka voi lähettää sinulle yksityisviestejä)
- Henkilökohtaisten tietojen (ml. kuvat itsestäsi ja perheestäsi) jakamisen välttäminen sosiaalisessa mediassa
- Lähipiirisi ohjeistaminen siihen, etteivät nämä jaa sinua koskevia henkilökohtaisia tietoja (ml. kuvia itsestäsi ja perheestäsi) sosiaalisessa mediassa
- Yksityisyyttä parantavat muutokset laitteisiin (esim. tietokoneen kameran peittäminen tarralla)
- Tiedostojen säilyttäminen vain tietokoneesi kovalevyllä (ei esimerkiksi pilvipalveluissa)
- Tietokoneen pitäminen kokonaan poissa internetistä [air-gapping]
- Prepaid-liittymien tai -puhelinten käyttäminen
- Erillisen “toimituspuhelimen” käyttäminen (tätä tarkoitusta varten yhteiskäytössä oleva puhelin, jonka numeroa ei voida yhdistää tiettyyn henkilöön)
- Laitteiden sulkeminen kokonaan tärkeiden tapaamista aikana (esim. lähteiden tai kollegojen kanssa jne.)
- Datan säilyttäminen pilvipalvelussa tai verkkolevyllä, jotta sitä ei ole mahdollista tuhota, varastaa tai takavarikoida
- Digitaaliseen turvallisuuteen liittyvään koulutukseen osallistuminen

B. Turvakäytännöt ja tietoturva fyysisessä ympäristössä I

- Koodinimien käyttö viestinnässä ja/tai muistiinpanoissa
- Lähteisiin yhteydessä oleminen välikäsien kautta
- Uusien lähteiden tapaaminen julkisilla paikoilla
- Uusien lähteiden tapaaminen toisen henkilön kanssa (ei yksin)
- Arkaluontoisista tiedoista keskusteleminen vain kasvotusten
- Digitaalisen datan postittaminen tai välittäminen eteenpäin fyysisesti (esim. USB-tikulla)
- Arkaluontoisten juttujen siirtäminen yleiseen toimitusjärjestelmään vasta juuri ennen julkaisua
- Riskialttiista aiheista raportointi työryhmänä (yksittäisen journalistin sijaan)
- Artikkelien julkaisu tiedotusvälineen tai työryhmän nimellä (yksittäisen journalistin nimen sijasta)

C. Turvakäytännöt ja tietoturva fyysisessä ympäristössä II

- Hälytysjärjestelmän asentaminen kotiin
- Pippurisumutteen tai muun itsepuolustusvälineen kantaminen
- Henkilökohtaisen, mukana kannettavan hälytysjärjestelmän hankkiminen (turvapainike tms.)
- Kodin ja työpaikan välisen kulkureitin vaihteleminen
- Fyysiseen turvallisuuteen liittyvään koulutukseen osallistuminen
- Itsepuolustuskurssille osallistuminen
- Paperisten muistiinpanojen ja/tai tietojen säilyttäminen lukitussa kaapissa tai kassakaapissa
- Paperisten dokumenttien silppuaminen
- Datasäilöjen hävittäminen fyysisesti (esim. kovalevyjen tai USB-tikkujen tuhoaminen)
- Tietojenluovutuskiellon tekeminen
- Turvakiellon hakeminen henkilökohtaiseen turvallisuuteen liittyvistä syistä
- Muutto toiseen asuntoon, kaupunkiin tai ulkomaille turvallisuussyistä
- Yhteydenotto viranomaisiin (esim. poliisiin) henkilökohtaiseen turvallisuuteesi liittyvistä syistä

B. Turvakäytännöt ja tietoturva II

2. Tietoturvan lisäämiseksi ja yksityisen viestinnän mahdollistamiseksi on olemassa useita välineitä ja teknologioita. Mistä seuraavista olet tietoinen ja/tai mitä niistä käytät työssäsi?

	Käytän säännöllisesti (Ei välttämättä kaikessa viestinnässä, mutta aina kun näen sen tarpeelliseksi)	Olen kokeillut, mutta en käytä säännöllisesti	Olen kuullut, mutta en ole kokeillut itse	En ole kuullut aikaisemmin
Salauksen sisältävät sähköpostipalvelut (esim. ProtonMail, GPG, Mailvelope)				
Salauksen sisältävät viestintä- ja puhelusovellukset matkapuhelimelle (esim. Signal, Threema, WhatsApp, Wire, Wickr Me, Telegram, Viber…)				
Salauksen sisältävät viestintä- ja puhelusovellukset tietokoneelle (esim. Signal, Threema, WhatsApp, Wire, Wickr Me, Telegram, Viber…)				
Dokumenttien/kansioiden kryptaaminen				
Kovalevyn kryptaaminen				
Itsetuhoutuvat tiedostot (tiedostot, jotka häviävät asetetun määräajan kuluttua)				
Tietojenpoisto-ohjelmat (esim. BitRaser, File Eraser, Eraser, Secure Eraser, File Shredder, Hardwipe…)				
Sanasanojen hallintaohjelma; Salasanaohjelmisto (password manager)				
Vahvojen salasanojen käyttö				
Kaksivaiheisen tunnistautumisen käyttö				
Tiedostojen salattuun jättämiseen tarkoitettu järjestelmä (esim. SecureDrop)				
Anonyymi verkkoselaaminen (esim. Tor)				
Yksityiset ja anonyymit käyttöjärjestelmät (esim. Tails)				
Virtuaalisen erillisverkon (VPN) ja/tai IP-osoitteen peittäjien/blokkaajien käyttö				

3. Miten hyvin koet pystyväsi nykyisillä taidoillasi ja välineilläsi takaamaan itsesi, lähteidesi ja viestintäsi turvallisuuden (sekä fyysisessä että digitaalisessa ympäristössä)?

5 = Täysin	4	3	2	1 = En ollenkaan

4. Miten arvioisit työnantajaltasi tai tiedotusvälineeltäsi saamaasi tukea itsesi, lähteidesi ja viestintäsi turvallisuuden takaamisessa (sekä fyysisessä että digitaalisessa ympäristössä)?

(Jos työskentelet freelancerina tai yrittäjänä, vastaa perustuen siihen tiedotusvälineeseen, jolle teet eniten töitä)

5 = Täysin riittävää	4	3	2	1 = Ei ollenkaan riittävää

C. Taustatiedot

1. Sukupuolesi?
- Nainen
- Mies
- Muu

2. Ikäsi vuosina?

3. Mikä on korkein suorittamasi koulutus tai tutkinto?
- Peruskoulu
- Ylioppilastutkinto
- Ammattitutkinto
- Yliopisto- tai ammattikorkeakoulututkinto (AMK-tutkinto, kandidaatintutkinto, maisterin tutkinto, tohtorin tutkinto tms.)
- Muu koulutus tai tutkinto, mikä?

4. Oliko opintojesi pääaine/opintosuuntaus journalismi tai muu viestinnän ala?
- Kyllä
- Ei

5. Kuinka monta vuotta työkokemusta sinulla on journalistisesta työstä?
- Vähemmän kuin vuosi
- 2–5 vuotta
- 6–10 vuotta
- 11–15 vuotta
- Yli 15 vuotta

6. Mikä näistä vaihtoehdoista kuvaa parhaiten tämänhetkistä työsuhdettasi?
- Vakituinen työsuhde
- Määräaikainen työsuhde
- Itsensätyöllistäjä (freelancer tai yrittäjä), joka työskentelee suurimman osan ajasta yhdelle työantajalle
- Itsensätyöllistäjä (freelancer tai yrittäjä), useita eri työnantajia
- Muuntyyppinen työsuhde (esim. tarvittaessa töihin tuleva [TTT], nollatuntisopimus jne.)
- Muu työsuhde, mikä?

7. Mikä näistä kuvaa parhaiten tiedotusvälinettä, jossa pääosin työskentelet?
(Jos työskentelet freelancerina tai yrittäjänä, valitse vaihtoehto, joka kuvaa parhaiten sitä tiedotusvälinettä, jolle teet eniten töitä)

- Sanomalehti (sisältäen sen verkkosivut)
- Aikakauslehti (sisältäen sen verkkosivut)
- Kaupallinen radio- tai tv- kanava (sisältäen radio, tv ja näiden verkkosivut)
- Yleisradioyhtiö (sisältäen radio, tv ja näiden verkkosivut)
- Uutistoimisto
- Itsenäinen verkkolehti tai -sivusto (vain verkossa julkaistava)
- Muu tiedotusväline, mikä?

8. Mikä näistä vaihtoehdoista kuvaa parhaiten yleisökattavuutta siinä tiedotusvälineessä, jossa pääosin työskentelet?
Jos työskentelet freelancerina tai yrittäjänä, valitse vaihtoehto, joka kuvaa parhaiten sitä tiedotusvälinettä, jolle teet eniten töitä)

- Paikallinen tai alueellinen tiedotusväline
- Valtakunnallinen tiedotusväline

9. Mikä näistä vaihtoehdoista kuvaa parhaiten nykyistä työtehtävääsi?
- Toimittaja
- Päällikkötoimittaja (esim. toimitussihteeri, toimituspäällikkö, osastoesihenkilö tai tuottaja)
- Päätoimittaja
- Muu työtehtävä, mikä?

Liite 2: Tutkimuksen teemahaastattelurunko

A. Johdanto

1. Tutkiva journalismi on käsite, joka voidaan ymmärtää monella tavalla. Kuvailisitko itseäsi tutkivaksi journalistiksi, ja miten itse määrittelet tämän käsitteen sisällön? Miten tutkivuus näkyy juuri sinun työssäsi?

B. Turvallisuuden tunne ja uhkatekijät

2. Yleisesti ottaen, kuinka riskialtista tai vaarallista on toimia tutkivana journalistina Suomessa? Mitkä ovat mielestäsi keskeisimmät haasteet ja uhat työn turvallisuuteen ja tietoturvaan liittyen? Onko tässä tapahtunut muutoksia sinä aikana, kun olet toiminut tutkivana journalistina?

3. Miten turvalliseksi tai riskialttiiksi koet oman tilanteesi journalistina? Millaisista turvallisuuteen ja tietoturvaan liittyvistä asioista olet itse huolissasi? Onko tässä tapahtunut muutoksia työurasi aikana?

C. Riskitilanteet ja niiden käsittely

4. Oletko kohdannut työssäsi tilanteita, joissa olet ollut huolissasi tietoturvastasi tai tilanteissa, joissa olet kokenut turvattomuutta?
    - Millaisia huolia tai tapauksia nämä ovat olleet?
    - Milloin ja millaisten aiheiden yhteydessä nämä ovat tapahtuneet?
    - Miten toimit tilanteessa? Miten pyrit varmistamaan tietoturvasi ja turvallisuutesi?
    - Miten osasit turvautua näihin toimiin? Pyysitkö apua tai tukea, tai antoiko joku sinulle sitä? Miten tiedotusvälineesi/työnantajasi toimi tilanteessa? Tunsitko, että sinulla oli riittävät valmiudet tilanteen hoitamiseen? Mitä muuta tukea olisit kaivannut?

    A. Tuleeko mieleesi tapauksia, joissa olisit ollut huolissasi fyysisestä turvallisuudestasi tai muuten fyysisiin turvallisuusuhkiin liittyviä tapauksia (henkilökohtainen turvallisuutesi, työpaikkasi, kotisi tai autosi turvallisuus jne.)
    B. Tuleeko mieleesi tapauksia, joissa olisit ollut huolissasi tietoturvasta liittyen a) viestintään lähteiden ja kollegoiden kanssa, b) tietojen ja dokumenttien säilyttämiseen ja jakamiseen, tai c) tietotekniikkaan ja sen käyttöön kuten laitteisiin, kuten puhelimiin, tietokoneisiin, verkkokäyttöön, salasanoihin.

D. Turvakäytännöt ja niiden käyttöönottoon ja hyödyntämiseen liittyvät haasteet

5. Tietoturvan ja turvallisuuden edistämiseen voidaan käyttää lukuisia erilaisia välineitä ja käytäntöjä. Niiden käyttö ei kuitenkaan ole yleensä tarpeen kaikissa tapauksissa. Millä tavoin teet yleensä päätöksiä siitä, millaisia turvakäytäntöjä kulloinkin on tarpeen hyödyntää?

    - Esitietokyselyssä ilmoitit, että hyödynnät tiettyjä välineitä ja käytäntöjä säännöllisesti, muttet aina. Miten päätät sen, milloin näiden käyttö on perusteltua?
    - Esitietokyselyssä ilmoitit, että olet kokeillut tiettyjä välineitä ja käytäntöjä, muttet käytä niitä säännöllisesti. Miksi olet päätynyt näiden osalta tällaiseen ratkaisuun)
    - Esitietokyselyn perusteella on tiettyjä välineitä ja käytäntöjä, joista olet kuullut, mutta et ole itse kokeillut niitä. Miksi et ole kokeillut näitä?

6. Mitkä ovat yleisimpiä haasteita turvakäytäntöjen (digitaaliset ja fyysiset) käyttöönottamisessa? Mitkä olleet sinun kohdallasi merkittävimpiä hankaluuksia ja esteitä? Miten olet pyrkinyt selättämään näitä haasteita?

E. Tuen saaminen

7. Koetko, että sinulla on riittävät tiedot ja taidot tietoturvasi ja fyysisen turvallisuutesi takaamiseksi? Millä osa-alueilla koet näin ja millä et? Mitä kautta olet oppinut turvakäytännöistä ja saanut tietoa niistä?
8. Miten arvioisit sitä tukea, jota olet saanut tiedotusvälineeltäsi/työnantajaltasi tietoturvaan ja turvallisuuteen liittyen? Mitä tiedotusvälineeltäsi/työnantajaltasi tekee sinun suojelemiseksesi? Koetko tämän tuen riittävänä? Koetko, että tässä olisi muutettavaa tai parannettavaa?
    - Oletko koskaan osallistunut työnantajasi tarjoamaan turvallisuuskoulutukseen? Mihin tämä koulutus keskittyi? Koitko sen hyödyllisenä? Millaista koulutusta itse kaipaisit?
    - Onko toimituksessanne tai tiedotusvälineelläsi/työnantajallasi turvallisuusohjeita tai toimintatapoja riskitilanteissa? Mitä mieltä olet niistä?

F. Lisättävää?

9. Onko sinulla mitään lisättävä tai täsmennettävää tietoturvaan, turvallisuuteen ja/turvakäytäntöihin liittyen? Onko mielessäsi mitään ajatusta, näkökulmaa tai aihetta, joista emme ole vielä keskustelleet?

English abstract

Risk Perceptions and Safety and Information Security Practices among Finnish Investigative Journalists

Investigative journalism is widely acknowledged as a high-risk form of reporting, with practitioners facing distinct safety and information security threats. This study examines the perceptions of work-related risks among Finnish investigative journalists and explores their safety and information security practices. Additionally, it investigates how journalists assess the need for safety and security practices in various situations, how they acquire knowledge and skills related to these practices, and barriers to adoption. The research material comprises thematic interviews with 12 Finnish investigative journalists, supplemented by data collected from pre-interview survey questionnaires. Findings indicate that Finnish investigative journalists are particularly concerned about source protection. They exercise significant autonomy in determining which safety and security practices to implement, often relying on individual case-by-case risk assessments. Responsibility for learning and maintaining skills related to safety and security commonly falls on the journalists themselves, although information and support are also shared collegially within the investigative journalism profession.

Key words: Journalism (profession), investigative journalism, safety, information security, security practices

Kirjoittaja

Ilmari Hiltunen, YTT, tutkijatohtori
Ilmari Hiltunen on journalistiikan tutkijatohtori Tampereen yliopiston Informaatioteknologian ja viestinnän tiedekunnassa. Hän on aikaisemmin tutkinut journalisteihin kohdistuvaa ulkoista vaikuttamista sekä suomalaista vasta- ja vaihtoehtomediaa. Hiltusen nykyinen tutkimusprojekti (2022–2024) käsittelee journalistien kohtaamaa häirintää ja uhkailua sekä näiden ilmiöiden vaikutuksia toimittajakunnan arjessa.