

“Tämä koskettaa meitä kaikkia”:

Vastaamon tietomurto ja luottamuksen menetyt

Mari-Luisa Mäki

Valtiotieteellinen tiedekunta

Sosiologia

Maisterintutkielma

Helsingin yliopisto

Toukokuu 2022



Tiedekunta – Fakultet – Faculty Valtiotieteellinen tiedekunta		Koulutusohjelma – Utbildningsprogram – Degree Programme Sosiaalitieteiden maisteriohjelma	
Tekijä – Författare – Author Mari-Luisa Mäki			
Työn nimi – Arbetets titel – Title “Tämä koskettaa meitä kaikkia”: Vastaamon tietomurto ja luottamuksen menetys			
Oppiaine/Opintosuunta – Läroämne/Studieinriktning – Subject/Study track Sosiologia			
Työn laji – Arbetets art – Level Maisterintutkielma		Aika – Datum – Month and year 05/2022	Sivumäärä – Sidoantal – Number of pages 74 + 11
<p>Tiivistelmä – Referat – Abstract</p> <p>Tutkielma käsittelee luottamuksen menetystä digitaalisen kriisin seurauksena. Kyseessä on tapaustutkimus, jossa aihetta tarkastellaan psykoterapiakeskus Vastaamon tietomurron jälkeisen mediaviestinnän kautta. Tämä laaja tietomurto- ja kiristystapaus tuli julkisuuteen lokakuussa 2020. Kymmeniä tuhansia arkaluonteisia henkilötietoja levisi julkisuuteen Vastaamon puutteellisen tietosuojan takia. Tutkielmassa tapausta lähestytään riskiyhteiskunnan näkökulmasta, tarkastellen luottamuksen ja epävarmuuden merkitystä ja vuorovaikutusta digitaalisessa ympäristössä. Lisäksi teoreettisessa viitekehityksessä hyödynnetään kriisitutkimuksen teorioita. Tutkimuskysymysten avulla aihetta käsitellään kahdella eri tasolla. Ensimmäinen taso kohdistuu yritykseen, eli Vastaamon pyrkimykseen palauttaa luottamusta. Toinen taso on yhteiskunnallinen, jolla tarkastellaan tietomurron synnyttämiä uhkakuvia.</p> <p>Tutkielman aineistona toimii media-aineisto. Vastaamon tiedotteet edustavat yrityksen kriisiviestintää ja Ylen uutiset pyrkimystä yhteiskunnalliseen palautumiseen kriisistä. Analyysi toteutetaan aineistolähtöisesti, rajaten sen ajallisesti tietomurron julkitulosta Vastaamon konkurssiin. Vastaamon tiedotteita analysoidaan sisällönanalyysin avulla. Rivittäisen koodauksen jälkeen muodostetaan kaksi laajaa teemaa liittyen tekijöihin, jotka tiedotteissa esiintyvät luottamusta rakentavina tai haittaavina. Ylen uutisten avulla luodaan tapahtumien kulkua kuvaava aikajana, minkä lisäksi niille on tehty lähiluenta. Lähiluennassa nostetaan esille yhteiskunnallisia uhkakuvia, jotka asettuvat yhteiskunnan eri tasoille.</p> <p>Tutkielmassa havaitaan, että Vastaamo käytti tyypillisiä kriisiviestinnän keinoja pyrkiessään tilanteenhallintaan. Luottamusta pyrittiin palauttamaan viestimällä läpinäkyvästi, korostamalla tehtyä yhteistyötä asiantuntijatahojen kanssa sekä osoittamalla resurssit uhrien auttamiseen ja tukemiseen. Yrityksen arvoja ja mainetta korostettiin samalla kun viestittiin lisätoimenpiteistä, jotka Vastaamo käynnisti tietomurron julkitulon jälkeen. Tietomurron digitaalinen ympäristö vaikeutti luottamuksen rakentamista, sillä siihen liittyi epävarmuutta tapahtuneesta, anastetut tiedot nousivat yhä uudelleen pinnalle ja Vastaamo kärsi taloudellisesta ahdingosta. Yhteiskunnalliset uhkakuvat liittyivät yksityisyyden menettämiseen, terveydenhuoltojärjestelmien mahdollisiin puutteisiin, tietomurron toistumiseen muissa yrityksissä ja huoleen luottamuksen menettämisestä niin terveydenhuollon palvelujen alalla kuin digitaalisessa yhteiskunnassa ylipäänsä. Lisäksi uutisten analyysissä nousi esille huoli siitä, ettei digitaalisista kriiseistä ole tarpeeksi tietoa ja ymmärrystä.</p> <p>Analyysin pohjalta Vastaamon tietomurto määritellään digitaalisesti suuronnettomuudeksi. Tutkielma osoittaa, että tietomurto on piirteiltään tyypillinen riskiyhteiskunnalle toteutunut uhka. Se vaikutti moneen eri tahoan ja vaati monimutkaisia yhteistyön verkostoja ratkaisujen löytämiseksi ja normaaliin palaamiseksi. Luottamusta pyrittiin palauttamaan niin yrityksen kuin yhteiskunnan tasolla, josta vain jälkimmäisessä onnistuttiin. Tutkielmassa nostetaan esille riskiyhteiskunnalle tavanomaisia piirteitä, joissa luottamus on jatkuvasti koetuksella. Samalla luottamus toimii tärkeänä keinona hallita epävarmuutta. Kyse ei lopuksi ollutkaan luottamuksen menettämisestä vaan digitalisaation tuomasta hallitsemattomuudesta. Tutkielman lopussa pohditaan luottamuksen ristiriitaisuutta digitaalisessa ympäristössä ja tietomurtoa varoittavana esimerkkinä digitalisaation ongelmakohdista.</p>			
Avainsanat – Nyckelord – Keywords tietomurto, digitaalinen yhteiskunta, riskiyhteiskunta, luottamus, tapaustutkimus			
Ohjaaja tai ohjaajat – Handledare – Supervisor or supervisors Minna Ruckenstein ja Anu Katainen			
Säilytyspaikka – Förvaringställe – Where deposited Helsingin yliopiston kirjasto, Helsingfors universitets bibliotek, Helsinki University Library			
Muita tietoja – Övriga uppgifter – Additional information			

Sisällys

1 Johdanto	1
2 Vastaamon tietomurron esittely	4
2.1 Tietomurtoon liittyvät tapahtumat Ylen uutisten mukaan	5
3 Aikaisempi tutkimus	10
3.1 Digitaalisen ajan riskiyhteiskunta	10
3.2 Luottamus ja epävarmuus	13
3.3 Kriisi ja kriisiviestintä	16
3.3.1 Kriisi ja media	17
3.3.2 Kriisinjälkeinen retoriikka luottamuksen palauttajana	18
4 Tutkimuskysymykset	19
5 Tutkimuksen toteutus	21
5.1 Tapaustutkimus	21
5.2 Aineisto	22
5.3 Sisällönanalyysi ja lähiluenta	24
5.4 Aineiston käsittely	25
6 Analyysi	27
6.1 Pyrkimys palauttaa luottamusta	27
6.1.1 Pyrkimys läpinäkyvyyteen	28
6.1.2 Yhteistyö ja asiantuntijatieto	30
6.1.3 Uhrit ja asiakkaat edellä	32
6.1.4 Vastaamon panos ja viestintä vakaasta tilanteesta	33
6.1.5 Jaettujen arvojen korostaminen	36
6.2 Luottamusta ja tilanteenhallintaa haittaavat tekijät	38
6.2.1 Rikoksen tyyppi	39
6.2.2 Epävarmuus	40
6.2.3 Avointa viestintää rajoittavat tekijät	41
6.2.4 Vastaamon sisäinen konflikti	41
6.2.5 Tietomurron seuraukset	42
6.3 Poikkeuksellisuus	43

6.4 Yhteiskunnalliset uhkakuvat	44
6.4.1 Tietomurron uhrit – “kuin löysässä hirressä”	45
6.4.2 Varoittava esimerkki: Vastaamo	48
6.4.3 Terveysthuollon sektori ja valvonta – kyseenalaistetut tahot	50
6.4.4 Muut digitaaliset palvelut ja kriisien auttajat – kriisin dominoefekti	53
6.4.5 Yhteiskunnallinen taso – digitaalisen ympäristön kauaskantoiset uhat	56
7 Pohdinta – Vastaamo digitaalisen yhteiskunnan laineilla	60
7.1 Vastaamon pyrkimys palauttaa luottamusta kriisiviestinnän keinoin	60
7.2 Tietomurron uhkakuvat – hallitsemattomuus digitaalisessa riskiyhteiskunnassa	62
8 Lopuksi – miten luottaa hallitsemattomaan?	66
Lähteet	72
Liitteet	75
Liite 1. Lista Vastaamon tiedotteista	75
Liite 2. Lista käytetyistä Ylen uutisista	76
Liite 3. Lisäksi aikajanassa käytetyt Ylen uutiset	84

1 Johdanto

Riskiyhteiskunnassa kaiken toiminnan ja vuorovaikutuksen ytimessä on luottamus. Se koskettaa niin yksilöitä kuin organisaatioita ja tekee yhteiskunnan olemassaolon mahdolliseksi. Luottamus on yksi tavoista hallita arjen riskejä ja epävarmuutta. Tähän mennessä Suomen suurin tietomurto toi silmiinpistävästi esille luottamuksen yhteiskunnallisen merkityksen. Psykoterapiakeskus Vastaamon tietomurto tuli julkisuuteen lokakuussa 2020, jolloin kymmeniä tuhansia Vastaamon asiakkaita lähestyttiin kiristysviesteillä. Kiristys kuului: ellei lunnaita makseta, asiakkaiden ja henkilökunnan arkaluontoisia potilas- ja henkilötietoja vuodetaan julkisuuteen. Seuraavien päivien aikana potilastietoja julkaistiin pimeässä verkossa. Digitaalinen yhteiskunta joutui kriisin keskelle, kun luottamuksen menetys paljasti sen merkityksen. Tuhannet psykoterapia-asiakkaat joutuivat erittäin vaikeaan tilanteeseen. Digitaalisessa ympäristössä tapahtuneella onnettomuudella oli pitkälle kantautuvia ja vakavia seurauksia ei-digitaalisessa todellisuudessa.

Tarkastelen tutkielmassani, miten Vastaamo on yrityksenä pyrkinyt palauttamaan luottamusta, sekä millaisia merkityksiä tietomurto sai mediavälitteisessä yhteiskunnallisessa keskustelussa. Toteutan työn laadullisena tapaustutkimuksena. Aineistona käytän Vastaamon nettisivujen tiedotteita ja Ylen uutisia. Van Dijckin (2014) mukaan yhteiskunnan digitalisaation kriittinen tutkimus on ehdottoman tärkeää ja tutkijoilla on merkittävä asema sosiaalisen luottamuksen rakentamisessa. Tutkimalla Vastaamon tietomurtoa pyrin osallistumaan tähän työhön. Tutkin digitaalista ympäristöä riskiyhteiskunnassa ja sitä, miten luottamus ja epävarmuus vaikuttavat sen toimintaan. Työ lisää ymmärrystä digitaalisen kriisin toiminnasta ja sen vaikutuksista laajemmin yhteiskunnassa. Pohdin työssä lisäksi digitaalisen yhteiskunnan ongelmakohtia ja mahdollisia ratkaisuja niihin. Tietomurto on esimerkki tapauksesta, jossa puutteellisella tietoturvalla on merkittäviä seurauksia sekä yksilöille että yhteiskunnalle. Luottamuksen ja riskiyhteiskunnan käsitteiden avulla tarkoitukseni on kytkeä tapahtumat laajempaan digitalisaatioon ja teknologian tutkimukseen liittyvään keskusteluun.

Riskiyhteiskunta on sosiologiaan ja modernisaatioon liittyvä käsite, joka nousi suosituksi 1980 ja 1990-lukujen aikana (Caplan, 2000). Riskiyhteiskunta on yhteiskunnallisen järjestäytymisen muoto, jossa organisaatioiden ja kansalaisten prioriteetiksi nousee tarve suojautua erilaisilta riskeiltä (Beck, 1992). Sen pääpiirteisiin kuuluvat epäily, epävarmuus ja teknologian tuomat riskit (Giddens, 1990, 1991; Beck, 1992). Riskiyhteiskunnan näkökulmasta on tutkittu erilaisia teknologian aiheuttamia riskejä, mutta nimenomaan digitaalisen teknologian riskejä on tutkittu vähemmän. Digitaalinen ympäristö on viimeaikainen teknologia, joka sopii riskiyhteiskunnan teoreettiseen kehykseen. Arjen digitalisaatio ulottuu monelle elämän osa-alueelle ja se on siirtänyt palvelut, vuorovaikutuksen, vapaa-ajan ja työn internetiin. Se on globaali ja siihen liittyy eri tason riskejä, jotka ovat pitkälti näkymättömiä. Näitä riskejä vastaan ovat muodostuneet turvallisuutta myyvät markkinat virustorjuntaohjelmien ja tietoturvan muodoissa. Digitaalista ympäristöä on tutkimassa ja kehittämässä laaja joukko asiantuntijoita ja heidän muodostamia asiantuntijajärjestelmiä. Toimiakseen sujuvasti se vaatii monen eri yhteiskunnallisen toimijan yhteistyötä. Tietomurto on yksi riskiyhteiskunnan riskeistä, joka Vastaamon tapauksessa toteutui.

Riskiyhteiskunnan lisäksi työni keskeisiä käsitteitä ovat luottamus, epävarmuus ja kriisiviestintä. Jotta kompleksinen yhteiskunta voisi toimia sujuvasti, on se riippuvainen kansalaisten luottamuksesta sen järjestelmiin. Luottamus on tärkeä väline, jolla käsitellään riskiyhteiskunnalle tyypillisiä epävarmuuden tunteita (Luhmann, 2017; Sztompka, 1999). Aikaisempi tutkimus luottamuksesta digitaalisessa ympäristössä painottuu yksilöiden kokemuksiin ja arjen käytäntöihin (esimerkiksi Pink, Lanzeni & Horst 2018 ja Steedman, Kennedy & Jones, 2020). Luottamuksesta on kuitenkin kirjoitettu myös yhteiskunnallisessa kontekstissa ja se on sovellettavissa digitaaliseen ympäristöön (Luhmann, 2017; Sztompka, 1999). Vastaamon tietomurto oli medioitunut kriisi, joten sitä koskevat käsitykset olivat jatkuvassa muutoksessa mediaviestinnän edetessä (Sellnow & Seeger, 2013). Tietomurto aiheutti epätavallisen tilanteen, jossa vaakaana ja luotettavana pidetyt yhteiskunnalliset rakenteet ja järjestelmät joutuivat koetukselle. Tutkielmani teoreettiset käsitteet liittyvät siis keskeisesti siihen, miten yhteiskunta toimii ja miten ymmärrämme sitä.

Yhteiskunnan digitalisaatiolla viitataan tässä tutkielmassa etenkin palvelujen digitalisoitumiseen. Suomen vuoden 2019 hallitusohjelmassa palveluiden digitalisaatio sekä teknologian hyödyntäminen palveluiden kehittämisessä ja uudistamisessa mainitaan useassa kohdassa (Valtioneuvosto, 2019, 73, 107–108, 160–161). Digitaalisten palveluiden kehitys on nopeuttanut niitä ja sähköiset järjestelmät voivat arkistoida vuosien tiedot. Potilastietojen kirjaaminen sähköiseen järjestelmään on helpottanut asiointia ja mahdollistanut tietojen helpon siirtämisen asiakkaiden muuttaessa tai asioidessa eri pisteissä. Digitaalisessa ympäristössä ja kehityksessä on kuitenkin vaaransa. Etenkin terveydenhuollon järjestelmissä säilytetään asiakkaiden henkilötietoja ja potilaskirjauksia, joiden päätyminen ulkopuolisten käsiin voi johtaa tietojen väärinkäyttöön ja vakaviin yksityisyyden loukkauksiin. Kyberhyökkäysten, hakkerointien ja tietovuotojen yleistyessä yritysten ja organisaatioiden tulee ottaa tietoturva entistä enemmän huomioon ja pitää se ajan tasalla. Täydellistä tietoturvajärjestelmää on kuitenkin käytännössä mahdotonta rakentaa.

Vastaamon tietomurto herätti julkista keskustelua tietoturvasta ja ihmisten luottamuksesta digitaalisiin alustoihin, jotka sisältävät heistä tietoja ilman, että he ovat niistä tietoisia tai pystyisivät niitä hallitsemaan. Ihmiset joutuvat jokapäiväisessä teknologian käytössään luottamaan siihen, että teknologia toimii odotusten mukaisesti. Heillä on hyvin rajoitetut mahdollisuudet, jos ollenkaan, vaikuttaa omien tietojen hallintaan, kun ne ovat kerran päätyneet verkkoon. Näin laaja tietomurto on Suomessa poikkeuksellinen tapaus, eikä vastaavanlaisesta tapauksesta ole vielä aikaisempaa tutkimusta Suomen kontekstissa. Edellinen verrattavissa oleva tietomurto tapahtui vuonna 2011. Kyseessä oli Itä-Suomen yliopiston ja Työtehoseuran järjestelmistä lähtenyt tietovuoto, jonka seurauksena yli 16 000 henkilön tietoja tuli julkisiksi. Tekijää ei koskaan saatu kiinni ja vuodetuilla tiedoilla tehtiin petoksia monta vuotta tietomurron jälkeen, mahdollisesti edelleen (Yle, 2017; 2021). Vastaamon tietomurrosta erityisen tekee laajuutensa lisäksi se, että tietovuodon uhreja olivat psykoterapiakeskuksen asiakkaat, joiden potilastiedot sisälsivät erittäin arkaluonteisia tietoja. Lisäksi niihin kohdistui kiristystoimintaa.

Aloitan työn esittelemällä Vastaamon tietomurron tapausta yksityiskohtaisemmin. Tämä antaa käsityksen tapahtuneesta tietomurron julkitulosta alkaen noin vuoden päähän siitä. Esittelen tämän jälkeen keskeisen kirjallisuuden ja teorian. Tutkimuskirjallisuus ulottuu sosiologian, viestinnän, teknologiatutkimuksen ja kriisitutkimuksen aihepiireihin. Nostan esille kaksi tutkimuskysymystäni, joista toinen keskittyy Vastaamon viestintään ja toisessa on puolestaan laajempi yhteiskunnallinen medianäkökulma. Sitä seuraa luku tutkimuksen toteutuksesta, jossa kuvailen käyttämäni aineiston ja menetelmän. Analyysin olen jakanut kahteen osaan. Ensimmäinen osa keskittyy Vastaamon pyrkimykseen palauttaa luottamusta ja toisessa osassa käyn läpi uutisissa esiin nousseita yhteiskunnallisia uhkakuvia. Tämän jälkeen yhdistän analyysin löydökset tutkimuskirjallisuuteen ja teoreettisiin viitekehyksiin. Lopuksi pohdin saamiani tuloksia ja niiden merkitystä yhteiskunnallisen hyödyn ja tulevan tutkimuksen kannalta.

2 Vastaamon tietomurron esittely

Psykoterapiakeskus Vastaamo tarjosi mielenterveyspalveluita eri toimipisteissä ympäri Suomea sekä verkkoyhteyden välityksellä etävastaanotoilla. Se perustettiin yksityisenä perheyrittäjänä vuonna 2008. Suomalaisen Työn Liitto oli myöntänyt Vastaamolle vuonna 2014 Yhteiskunnallinen yritys -kunniamerkin. Merkki kertoo yrityksen tuottavan yhteiskunnallista hyvää ja pyrkivän kestävän hyvinvoinnin rakentamiseen (Suomalaisen Työn Liitto, 2022). Vastaamo oli määritellyt yhteiskunnalliseksi tehtäväkseen psykoterapiapalveluiden paremman saatavuuden, sekä mielenterveyttä edistävän työn. Vastaamon sivujen mukaan yrityksellä oli vuonna 2020 18 000 potilasta ja se toimi 22 paikkakunnalla. Asiakkaista yli 2 000 henkilöä oli ohjattu Kansaneläkelaitoksen (Kela) kautta Vastaamon kuntoutusterapiapalveluihin ja 200 potilasta vaati-vaan lääkinälliseen kuntoutukseen. Yrityksellä oli töissä noin 400 terapeuttia. Kela oli tehnyt Vastaamon kanssa sopimuksen, jonka mukaan Vastaamo toimi palveluntuottajana. Lisäksi useampi eri alueiden sairaanhoitopiiri oli ohjannut potilaita Vastaamon psykoterapiapalveluihin ostopalvelusopimuksella. Tietomurto saattoi koskettaa kaikkia Vastaamon asiakkaita marraskuuhun 2018 mennessä ja osittain sen jälkeenkin. Yhteensä uhreja on arvioitu olevan yli 32 000.

2.1 Tietomurtoon liittyvät tapahtumat Ylen uutisten mukaan

Ensimmäinen tietomurto Vastaamon potilastietojärjestelmään tapahtui marraskuussa 2018 ja toinen tapahtui maaliskuussa 2019. Toisen tietomurron yhteydessä tietokanta tyhjennettiin ja jäljelle jätettiin kiristysviesti. Tiedossa ei ole oliko murtautuja sama vai eri henkilö. Kesäkuussa 2019 Vastaamon perustajat myivät 70 prosenttia yrityksen osakkeista lähes 10 miljoonalla pääomasijoittajan omistamalle Intera Partnersin holding-yhtiölle, PTK Midco Oy:lle. Ennen tätä Vastaamo oli perheyrittäjä, jonka toimitusjohtajana toimi Ville Tapio.

28. syyskuuta 2020 kiristäjä otti ensimmäistä kertaa yhteyttä Vastaamoon ja vaati lunnaita yritykseltä, lähestyen toimitusjohtajaa ja kahta muuta työntekijää kiristysviestillä. Hän uhkasi julkaista potilastietoja, ellei yritys suostu maksamaan bitcoineilla 450 000 euroa vastaavaa summaa. Hänen mukaansa hänellä oli 40 000 potilaan tiedot. Vastaamo ilmoitti asiasta poliisille ja tutkinta alkoi.

21. lokakuuta kiristäjä julkaisi 100 potilastietoa Torilaudan ja Ylilaudan keskustelufoorumeissa. Kiristäjä ilmoitti foorumeilla myyvänsä tiedot eteenpäin halukkaille. Nämä sivustot mahdollistavat anonyymien toiminnan salaamalla tietoliikenteen, eikä sivustojen käyttö ole itsessään rikollista. Mahdollisuus anonymiteettiin tekee kuitenkin sivustoista houkuttelevia rikolliseen toimintaan. Samana päivänä tietomurto tuli ilmi julkisuudessa. Tässä vaiheessa Vastaamo ei ollut vielä ilmoittanut siitä asiakkaille, joten suurin osa kuuli tietomurrosta valtavirtauutisista. Illalla Vastaamo lähetti ensimmäisen tiedotteen asiakkailleen.

23. lokakuuta kiristäjän arveltiin vahingossa julkaisseen kaikki potilastiedot Tor-verkossa. Verkkoon oli ilmestynyt isokokoinen tiedosto, jonka koko sisällön tai osan siitä muut käyttäjät ehtivät lataamaan. Tähän mennessä kiristäjä oli julkaissut 300 potilastietoa. Muut käyttäjät, jotka saivat ladattua tiedoston, varmistivat sen sisältävän anastettuja tietoja. Tietoja alettiin julkaisemaan ja myymään eteenpäin. Potilastiedot lähtivät leviämään ja alkuperäinen kiristäjä menetti tietojen hallinnan. Pian tiedoston julkaisun jälkeen vuotosivu kaatui ja lakkasi toimimasta tuntemattomasta syystä.

24. lokakuuta Vastaamon asiakkaat alkoivat saamaan lunnasvaateita sähköpostitse. Ei ole tietoa siitä, oliko kiristyksen takana alkuperäinen kiristäjä vai muu käyttäjä, joka oli saanut haltuunsa potilastiedot. Lunnasvaatimukseen kuului bitcoineja 200 euron edestä, jos uhri maksoi vuorokauden sisään. Summa nousi 500 euroon uhrin maksaessa kolmen vuorokauden sisällä. Kiristäjä lupasi poistaa tiedot, jos uhri maksoi lunnaat. Jos maksua ei toteutettu, kiristäjä puolestaan uhkasi julkaista tiedot. Ylen tietojen mukaan ainakin 14 ihmistä maksoivat lunnaat.

25. lokakuuta Keskusrikospoliisi (KRP) piti tiedotustilaisuuden Vastaamon tietomurrosta. Siinä vaiheessa tuhannet ihmiset olivat tehneet asiasta rikosilmoituksen. Tiedotustilaisuuden aikana uhreille annettiin ensimmäisiä toimintaohjeita tietojensa turvaamiseksi. Ohjeistus koski myös havaintoja arkaluontoisesta aineistosta, sillä tietojen käsittely on itsessään rikos. Rikostutkinta ja eri tahojen selvittelyt Vastaamon omasta toiminnasta ja tietosuojasta alkoivat. Asiantuntijoita, yksityisiä terapeutteja ja kolmannen sektorin mielenterveysapua tarjoavia henkilöitä haastateltiin. Sisäministeri Maria Ohisalo pyysi ministeriryhmän koolle asian tiimoilta. Presidentti Sauli Niinistö kommentoi tietomurtoa Ylen haastattelussa.

26. lokakuuta Vastaamo erotti toimitusjohtaja Ville Tapion. Yhtiön mukaan Tapio oli salannut jälkimmäisen tietomurron puolentoista vuoden ajan. Tapio väitti myöhemmin, etteivät Vastaamon tietosuojasta vastaavat työntekijät olleet ilmoittaneet hänelle tietomurrosta, eikä hänellä ollut asiasta tietoa. Vastaamon ostanut pääomasijoittaja nosti syytteen esittäen, ettei kauppooja olisi tehty, jos tietomurto olisi ollut tiedossa. 26. päivä tuli ilmi, että myös Vastaamon terapeutit olivat saaneet kiristysviestejä. Tietomurron uhreille avattiin viranomaissivusto, jolta löytyivät suositellut toimintaohjeet. Puoluejohtajat kommentoivat tietomurtoa.

27. lokakuuta Asiakastieto teki Vastaamon kanssa yhteistyötä, tarjoten uhreille maksuttomat turvapalvelut, joiden avulla voitiin ehkäistä tietojen hyväksikäyttöä. Samalla uutisten haastattelemat asiantuntijat nostivat esille Vastaamon tekemiä viestinnän ja tietosuojan virheitä. Hallitus alkoi selvittämään ratkaisuja uhrien tilanteeseen, kuten henkilötunnuksen vaihtamista. Samana päivänä kiristäjän asettama lunnaiden maksuaika umpeutui, mutta mitään ei tapahtunut.

28. lokakuuta poliisi oli saanut jo 15 000 rikosilmoitusta. Hallitus otti virallisesti kantaa tietomurtoon ja uhrien asemaan. Vastaamosta löytyi myös muita ongelmallisiksi todettuja toimintatapoja, kuten laskujen oheen kirjoitettuja henkilötunnuksia.

29. lokakuuta kiristäjä tyhjensi tilit, joille lunnaat oli maksettu. Poliisi yritti jäljittää kiristäjän kryptovaluutan liikkeiden avulla. Suojelupoliisi arvioi epätodennäköiseksi, että tietovuodon taustalla olisi valtiollisia toimijoita.

4. marraskuuta Helsingin kaupunki asetti Vastaamon palvelut ostokieltoon. Helsingin kaupunki oli hankkinut ostopalveluita yritykseltä, mutta päätti lopettaa sopimukset johtuen Vastaamon epäselvästä tietoturvatilanteesta. 5. marraskuuta Kela lopetti uusien asiakkaiden ohjaamisen Vastaamoon, sillä se ei saanut vastausta 23. lokakuuta lähetettyyn selvityspyyntöön Vastaamon tietoturvan tilasta.

Marraskuun aikana tuli tiputellen tietoja eri sairaanhoitopiireistä, joiden listoilta löytyi tietomurron uhreja. 9. marraskuuta tehtyjen rikosilmoitusten lukumäärä nousi 25 000:een. Samana päivänä liikenne- ja viestintäministeriö perusti eri alojen asiantuntijoista koostuvan työryhmän, jonka tarkoituksena oli arvioida kriittisten toimialojen tietoturvaa ja muutostarvetta. Henkilötunnuksen vaihtamisen helpottamista harkittiin ministeriöissä. Lopulta kuitenkin todettiin, että oli parempi panostaa juurisyöhyn, eli vahvaan tunnistautumiseen, joka voisi estää henkilötunusten väärinkäytön. 9. marraskuuta Heini Pirttijärvi aloitti Vastaamon hallituksen puheenjohtajana ja väliaikaisena toimitusjohtajana.

Melkein kuukausi tietomurron julkitulon jälkeen Vastaamon asiakkaat odottivat edelleen mahdollisuutta tarkistaa potilastietorekisterinsä, johon heidän tietonsa kirjattiin hoidon aikana. Vastaamo otti käyttöön sähköisen järjestelmän 16. marraskuuta.

18. marraskuuta Sosiaali- ja terveysalan lupa- ja valvontaviranomainen Valvira teki tarkastuksen Vastaamoon liittyen potilasturvallisuuteen ja potilastietojärjestelmän valvontaan. Valvira totesi yrityksen korjanneen puutteet, eikä havainnut uusia. Tämän johdosta Kela päätti jälleen ohjata asiakkaita Vastaamoon.

Joulukuussa poliisin tutkinta eteni. Tapauksen rikosnimikkeitä olivat törkeä tietomurto, törkeä kiristys ja törkeä yksityiselämää loukkaavan tiedon välittäminen. Syyllisiä etsittiin Vastaamon omista työntekijöistä ja poliisi teki koti- ja laite-etsintöjä. Poliisi epäili kahta Vastaamon tietojärjestelmistä vastuussa ollutta työntekijää tietosuojarikoksesta. Tapauksen tutkinta ulottui myös Suomen ulkopuolelle. Ketään ei kuitenkaan otettu kiinni.

5. Tammikuuta 2021 Vastaamon pääomistaja Intera Partners teki poliisille tutkintapyynnön yrityskaupasta. 9. tammikuuta Vastaamon hallitus kutsui yhtiökokouksen kokoon arvioidakseen yrityksen tulevaisuutta huonontuneen taloudellisen tilanteen valossa. Hallitus erosi sovittuaan asiasta.

20. tammikuuta Kela ilmoitti purkavansa sopimuksensa Vastaamon kanssa. Kelan tekemässä tarkastuksessa tuli ilmi, että kaikki Vastaamon terapeutit eivät vastanneet vaativan lääkinnällisen kuntoutuksen yksilöterapian kilpailutuksessa asetettuja vaatimuksia. Sopimusten purkamisella oli vaikutusta noin sadalle asiakkaalle.

22. tammikuuta julkaistuihin oikeuden asiakirjoista selvisi, että Vastaamon potilastietokanta oli saattanut olla suojaamatta ilman palomuuria avoimessa verkossa puolentoista vuoden ajan.

26. tammikuuta Heini Pirttijärvi erosi tehtävästään.

27. tammikuuta 2021 potilastiedot ilmestyivät jälleen Tor-verkkoon. Niitä oli tällä kertaa 32 000. Tämän jälkeen poliisille saapui vielä noin sata rikosilmoitusta.

29. tammikuuta Vastaamo asetettiin selvitystilaan. Selvitystilan tarkoituksena oli arvioida taloudellista tilannetta. Käytännössä se mahdollisti osakeyhtiön purkamisen, vaikka yritys ei ollut konkurssissa. Selvitysmies alkoi etsimään Vastaamolle ostajia. Terapiatoiminta jatkui normaalisti.

11. helmikuuta Vastaamo haki konkurssiin. Yrityksen varojen määrä oli selvitysmiehen mukaan 2,2 miljoonaa ja velkoja oli kertynyt yli 5,9 miljoonan edestä. Ostajaksi löytyi Verve Terapia Oy, jonka omistaja on KK-Verve Oy.

1. maaliskuuta toteutui hallinnonluovutus ja toiminta jatkui Vervessä. Vaikka osa asiakkaista siirtyi Vervelle, heidän potilastietojaan ei siirretty. 10. huhtikuuta Vastaamon potilastiedot siirrettiin Kelan arkistoon.

19. huhtikuuta Valvira esitti, että Vastaamo laiminlöi velvollisuuksiaan ja epäonnistui omavalvonnassa. Tämä perustui Vastaamon antamiin kirjallisiin selvityksiin. Puutteet koskivat johtajalle säädettyjen tehtävien hoitamista sekä potilasasiakirjojen käsittelyä.

20. kesäkuuta tietomurron uhreja rohkaistiin hakemaan vahingonkorvauksia oman harkinnan mukaan. Korvauksia pystyi hakemaan konkurssipesästä 29. kesäkuuta asti. Korvauksissa otettiin huomioon henkisten kärsimysten lisäksi tietojen suojaamiseen ja luottokieltoihin menneet kulut sekä mahdolliset taloudelliset vahingot, jotka johtuivat tietojen väärinkäytöstä, kuten pikavipeistä tai luoton nostamisesta. Jos rikostutkinta etenisi syyllisen kiinni saamiseen asti, pystyisi korvauksia hakemaan myös rikolliselta. Utisoinnissa todettiin, että korvaukset tulisivat olemaan todennäköisesti vähäisiä asianosaisten suuren määrän takia. Poliisi aloitti uhrien kuulemisen syksyllä.

18. elokuuta poliisi kertoi tutkivansa Tor-verkkoon ilmestynyttä hakukonetta, jonka avulla pystyi etsimään vuodetusta tietokannasta tietoja Vastaamon asiakkaista.

9. lokakuuta konkurssipesä arvioi asiakkaiden vahingonkorvauksia. Arvion mukaan yksityishenkilöt pystyivät enimmillään saamaan 2 500 euron korvaukset. Ensin konkurssipesästä kuitenkin maksettaisiin velkojille, kuten pankeille, joten yksityishenkilöiden korvaukset jäisivät vähäisiksi. 17. marraskuuta vaikutti todennäköiseltä, että uhrien korvaukset jäivät alle sadan euron, jos sitäkään. Konkurssipesän varoiksi arvioitiin 1,4 miljoonaa, kun taas velkoja oli 23 miljoonaa.

27. lokakuuta uutisoitiin asiakastietolain uudistuksesta, jonka mukaan yksityisiä terveydenhuollon palveluja liitetään entistä enemmän Kanta-palveluun, joka takaisi paremman potilastietosuojan. Uhrien kuuleminen aloitettiin sähköisesti poliisin luomalla alustalla. Poliisin mukaan laajaa tietojen väärinkäyttöä ei havaittu. Tutkinta jatkuu edelleen.

16. joulukuuta tietosuojavaltuutettu määräsi GDPR-lainsäädännön mukaisesti Vastaamolle 600 000 euron seuraamusmaksun erittäin vakavista tietoturvaluotteluista. Määräyksen mukaan henkilötietoja ei oltu asianmukaisesti suojattu luvattomalta ja lainvastaiselta käsittelyltä. Yritys oli rikkonut tietosuojasetuksia, mistä se sai huomautuksen. Lisäksi Vastaamon olisi pitänyt ilmoittaa tietomurrosta asiakkaille aikaisemmin. Tietosuojavaltuutetun mukaan rikkomukset olivat olleet pitkäkestoisia ja huolimattomuus törkeää.

3 Aikaisempi tutkimus

3.1 Digitaalisen ajan riskiyhteiskunta

Tässä tutkielmassa käsitelen tietomurtoa riskiyhteiskunnan näkökulmasta. Sosiologit Ulrich Beck, Anthony Giddens ja Zygmunt Bauman tunnetaan kyseisen aiheen teoreetikoina. Beck on kirjoittanut riskiyhteiskunnan ohessa teknologian uhista, riskin käsitteestä ja refleksiivisestä modernisuudesta (1990, 1992). Teknologialla Beck ei tarkoita digitaalista teknologiaa, vaan laajemmin erilaisia keksintöjä ja koneita. Esimerkiksi Beckin vuonna 1992 ilmestyneessä kirjassa *Risk Society* teknologiaa edustavat kemikaalit. Beckin ajatukset sopivat kuitenkin sovellettavaksi myös digitaalisen teknologiaan, mihin palaan työn loppupuolella. Lahti (1998, 140) tiivistää sosiologien näkemykset riskiyhteiskunnasta kahteen osaan: teknologia tuo mukanaan riskejä, jotka päätyvät muokkaamaan yhteiskuntaa, ja nämä riskit voidaan nähdä sekä positiivisina että negatiivisina.

Beck määrittelee riskin “järjestelmällisenä tapana käsitellä modernisaation tuomia vaaroja ja epävarmuuksia” (1992, 21). Riskit eroavat Beckin mukaan esimoderneista vaaroista sillä, että ne juontuvat modernisaation tuomasta muutoksesta ja epäilyksen globalisaatiosta (1992, 21). Riski, luottamus ja epävarmuus ovat vahvasti toisiinsa linkittyneitä käsitteitä. Muiden tutkijoiden tekemien määritelmien mukaan riskeissä on kyse potentiaalisesta menetyksestä tai epävarmuudesta liittyen siihen, miten uskomme tilanteen kehittyvän (Luhmann, 1993, 21–26; Lahti, 1998, 184; Sellnow & Seeger, 2013, 189). Tässä työssä en erottele termien riski, vaara ja uhka välillä, vaan käytän niitä synonyymeinä.

Riskiyhteiskuntakeskustelu liittyy vahvasti modernisaatioon, jonka käsitän giddensiläisittäin Euroopassa 1600-luvulla alkaneena ilmiönä, joka liittyy sosiaalisen elämän malleihin (Giddens, 1990, 1). Beck (1992, 13) käsittää modernisaation riskien luonteen muutoksena. Esimodernit riskit eivät olleet ihmisten hallittavissa, kuten esimerkiksi luonnonilmiöt. Tämän jälkeen teollisuusyhteiskunta toi mukanaan rajatumpia riskejä, kuten liikenteeseen tai työhön liittyvät riskit. Nyky-yhteiskunnassa riskit ja vaarat ovat lähempänä jokaista yksilöä, ne ovat laajoja mittasuhteiltaan, niistä ollaan tietoisempia, mutta yksilöt ovat verrattain avuttomia niiden edessä. (Beck, 1992, 22.) Näitä riskejä ovat esimerkiksi luonnon saastuminen, ilmastonmuutos ja ydinsodat. Digitaaliset teknologiat ja media tiedottavat joka tunti uusista tapahtumista ja mahdollisista vaaroista. Tiede, media ja teollistuminen tuottavat riskejä lisäämällä tietoisuutta niistä (Giddens, 1990, 84; Beck, 1992, 32). Ihmisten käsitykset vaarasta ovat muuttuneet, eli arki ei ole välttämättä muuttunut modernisaation myötä vaarallisemmaksi. Ihmisten käsitys riskeistä on Beckin mukaan enemmänkin sosiaalisesti rakennettu, kuin faktoihin ja tieteeseen perustuvaa (Beck, 1992, 32). Siinä missä aikaisemmin ihmisiä yhdisti luokkaidentiteetti, Beck näkee, että riskiyhteiskunnassa yhteisinä tekijöinä ovat ihmisten kokema pelko ja ahdistus riskejä kohtaan ja yhteinen tarve suojautua niiltä (Beck, 1992, 49). Sekä Beckin (1992) että Giddensin (1994) mukaan nykyajan vaarat ovat kuitenkin yhä useammin ihmisten itsensä valmistamia ja toteutukseen hyvin tuhoisia laajalla mittakaavalla. Vaarat liittyvät ihmisten itsensä luomaan teknologiaan. Syntyy riskien sykli, jossa uuden teknologian avulla saatetaan yrittää estää jo käyttöön otetun teknologian aiheuttamia riskejä.

Riskiyhteiskunnan vaarat eivät ole rajattuja ajan tai paikan mukaan, eikä riskejä voi välttää. Elämän ja yhteiskunnan ydinkysymykset pyörivät sen äärellä, miten riskejä voisi vähentää. (Beck, 1992, 22; 29–30.) Riskejä ja vaaroja ei voi enää havaita aistein ja ne ovat näkymättömiä, mikä vahvistaa asiantuntijajärjestelmien tarvetta (Giddens, 1990, 83–84). Beckin (1992, 22) mukaan riskiyhteiskunnassa turvallisuutta valvovat viranomaiset ja instituutiot eivät kuitenkaan enää pysty hallitsemaan kaikkia riskejä kuten ennen, sillä niitä on yhä vaikeampi arvioida. Beck (1992) esittää, että yhteiskunnan täytyy oppia itsekriittiseksi (eli refleksiiviseksi) ja tunnistaa riskien aiheuttama epävarmuus, jotta riskien vähentämiseksi voidaan löytää ratkaisuja.

Asiantuntijajärjestelmiä ovat asiantuntemukseen pohjautuvia auktoriteettisia järjestelmiä. Ne vaativat ihmisten luottamuksen puolelleen toimiakseen (Giddens, 1990, 26; Luhmann, 2017, 58). Entistä tarkemman asiantuntijatiedon tarpeen lisääntyessä kokonaiskuva jää yhä enemmän hämärän peittoon. Giddensin (1991, 31) mukaan tämä aiheuttaa hallitsemattomuutta ja epävarmuutta. Lisäksi asiantuntijoidenkin piirissä on olemassa ristiriitoja, joten tieto näyttäytyy entistä epävarmemmalta ja alati muuttuvalta, lisäten maallikkojen epäilyä (Beck, 1992, 72–73). Jotta elämä voisi kuitenkin jatkua, eikä yksilöiden elämä pysähtyä riskien valtavan määrän takia, tulee ihmisten uskoa ”sokeasti” asiantuntijajärjestelmiä (Giddens, 1991, 141). Riskien arvioimisesta tulee jaettu osa arkea.

Bauman (1993) esittää kritiikkiä Beckin riskiyhteiskuntateoriaa kohtaan, samalla täydentäen sitä. Hän muun muassa esittää, että tieto, jonka maallikot saavat riskeistä, vähentää heidän toimintamahdollisuuksiaan sen sijaan että lisääisi niitä. Tämä perustuu siihen, että tiedon tullessa lähelle yksilöä, siitä tulee jokaisen yksilöllinen ongelma sen sijaan, että sitä käsiteltäisiin yhteiskunnallisena, kollektiivisena ongelmana. Riskien välttäminen jää jokaisen omalle vastuulle, jolloin myös syyllisyys kohdistuu yksilöihin. Samalla Bauman (1993) muistuttaa, miten yhteiskunnalliset vaarakuvat synnyttävät markkinaraon, joka tarjoaa vakuutuksia, palveluja, lääkkeitä ja esineitä, jotka suojaavat riskeiltä, siirtävät vastuuta ja minimoivat vaaran.

Bauman esittää, että vaikka tieteellä ja teknologialla on roolinsa riskien ja uhkakuvien päihittämisessä, ne samalla ylläpitävät vaaroja tuottavaa koneistoa jakamalla niistä tietoa (1993, 206–207). Baumanin mukaan teknologiaa täytyy ajatella pitkällä tähtäimellä: tulevaisuuden mielikuvissa tulisi ottaa huomioon asioita, jotka eivät ole vielä tapahtuneet. Tämä toimii keinona hallita epävarmuutta ja aidosti hyväksyä se osana elämää.

3.2 Luottamus ja epävarmuus

Niklas Luhmann tunnetaan sosiologina, jonka luottamusta käsittelevät työt ovat raivanneet tietä seuraaville tutkijoille. Kirjassaan *Trust and Power* (alkuperäispainos 1973, uudistettu painos 2017), Luhmann käsittelee luottamusta yhteiskunnan lisääntyvän monimutkaisuuden, epävarmuuden ja riskien täyttämässä kontekstissa. Luhmannin mukaan luottamuksen merkitys voimistuu modernisaation myötä entisestään. Myöhemmin Giddens (1990, 1991) sekä Beck ja Lash (1994) kehittivät Luhmannin teoriaa eteenpäin, esittäen luottamuksen ja sen häilymisen olevan yksi modernisaation pääpiirteistä. Beckin ym. (1994, 90) mukaan nykyajan rakenteet ovat lähes täysin riippuvaisia potentiaalisesti epävakaina luottamuksen mekanismeista. Tämän takia luottamus on tärkeä apuväline riskien ja epävarmuuden käsittelemiseen (Luhmann, 2017, 27; Sztompka, 1999, 40). Luottamuksen avulla pyritään vähentämään elämän monitahoisuutta ja tekemään elämän kaotisuudesta käsiteltävää (Luhmann, 2017, 27–33; 43, Sztompka, 1999, 21). Luottamuksen syntyminen vaatii paradoksaalisesti riskin, että se saatetaan rikkoa tai hyväksikäyttää: luottamusta pitää koetella, jotta se voidaan todeta aidoksi (Luhmann, 2017, 46–47; Clark, 2014, 19). Luhmannin mukaan luottamus kohdistuu aina tulevaan, joka sisältää monia eri mahdollisuuksia ja tapahtumia, joita emme voi ennalta nähdä (2017, 12; 15). Luottamus on siis yksi arjen sujumuuden ja jatkuvuuden perusedellytyksistä, sillä ilman luottamusta jokainen teko näyttäytyisi riskinä (Luhmann, 2017, 5).

Luottamusta käsitteenä on esitetty erittäin vaikeaksi analysoida, määrittellä tai tutkia (Luhmann, 2017, 6–9; Harper, 2014, 7–8). Sitä on verrattu muun muassa totuuden käsitteeseen, esittäen, että sen filosofinen luonne ei anna mahdollisuutta tutkia sitä tyhjentävästi (Clark, 2014). Selkeää yhtenäistä linjaa aiheesta ei ole muodoutunut (Harper, 2014, 7). Harper osoittaa kuitenkin piirteitä, joka vaikuttaa olevan läsnä luottamukseen liittyvässä kirjallisuudessa: siinä yleensä käsitellään tilanteita, joissa luottamus ei ole läsnä, eli tutkitaan epäluottamusta tai luottamuksen menettämisen jälkeistä tilannetta (Harper, 2014, 10). Myös tässä tutkielmassa käsitellen tilannetta vasta siinä vaiheessa, kun luottamus on jo menetetty. Luottamuksen menettäminen ja sen puute voi käänteisesti tuoda esille sen merkityksiä ja tarkoituksia.

Sztompkan *Trust: A Sociological Theory* (1999) teos esittelee tutkimukseni kannalta hyödyllisiä sosiologisia näkökulmia luottamukseen. Sztompka määrittelee luottamuksen seuraavalla tavalla: ”luottamus on vedonlyöntiä muiden tahojen tulevista ehdollisista toimista” (Sztompka 1999, 25). Luottamuksessa on siis aina kyse vuorovaikutuksesta luottavan ja luotettavan tahon välillä. Clark puolestaan muotoilee luottamuksen näin: ”luottamus on suhde luottajan ja luotettavan välillä, jossa luottaja uskoo luotettavan toimivan luottajan hyväksi” (Clark, 2014, 17). Luottaja ei voi aina olla varma luotettavan kyvystä tai aikomuksesta toimia odotetusti, joten luottajan on käytettävä erilaisia tapoja arvioida luotettavuutta. Tämä tapahtuu muun muassa tiedon, kokemusten, kunnioituksen ja tunnereaktion kautta. Nämä tekijät ovat myös osa luottamuksen syntymisen edellytystä. (Clark, 2014.)

Luottamukseen liittyy siis aina odotus toiminnasta. Odotusten normalisaatio johtaa siihen, että luotettavaa tahoa pidetään vastuuvollisena. (Sztompka, 1999, 57). Esimerkiksi Vastaamolta odotettiin vastuunottoa, kun tuli ilmi, että yrityksen tietosuojassa oli puutteita. Sztompka (1999, 53–54) jaottelee odotukset kolmeen kategoriaan. Instrumentaaliseen luottamukseen liittyvät odotukset kuten toistuvuus, järkevyyt ja tehokkuus. Tietomurron jälkeen Vastaamon odotettiin toimivan järkevästi ja tehokkaasti, jolloin yritys olisi osoittanut olleensa kriisivalmiudessa. Vastaamon asiakaspalvelu kuitenkin ruuhkautui, eikä yritys ollut kehittänyt kätevää tapaa tarkistaa rekisteritietoja. Uhrit joutuivat pettymään tiedon saatavuuteen ja ohjeistukseen Vastaamon puolelta. Aksiologiseen luottamukseen liittyy puolestaan moraalisuus, empatia, reiluus ja rehellisyys. Vastaamolta odotettiin rehellisyyttä ja myötätuntoa tietomurron uhreja kohtaan. Kolmas luottamukseen perustuva odotus liittyy siihen, että vastuussa oleva taho asettaa itsensä takalalle ja toimii toisen hyväksi. Tämä edellytti Vastaamon asettavan yhtiön toiminnan toissijaiseksi ja keskittämään resurssit aiheutuneen vahingon korvaamiseen. Vaikka Vastaamo pyrki luomaan palveluita tietomurron uhreille ja auttamaan yrityksen oman taloudellisen edun kustannuksella, se toimi pikemminkin maineenhallinnan keinona kuin aidosti epäitsekäänä toimintana.

Tutkimukseni kannalta on olennaista, ettei Vastaamon tapauksessa luottamusta oltu etukäteen pohdittu – ihmisillä on tapana luottaa terveystalouteen ja luottamusta pidetään itsestäänselvyytenä. Elleivät asiakkaat olisi luottaneet yritykseen, he eivät olisi hakeutuneet sen asiakkaiksi. On myös otettava huomioon, että Suomessa luottamus instituutioihin, valtioon ja sairaanhoitoon on yleisestikin korkealla (Eurobarometer, 2009; Gaskell & Gottweis, 2011, 160). Van Dijk (2014) nostaa esille institutionaalisen luottamuksen. Hänen mukaansa käyttäjillä on tapana luottaa yhteiskunnan julkisiin tahoihin (kuten poliisi, terveydenhuolto tai akateeminen tutkimus) sen suhteen, että he eivät väärinkäytä heidän tietojansa (2014, 204). Kouvon ja Kankaisen (2009, 586) mukaan Suomessa vahva luottamus selittyy pohjoismaisen hyvinvointivaltion mallilla, jossa painottuu universaali sosiaalipolitiikka sekä laadukkaat palvelut.

Digitalisaatio on tuonut teknologian kuitenkin osaksi lähes kaikkia yhteiskunnallisia palveluja. Teknologian monimutkaisuuden lisääntyessä on todennäköistä, että löytyy alueita, joihin ei voi luottaa täysin tai teknologia pettää tavalla tai toisella (Sztompka, 1999, 12–13). Yhteiskunnan kehittyessä luottamus siirtyy yksittäisistä henkilöistä laajempiin ja abstrakteimpiin objekteihin, kuten organisaatioihin, systeemeihin ja teknologiaan (Giddens, 1991, 21). Pink, Lanzeni ja Horst (2018) tuovat esille ihmisten ja teknologian ristiriitaisen suhteen, jossa on selkeitä hyötyjä, mutta myös jatkuvia huolia sekä vaihtokauppoja, joita käydään henkilökohtaisen datan avulla. Pink ym. (2018, 5) kirjoittavat, että ”datan kanssa eläminen tarkoittaa elämistä epävarmuuden kanssa”. Niin pitkään kuin yksilöillä ei ole varmaa tapaa hallita tietojansa, tulee levottomuuden tunne olemaan läsnä.

Miten luottamusta sitten voidaan ylläpitää tai rakentaa digitaalisessa yhteiskunnassa? Sztompkan mukaan makrotason luottamusta voidaan rakentaa poliittisella päätöksenteolla ja linjausten asettamisella (Sztompka, 1999, 134–135). Tämä konkretisoitui Vastaamon tietomurron jälkiselvittelyissä, kun esimerkiksi asiakastietolakeja uudistettiin. Nopea kehitys, uudet teknologiat ja palvelujen muuttuvat muodot ovat kuitenkin haasteita kankeasti ja usein hitaasti tapahtuvalle sääntelylle.

3.3 Kriisi ja kriisiviestintä

Luottamuksen palauttaminen ja kriisiviestintä kulkevat käsi kädessä. Kriisinhallinnan teoreettinen kenttä liittyy pitkälti epävarmuuden hallintaan (Sellnow & Seeger, 2013, 188). Kriisiviestintäkirjallisuus usein kohdistuu suuren luokan poliittisiin kriiseihin, epidemioihin (kuten veden tai elintarvikkeiden saastumiseen) ja luonnonkatastrofeihin. Myös yritysten kriiseistä on paljon kirjallisuutta, etenkin erilaisten oppaiden muodossa. Digitaalisia kriisejä on käsitelty puolestaan vähemmän.

Tietomurron jälkeen toteutettiin kriisinhallintaa, jolla on ainakin neljä tehtävää: vaarojen lieventäminen, valmius auttaa uhreja, palautuminen ja hätätoimet (Lindell & Perry, 2004, 6–14). Kriisinhallintaan liittyy monenlaisten sidosryhmien yhteensovittaminen, yhteistyö ja mediavälitteinen tiedotus. Vuorovaikutuksellisesti tästä syntyy monimutkainen verkosto. (Sellnow & Seeger, 2013, 105.) Jotta tämä verkosto voisi toimia sulavasti, tarvitaan sidosryhmien välistä viestintää. Kriisiviestintä voidaan määritellä viestinnäksi, jossa kriisin kontekstissa jaetaan merkityksiä toisille osapuolille, tavoitteena estää ja vähentää kriisin aiheuttamaa vahinkoa. (Sellnow & Seeger, 2013, 14.) Sellnow ja Seeger (2013) painottavat kriisiviestinnän merkitystä nyky-yhteiskunnassa. Kriisit ovat luonnostaan odottamattomia ja ne tuovat mukanaan epävarmuutta, mutta niihin voidaan valmistautua ennalta luomalla toimiva kriisistrategia.

Kriiseillä on suuri voima muuttaa yhteiskunnan rakenteita (Sellnow & Seeger, 2013). Niillä on tapana olla yhteiskunnan sektoreiden ylittäviä tapahtumia, joiden käsittelyyn ja jälkipuintiin osallistuu erilaisia kriisivalmiudessa olevia toimijoita. Vastaamon tapauksessa näitä toimijoita olivat esimerkiksi kolmannen sektorin toimijat, jotka tarjosivat uhreille kriisiapua. Vaikka kriisitilanteet ovat usein uniikkeja, tietyt piirteet toistuvat kriisistä toiseen. Näitä ovat Sellnowin ja Seegerin (2013, 3) mukaan odottamattomuus, uhka, epävarmuus, tarve välittömään toimintaan ja apuun, sekä ajatus, että tapahtuma tulee toistumaan, joten tulevaisuutta varten tarvitaan keinoja vastaavien tapahtumien varalle. Kaikki nämä piirteet toteutuivat Vastaamon tietomurron kohdalla.

Kriisintutkimuksen alalla on ollut erimielisyyttä siitä, milloin voidaan puhua kriisistä. Esimerkiksi tapahtuman uhkaavuudella ja aiheutuneilla vahingoilla voidaan ajatella olevan merkitystä (Sellnow & Seeger, 2013). Coombs ja Holladay (2010, 640) ovat taas esittäneet pohjautuen Hermannin teokseen (1963), että kriisin ydin on siinä, että se loukkaa ja rikkoo vahvana pidettyjä olettamuksia sekä sidosryhmien välisiä suhteita. Sellnowing ja Seegerin (2013, 236) mukaan kriisit koskettavat tärkeitä sosiaalisia rakenteita ja arvoja, kuten turvallisuuden tunnetta, oikeudenmukaisuutta tai rehellisyyttä. Kyse voi olla myös ihmisten käsityksestä tilanteesta: tapahtumien esittäminen tietyllä tavalla muuttaa ihmisten näkemyksiä niistä (Sellnow & Seeger, 2013, 6).

3.3.1 Kriisi ja media

Median tavalla esittää kriisi on vaikutusta siihen, miten tapahtunutta käsitellään julkisuudessa, millaisia mielikuvia siitä syntyy ja kuinka näkyväksi tapahtuma muodostuu. Media ja uutiset lisäävät nopean uutissyklinä myötä kriiseihin aikasensitiivisen ulottuvuuden (Sellnow & Seeger, 2013, 30). Ne tiedottavat tapahtumista nopeasti ja laajasti. Media toimii portinvartijana organisaatioiden ja kansalaisten välillä, joka vaatii selvitystä heti kriisin puhjetessa, kun asioiden kulusta ei välttämättä ole vielä varmaa tietoa. Uhrien tarinat saavat yleensä runsaasti mediahuomiota. Medialla on myös iso rooli yhteisöllisyyden rakentamisessa ja kriisistä palautumisessa. (Sellnow & Seeger, 2013, 138–139.)

Tässä tutkimuksessa hyödynnän uutisten kehysteoriaa käsitellessäni tiedotteita ja uutisia. Kehystyksessä tietyt asiat nostetaan keskiöön, kun taas toiset jäävät pois. Organisaatiot pyrkivät tyypillisesti luomaan positiivista mainekuvaa, jonka media joko hyväksyy tai kehystää uudelleen. Kehystys johtaa suoraan organisaation mainekuvan syntymiseen. (Sellnow & Seeger, 2013, 140.) Hyödynnän myös fokusteoriaa tarkastellessani tietomurron jälkipuinnin tuottamia tuloksia. Fokusteorian avulla tutkitaan miksi jotkin kriisit nousevat uutisoinnin kohteeksi enemmän kuin toiset. Siinä keskitytään julkisen keskustelun sisältöihin, kuten syyllis(t)en etsintään,

kriisin ratkaisuihin ja kriisin aiheuttamiin poliittisten linjausten muutoksiin (Sellnow & Seeger, 2013, 143–145).

Korpiola (2011) käsittelee kirjassaan *Kriisiviestintä digitaalisessa julkisuudessa* mediamaisen nopeaa muutosta ja sitä, miten kriisin tapahtuessa tulisi toimia digitaalisessa julkisuudessa, painottuen organisaatioviestinnän näkökulmaan. Kyseessä on enemmänkin opas yrityksille, mutta teen siitä muutamia nostoja, sillä se tarjoaa näkökulman yrityksen kriisiviestinnästä digitaalisessa julkisuudessa. Kriisin sattuessa yrityksen viestintä ja sidosryhmäsuhteet häiriintyvät, jolloin kriisiviestintää tarvitaan palauttamaan yhteys ja luottamus ennalleen. Korpiola tiivistää näin: ”Ilman luottamuksen palauttamista ei ole maineen hallintaa” (2011, 49). Kriisiviestinnän epäonnistuessa, yritys kohtaa mainekriisin. Mainekriisin sattuessa organisaation tai sen edustavan henkilön maine tulee kyseenalaistetuksi julkisuudessa (Korpiola, 2011, 12). Iso kriisi voi aiheuttaa kielteistä mainetta myös koko toimialaan (Korpiola 2011, 49–50). Silloin yhden yrityksen mainekriisi voi vaatia kriisiviestintää kaikilta toimialan toimijoilta.

3.3.2 Kriisinjälkeinen retoriikka luottamuksen palauttajana

Kriisin jälkeen yrityksille ja organisaatioille syntyy tarve palauttaa luottamusta ja toteuttaa maineenhallintaa. Mediassa se tapahtuu kriisinjälkeisen retoriikan avulla. Sekä Vastaamon tiedotteet, että Ylen uutiset edustavat tätä retoriikkaa: toinen edustaa yrityksen ja toinen valtion. Sellnowin ja Seegerin (2013, 164) mukaan retoriikka vastaa tyypillisesti kolmeen asiaan: todisteiden hankintaan, tarkoituksenmukaisuuteen ja vastuuseen. Todisteiden hankinnassa tarkastellaan tapahtunutta eri näkökulmista, yrittäen päätellä annetun kuvan totuudenmukaisuutta. Esimerkiksi Ylen uutisissa pyydettiin eri asiantuntijoiden näkökulmia tapahtuneeseen. Tarkoituksenmukaisuudessa tutkitaan sitä, oliko tilanne estettävissä vai oliko se pikemminkin onnettomuus. Vastaamon tapauksessa kyseistä tutkintaa edustivat poliisi ja tietoturva-asiantuntijat, jotka selvittivät Vastaamon tietoturvaa. Vastuun kysymyksissä päätetään siitä, kuka tilanteessa on syyllinen, vai onko sellaista ollenkaan.

Hyödynnän Benoitin (ensipainos 1995, toinen painos 2014) mainekuvan korjauksen teoriaa käsitellessäni Vastaamon tiedotteita. Teoriaa on käytetty kriisintutkimuksen alalla runsaasti (Sellnow & Seeger, 2013, 172). Mainekuvaa on yleensä mahdotonta korjata tasolle, joka vallitsi ennen kriisiä. Ennen korjausten aloittamista organisaation tulee kysyä, mitkä käsitykset uhkaavat mainetta ja mille yleisölle maineen korjaus tulee osoittaa. (Benoit, 2014, 5; Sellnow & Seeger, 2013, 168.) Benoitin (2014) mukaan maineen korjaus sisältää viisi strategiaa, jotka ovat kieltäminen, vastuun hylkääminen, hyökkäysten torjuminen, korjaavat toimenpiteet ja häpeä. Tapahtuneen tai syytösten kieltämisen lisäksi kieltäminen voi myös olla vastuun siirtämistä toiselle taholle. Vastuun kieltämisessä hyväksytään tapahtunut, mutta kielletään organisaation vastuu siitä. Hyökkäysten torjuminen tapahtuu väheksymällä tapahtunutta, hyökkäämällä syyttävää tahoa kohtaan tai korvaamalla vahingot. Korjaavien toimenpiteiden tulee mennä pelkkiä korvauksia pidemmälle. Silloin pyritään palauttamaan kriisiä edeltänyt normaali ja luvataan estää tapahtumaa toistumasta (Benoit, 2014, 26; Sellnow & Seeger, 2013, 170). Häpeän strategia eroaa kaikista muista niin, että siinä organisaatio hyväksyy täysin tapahtuneen ja oman vastuunsa, pyytäen anteeksiantoa. Anteeksiannon saamista varten on hyväksyttävä vastuu. Häpeän strategiassa organisaatio pyrkii aidosti auttamaan ja korvaamaan vahingot uhreille (Benoit, 2014, 26; Sellnow & Seeger, 2013, 170.) Benoitin teoriaa on kritisoitu siitä, että se kertoo miten organisaatiot voivat välttää ansaitun rangaistuksen (Sellnow & Seeger, 2013, 172). Samantyyppisiä strategioita esitetään esimerkiksi kriisiviestinnän oppaissa (esimerkiksi Korpiola, 2011). Strategian ideana ei kuitenkaan ole Benoitin mukaan piilotella asioita ja hämätä yleisöä, vaan viestiä rehellisesti ja avoimesti jos organisaatio on tehnyt virheitä tai toiminut epäeettisesti (Benoit, 2014, 38; Sellnow & Seeger, 2013, 172).

4 Tutkimuskysymykset

Lähestyn tutkimusaiheeni luottamuksen ja kriisiviestinnän näkökulmasta, joiden taustana toimivat digitaalinen ympäristö ja riskiyhteiskunta. Pohdin työssä luottamuksen ja digitaalisen ympäristön vuorovaikutusta ja luonnetta. Nostan samalla digitaalisen kriisin erityispiirteitä esiin. Vastaamon tietomurto yhdistyy laajempaan yhteiskunnalliseen kontekstiin tietomurron

seurausten ja mediakeskustelun kautta. Mediakeskustelu liittyy riskiyhteiskuntaan ja tietomurron aiheuttamiin uhkakuihin.

Näiden teoreettisten viitekehysten sekä tutkimusaiheen pohjalta tutkimuskysymykseni muodostuvat kahdesta eri näkökulmasta.

1. Miten Vastaamo pyrki palauttamaan luottamusta?
2. Minkälaiseksi uhkaksi tietomurto määrittyi yhteiskunnallisessa keskustelussa?

Ensimmäinen kysymys on suppeampi ja kohdistuu Vastaamon viestintään. Tämän tason avulla syvennyn kriisiviestinnän ja luottamuksen ulottuvuuksiin. Hyödynnän kriisiviestinnän ja kriisinjälkeisen retoriikan malleja. Pyrin erottelamaan konkreettisia kriisinhallinnan toimintatapoja, jotka ovat havaittavissa Vastaamon viestinnässä. Samalla pääsen tarkastelemaan kääntöpuolta, eli sitä, miten digitaalinen ympäristö vaikuttaa luottamuksen palauttamiseen ja millaisia esteitä se loi tässä tapauksessa.

Toinen tutkimuskysymys laajentaa ensimmäisen kysymyksen näkökulmaa yhteiskunnalliseksi. Tämä kysymys pyrkii vastaamaan siihen, millainen merkitys tapahtumalla on. Tietomurto aiheutti kiivasta yhteiskunnallista keskustelua ja siihen liitettiin erilaisia uhkakuvia. Mediassa aktiivisesti luotiin tietynlainen näkemys tapahtuneesta. Se vaikutti sekä luottamuksen menettämiseen että yhteiskunnallisiin pyrkimyksiin palauttaa luottamusta ja palata sitä kautta normaaliin. Tämän kysymyksen avulla syvennyn enemmän riskiyhteiskunnan näkökulmaan ja teoriaan, johon myös nivoutuu luottamus. Uhkakuvien kautta pääsen tutkimaan yhteiskunnallisen tason mediavälitteistä kriisinhallintaa ja luottamuksen palauttamista. Pyrin vastaamaan kahteen tutkimuskysymykseeni laadullisin menetelmin.

5 Tutkimuksen toteutus

5.1 Tapaustutkimus

Käsittelen Vastaamon tietomurtoa tapauksena digitaalisen ympäristön kriisistä ja sen jälkeisistä toimista. Tapaustutkimuksessa syvennytään yksittäiseen ja uniikkiin tilanteeseen, jota pyritään ymmärtämään yksityiskohtaisen tarkastelun avulla (Laine, Bamberg & Jokinen, 2007; Simons, 2009). Tapaustutkimusta käytetään monilla eri tieteenaloilla ja se sopii monenlaisen aineiston käsittelyyn (Simons, 2009). Tapaus on rajattu yleensä tiettyyn ajanjaksoon. Se voi olla hetkelinen ilmiö tai pidempiaikainen tapahtumakulku, kuten Vastaamon tapauksessa. Tapaustutkimus voidaan toteuttaa erilaista metodologiaa käyttämällä, eli se ei määrää tutkimuksen kulkua. Sen sijaan tapaustutkimusta voidaan ajatella näkökulmana tai lähestymisstrategiana tutkimukseen (Laine, Bamberg & Jokinen, 2007; Simons, 2009). Tässä työssä kyse on useamman kuu-kauden kestävästä tapahtumakulusta, jossa käsittelen tietomurron julkituloa ja sen jälkeistä ajanjaksoa. Käytännössä tapahtumat alkoivat kuitenkin jo useamman vuoden takaa, tietomurron tapahtumahetkellä tai sitä ennen, kun potilastiedot jäivät ilman suojaa. Kuten aikaisemmin esit- telemässäni aikajanassa näkyy, tietomurron julkitulon jälkeen vielä vuodenkin päästä on ilmen- nyt merkittäviä siihen liittyviä seurauksia.

Simons (2009, 5) muistuttaa, että tarina ja sen kerronnan tapa ovat erillisiä toisistaan. Se tulee esille tässä työssä, sillä analyysissä käyttämäni aineisto edustaa viestintää, jolla on jokin pää- määrä. Kirjoitetun aineiston käyttö auttaa perehtymään tapaukseen syvällisemmin ja selvittää sen taustaa. Siitä voi löytää kirjoitukseen koodattuja arvoja ja käsityksiä sekä selityksiä toimin- nasta. (Simons, 2009, 63.) Laadullisessa tapaustutkimuksessa on huomioitava erityisesti, että tutkijan on mahdotonta olla täysin objektiivinen ja hänestä jää jälki tutkimukseen. Tämä koskee niin aineiston keruuta kuin analyysiä, johon liittyy aina tulkintatyötä (Simons, 2009, 117–118). Prosessiin liittyy myös arviointi siitä, mikä osa aineistosta on pätevää ja luotettavaa ja mitä tulee jättää kehysten ulkopuolelle, huomioiden kuitenkin tutkimusasetelman rajat (Simons, 2009, 127–128). Osa aineistosta jää siis väijäämättä tutkimuksen ulkopuolelle. Nämä valinnat voi- daan pohjata niin ikään erilaisiin menetelmiin. Tämän työn kannalta olennaisin niistä on trian- gulaatio. Siinä otetaan huomioon erilaisia näkökulmia eri aineiston kohdalla, eli toisin sanoen

vertaillaan. Käytän työssäni kahdesta eri lähteestä olevaa aineistoa, joka käsittelee samaa tapahtumaa. Triangulaation avulla voidaan validoida käsiteltävät aiheet ja lisätä runsautta tutkittavaan kohteeseen (Simons, 2009, 130).

Tapaustutkimus voidaan rakentaa aineistolähtöisesti, aineistojen vertailun kautta tai luomalla yhtenäinen tarina aineistosta (Simons, 2009, 168). Tässä tutkimuksessa käytän kaikkia kolmea tapaa: aloitan aineistolähtöisesti tutkimaan tapausta, vertailen aineistoja ja päädyn koherenttiin ja yhtenäiseen tapahtumien kulkuun ja tarinaan siitä, mitä tapahtui ja mitä merkityksiä siihen liittyi.

5.2 Aineisto

Käytän tutkimukseni yhtenä aineistolähteenä Vastaamon nettisivuilla julkaistuja tiedotteita. Kyseinen aineisto edustaa Vastaamon kriisiviestintää. Vastaamon konkurssin myötä myös sivustojen ylläpito loppui, mutta niiden sisältö on edelleen saatavilla. Tiedotteet ovat eri pituisia ja uutismaisia tekstejä, joissa kerrotaan muun muassa mitä on tapahtunut, miten asiakkaiden tulisi toimia ja mitä Vastaamo on tehnyt korjatakseen tilannetta. Tiedotteita oli yhteensä 27 sivua, johon sisältyi 21 tiedotetta ja Usein kysytyä -osio (Liite 1). Tiedotteiden viestintä on suunnattu Vastaamon asiakkaille, tietomurron uhreille ja muille tietomurrosta kiinnostuneille, esimerkiksi medialle. Tiedotteiden tarkoituksena voidaan ajatella olevan uutisoinnin lisäksi myös läpinäkyvyyteen pyrkivä viestintä, joka itsessään on osa kriisitoimenpiteitä ja maineenhallintaa. Vastaamon sivustolla ei ollut muita tiedotteita Ajankohtaista-osiossa ennen tietomurtoa, joten se todennäköisesti luotiin osana tietomurron julkitulon jälkeisiä toimenpiteitä. Tiedotteet on kirjoitettu Vastaamoa edustavasti, todennäköisesti Vastaamon viestintävastaavan tai kriisiviestintäammattilaisen laatimana.

On otettava huomioon, että tiedotteet on julkaistu Vastaamon omilla sivuilla ja ne ovat olleet osa maineenhallinnan strategiaa. Tiedotteista saattaa piirtyä yksipuolisen positiivinen vaikutelma yhtiöstä, joka on päätnyt tahtomattaan vaikeaan tilanteeseen. Nettisivujen aineisto antaa

kuitenkin näkökulman Vastaamon keinoihin pyrkiä maineen- ja tilanteenhallintaan. Tämä tiedoteaineisto vastaa ensimmäiseen tutkimuskysymykseen, eli Vastaamon pyrkimykseen palauttaa luottamusta tietomurron jälkeen.

Tiedotteiden lisäksi käytän Yleisradion (Yle) sivustolla julkaistuja uutisia Vastaamosta täydentämään ymmärrystä tapahtuneesta ja selvittämään tapauksen yhteiskunnallista ulottuvuutta. Vastaamo ajautui konkurssiin viiden kuukauden päästä siitä, kun tietomurto tuli ilmi. Ylen uutiset tarjoavat ulkopuolisen näkökulman tietomurtoon ja niissä tulee ilmi Vastaamon tiedotteissa mainitsematta jääneitä asioita. Uutisissa aihetta lähestytään laajemmin, ottaen huomioon erilaiset yhteiskunnalliset instituutiot ja muut toimijat, joita tietomurto kosketti. Yle on Suomen eduskunnan alaisena toimiva ja lähes täysin valtion omistama media. Siinä missä Vastaamon tiedotteet olivat osa yrityksen kriisinhallintaa, Yle edustaa laajempaa, yhteiskunnallista näkökulmaa. Ylen voi ajatella pyrkivän ymmärtämään ja selittämään ajankohtaisia tapahtumia, löytämään ja vaatimaan vastauksia, kertomaan tapahtuneesta ja palauttamaan yhteiskunnallista tilannetta ja luottamusta. Uutiset edustavat yhteiskunnallista merkityksenantoa: ne rajaavat, määrittelevät ja muotoilevat tapahtuneen uhkia, mielikuvia ja laajuutta. Julkaistujen uutisartikkeleiden määrä kertoo jo siitä, että kyseessä on merkittävä mediatapahtuma.

Ylellä on julkaistu lähes 200 uutisartikkelia Vastaamosta alkaen lokakuusta 2020 maaliskuun alkuun 2021, eli tietomurrosta konkurssiin. Näistä poimin 120 uutista (Liite 2). Valikoin ne artikkelit, jotka olivat suoraan yhteydessä Vastaamon tietomurtoon. En esimerkiksi huomionnut kolumneja, videoita tai sellaisia julkaisuja, joissa Vastaamo oli mainittu ohimennen. Maaliskuun 2021 jälkeen Vastaamoon liittyen on ilmestynyt lisää uutisia, jotka koskevat lähinnä oikeudellisia ja taloudellisia konkurssipesän, velkojen, korvausten sekä sakkojen selvittelyjä. Poliisin rikostutkinta on edelleen käynnissä ja tietomurron ja kiristyksen tekijää ja/tai tekijöitä etsitään. Olen lukenut myös konkurssin jälkeen tulleet uutiset ja mainitsen niitä tässä työssä, mutta ne eivät olleet osa analyysiä. Tutkielman liitteissä olen erotellut analyysissä käyttämäni

uutiset ja ne, jotka olen lukenut ja hyödyntänyt luvun 2 aikajanassa (Liitteet 2 ja 3). Ylen uutisten avulla pyrin vastaamaan toiseen tutkimuskysymykseen, eli siihen, millaisia uhkakuvia tietomurrosta syntyi.

5.3 Sisällönanalyysi ja lähiluenta

Valitsin aineiston käsittelytavaksi sisällönanalyysin, sillä sen avulla pystyn tutkimaan tiedotteissa esille nousevia ilmiöitä ja asiasisältöjä. Sisällönanalyysi on laadullinen metodologia, joka voi olla aineisto- tai teorialähtöistä. Sen avulla pyritään saamaan aikaiseksi käsitteellisiä tiivistyksiä sosiaalisesta ilmiöstä ja tulkitaan merkityksiä ja merkitysmallmoja (Corbin & Strauss, 2012). Sisällönanalyysin eri vaiheissa tekstiä pilkotaan, sen rakennetta rikotaan, minkä jälkeen tehdään yhdistelytyötä, muodostaen teemoja tai kategorioita. Tässä työssä käytän käsitettä teema, joka pitää sisällään aiheeltaan läheisiä koodeja. Menetelmä tuo aineistolähtöisyyttä, jonka avulla saattaa nousta esiin jotain olennaista, mitä en ole osannut ottaa huomioon tutkimuskysymysten muotoiluvaiheessa tai aloittaessani tekemään analyysiä.

Ylen uutisten käsittelyyn käytin lähiluennan metodologiaa. Lähiluenta on kirjallisuudentutkimuksesta lähtöisin oleva metodi, mutta siitä on tullut vuosien mittaan varsin poikkitieteellinen (Pöysä, Järviluoma & Vakimo, 2010, 331; Brummet, 2018, 28). Lähiluennalle ei ole tiukkaa määritelmää, ja Pöysä ym. (2010, 331) määrittelevät sen “kaikkena huolellisena ja ymmärtävänä teoksen tulkintana”. Lähiluvun avulla voidaan yhdistää teoria ja empiria ja se sopii myös aineistojen vertailuun (Pöysä ym., 2010, 333–334; Brummet, 2018, 28). Kyse ei kuitenkaan ole tietystä metodologiasta, vaan “suhteellisen vapaana valittavasta joukosta tekstin tulkinnan kannalta strategisia käsitteitä ja näkökulmia” (Pöysä, 2010, 335). Lähiluvun yksi piirteistä on useampaan kertaan aineiston lukeminen ja läpikäyminen. Lukeminen on joka kerralla erilaista: nopeaa, hitaampaa, sisältöön keskittyvää, yleiskuvaa katsovaa. (Pöysä ym., 2010, 338–339) Sisällönanalyysin tapaan tekstistä voidaan etsiä samankaltaisia teemoja ja yhdistellä niitä. Lukemisen ohella tehdyt muistiinpanot ja tekstin tulkinnat ovat myös osa prosessia (Pöysä ym., 2010,

339–340). Metodin avulla valikoidaan tarkasteltavaksi tekstistä tutkimuksen kannalta merkittäviä kohtia. Esimerkiksi tekstin sisäiset metaforat voivat olla tarkastelun kohteena ja kertoa syvällisemmin tekstin merkityksistä ja tavoitteista. Lähiluennan avulla voi tarkastella tekstin sana-, lause-, tai kokonaistasoa. (Pöysä ym., 2010, 342–343.)

Lähiluennassa aineiston käsittelyäni ohjasi myös kehysteoria. Kehysteorialla on pitkät akateemiset ja monitieteelliset perinteet. Nykyään se on journalismitutkimuksen käytetyimpiä teorioita ja analyysimenetelmiä. (Sellnow & Seeger, 2013.) Teoria käsittelee sitä, miten uutiset esitetään yleisölle ja miten se vaikuttaa yleisön käsityksiin tapahtumasta. Kehystäminen siis aktiivisesti luo todellisuutta ja käsitysmaailmaa tapahtuneesta. Kehysteoria on joustava ja sopii monenlaiseen tutkimusasetelmaan. Kriisintutkimuksen kentällä sen kritiikki on lähinnä koskenut sitä, että tutkijat ovat rajoittaneet sen käytön uutisten ja julkaisujen analysoimiseen (Sellnow & Seeger, 2013, 143). Yhdistin sen lähiluennan oheen, sillä se auttoi minua pohtimaan uutisten ympärille asetettuja kehyksiä ja teemoja. Kehysteoria yhdistetään usein kehysanalyysiin, mutta tässä tutkimuksessa pitäydyn sisällönanalyysissä ja lähiluennassa. Kehysteoria toimii vain teoreettisena työkaluna, ei metodina.

5.4 Aineiston käsittely

Hyödynsin sisällönanalyysissä Atlas.ti -ohjelmaa, jonka avulla käsitteelin tekstiaineistoa. Ensin tutustuin tiedotteisiin lukien ne läpi. Tämän jälkeen aloin tekemään rivittäistä koodausta. Tein Vastaamon tiedotteille rivittäisen analyysin, sillä halusin lähestyä analyysiä aineistolähtöisesti. Tutkimuskysymykseni ohjasivat analyysiä kuitenkin jonkin verran. Koodauksessa teksti pilkotaan merkitysten mukaan (Corbin & Strauss, 2012). Tämän jälkeen palaset yhdistetään teemoihin, eli samanlaisten aiheiden mukaisiin ryhmiin. Teoreettinen näkökulma ja viitekehykset tulivat mukaan tutkimuksen tekoon vasta alkaessani yhdistelemään koodeja yhteen, jolloin teemat alkoivat muodostumaan. Sisällönanalyysi oli tässä tutkimuksessa kaksivaiheinen: ensin paloitteletin tiedotteet palasiksi, joista syntyi 85 koodia. Huomasin jo analyysin alkuvaiheessa, että

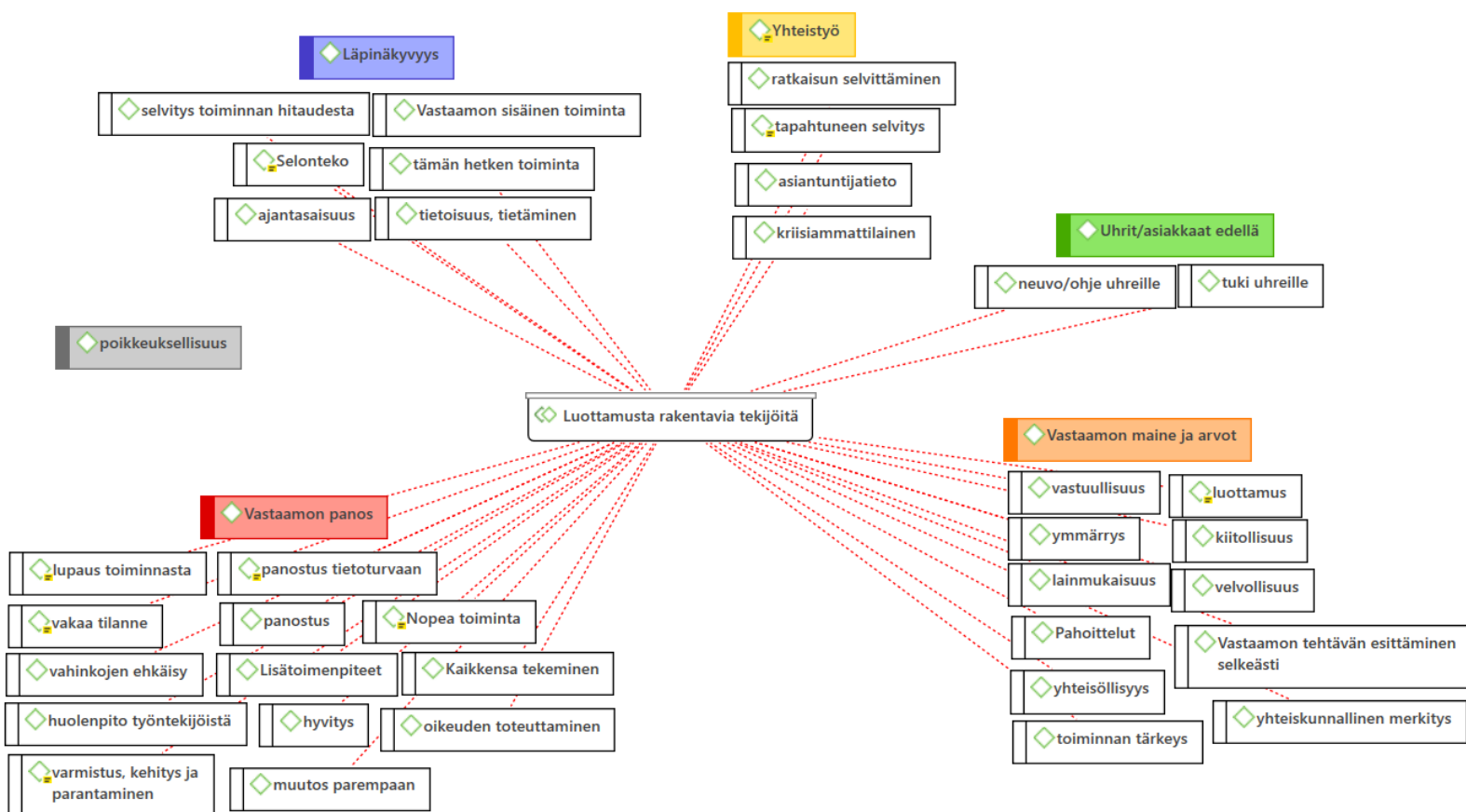
pystyin jakamaan koodit suurpiirteisesti kahteen teemaan. Toinen liittyi Vastaamoon pyrkimykseen ylläpitää mainetta ja rakentaa luottamusta, kun taas toinen toimi vastavoimana, eli haittasi maineenhallintaa. Näiden alle muodostuivat tarkemmat alateemat, joita tuli kuhunkin isoon teemaan viisi. Sisällönanalyysiin liittyy aina jonkinasteista subjektiivisuutta, sillä koodaus ja teemojen luominen on pitkälti tutkimuksen tekijän tulkintatyötä. Palasin useamman kerran analyysin aikana pohtimaan etenkin alateemoihin sijoittamiani koodeja, ennen kuin päädyin niiden lopulliseen muotoon. Jaoteltuani tiedotteiden koodit kahteen ryhmään, tarkastelin niitä visualisointityökalun avulla. Tein kummastakin miellekarttaa muistuttavan visualisoinnin, jotka esittelen analyysin ohella (Kuva 1, s.27 ja Kuva 2, s.38).

Tiedotteet koodattuani, siirryin Ylen uutisten luentaan. Hain Ylen nettisivujen hakukoneella kaikki uutisartikkelit liittyen Vastaamoon hakusanalla “Vastaamo”. Rajasin uutisten haun alkaen lokakuusta 2020 ja loppuen maaliskuuhun 2021. Kopioin uutiset tekstinkäsittelyohjelmaan valikoiden ne, jotka suoraan liittyvät Vastaamoon. Tutustuin myös esimerkiksi kolumneihin ja niihin uutisiin, joissa Vastaamo oli mainittu, mutta en ottanut niitä analyysiin mukaan. Lisäksi luin kaikki maaliskuun 2021 jälkeen tulleet uutiset. Käytyäni uutiset läpi, minulla oli paljon muistiinpanoja ja alustavia teemoja. Luin uutiset kertaalleen jo siinä vaiheessa, kun arvioin tulisiko ne ottaa osaksi analyysiä. Ensimmäisellä lukukerralla keskityin kokonaiskuvan hahmottamiseen. Tämän jälkeen luin uutiset uudestaan, tehden merkintöjä suurpiirteisesti teemoittain. Tällä kertaa keskityin enemmän uutisten sisältöön ja siihen, mitä aihealuetta ne koskivat. Muistiinpanojani hyödyntäen kävin uutiset vielä kerran läpi, tällä kertaa etsien uhkakuvia ja viittauksia niihin. Ennen analyysin tulosten kirjoittamista auki, hahmottelin uutisista muodostuneen visualisoinnin, jonka esittelen analyysiluvussa (Kuva 3, s.45). Kyseisessä kuvassa näkyvät digitaalisen yhteiskunnan eri tasot, joilla uhkakuvat ilmenivät uutisten pohjalta.

6 Analyysi

Seuraavaksi esittelen aineistoesimerkein analyysistä esiin nousseita ilmiöitä ja huomioita. Ensin esittelen keinoja, joilla Vastaamo pyrki palauttamaan luottamusta. Tämän jälkeen esittelen tekijät, jotka nousivat tiedotteissa kriisinhallintaa ja luottamusta haittaavina. Lopuksi käsittelen Ylen uutisissa esille tulleet uhkakuvat. Liitän visualisoinnit jokaisen osion alkuun ja käytän niitä pohjana, jonka avulla selitän analyysin auki.

6.1 Pyrkimys palauttaa luottamusta



Kuva 1. Visualisointi luottamuksen palauttamiseen liittyvistä teemoista Vastaamon tiedotteissa.

6.1.1 Pyrkimys läpinäkyvyyteen

Yksi viestintästrateginen tapa luottamuksen palauttamiseen on tehdä viestinnästä mahdollisimman läpinäkyvää ja totuudenmukaista. Vastaamon tiedotteita julkaistiin tiuhaan tahtiin, heti tietomurron jälkeen lähes päivittäin, mikä antoi kuvan ajantasaisuudesta. Ajantasaisuutta korostettiin myös tiedotteiden sisällössä.

Nykytiedon mukaan tietomurron kohteena oli asiakasrekisterimme marraskuussa 2018. (T3)

Olemme pyrkineet tällä sivulla tiedottamaan selvityksen etenemisestä ajantasaisesti sekä päivittäneet tietoja käytännön neuvoista ja saatavissa olevasta tuesta. (T11)

Läpinäkyvään viestintään kuului kertomus tehdystä ja sillä hetkellä meneillään olevasta toiminnasta. Siinä korostui asiakkaiden auttaminen. Toimintaa kuvailtiin yksityiskohtaisesti, kuten seuraavassa esimerkissä tulee ilmi.

Asiakaspalveluun tuli kuukaudessa yli 10 000 puhelua, joista valitettavasti vain osaan pystyttiin ruuhkahuipussa vastaamaan. Sähköposteja tuli lähemmäs 6 000, joista suurin osa ensimmäisellä viikolla kriisin julkitulon jälkeen. Asiakaspalveluun rekrytoitiin lisää ihmisiä kiireellisesti ja enimmillään puheluihin ja sähköposteihin vastasi 12 ihmistä. Ajalla 16.11.-21.11.2020 puheluita tuli enää 50-100 päivässä. Lähes kaikkiin puheluihin saadaan nyt vastattua. (T11)

Tiedotteissa, jossa nostettiin esiin asiakkaiden närkästyttämää palvelujen hitautta, tehtiin selontekoa. Seuraavassa aineistoesimerkissä esiintyy puolustuspuhetta (prosessin vaatima huolellisuus), jolla selitettiin rekisteritietopyyntöjen käsittelyn hitautta.

Prosessi on asian vaatimasta huolellisuudesta johtuen hidas, mutta selvitämme kaikkia mahdollisia keinoja nopeuttaa prosessia. (T4)

Myös yhtiön sisäisten asioiden hoitamisesta ja tapahtuneen selvittelystä tiedotettiin. Tiedotteissa kerrottiin muun muassa Vastaamon “*sisäisestä selvityksestä*”, sekä tehdyistä toimenpiteistä: “*Maaliskuussa 2019 toteutettu hyökkäys sai Vastaamon korjaamaan asiakastietojärjestelmän suojauksessa olleen puutteen ja tekemään muita tietojärjestelmiä suojaavia toimenpiteitä.*” (T5). Myös yhtiön johdon toimintaa selostettiin: “*Yhtiön johdon tärkein tehtävä on asiakkaiden tukeminen poikkeuksellisen vakavan ja raskaan tilanteen keskellä.*” (T5). Tämä tiedote ilmestyi samana päivänä, kun hallitus vapautti toimitusjohtajan tehtävästään. Yhtiön hallituksen toiminta tuli uudemman kerran esille, kun se joutui selvittämään Vastaamon toimintaa jatkossa.

Vastaamon hallitus sai 4.1.2021 päätökseen tehtävänsä selvittää vaihtoehtoisia malleja liiketoiminnan jatkamiselle. Hallitus on jättänyt tunnistetut ratkaisumallit omistajien päätettäväksi ylimääräisessä yhtiökokouksessa 28.1.2021. Yhtiökokouksen päätöksistä tiedotetaan erikseen. Sovitun tehtävän tultua suoritetuksi hallitus erosi tehtävästään. (T16)

Toiminnan läpinäkyvyyttä korostettiin etenkin tietoturvakysymysten kohdalla. Tietomurron kannalta oli jo myöhäistä olla varovainen, mutta tiedotteissa pyrittiin välittämään kuva siitä, että ainakin sen jälkeen on toimittu tietoturva huomioon ottaen, varmistaen samalla, ettei tapahtunut vahinko laajene entisestään.

Kriisipuhelimessa asioinnista ja maksuttomasta keskustelusta ei tehdä potilaskirjauksia. (T4)

Tiedot luovuttaa tarkastettavaksi terveydenhuollon ammattihenkilö eli Vastaamon terveydenhuollon palveluista vastaava johtaja, joka tekee merkinnän tarkastusoikeuden käyttämisestä potilaan tietoihin. (T8)

Pyydetyt tiedot voidaan toimittaa vahvasti tunnistautuneille henkilöille käyttämällä suojattua sähköpostia. (T14)

Myös yhteistyössä muiden tahojen kanssa tuotiin esille tietoturvakäytäntöjä: “*Asiakastieto sitoutuu tuhoamaan suostumukseen liittyvät tiedot viipymättä, kun niitä ei enää tarvita.*” (T13)

6.1.2 Yhteistyö ja asiantuntijatieto

Tietomurron julkitulon jälkeen Vastaamo aloitti yhteistyön erilaisten tahojen kanssa selvittääkseen tilannetta. *“Teemme kaikkemme selvittääksemme tapahtunutta yhdessä viranomaisten kanssa”* (T3), kirjoitettiin toistuvasti tiedotteissa. Tiedotteissa painotettiin jatkuvaa yhteistyötä, selvitystä tapahtuneesta sekä tapahtuneen vahingon leviämisen estämistä. Tapahtumien selvitessä ja konkurssin lähestyessä, lupaukset muuttuivat realistisemmiksi. Eri vaiheessa tutkintaa lupauksiin lisättiin tai poistettiin ajatus siitä, että toiminta pyrkii *“syyllisen tai syyllisten löytymiseen”* (T3, T5 ja T21), *“luottamuksellisen tiedon leviämisen estämiseen”* (T1, T2 ja T6), *“uhrien tukemiseen”* (T6) tai *“tapahtuneen syiden, seurausten ja vaikutusten selvittämiseen”* (T11, T14, T17, T18 ja T20). Yhteistyöllä oli siis erilaisia tarkoituksia. Viranomaistahojen sekä tietoturva-asiantuntijoiden kanssa työskentely edusti tapahtuneen selvittämistä. Myöhemmin Asiakastiedon palvelut tarjosivat ratkaisuja asiakkaiden tietojen väärinkäytön ehkäisyyn.

Pyrimme myös tarjoamaan luottotietopalveluiden toimittajien kanssa tietomurron uhreille ratkaisuja, joilla voidaan ehkäistä ja valvoa henkilötietojen väärinkäyttöä. (T4)

Tietoturva-asiantuntijoiden sitoutumattomuutta ja ulkopuolisuutta painotettiin, antaen kyseiselle yhteistyölle enemmän painoarvoa. Viestintä antoi kuvan siitä, että tietoturvan haavoittuvuudet on korjattu ja järjestelmä kehitetty paremmaksi kuin ennen tietomurtoa.

Kehitämme jatkuvasti tietoturvaamme sekä tietosuojaa ja teemme lisätoimenpiteitä omien selvitystemme ja viranomaistutkinnan valmistuessa. (T1)

Vastaamon tietojärjestelmiä on tarkistettu, ne ovat vahvasti suojattu ja niiden käyttöä valvotaan tehostetusti tietoturva-ammattilaisten toimesta. (T3)

Kela ja Valvira edustavat viranomais- ja asiantuntijatahoja, jotka ovat merkittäviä yhteiskunnallisia toimijoita. Heidän päätöksillään on suuri vaikutus Vastaamon tulevaisuuteen ja toimintaan. Erityisesti heidän myönteisistä päätöksistään tiedotettiin ahkerasti. Yksi tiedotteista käsiteli pelkästään Valviran tekemää tarkistusta.

Valvira ei havainnut tarkastuksessaan sellaisia puutteita, jotka edellyttäisivät potilas-tietojärjestelmän käytön rajoittamista tai välitöntä puuttumista Vastaamon tuottamiin palveluihin. [– –] Tarkastuksessa todettiin, että Vastaamo on tunnistanut tietomurtoon johtaneet syyt ja ryhtynyt asianmukaisiin toimenpiteisiin potilasturvallisuuden varmistamiseksi. Vastaamon järjestelmien tietoturvan nykytasoa on parannettu ulkopuolista asiantuntija-apua hyödyntäen. (T9)

Myös Kelan päätöksestä jatkaa asiakkaiden ohjaamista Vastaamoon tiedotettiin: *“Kela on 20.11.2020 päättänyt ohjata jälleen asiakkaita Vastaamoon ensi viikosta alkaen.”* (T10). Vastaamon tiedotteissa ei kuitenkaan mainittu esimerkiksi myöhemmin sitä, kun Kela irtisanoi sopimuksensa Vastaamon kanssa.

Asiantuntijatietoa painotettiin Vastaamon viestinnässä myös silloin, kun uudeksi hallituksen puheenjohtajaksi ja väliaikaiseksi toimitusjohtajaksi valittiin Heini Pirttijärvi. Hän nousi Vastaamon tiedotteissa esille kriisiammattilaisena, joka toi asiantuntijuuttaan Vastaamon kriisin keskelle. Hallituksen edellinen puheenjohtaja Tuomas Kahri kuvaili Pirttijärveä *“kokeneena muutosjohtajana”* (T7). Samassa tiedotteessa esiteltiin muita uuden hallituksen jäseniä, joiden asiantuntijuutta *“vaikeissa muutostilanteissa”* sekä *“monipuolista kokemusta terveydenhuollon palveluyrityksissä”* tuotiin esille. Viestinnässä pyrittiin luomaan Vastaamon johtohenkilöistä vakaa ja asianosaava kuva. Hallituksen ja toimitusjohtajan lisäksi myös muun henkilökunnan asiantuntemusta korostettiin: *“Sekä vanhat että uudet asiakkaat saavat keskusteluapua osavilta terapeuteiltamme.”* (T14)

Kelan, Valviran ja tietoturva-asiantuntijoiden maininnat ovat merkityksellisiä. Jos luotettavat asiantuntijatahot hyväksyvät yrityksen järjestelmän ja toiminnan, on helpompaa kääntää maine myönteiseksi ja rakentaa luottamusta julkisuudessa. Asiantuntijoiden näkemyksistä ja päätöksistä tiedottaminen antoi lisäarvoa Vastaamon toiminnalle ja sen jatkumiselle. Asiantuntijatie-toon voi liittää kaksi eri merkitystä: toiminta ja symbolinen arvo. Osa yhteistyökumppaneista

edusti aktiivista toimintaa, kuten tapahtuneen selvitystä, tietosuojan tarkistamista, uhrien auttamista ja luottotietojen suojaamista. Toisaalta yhteistyötahoilla on merkittävää symbolista arvoa, jonka avulla tiedotteissa pyrittiin rakentamaan luottamusta.

6.1.3 Uhrit ja asiakkaat edellä

Tiedotteissa tuotiin esille uhrien ja asiakkaiden asema kriisin keskellä. Termejä ”uhri” ja ”asiakas” käytettiin vaihtelevasti. Monen Vastaamon työntekijän henkilötiedot vietiin murrossa, jolloin näkökulma laajeni asiakkaista tietomurron uhreihin. Selvitystilasta kertovassa tiedotteessa painotus uhreista muuttui jälleen asiakkaisiin, joiden terapia saattoi jäädä kesken, jos Vastaamo päätyisi konkurssiin. Tiedotteissa uhrien hätää ja ahdinkoa oikeutettiin ja normalisoitiin. Niissä oli usein lämmin sävy, jolla kohdistettiin myötätuntoa uhreja kohtaan.

Kohtaamisissa suurin osa ihmisistä on luonnollisesti ollut järkyttyneitä ja huolissaan. Monet asiakkaamme ovat olleet huolissaan myös toisten asiakkaidemme ja henkilöstön jaksamisesta. Asiakaspalvelijamme haluavat kiittää asiakkaitamme välittämisestä, lämpimistä sanoista ja myötätunnosta. (T11)

Edellä olevassa aineistoesimerkissä ymmärrys kohdistui myös asiakkaiden ja terapeuttien väliseen vuorovaikutukseen ja suhteeseen.

Suurin osa tiedotteista sisälsi uhreille tarkoitettua ohjeistusta. Vastaamon sivuilla päivitettiin Usein kysytyjä kysymyksiä -osiota, sekä kriisitukea tarjoavien tahojen yhteystietoja. Heti tietomurron jälkeisissä tiedotteissa ohjeistettiin mistä kiristysviestin tunnistaa ja mitä tulee tehdä, jos sellaisen on saanut.

Mikäli olet joutunut kiristysten ja uhkauksen kohteeksi, kehotamme sinua asianomistajana välittömästi ilmoittamaan tästä kotipaikkasi poliisille ja tekemään asiasta sähköisen rikosilmoituksen. (T3)

Lisäksi tiedotteissa mainittiin selkeästi tavat, jolla Vastaamo lähestyi asiakkaitaan, jotta oikeat yhteydenotot osattaisiin erottaa vilpillisistä.

Lähestymme asiakkaita ensisijaisesti sähköpostin välityksellä. Jos Vastaamossa ei ole asiakkaan sähköpostiosoitetta, lähetämme kirjeen, jolloin asiakkaan tavoittaminen valitettavasti kestää hieman kauemmin. (T3)

Tiedotteissa mainittiin lisäksi tietomurron jälkeiset toimenpiteet, joiden avulla pyrittiin tukemaan uhreja. Näitä olivat kriisipuhelimet ja terapeuttien tarjoamat keskustelut sekä kriisiapu. Terapeutit olivat sekä auttajan, että uhrin rooleissa. Tiedotteiden mukaan yhtiö oli järjestänyt “sekä sisäistä että ulkoista tukea henkilöstölle, joka toimii erittäin suuren paineen alaisena tällä hetkellä” (T4). Henkilöstön tukeminen tuotiin asiakkaiden tukemisen rinnalle, painottaen sitä, kuinka tärkeää työtä henkilöstö tekee (T6 ja T7). Seuraavassa esimerkissä korostetaan Vastaamon terapeuttien proaktiivista toimintaa.

Monet [terapeutit] ovat myös erikseen soittaneet perään sellaisille asiakkaille, joista on ollut huolta tai joista terapeutti ei ole kuullut vähään aikaan. Asiakkaita on aktiivisesti ohjattu kriisiavun ja neuvonnan piiriin. (T11)

Tiedotteiden asiakkaat edellä -narratiivi jatkui konkurssiin asti. Niissä tuli esille Vastaamon viestintästrategia, jossa painotettiin vastuullisuutta ja huolenpitoa asiakkaista ja henkilökunnasta, jotka joutuivat yllättäen kriisin keskelle. Oli odotusten mukaista, että Vastaamo tarjoaisi heille apua ja tukea. Tarjotun avun ja tuen tuli ottaa erityisten hyvin huomioon tietoturva, ettei avun hakemisesta synny seuraavaa riskitekijää. On kuitenkin eri asia, näkivätkö uhrit nämä toimenpiteet riittävinä ja toteuttiko Vastaamo vastuunsa uhrien näkökulmasta.

6.1.4 Vastaamon panos ja viestintä vakaasta tilanteesta

Kuten edellä esitellyt teemat tuovat esille, viestinnässä nostettiin etusijalle Vastaamon toiminta ja teot tietomurron jälkeen. Kyseisen viestinnän voi jakaa kahteen osaan: mitä Vastaamo on

tehnyt ja miten. Yritys on tehnyt kaikkensa ja parhaansa, se on pyrkinyt olemaan mahdollisimman nopea tiedottamisessaan ja tarkistaa, varmistaa, kehittää sekä parantaa tietoturva, auttaen samalla uhreja. Lisäresurssien käyttöönotto rahallisesti ja henkilöstöä lisäämällä viesti Vastaamon pyrkimyksestä toipua kriisistä ja vastata uhrien tarpeisiin: “*Vastaamo itse tekee hartiavoimin töitä tiedottaakseen ja ohjeistaakseen*” (T4); “*Puramme asiakirjojen toimituksen ruuhkaa lisäresurssien turvin*” (T14). Vastaamo kuvataan yhtenäisenä ja empaattisena toimijana, joka haluaa “*tarjota psykoterapian ammattilaistemme tukea asiakkaillemme, joita asia koskettaa*” (T4).

Nopean toiminnan korostaminen piirsi kuvan yhtiöstä, joka tietomurrosta tiedon saatuaan ryhtyi viipymättä toimiin. Pyrkimys selvittää tapahtunutta ja toteuttaa oikeutta saamalla rikollisen tai rikolliset vastuuseen esitettiin myös yhteiskunnallisena vastuuna.

Asiasta ilmoitettiin välittömästi Keskusrikospoliisille, joka aloitti asiasta rikostutkinnan. Tapahtumasta tehtiin välittömästi ilmoitukset myös Suomen kyberturvallisuuskeskukselle, Valviralle sekä tietosuojavaltuutetulle. (T5)

Vastaamo lähetti heti ilmoitukset tietoturvaloukkauksesta niin asiakkaille kuin työntekijöille. (T11)

Pyrkimyksestä jatkuvaan kehitykseen tietoturvan saralla ei puhuta vain tietomurron valossa, vaan tietoturvasta tehdään selontekoa myös menneistä tapahtumista, kuten yrityskaupan yhteydessä vuonna 2019. Muodostuu kuva siitä, että tietoturvasta on aina pyritty pitämään huolta.

[Tietoturvan] *Tarkastus teetettiin yrityskauppaprosessin yhteydessä. Selvityksessä ilmeni useita kehityskohteita, mutta ei kriittisiä tietoturvapuutteita. Vastaamon tietojärjestelmien kehitystyö on sen jälkeen ollut jatkuvaa.* (T5)

Vastaamo on voittoa tavoitteleva yritys, jolle esimerkiksi henkilöresurssien lisääminen on liiketoiminnan ja taloudellisen tilanteen kannalta haitallista. Tässä yhteydessä lisäresurssit olivat

myös osa maineenhallintaa. Esimerkiksi tiedotteessa T15 Vastaamo kertoi tehneensä joululahjoituksen Mieli ry:lle, joka oli tarjonnut nopeasti kriisiapua tietomurron uhreille. Tähän aikaan Vastaamon huonontunut taloudellinen tilanne oli jo tiedossa, joten lahjoitus voitiin nähdä kiittolisuuden osoituksen lisäksi tapana ylläpitää mainetta ja viestiä tilanteen vakaudesta.

Toiminnan jatkuminen normaalina vie ajatukset pois kriisistä. Vaikka kriisi vaikutti yhtiöön monella tapaa, tiedotteissa muistutettiin peruslähtökohdista korostaen tilanteen vakautta. Tiedotteessa T17 tuotiin esille uusien asiakkaiden saaminen, millä myös murrettiin kuvaa yhtiöstä konkurssin partaalla.

Toimintamme jatkuu normaalisti: meiltä saa terapiapalveluita, terapeutit saavat palkkansa ja vastaamme velvoitteistamme. (T12)

Tietoturva-loukkausten julkitulon jälkeen useimmat asiakkaamme ovat jatkaneet hoitoaan Vastaamon terapeuttien kanssa. Saamme jatkuvasti myös uusia asiakkaita. (T17)

Resurssien lisääminen tapahtuneen selvittämiseksi, kulut uhrien tukemiseksi, hyvitykset ja tietoturvan vahvistaminen aiheuttivat Vastaamolle suuria kertaluontoisia kuluja, jotka lopulta ajoivat Vastaamon konkurssiin (T18). Tiedotteissa toistuu myös viesti siitä, että Vastaamo on tehnyt kaikkensa kyseisessä tilanteessa.

Olemme tehneet paljon töitä sen eteen, että asiakkaat voivat luottaa siihen, että heidän tietonsa ovat turvassa, ja hakeutua terapeuttiemme vastaanotoille rauhallisin mielin. (T9)

Vastaamon asiakaspalvelu on tehnyt parhaansa vastatakseen asiakkaiden kysymyksiin ja välittääkseen asiakkaille mahdollisimman ajantasaista, faktapohjaista ja vahvistettua tietoa tapahtuneesta. (T11)

Senkin jälkeen, kun Vastaamo asetettiin selvitystilaan, tiedotteissa pysyi vakaa lupaus toiminnasta ja siitä, että asiakastapaamisia pyritään järjestämään kaikesta huolimatta: *“Selvitystilasta*

huolimatta yhtiön toimintaa pyritään jatkamaan toistaiseksi”; *“Vastaamon toiminta jatkuu selvitystilan ajan ja rohkaisemme asiakkaita jatkamaan terapiaansa”* (T19). Yrityksen päätyessä konkurssiin viesti jatkui samana ja tiedotteissa kirjoitettiin miten Vastaamon on *”sitkeistä yrityksistä huolimatta”* päätyneet konkurssiin (T20).

6.1.5 Jaettujen arvojen korostaminen

Vastaamon tiedotteissa toistuivat tietyt arvot ja piirteet, jotka voidaan liittää yrityksen maineeseen. Esimerkiksi hallituksen puheenjohtaja Tuomas Kahri toi yhtiön linjaa esille heti ensimmäisessä tiedotteessa.

Psykoterapiapalveluita tarjoavana yhtiönä asiakastietojen luottamuksellisuus on meille äärettömän tärkeitä ja kaiken toimintamme lähtökohta. (T1)

Tiedotteissa nousi esille tapa viestiä yrityksestä yhteisönä. Kriisin jaettu kokemus toi tätä yhteisöä tiiviimmin yhteen. Kaikki olivat *”samassa veneessä”*. Seuraava aineistoesimerkki konkretisoi yrityksen yhteiskunnalliseen merkityksellisyyteen, yhteisöllisyyteen ja luottamuksen rakentamiseen liittyvää viestintää.

Psykoterapiapalveluille on suuri kysyntä, ja siksi on yhteiskunnallisesti tärkeää, että hoitosuhteita pystytään jatkamaan. Sekä vanhat että uudet asiakkaat saavat keskustelun apua osaavilta terapeuteiltamme. Koko Vastaamon henkilöstö tekee lujasti töitä sen eteen, että asiakkaat voivat hakeutua terapeuttiemme vastaanotoille rauhallisin mielin. Tämä luottamus pitää lunastaa päivittäin, ja siihen me Vastaamossa olemme sitoutuneita. (T14)

Tiedotteissa ei mainita suoraan Yhteiskunnallinen yritys -merkkiä, mutta yhteiskunnallisen hyvän tuottaminen on esillä tiedotteissa. Lisäksi kriisinjälkeisen toiminnan lainmukaisuutta ja velvoitteiden toteuttamista tuotiin esille.

Tiedotamme tietosuojalain velvoittamalla tavalla kaikkia asiakkaita, joiden tiedot ovat tämän hetken tiedon valossa joutuneet tietoturvaloukkauksen kohteeksi. (T2)

Valvonta tapahtuu sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain perusteella. Valvira jatkaa myös Vastaamon toiminnan asianmukaisuuden valvontaa yksityisestä terveydenhuollosta annetun lain perusteella. (T9)

Pahoittelut ja toisaalta kiitollisuus toistuivat tiedotteissa vuorotellen. Kiitollisuutta osoitettiin etenkin yhteistyökumppaneille ja kriisiapua nopeasti tarjonneille kolmannen sektorin toimijoille. Myös henkilökuntaa kiitettiin tärkeästä työstä.

Kiitämme lämpimästi kaikkia yhteiskunnallisia toimijoita ja erityisesti kolmannen sektorin ja kirkon auttajia. (T15)

Kiitämme henkilöstöämme heidän valtavasta sitoutumisestaan asiakkaiden auttamiseen tilanteessa, jossa suuri osa terapeuteista on myös itse joutunut tietomurron ja kiristyksen uhriksi. (T11)

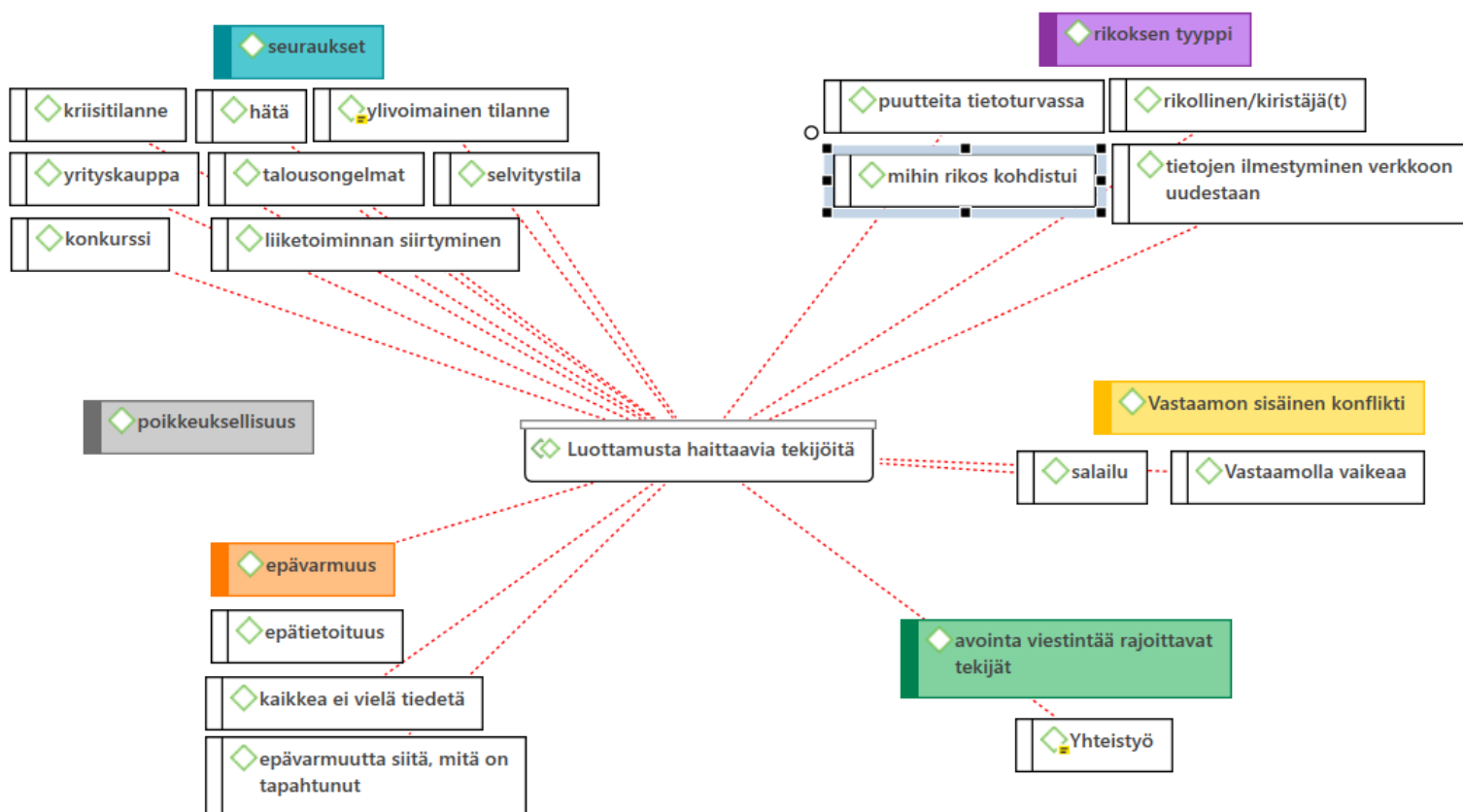
Pahoittelut puolestaan suunnattiin ensisijaisesti uhreille ja asiakkaille. Myöhemmin pahoitteluja osoitettiin myös työntekijöille. Pahoittelut toistuivat lähes jokaisen tiedotteen päätteeksi, joskus useamman kerran yhdessä tiedotteessa. Tiedotteissa pahoiteltiin tapahtunutta tietovuotoa, tietoturvan puutteita, tietojen uudestaan ilmestymistä verkkoon, tietojen leviämisestä ja tilannetta ylipäänsä.

Olemme syvästi pahoillamme tapahtuneesta ja tietomurron kohteeksi joutuneiden asiakkaidemme puolesta. Pyydämme anteeksi niitä puutteita tietoturvassa, joiden seuraukset ja inhimillinen hinta on muodostunut äärimmäisen raskaaksi. (T5)

Tiedotteissa nojattiin siihen käsitykseen, että Vastaamolla on yhtiönä tietty maine. Sen yhteiskunnallista merkitystä ja toiminnan tärkeyttä nostettiin esille etenkin siinä vaiheessa, kun mediassa Vastaamon maine alkoi hajoamaan.

6.2 Luottamusta ja tilanteenhallintaa häiritsevät tekijät

Seuraavaksi esittelen aineistoesimerkein Vastaamon tiedotteista nousseita tekijöitä, jotka hankaloittivat ja toimivat esteinä tilanteen hallinnalle. Nämä tekijät selittävät osittain miksi luottamusta oli niin vaikea palauttaa.



Kuva 2. Visualisointi tekijöistä Vastaamon tiedotteissa, jotka häiritsevät maineenhallintaa ja luottamuksen palauttamista.

6.2.1 Rikoksen tyyppi

Koska kyseessä oli digitaalisessa ympäristössä tapahtunut tietomurto ja kiristys, siihen liittyi ennakoimattomia piirteitä. Ensimmäisissä tiedotteissa Vastaamoon viitattiin ”tietomurron ja kiristuksen uhrina” (T1). Tietomurron digitaalinen luonne johti siihen, että anastetut tiedot lähtivät nopeasti leviämään. Sen estäminen ei ollut realistista ja vahinko oli jo ehtinyt tapahtua. Tietojen leviäminen tuotiin uudemman kerran esille pahoitteluiden yhteydessä, sillä tiedot nousivat yhä uudelleen pintaan ennen konkurssia, eikä niitä pystytty mitenkään hallitsemaan.

Olemme syvästi pahoillamme tietoturva-loukkauksen ja kiristuksen kohteeksi joutuneiden asiakkaidemme puolesta ja siitä, että varastettuja asiakastietoja on edelleen leviitetty. (T21)

Tiedotteissa kerrottiin myös tietoturva-asiantuntijoiden selvityksestä, jonka mukaan tietomurtoja oli kaksi yhden sijaan.

On todennäköistä, että järjestelmäämme on tunkeuduttu myös marraskuun lopun 2018 ja maaliskuun 2019 välisenä aikana. Tiedossamme ei ole, että tässä yhteydessä tietokanta olisi varastettu, mutta on mahdollista, että yksittäisiä tietoja on tarkasteltu tai kopioitu tuossa aikavälissä. Emme pysty yksilöimään kenen tietoja on mahdollisesti voitu luvattomasti tarkastella. (T3)

Ensimmäisestä tietomurrosta oli kulunut jo puolitoista vuotta, joten syyllisten jäljittäminen ja toisaalta tapahtuneen selvittäminen oli vaikeaa. Lisäksi syyllisistä ei ollut mitään varmaa tietoa, eikä ole tutkielman kirjoittamispäiväänkään mennessä.

Syyllistä tai syyllisiä ei valitettavasti ole vielä saatu selville eikä kiinni. (T17)

Samalla Vastaamon oman järjestelmän puutteet ja murtojen salailu tekivät yhtiöstä osasyllisen ja antoivat siitä vastuuttoman kuvan. Tätä näkökulmaa ei nostettu tiedotteissa esille, mutta tietoturvapuutteista oli kuitenkin maininta.

Vastaamon asiakastietojärjestelmän suojauksessa on ollut puute, jota hyödyntämällä rikolliset ovat päässeet käsiksi silloiseen asiakastietokantaan. (T5)

Arkaluontoisten tietojen leviäminen ja yhä uudelleen ilmestyminen internetiin aiheutti kriisin pitkittymisen ja uhkatilanteen jatkumon. Vastaamon tietoturvan tarkastuksessa tuli ilmi puutteita, samalla kuin moni asia jäi epäselväksi: miten ja mitä tietoja on tarkasteltu, mitä tietoja on voitu kopioida tai käyttää, kuka on ollut näiden takana ja miten hänet tai heidät saadaan kiinni. Seuraavaksi esittelen epävarmuutta, joka oli yksi tämän rikoksen ydinpiirteistä.

6.2.2 Epävarmuus

Epävarmuus on iso osa kyseisen tietomurron luonnetta ja se ulottuu myös laajemmin rikoksen ulkopuolelle. Tiedotteissa nostettiin esille jatkuvasti sitä, että kaikkea ei vielä tiedetä.

Valitettavasti emme voi varmentaa yksittäisen rekisterissä olleen asiakkaan osalta, onko murron yhteydessä hankittuja tietoja levitetty tai käytetty ja jos on, niin missä laajuudessa. (T2)

Selvitystyössä ei ole ollut mahdollista saada täyttä varmuutta asioiden kulusta. (T5)

Tiedotteissa painotettiin, että esitetyt tiedot ovat ”nykytietoa” ja asiankulut ”todennäköisiä”, joten niihin mahtui aina jonkin verran epävarmuutta. Selvitystyö vaati myös aikansa, joten tapahtumien kulku avautui pikkuhiljaa, mikä vaikeutti selkeää ja varmaa viestintää.

Tietomurron suuruusluokka ja koko tapahtumakulku on selvinnyt asteittain itse kiristysviestin ja tietoturvaloukkauksen julkitulon jälkeen. (T11)

Tapahtumiin liittyvät selvitykset ja tutkimukset ovat edelleen kesken. (T17)

Tietomurtoon liittyvän epävarmuuden lisäksi myös yritystoiminnan tulevaisuus jäi hämärän peittoon, kun tuli selväksi, että talousongelmat vaikeuttavat Vastaamon toimintaa. Selvitystilan

aikana epävarmuus Vastaamon toiminnasta oli huipussaan. Myös Verveen siirryttäessä tilanne oli epävarma, kuten selviää tiedotteesta T20: *“Kauppaan liittyen moni asia on vielä auki.”*

6.2.3 Avointa viestintää rajoittavat tekijät

Yhteistyötä asiaa selvittävien tahojen kanssa käytettiin tiedotteissa rajoittavana tekijänä avoimelle viestinnälle. Näitä tahoja olivat poliisi, tietoturva-asiantuntijat ja Valvira.

Koska [Valviran] valvontaprosessi on kesken, siitä ei voida kertoa tässä vaiheessa enempää. (T9)

Vastaamon nettisivujen Usein kysytyt kysymykset -osiossa yksi ensimmäisistä julkaisuista liittyi siihen, miksi viestintä tietomurrosta oli niin hidasta, että suurin osa uhreista kuuli tapahtuneesta ensimmäistä kertaa valtavirtauutisten kautta. Ensimmäisessä tiedotteessa hallituksen puheenjohtaja Kahri otti tähän kantaa.

Käynnissä olevan poliisitutkinnan takia emme ole aikaisemmin saaneet viestiä aiheesta, sillä tutkintateknisistä syistä asiaa ei ole haluttu julkistaa. (T1)

Tiedotteiden mukaan Vastaamo seurasi viranomaisohjeita, eikä sen takia voinut kertoa tapahtuneesta aikaisemmin. Yhteistyöllä oli siis iso rooli luottamusta rakentavana tekijänä, mutta samalla sitä käytettiin tiedotteissa selityksenä rajoittaa yrityksen viestintään. Kuten myöhemmin tuli ilmi, Vastaamo viesti tapahtuneesta asianosaisille vasta tietoturvaluottuutetun niin määrätessä.

6.2.4 Vastaamon sisäinen konflikti

Vastaamon sisäinen konflikti oli yksi tietomurron seurauksista, mutta se myös toimi itsessään esteenä luottamuksen rakentamiselle. Konfliktiin liittyi toimitusjohtaja Ville Tapion tietomurron ja tietoturvaluottuutteden pimittäminen toisen tietomurron jälkeen.

Yhtiön nykyiselle hallitukselle ja pääomistajalle ei ole kerrottu maaliskuun 2019 tietomurrosta eikä yhtiön järjestelmissä olleista tietoturvaluotteluista. (T5)

Koska tiedot oli pimitetty ennen yrityskauppaa, pääomistaja käynnisti oikeudellisia toimenpiteitä, mikä toi mukanaan turbulenssia ja epävarmuutta.

Vastaamon hallituksen tiedossa on, että yhtiön pääomistaja PTK Midco Oy on maanantaina 26.10.2020 käynnistänyt oikeudellisia toimenpiteitä, jotka liittyvät toukokuussa 2019 allekirjoitettuun yrityskauppaan Vastaamosta. (T5)

Pelkästään tietomurtoon reagoimiseen meni Vastaamolla resursseja, mutta samalla niitä kuluttivat myös yrityksen sisäiset konfliktit, jotka vaikeuttivat luottamuksen rakentamista niin ulkoisesti, kuin sisäisesti. Salailu ja tapahtumien pimittäminen, sekä julkinen paine teki tilanteesta haastavan niille tahoille, jotka olivat ensisijaisesti vastuussa tilanteen ratkaisusta ja tuen järjestämisestä uhreille. Samalla myös suurin osa henkilöstöstä tarvitsi apua ja tukea. Vaikka heistä ei ollut potilaskertomuksia, heidän henkilötietojaan pystyttiin kuitenkin käyttämään identiteettivarkauksiin ja huijauksiin.

6.2.5 Tietomurron seuraukset

Tiedotteissa käsitellyt tietomurron seuraukset koskivat uhrien lisäksi Vastaamon toimintaa ja taloutta. Tiedotteissa ei tullut esille seurauksia muille tahoille, joita tietomurto kosketti – tämä näkökulma tulee esille Ylen uutisissa. Tilanne oli yritykselle odottamaton. Tiedotteissa mainitaan, että vaikka tietomurtoon asti taloudellinen tilanne on ollut vakaa, kriisiin liittyvät toimenpiteet olivat horjuttaneet sitä merkittävästi, minkä takia Vastaamon hallitus joutui tekemään Patentti- ja rekisterihallitukseen ilmoituksen oman pääoman menettämisestä.

Yhtiön operatiivinen toiminta on ollut taloudellisesti vakaata ja hyvin ennustettavaa. Tilanne johtuu erityisesti suurista kertaluontoisista kulueristä, jotka liittyvät tietomurron ja siihen johtaneiden syiden selvittämiseen ja tietoturvan vahvistamiseen, sekä tuen

ja hyvitysten tarjoamiseen uhreille. Näihin kuluihin ei ole voitu ennalta varustautua.
(T12)

Vastaamon jouduttua selvitystilaan, tilannetta kuvattiin tiedotteissa ”ylivoimaiseksi”. Taloudellisesti yritys oli ajautunut niin pahaan ahdinkoon, ettei hallitus nähnyt vaihtoehtoja konkurssille.

Vastaamon hallitus, johto ja omistajat selvittivät huolellisesti kaikkia muita vaihtoehtoja, kuten rahoitusratkaisuja, yritysjärjestelyitä ja toiminnan uudelleenjärjestelyitä. Toistaiseksi niiden toteuttaminen on osoittautunut ylivoimaiseksi. (T18)

Taloudellista tilaa vaikeutti myös vuonna 2019 tehty yrityskauppa. Vastaamon toiminnan päättyminen oli yksi konkreettisimmista tietomurron seurauksista.

6.3 Poikkeuksellisuus

Kriisitilanteet ovat poikkeuksellisia, muuten ne eivät olisi kriisejä. Tietomurrosta tiedottamiseen kuului poikkeuksellisuuden korostaminen. Analyysin aikana se osoittautui vaikeaksi koodiksi asettaa tiettyyn teemaan, joten jätin sen niiden ulkopuolelle. Poikkeuksellisuus oli kuitenkin oleellinen tietomurron piirre. Poikkeuksellisuus toimi samanaikaisesti sekä luottamusta rakentavana että luottamusta rikkovana tekijänä. Tietomurto oli poikkeuksellisen laaja ja arkaluontoisilla tiedolla tehdyt kiristykset ovat melko harvinaisia. Tietoturva on Suomessa yleensä niin korkealla ja valvotulla tasolla terveydenhuollon sektorilla, ettei tällaisia tietomurtoja pääse tapahtumaan. Tilanteen poikkeuksellisuus toi mukanaan vaikeuden toimia oikein, sillä mitään ennalta hyväksi todettua tai varmaa toimintatapaa ei ollut olemassa. Poikkeuksellisuudesta viestittiin tiedotteissa nostamalla esiin huolenpito ja tuki asiakkaille ja henkilökunnalle.

Vastaamon tärkein tehtävä nyt on asiakkaiden ja työntekijöiden tukeminen poikkeuksellisen vakavan ja raskaan tilanteen keskellä. (T6)

Tiedotteista ei jää epäselväksi, että kyseessä on nimenomaan kriisitilanne. Kriisin ytimessä ovat uhrin ja varsinkin tiedotteiden alkupuolella myös Vastaamo esitettiin uhrina.

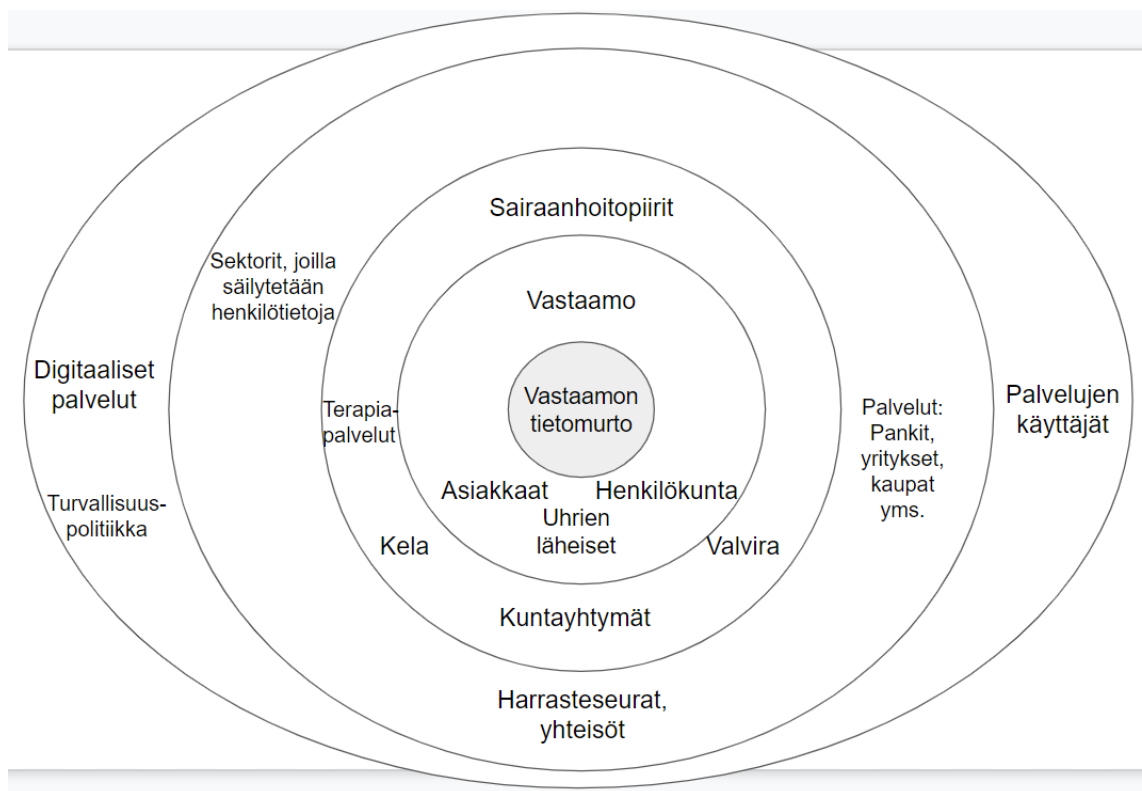
Kriisitilanteesta johtuva hätä on suuri. (T4)

Yhteistyö, viranomaisten tuki ja etenkin kolmannen sektorin apu on auttanut tietomurron uhriksi joutuneita pahimman kriisivaiheen yli. (T15)

Yllä olevassa aineistoesimerkissä mainitaan, että ”pahimman kriisivaiheen yli” on päästy. Kyseisen tiedotteen perusteella kriisin pahin vaihe alkoi tietomurron tultua julkiseen tietoon, eli kiristäjän lähettäessä kiristyskirjeitä asiakkaille. Kriisi ei kuitenkaan missään vaiheessa loppunut. Uhreille kriisi ei loppunut edes konkurssiin, sillä tiedot ovat edelleen verkossa ja hallitsemattomissa.

6.4 Yhteiskunnalliset uhkakuvat

Seuraavaksi siirrän näkökulman Vastaamoa laajemmalle, yhteiskunnalliselle tasolle. Vastain näin toiseen tutkimuskysymykseeni eli siihen, millaiseksi uhkaksi tietomurto määrittyi. Ylen uutiset luovat laajempaa taustaa ja yhteyksiä niin tietomurrolle kuin Vastaamon tiedotteille. Olen jakanut uutisissa esiin nousseet teemat neljään tasoon, joilla tietomurto muodostui uhkaksi. Aloitan yksilötasolta, eli tietomurron uhreista. Seuraavaksi tulee yritystaso, mutta Vastaamolle aiheutuneet uhkakuva tulivat jo pitkälti esille tiedotteissa. Tässä tuon esille niitä kohtia, mitä tiedotteissa ei mainittu. Kuvassa 3 olen asettanut yksilöt ja Vastaamon samalle tasolle, sillä tietomurrolla oli suurin vaikutus näihin kahteen toimijaan. Yritystason jälkeen käsittelen uhkakuvia koskien terveydenhuollon sektoria. Tämän jälkeen laajennan näkökulmaa myös muihin digitaalisiin palveluihin. Lopuksi tuon esille yhteiskunnallista riskikeskustelua tietomurron synnyttämistä uhkakuvista.



Kuva 3. Uutisten lähiluennassa muodostuneet digitaalisen yhteiskunnan tasot, joita tietomurron uhkakuvat koskettivat.

6.4.1 Tietomurron uhrin – “kuin löysässä hirressä”

Suurinta vahinkoa tietomurrosta kärsivät kymmenet tuhannet uhrin. Uutisissa esiin nostettuja yksilötason uhkakuvia olivat 1) tietomurron seuraukset uhreille (tietojen väärinkäyttö), 2) seurausten pitkäaikaisuus, 3) hoidon päättymisen asiakkaille ja töiden päättymisen Vastaamon henkilöstölle, 4) neuvottomuus, 5) tietoisuus uusista riskeistä ja 6) tietojen suojaamisen tehottomuus ja järjestelmien ulkopuolelle jääminen.

Asiakas kuitenkin varsin voimaton, jos terveydenhuoltoalan tietoturva pettää, kuten Vastaamon tapauksessa on käynyt. (U19)

Keskivertokansalainen ei ole ehkä aiemmin ollut huolissaan omasta tietosuojastaan tai sen riskeistä, mutta nyt sekin voi mietittyä. (U46)

Ensin viedään terveystiedot sitten uhrin pitää pelätä, että identiteettikin varastetaan. Anastettuja henkilötietoja voidaan käyttää vuosienkin jälkeen esimerkiksi varkauksien ja petosten tekoon. Tästä voi koitua uhrille merkittävää vahinkoa. (U49)

Tietomurron jälkeen uutisissa puhuttavin teema oli uhrit. Asiakkaiden ja henkilökunnan lisäksi uhreja saattoivat olla asiakkaiden läheiset, jos heistä oli kirjattu tietoja potilaskertomuksiin. Uhrien asemaa ja tilannetta käytiin läpi uutisissa yhä uudestaan, uhreja haastateltiin ja heille uutisoitiin uusimmista suositelluista toimenpiteistä.

Yksilötasolla tietomurto aiheutti paljon henkistä kärsimystä. Huoli liittyi uhkiin ja pelkoihin seurauksista, joita tietomurto aiheuttaa. Uhrien kannalta näitä uhkia ovat identiteettivarkaudet, henkilökohtaisten tietojen väärinkäyttö, kiristys, huijaukset ja henkilökohtaisten tietojen paljastuminen, jota seuraa kasvojen menetys. Joillekin pelkkä terapiassa käynnin paljastuminen aiheutti murhetta (U14). Näitä asioita ehkäistäkseen, uhreja neuvottiin hankkimaan luotto- rekisteröinti- ja osoitteenmuutoskiellot.

Maija sai keskiviikkona lukea Ylen uutisista, että hakkerit ovat varastaneen psykoterapiakeskus Vastaamon potilaiden arkaluontoisia tietoja.

Siitä lähtien hän on elänyt pelossa.

Ovatko terapiakertomukseni jossain ihmisten nähtävillä? Onko henkilötietoni jo myyty jonnekin? Perustaako joku nyt minun nimissäni yrityksen tai ottaa pikavipin? (U18)

Pelko, yksityisyyden menettäminen, tietojen turvaaminen, epätietoisuus, epävarmuus, odotus pitkästä oikeusprosessista, huoli oman hoidon jatkumisesta. Pitkälti näistä asioista koostuivat uutisissa tietomurron uhrien kokemukset ja uhkakuvat. Uutisissa esiintyvät asiantuntijat kritisoivat Vastaamon toimintaa siitä, ettei asiakkailta ollut heti mahdollisuutta tarkistaa rekisteritietonsa (U30). Kiristys teki tietomurrosta entistä mutkikkaamman. Uhkana oli joko menettää rahansa, menettää tietonsa tai molemmat, kuten kävikin lunnaat maksaneille (U69).

– Koko ajan olen pelännyt, etten kerkeä ilmoittamaan kaikkialle henkilötietojeni vuotamisesta. Se on ollut stressaavaa ja väsyttävää. [– –] Maria ahdistaa nimenomaan henkilötietojen vuotaminen, ei niinkään arkojen potilaskertomusten tuleminen julkiseksi.

[– –] Mieltä painaa odottaminen ja epätietoisuus siitä, miten henkilötietoja mahdollisesti käytetään hyödyksi. Samalla vaivaa tieto siitä, että poliisin rikostutkimus ja mahdolliset oikeudenkäynnit kestävät pitkään.

Nyt Maria pelottaa, että tietovuoto haittaa hänen toipumistaan. (U88)

Monille Vastaamon asiakkaille tietomurto tarkoitti epävarmuutta oman hoidon jatkumisesta. Vastaamon tulevaisuus oli vaakalaudalla, mikä tarkoitti, että myös potilaiden tulisi mahdollisesti etsiä uusi paikka terapiakäynneille. Tästä kirjoitettiin uutisissa esimerkiksi Kelan lopettaessa potilaiden ohjaamisen Vastaamolle. Kelalta tuli Vastaamoon tuhansia potilaita ja Kela ei voinut lupautua hankkimaan uutta terapeuttia, jos Vastaamon tietoturva havaittaisiin puutteelliseksi (U81). Asiakkaat jatkoivat Vastaamolla, mutta heitä uhkasi terapiakäyntien keskeytyminen jo muutenkin stressintäyteisessä kriisitilanteessa. Asiakkaana olleet uhrin jäivät siis hyvin epävarmaan tilanteeseen, tyhjän päälle. Vastaamon työntekijät ja terapeutit puolestaan olivat jäämässä konkurssin myötä ilman työpaikkaa pitkään jatkuneen kriisitilanteen jälkeen (U116).

Tietomurto vaati lisätoimenpiteitä uhreilta. Erialaisten kieltojen hankkimisen lisäksi henkilöllisyyttään saatettiin suojata eri tavoin. *“Esimerkiksi henkilötietojen piilottamista, kanta-asiakkuuksien lopettamista, netissä tehtyjen rekisteröitymisten purkamista ja niin edelleen”*, kommentoi yksi uhreista neljän kuukauden päästä tietomurrosta (U119).

Kielloista, estoista ja itsensä suojaamisesta on tullut "Annalle" jokapäiväinen työ. Jopa it-ekspertit ja poliisi ovat neuvottomia. (U119)

Edellä olevassa esimerkissä viitataan myös siihen, että asiantuntijatietokin oli pettänyt, eivätkä uhrin saaneet tarvittavaa tukea tietojensa suojaamiseen. Tietojen uudelleen ilmestyminen verkkoon tarkoitti monelle rikoksen pitkittymistä koskevien uhkien realisoitumista. Tietojen leviäminen verkossa tarkoitti, ettei koskaan voinut tietää milloin ja miten tietoja hyväksikäytetään.

Identiteettivarkauden kohteeksi joutuneet ihmiset ovat löysässä hirressä.

– Uhrin kannalta tilanne on erittäin epämiellyttävä. On hankalaa arvioida, millä todennäköisyydellä ja milloin voi joutua rikoksen uhriksi, Ulkuniemi toteaa. (U117)

Takuuvarmaa tapaa suojata tietoa ei ole, joten vaikka kaikki suojautumiskeinot otettiin käyttöön, tietojen väärinkäyttöön jäi kuitenkin mahdollisuus. Tietomurron jälkeen tuli ilmi, että helppoa keinoa vaihtaa esimerkiksi henkilötunnusta ei ole. Vaikka uhri tekisi kaikki kiellot, henkilötunnusta pystyy kuitenkin käyttämään väärin. Moni tämänhetkisistä palveluista toimii tunnistautumisen kautta, joista osaan käy pelkkä henkilötunnus. Tunnuksen vaihtaminen saattaa johtaa valtavaan järjestelmien tietokatoon, sillä henkilöä ei voida enää yhdistää hänen vanhoihin tietoihinsa. Olemassa olevien toimenpiteiden tehottomuus ja toisaalta järjestelmien ulkopuolelle jääminen muodostui uhkakuvaksi uhreille, jotka halusivat taata tietojensa turvan. Keskustelu henkilötunnusten vaihtamisesta kuumeni Ylen uutisoinnissa ja esimerkiksi hallitus kokoon-tui keskustelemaan asiasta pian tietomurron jälkeen. Asiassa ei kuitenkaan edistytty, eikä päätöksiä tehty. Poliitikoilta odotettiin toimia ja uutisissa toistui kuva neuvottomasta uhrista, jolla ei ollut mahdollisuutta vaikuttaa asioihin (U119).

6.4.2 Varoittava esimerkki: Vastaamo

Uutisissa käytettiin usein lähteenä Vastaamon tiedotteita ja niistä raportointiin pitkälti samat asiat. Ylen uutisissa haastateltiin Vastaamosta lähinnä hallituksen puheenjohtaja Tuomas Kahria, sekä myöhemmin uutta puheenjohtajaa Heini Pirttijärveä. Heidän puheenvuoronsa edustivat Vastaamon maineenhallintaa ja niissä toistuvat tiedotteiden viestit. Ylen uutisista voi nähdä, miten tietomurtoa uudelleen kehystetään tiedotteisiin verrattuna. Esimerkiksi Vastaamon taloudellinen ahdinko tietomurron jälkeen oli Ylen uutisoinnissa aikaisemmin esillä (U52). Osa asiakkaista ja terapeuteista lähti Vastaamolta, mistä mainittiin vain ohimennen tiedotteissa. Tiedotteissa ei mainittu, että Kela lopetti uusien asiakkaiden ohjaamisen Vastaamoon marras-kuussa. Tiedotteissa ei myöskään mainittu, että Kela ja Pirkanmaan sairaanhoitopiiri alkoivat purkaa sopimuksiaan Vastaamon kanssa (U114). Syynä oli Kelan selvitys, jonka mukaan osa Vastaamon psykoterapeuteista ei täyttänyt vaatimuksia, jotka on asetettu vaativan lääkinällisen kuntoutuksen yksilöterapijan kilpailutuksessa (U107). Myös Helsingin kaupunki asetti Vastaamon palvelut ostokieltoon (U80). Tietomurto asetti Vastaamon suurennuslasin alle. Yritykseen kohdistui tietomurtoselvitysten lisäksi toiminnantarkastuksia. Vastaamo oli esimerkiksi tietoturvasääntöjen vastaisesti lähettänyt asiakkaille suojaamattomalla sähköpostiyhteydellä

henkilötunnuksia sisältäviä asiakirjoja ja laskuja (U57). Voi olla, että ilman tietomurtoa näitä puutteita ei oltaisi huomattu.

Yle lainaa Iltalehteä, jonka mukaan Vastaamo palkkasi kriisiviestintään ja maineenhallintaan erikoistuvan Tekirin hoitamaan viestintää (U50), mistä ei ollut mainintaa tiedotteissa. Samassa artikkelissa on haastateltu asiantuntijaa, jonka mukaan Vastaamon kriisiviestintä oli epäonnistunut. Viestinnän virheitä olivat esimerkiksi viestiminen vasta pakon edessä, yrityksen uhriutumisen, valmistautumattomuus kriisiin sekä puutteellinen ja myöhäinen ohjeistus uhreille. Vastaamon valmiustautumattomuudesta kertoi esimerkiksi se, että suojattu sähköinen järjestelmä, jonka kautta asiakkaat pystyivät tarkistamaan rekisteritietonsa valmistui vasta viikkoja tietomurron julkitulon jälkeen. Ennen tätä asiakkaita vaadittiin hakemaan tiedot Vastaamon tiettyistä toimipisteistä, joita koko Suomessa oli vain viisi, minkä lisäksi toimipisteet olivat auki hyvin rajoitettuna aikoina. Tehdessään ilmoituksen tietomurrosta tietosuojavaltuutetulle Vastaamo oli Ylen mukaan esittänyt, ettei jokaiselle asiakkaalle erikseen asiasta ilmoittaminen ole tarpeen.

Vastaamo ilmoitti tapahtuneesta tietosuojavaltuutetulle seuraavana päivänä. Samalla yritys katsoi, että uhreille ei olisi tarpeen tiedottaa henkilökohtaisesti.

– Se vaatisi kohtuutonta vaivaa ja loukkauksesta ilmoitetaan julkisella tiedonannolla, ilmoituksessa todettiin. (U90)

Vastaamo oli arvioinut tietomurron laajuuden vähäisemmäksi kuin mitä se todellisuudessa oli. Alkuun arvio oli, että tietomurto koskettaa noin tuhatta ihmistä (U93). Vastaamon ilmoittaessa tietomurron uhreille tilanteesta, viesti lähetettiin suojaamattoman sähköpostiyhteyden kautta (U74).

Eräs Ylen uutisten haastattelema uhrin äiti kuvasi tilannetta vastuuttomaksi Vastaamon puolesta.

Se on kuin lainaisin hyvän ystäväni kotia alueella, jossa on paljon asuntomurtoja. Jättäisin oven auki, talo tyhjennettäisiin, ja sitten minä vain pahoittelisin tilannetta. Kyllähän minun pitäisi auttaa rikosilmoituksen teossa, uusien kalusteiden hankinnassa ja niin edelleen. Nyt Vastaamo uhriutuu tässä, vaikka he jättivät oven selälleen, hän sanoo. (U18)

Vastaamon toimintaa ei nähty hyväksyttävänä niin asiantuntijoiden kuin uhrien näkökulmasta. Vastaamon mainekriisistä kirjoitetaankin uutisissa viikko tietomurron julkitulon jälkeen siihen sävyyn, että maine on jo menetetty.

Myös uhka mainehaitasta on Vastaamon kohdalla jo toteutunut. Asiakkaiden ja yhteistyökumppaneiden luottamus yhtiöön on kokenut kolauksen. (U51)

Myös Suomalaisen Työn Liitolle tilanteessa oli riski maineuhalle, sillä se oli aikaisemmin myöntänyt Yhteiskunnallinen yritys -merkin Vastaamolle. Nyt yritys osoittautui epäluotettavaksi ja maineensa menettäneeksi. Yle uutisoi, että Suomalaisen Työn Liitto pohti, pitäisikö merkki ottaa pois Vastaamolta (U73). Eli myös kaikki Vastaamon kanssa yhteistyössä olleet yritykset joutuivat maineriskiinkin.

6.4.3 Terveysthuollon sektori ja valvonta – kyseenalaistetut tahot

Tietomurto paljasti järjestelmien heikkouden, jota ei oltu otettu huomioon aikaisemmin. Sosiaali- ja terveydenhuoltoalan tietoturva tuli tietomurron jälkeen kyseenalaistetuksi ja uhatuksi.

Psykiatriakeskus Vastaamon tietomurto on tuonut esiin potilastietojärjestelmien haavoittuvuuden Suomessa. (U83)

Erityiseksi huolenaiheeksi nousi kansallinen Kanta.fi -järjestelmän tietoturva. Terapiakäyntien kirjaaminen Kantaan on puhuttanut aikaisemminkin, sillä sen on ajateltu vaikuttavan luottamukseen terapeutin ja potilaan välillä (U109). Tietojen kirjaaminen Kantaan helpottaa kuitenkin merkittävästi erilaisia siirtymiä, asiakkaan muuttaessa eri paikkakunnalle tai terveydenhuollon yksikön vaihtuessa. Tiedot ovat saatavilla yhdestä tietokannasta, jolloin tiedot ovat myös asiakkaalle saavutettavampia. Kantaan jää myös digitaalinen jälki jokaisesta tietojen katselu-

kerrasta. Myös potilas voi tarkistaa mikä organisaatio on katsonut omia tietoja ja pyytää selvitystä tarvittaessa (U109). Kannan tietoturvaan pohdittiin tietomurron jälkeen myös eduskunnan tasolla (U46, U98). Eri terveydenhuollon tahot eivät ole yhtä vahvasti sitoutuneita ylläpitämään tietosuojaa, mikä uhkaa lopulta koko järjestelmää.

On ajateltu, että omat sosiaali- ja terveystiedot ovat parhaiten turvassa, koska tiedot ovat hyvin henkilökohtaisia. Ovatko ne?

Alan tietoturva säädelään laissa, mutta kyse on siitä miten tarkasti säädöksiä noudatetaan. Jotkut tekevät tietoturvan eteen enemmän töitä kuin toiset. (U46)

Alan laajuus ja toimijoiden monimuotoisuus tarkoittaa vaikeasti hallittavaa ja valvottavaa kokonaisuutta. Yksittäiselle kansalaiselle voi olla vaikeaa tai jopa mahdotonta saada kokonaiskuva tilanteesta.

Yksittäisen ihmisen on vaikea arvioida sitä, miten eri sote-alan toimijat suojaavat tai eivät suojaa omia tietojaan, koska eri toimijoita on lukemattomia. (U46)

Julkisen terveydenhuollon sektorin vastuuta tietomurron tapauksessa tuotiin esille siinä, että heidän tulisi vähintäänkin huolellisesti valita kumppaninsa. Tietosuoja-asetuksen perusteella sairaanhoitopiirit voivat olla korvausvastuussa tietomurron uhreille (U114). Myös terveydenhuollon sektorilla oli epävarmuutta siitä, kuinka moni potilaista on joutunut uhriksi. Moni uutinen käsitteli tietomurron laajuutta käyden läpi mitkä kuntien sairaalat ovat saattaneet altistua tietomurrolle ja mitkä sairaanhoitopiirien järjestelmistä olivat turvassa. Uutisten mukaan ainakin Uudenmaan, Pirkanmaan, Varsinais-Suomen ja Kanta-Hämeen sairaanhoitopiireissä oli asiakkaita, joita tietomurto kosketti. Kaikki sairaanhoitopiirit, kuntayhtymät ja Vastaamon kumppanit voitiin nähdä osasyllisinä.

Rekisterinpitäjä kantaa vastuun vaikka valittu kumppani möhlisi. Jos sairaanhoitopiiri on ostanut palveluita, sen vastuulla on valita huolelliset ja luotettavat kumppanit.

Myös tietosuojavaltuutetun toimisto on todennut, että jatkossa sen arvioitavaksi voivat tulla myös Vastaamolle tehtäviä ulkoistaneiden organisaatioiden toimenpiteet. (U63).

Terveydenhuollon sektorin lisäksi Valvira joutui kyseenalaistetuksi esimerkiksi siitä, miksi Vastaamon kokoluokan yritystä ei oltu luokiteltu A-luokan järjestelmään (U30). Valvira erottaa

kaksi eri valvonnan järjestelmää terveydenhuollon tietoturvasa: A- ja B- luokan. A-luokan järjestelmään kuuluvat Kelan ylläpitämät Kanta-palvelut, sekä järjestelmät, joiden on tarkoitus liittyä Kantaan suoraan tai välityspalveluiden kautta. A-luokan järjestelmiä valvotaan säännöllisesti. B-luokkaan kuuluvat puolestaan yksityiset yritykset, joille riittää tietoturvasuunnitelman laatiminen ja toimittaminen Valviraan ennen toiminnan aloittamista. (Valvira, 2021). Tämän jälkeen tietoturvan valvonta perustuu omavalvontaan, eikä Valviran puolelta tehdä tarkastuksia, ellei jotain poikkeavaa tapahdu. Vastaamo kuului B-luokan järjestelmään, vaikka yrityksellä oli tietomurron julkitulon aikana yli 18 000 palveluja käyttävää asiakasta. Valviran toiminta yksityisen psykoterapiatoiminnan kohdalla käytiin läpi perinpohjaisesti uutisissa, mikä paljasti valvonnan perustuvan täysin omavalvontaan (U67). Valviran edustajat toivat itse esille uutisissa, että resurssien vähäisyys tarkoittaa sitä, ettei kaikkia yksityisiä järjestelmiä voida valvoa yhtä tehostetusti kuin kansallisia.

En halua marista resursseista, mutta totta kai valvonnan maltillinen lisääminen olisi hyödyllistä potilasturvallisuudelle ja asiakasturvallisuudelle. En usko, että se olisi edes yksityisen sektorin liiketoiminnan vastaista. (U67)

Valviran toiminnan läpikäyminen vahvisti uhkakuvaa siitä, että valvontaviranomaisten työ voi olla tehotonta ja tuloksetonta. Uutisissa todetaankin, että valvonta on enemmän reaktiivista kuin ennaltaehkäisevää ja yleensä asioihin puututaan vasta kun ongelma on ilmennyt (U61). Uhkakuvaksi syntyi valvonnan riittämättömyys ja vanhentunut toimintamalli. Voiko valvontaan erikoistuvaan tahoon luottaa tulevaisuudessakaan, jos he eivät pystyneet estää tietomurtoa ja pitää huolta valvonnan tasosta? Valvontajärjestelmä saattaa tarvita uudistusta ja päivitystä, jotta sen toiminta vastaisi uusia tarpeita.

Tietomurto aiheutti myös huolta sen suhteen, uskaltavatko asiakkaat hakeutua terapiapalveluihin. Kansalaisten epäluulon pystyi huomaamaan esimerkiksi kasvaneiden tietopyyntöjen määrässä koskien terveydenhuollon tietosuojaa (U46).

Ongelmallista psykoterapiakeskuksen tietomurron kohdalla on, että arkaluontoisten tietojen vuotaminen voi murentaa luottamusta avun hakemiseen. (U28)

Psykoterapiakeskus Vastaamon tietomurron jälkeen monelle terapiassa käyvälle on herännyt huoli siitä, miten ja missä omia potilastietoja säilytetään. Tämän on huomannut työssään Terapeuttitalon toimitusjohtaja Ritva Huusko.

– Asiakkaita pelottaa, että oman elämän arkaluonteiset asiat päätyvät väriin käsiin. (U109)

Kyseessä on yhteiskunnallinen uhka, jos kansalaiset eivät hakeudu tarvittavaan hoitoon luottamuspuolan takia. Yrityksille asiakkaiden epäluottamus tarkoittaa asiakasvirran tyrehtymistä ja mahdollisia liiketappioita. Ylen haastattelema terapeutti mainitsi, että vaikka luottamus yksittäisiä terapeutteja kohtaan tuskin vähenee, tietomurto sen sijaan aiheutti luottamuksen horjumista koko alaa kohtaan (U33). Terveystalolla työskentelevä johtava psykologi vahvisti, ettei peruutuksia terapiakäynneille ole tullut, mutta kyselyjä potilastietoturvasta on tehty. Hän puhui tietomurron kauaskantoisuudesta: *“Vastaamon tietovuoto herättää hämmennystä ja huolta niin paljon, että sen laineet ulottuvat pitkälle”* (U33).

Tämän tason uhkakuvia olivat seuraavat kolme asiaa: 1) potilastietojärjestelmien heikkoudet, 2) tietoturvan valvonnan tehottomuus ja epäonnistuminen ja 3) kansalaisten luottamuksen menetys terapiatoimintaan.

6.4.4 Muut digitaaliset palvelut ja kriisien auttajat – kriisin dominoefekti

Yksilötason huolet heijastuvat myös muihin kuin terveydenhuollon toimijoihin, kuten kaikkiin digitaalista tietokantaa käyttäviin yrityksiin. Myös vapaa-ajan seurat tai pienimuotoiset yhteisöt käyttävät toiminnassaan digitaalisia palveluita ja rekistereitä.

Tätä prosessia kannattaa seurata kaikkien, jotka käsittelevät henkilötietoja työssään tai vapaa-ajallaan. Tietosuojakysymyksiä eivät voi välttää enää urheiluseurataan. (U14)

Tietomurron takia uhrit huolestuivat tietojensa väärinkäytöstä esimerkiksi pankkiasioissa. Ylellä uutisoitiinkin pankkien joutuneen viestimään asiakkailleen siitä, ettei heidän tarvitse olla huolissaan tietojensa puolesta.

Pankit ovat viime päivinä joutuneet tiedottamaan ja rauhoittelemaan tietoturvasta huolestuneita asiakkaitaan.

Psykoterapiakeskus Vastaamon potilastietomurron jälkeen esimerkiksi Osuuspankki on tiedottanut verkkosivuillaan, ettei tietomurrossa ole viety pankkiasioinnin vaarantavaa tietoa. Samoin Säästöpankkiryhmä on tiedottanut, että pankkiasiointi ei ole vaarantunut.

Säästöpankkiryhmässä on vastattu yksittäisiin tietomurron uhriksi joutuneiden kyselyihin. Säästöpankkiryhmään kuuluvat itsenäiset Säästöpankit ympäri Suomen.

– Meiltä on kysytty esimerkiksi, onko tarpeen sulkea verkkopankkitunnuksia tai maksukortteja. Meidän viestimme on selvä, tällaista ei tarvitse Vastaamon tietomurron takia tehdä, toteaa tietoturvapäällikkö Vesa Pyyluoma Säästöpankkiryhmästä. (U76)

Yksityisen terveyssektorin yritykset Mehiläinen ja Terveystalo esiintyivät myös uutisissa vaikkeen tietoturvan olevan kunnossa (U33). Uhkakuvaksi syntyi dominoefekti: jos Vastaamon tietokanta vietiin, niin miksei sama voisi tapahtua muissakin yhtiöissä. Toisaalta jo vietyjen tietojen väärinkäyttö saattoi aiheuttaa ongelmia palveluiden käytössä. Vuodetut tiedot aiheuttivat kohonneen riskin petoksiin, jolloin esimerkiksi pankkien, kauppojen ja luottoja tarjoavien palvelujen tuli olla erityisen varovaisia, ettei asiakkaiden varoja päädy väärin käsiin.

Kriisitilanne vaati ponnistuksia niiltä tahoilta, jotka auttoivat uhreja tai selvittivät tapahtunutta. Tämä saattoi vaikuttaa yrityksen tasolla menoihin ja yksilötasolla kiireisempiin ja pidempiin työpäiviin. Suuri yhteydenottojen määrä Rikosuhripäivystykseen ja Mieli ry:hyn vaati lisäresursseja.

Psykoterapiakeskus Vastaamon tietomurron uhrit ovat kääntyneet poliisin ohella myös Rikosuhripäivystyksen puoleen.

Perjantaina päivystyksen chatissa keskusteluja käytiin kuusi kertaa enemmän kuin yleensä perjantaisin. Puhelimessa keskusteluja oli jopa kahdeksankertainen määrä tavanomaiseen verrattuna, kertoo suunnittelija Jenni Kreivi Rikosuhripäivystyksestä.

– Pystyimme reagoimaan nopeasti ja saimme ruuhka-apua palveluun. (U19)

Myös poliisi kertoi tiedotustilaisuudessaan, että heiltä on vaadittu nopeaa toimintaa ja lisäresursseja tilanteen kärjistyessä. Tässä on otettava huomioon, että myös auttavien tahojen puheen-
vuorot ovat osa mediaesitystä.

Tutkinta etenee kiivasta tahtia. Siitä kertoo se, että tutkijat tekee töitä lähes tauotta. Heitä on hälytetty töihin vapaalta. Kaikki ammattitaito, mitä poliisilla on käytössään, on valjastettu tämän asian tutkimiseen. (U26)

Poliisi tiedotti, että rikosilmoitusten suuren määrän takia sähköinen asiointipalvelu oli ruuhkautunut (U20). Myös Kuluttajaliitto tiedotti puhelinpalvelunsa ruuhkautuneen, minkä takia kaikkiin soittoihin ei pystytty vastaamaan (U30).

Toisaalta esimerkiksi F-Securen tietoturvajohdaja näki, että “*viralliset ja lailliset mekanismit ovat nyt pettäneet, siitä ei ole kahta puhetta*” (U53). Valviran valvonta nähtiin epäonnistuneena ja muilta viranomaistahoilta toivottiin nopeampaa ohjeistusta uhreille ja mahdollisuutta tarkistaa ovatko omat tiedot vuotaneet. Ensimmäisenä omien tietojen vuotamisen tarkastuspalvelua tarjosi psykologi Aapo Puskala, joka itse koodasi ohjelman. Kyseistä ohjelmaa odotettiin virallisilta tahoilta, joko poliisilta, tietosuojavaltuutetulta tai Vastaamolta. Hyvää tarkoittaenkin ohjelmaan liittyi laillisia ongelmia lähinnä rekisterinpidossa, jota tietosuojavaltuutettu selvitti (U53). Se nosti esiin uudemman kerran sen, ettei vastaavanlaisiin tilanteisiin olla varauduttu.

Tietoturvaauhkien vahvistuessa erilaiset kyberuhkia mittaavat ja estävät työkalut alkoivat ilmestymään eri toimijoilta, kuten Traficomilta ja Digi- ja väestötietovirastolta (U30, U42). Vastaa-
mon tapauksessa uhkaksi määrittyi myös epärehellinen toimitusjohtaja. Esimerkiksi Ylen haastattelema F-Securen tietoturvajohdajan mukaan tietomurto olisi voitu estää, jos yrityksen johto olisi ottanut tietosuojan vakavammin (U30). Yksi uhkakuvista on siis huonosti johdettu organisaatio ja sen sisällä ilmenevä epärehellisyys.

Kyberhyökkäys voi pysäyttää tai jopa lopettaa yrityksen tai organisaation toiminnan tai paljastaa arkaluonteisia tietoja. Tietoturva ei ole vain tekninen ongelma, vaan se kuuluu ylimmän yritysjohdon, hallituksen ja omistajien agendalle. (U30)

Digitaalisten palveluiden piirissä esiintyneet uhkakuvat olivat seuraavia: 1) huoli yritysten tietosuojasta, 2) kriisin dominoefekti ja vuodettujen tietojen väärinkäyttö, 3) kriisin vaatimat korkeat menot ja sen aiheuttamat ruuhkat, 4) odotusten pettäminen, ja 5) huonosti, epärehellisesti tai laiminlyövästi johdettu organisaatio ja sen seuraukset.

6.4.5 Yhteiskunnallinen taso – digitaalisen ympäristön kauaskantoiset uhat

Uutisissa puhuttiin muutoksesta, joka on teknologian tuomaa ja pelottavaa. Muutos liittyy etenkin teknologian välitteisesti tapahtuvaan rikollisuuteen, jonka määrä on ollut viime vuosina nousussa. *“Tämä kertoo muutoksesta, ja tämä on muutos todella huonoon suuntaan”*, kommentoi F-Securen toimitusjohtaja sitä, että tällä kertaa kiristetään potilastietojen avulla, kun yleensä rikokset on kohdistettu verkkokauppojen tietoihin (U55). Muutoksen ilmapiiri on havaittavissa eri teemoissa uutisissa, mutta kaikki ne liittyvät tavalla tai toisella digitalisaation kiihtymiseen: terapeutit eivät ole tyytyväisiä potilastietojärjestelmien digitaaliseen siirtymään (U109), kyberuhista puhutaan kansallisen turvallisuuspolitiikan yhteydessä (U68) ja koronapandemia on vauhdittanut eri elämän osa-alueiden siirtymistä verkkoon (U27). Lainsäädännön, turvallisuuden ja viranomaisten tulisi jotenkin pysyä mukana muutoksessa. Vastaamon tietomurto oli tämän muutoksen ilmentymä.

Vastaamon kaltaisilla esimerkeillä luottamus digitaaliseen yhteiskuntaan voi murentua.

Pahimmissa skenaarioissa yhteiskunta ja ihmiset haluaisivat luottamuspuolan takia palata takaisin kynä ja paperi -aikaan, jolloin menetettäisiin kaikki hyöty mitä digitaalisuudesta saadaan. (U46)

Vaikka kyseinen ääripään uhkakuva ei toteutunut, yllä oleva esimerkkilainaus kuvaa yhtä mahdollista luottamuksen menetyksen seurausta. Tietomurron yksi uhkakuvista oli yleinen luottamuksen menetys digitaaliseen yhteiskuntaan.

Uutisissa tuotiin esille asiantuntijanäkökulmia tietomurrosta ja sen seurauksista yhteiskunnalle. Haastateltavina olivat eri alojen professorit ja kyberturva-asiantuntijat. Heidän puheenvuoronsa

käsittelivät yleensä laajoja yhteiskunnallisia teemoja ja uhkakuvia. Kyberturvallisuuden työelämäprofessori Jarno Limnéll esiintyi useammassa uutisessa ja kuvasi yhdessä niistä tietomurtoa tärkeänä herätyksenä niin yrityksille kuin yksittäisille kansalaisille.

Tämä on kolaus suomalaiseen digitaaliseen yhteiskuntaan. Ihmiset miettivät nyt, miten tallennettujen, arkaluontoistenkin tietojen turvallisuuteen voi luottaa. Meillä on ollut vahva luottamus, että arkaluontoiset asiat pysyvät oikeissa käsissä. (U27)

Limnéll jatkaa samassa uutisessa, että kyseisen kriisin hoitaminen tulee vaikuttamaan siihen, millaisena luottamus pysyy tulevaisuudessa. Tietomurto toi esille sen, että yhteiskunnalliset toimijat eivät ole varautuneet vastaavanlaisiin digitaalisiin kriiseihin.

Digi- ja väestötietoviraston johtava erityisasiantuntija Kimmo Rousku haluaa herätellä yritysten johtoa tietoturva-asioissa. Hänen mukaansa digitaalisen maailman suuronnettomuuksiin on varauduttu Suomessa heikommin kuin esimerkiksi luonnonilmiöihin. (U42)

Yksi uhkakuvista oli myös se, ettei Vastaamon tapaus jää viimeiseksi. Uutisissa sisäministeri Maria Ohisalo toi esille kyberturvallisuutta, painottaen parempaa varautumista tuleviin tapauksiin.

Ohisalon mukaan kyberturvallisuutta koskeva uhka koettelee paitsi suomalaista yhteiskuntaa myös kansainvälisesti.

–Ensinnäkin tämä ei ole ensimmäinen kerta ja se, mikä on varmaa, niin tämä ei myöskään ole viimeinen kerta. Kyseessä on erittäin vakava tietomurto.

Hän sanoo, että Suomessa pitää olla enemmän keinoja puuttua tällaiseen uhkaan.

– Tässä pitää toimia nopeasti, koska rikollisetkin löytävät jatkuvasti uusia keinoja hyväksikäyttää yhteiskuntaa ja ihmisiä. (U21)

Ylen uutiset määrittelivät tietomurron yhteiskunnallisesti merkittäväksi tapahtumaksi ja sitä kuvailtiin erilaisin tavoin: lento-onnettomuudeksi (U14), erittäin järkyttäväksi (U62), poikkeuksellisen kylmäveriseksi (U69), kauhuesimerkiksi ja digitaaliseksi väkivallaksi (U75). Asiantuntijat ja ministerit pohtivat voisiko Onnettomuustutkintakeskus tutkia asiaa (U62, U75). Yhteis-

kunta nähtiin uhattuna: digitaalisen ympäristön heikkoudet johdattivat hakkerit ja kyberrikolliset hyökkäämään. Presidentti Sauli Niinistö kommentoi tietomurtoa “säälimättömän julmaksi” ja tiivistä sen vaikutukset kaikkia, eli koko yhteiskuntaa koskeviksi.

Tämä koskettaa meitä kaikkia. Jokaisesta meistä kertyy tietoa jatkuvasti eri alustoille. Se koskee meitä myös niin, että meillä kaikilla on oma sisin, jota haluamme varjella. Nyt sitä on loukattu, Niinistö sanoo Ylen haastattelussa. (U29)

Vastaamon tietomurtoa käsiteltiin kansallisen turvallisuuspolitiikan kannalta. Loppuvuoden turvallisuuspolitiikan yhteenvedoissa turvallisuustilanne nähtiin heikentyneenä esimerkiksi kyberhökkien takia, mihin Vastaamon tietomurto oli osasyy.

Myös Psykoterapiakeskus Vastaamon tietomurron kaltaisilla tapauksilla voi olla turvallisuusvaikutuksia. Ihmisten luottamus yhteiskuntaan voi heikentyä tai murrolla saatuja tietoja voidaan käyttää väärin vakoilussa, pahimmillaan esimerkiksi ihmisten painostuksen keinona. (U68)

Tietomurto esitettiin uutisissa Niinistön puheiden perusteella uudenlaisena, uuden teknologian tuomana ilmiönä, joka horjuttaa turvallisuuden tunnetta yhteiskunnassa (U105). Niinistön mukaan sana ”tietomurto” antaa tapauksesta liian harmittoman kuvan.

Kyberhyökkäykset ovat Niinistön mukaan hyökkäyksiä koko yhteiskuntajärjestystä kohtaan ja niitä pitää torjua paremmin. (U105)

Tietomurto asetettiin yhteiskunnallisten uhkakuvien kehikkoon, joihin tulee varautua ja ole-massa oleva tietotaito päivittää. Uutisissa tuotiin esille erittäin laaja yhteistyö, jossa yhdistyivät eri alojen asiantuntijoiden tieto ja pyrkimys auttaa uhreja, löytää rikollinen ja estää uusien tapauksien ilmentyminen. Yhteistyöstä muodostui monimutkainen verkosto tekijöitä, jotka osallistuvat tietomurron jälkiselvittelyyn. Uutisissa mainittiin valkohattuhakkerit, jotka auttoivat poliisia tai testasivat järjestelmien turvallisuutta. Poliisit kiittivät ahkerasta kansalaisyhteistyöstä, sillä verkossa liikkuvat silminnäkijät jättivät ennenäkemättömän paljon nettivinkkejä.

Ensimmäistä kertaa poliisi on saanut todella paljon vihjeitä ja vinkkejä tietoverkon niin sanotuilta silminnäkijöiltä. Tässä Vastaamo-tapauksessa on yhteiskunnallinen ulottuvuus. Aikaisemmin emme ole saaneet isoissakaan tietomurroissa näin merkittävästi yleisvihjeitä. Tämä on käänne tietoverkkorikosten tutkinnan osalta. (U91).

Liikenne- ja viestintäministeriö kokosi työryhmän, joka koostui eri ministeriöiden ammattilaisista. Ryhmän tavoitteena oli arvioida yhteiskunnallisten toimialojen tietoturvaa (U84). Kansalaisjärjestöt järjestivät kriisitukea ja media osallistui aktiivisesti uhrien ohjeistamiseen. Tietomurron jälkeen syntyi pienimuotoinen sosiaalisesta mediasta lähtöisin oleva kansanliike tunnistamalla #enjaa ja #enlue (U74). Poliitikot pohtivat miten uhreja voidaan auttaa ja estää vastaavat tilanteet tulevaisuudessa. Pääministeri Sanna Marin kommentoi tilannetta ja tietomurto oli hallituksen iltakoulun pääteema (U62). Tilanne nähtiin niin isona uhkana, että se sai monia yhteiskunnallisia tahoja liikkeelle.

Tietomurto lisäsi ymmärrystä tietoverkkorikoksista, minkä myötä huomattiin muutostarpeita. Asiantuntijoiden mukaan uudet uhat on otettavat huomioon yksi askel hakkereita edellä, joten valppaana tulee olla niin yksilö-, yritys- kuin valtiontasolla (U1). Tietomurto vauhditti luopumista pelkän henkilötunnuksen avulla tunnistautumisesta ja siirtymistä vahvaan tunnistautumiseen. Muutos haluttiin myös siihen, että kaikki potilastietojärjestelmät olisivat osa kunnallista Kanta-järjestelmää, joka takaisi paremman tietoturvan (U61). Uhkakuva oli tässä tapauksessa lainsäädännön vanhentuminen, sillä se ei pysynyt muutoksessa perässä. Kriisi vaati vanhojen ajattelutapojen päivittämistä.

Aiemmin tietoverkkorikokset on nähty uhrittomina rikoksina. Vastaamon tapaus osoittaa, että sellaisetkin henkilöt, jotka eivät ole koskaan käyttäneet älylaitteita, voivat joutua uhriksi koska heidän henkilötietojaan käsitellään jossain tietoverkoissa, kuvailee Kimmo Ulkuniemi. (U117)

Uutisissa käsiteltiin lisäksi tulevaisuuden näkymiä ja sitä, miten tietomurto saattaa muuttaa toimintatapoja. Yksityishenkilöt saattavat olla jatkossa tietoisempia asiasta ja vaatia parempaa tietoturvaa (U27). Viranomaistahoilla saattaa olla puolestaan parempi valmius käsitellä vastaavia tilanteita (U21).

Yhteiskunnallisen tason uhkakuvia olivat siis: 1) luottamus digitalisaatioon ja digitaaliseen yhteiskuntaan menetetään, 2) tapauksia tulee lisää, 3) yhteiskunnallinen turvallisuus on uhattuna,

4) yhteiskunnallisesti ei olla tarpeeksi varautuneita ja valmiita estämään tulevat tapaukset, 5) lainsäädäntö ja ajattelu on vanhentunutta, ja 6) tarvittavan tiedon ja ymmärryksen puute digitaalisista uhkakuvista.

7 Pohdinta – Vastaamo digitaalisen yhteiskunnan laineilla

Seuraavaksi tarkastelen analyysin tuloksia kirjallisuuden ja teoreettisten viitekehysten valossa. Ensimmäinen tutkimuskysymykseni kuului: miten Vastaamon on pyrkinyt palauttamaan luottamusta? Tiedotteiden analyysi kohdentui lopulta kahteen teemaan: millä keinoin Vastaamo pyrki hallitsemaan tilannetta sekä rakentaa luottamusta ja toisaalta siihen, mitkä digitaalisen ympäristön piirteet vaikeuttivat tätä prosessia ja miten kyseinen ympäristö aiheutti hallitsemattomuutta ja epävarmuutta. Toinen tutkimuskysymykseni oli: minkälaiseksi uhkaksi tietomurto määrittyi yhteiskunnallisessa keskustelussa? Uutisten luennassa huomasin uhkakuvien sijoittuvan monille eri yhteiskunnan tasoille, mikä kertoo tapahtuman merkittävydestä. Näitä tasoja oli yhteensä neljä: yksilötaso ja Vastaamo, terveydenhuollon sektori ja valvontaviranomaiset, muut digitaalisia palveluita tarjoavat tahot ja lopulta yhteiskunnallinen taso, joka kattaa koko digitaalisen ympäristön.

7.1 Vastaamon pyrkimys palauttaa luottamusta kriisiviestinnän keinoin

Olen kuvannut edellä, kuinka Vastaamo pyrki luottamuksen rakentamiseen tyypillisin kriisiviestinnän ja tilanteen hallinnan keinoin. Vastaamon kriisiviestinnässä on havaittavissa Benoitin (2014) mainekuvan korjaamisen strategioita. Benoitin viisi strategiaa olivat: 1) kieltäminen, 2) vastuun hylkääminen, 3) hyökkäysten torjuminen, 4) korjaavat toimenpiteet ja 5) häpeä. Näistä tiedotteissa toisia on hyödynnetty enemmän kuin toisia. Kieltämisen strategiaa esiintyi esimerkiksi silloin kun Vastaamo syytettiin tiedottamisen hitaudesta. Osa kieltämisen strategiaa oli myös toimitusjohtaja Ville Tapion nimeäminen syntipukiksi. Toinen strategia, vastuun hylkääminen toteutui korostamalla poikkeuksellisuutta, hakkerin syyllisyyttä ja häivyttämällä

taka-alalle Vastaamon tietosuojapuutteet. Kolmas strategia, hyökkäysten torjuminen oli tiedotteissa havaittavissa alkupuolella väheksymällä tapahtunutta (uhrien määrän aliarvioiminen) ja loppupuolella vahinkojen korvaamisella uhreille (luottokieltopalveluiden hyvittäminen). Tilanteen edetessä strategia neljä (korjaavat toimenpiteet) liukui kohti strategiaa viisi (häpeä, korjaavat toimenpiteet ja tulevien tapausten ehkäisy). Viides, häpeän strategia nousi esille etenkin Pirttijärven aloittaessa Vastaamolla, jolloin tiedotteissa korostui puhe luottamuksen palauttamisesta ja rakentamisesta. Korvauksiin asti Vastaamo ei kuitenkaan päässyt, vaan ne tulevat uhreille mahdollisesti konkurssipesän kautta. Lopulta tilanne oli niin hallitsematon, että ratkaisujen etsiminen osoittautui mahdottomaksi, eikä luottamusta Vastaamoon saatu korjattua.

Luottamuksen rakentamisessa on otettava huomioon odotukset (Sztompka, 1999). Tiedotteissa luvattiin selvittää tapahtunut, estää tietojen leviäminen ja löytää syylliset, mikä edusti myös yhtiön yhteiskunnallista veloitetta. Mikään näistä ei kuitenkaan realisoitunut. Korpiolan (2011) mukaan kriisiviestinnän tulisi noudattaa yrityksen arvoja, muuten se ei ole uskottavaa. Vastaamon lupaukset toiminnan jatkumisesta ja “vakaasta tilanteesta” kääntyivät nopeasti sitä vastaan, kun taloudelliset ongelmat nousivat esille. Kiristäjän hallussa olleet tiedot lähtivät leviämään, tilanteeseen liittyi liikaa epäselvyyttä, eikä Vastaamon tiedotus toteutunut tarpeeksi nopeasti, jolloin yrityksestä syntyi kriisiin huonosti valmistunut ja uhriutunut kuva julkisuudessa. Luhmannin (2017), Sztompkan (1999) ja Clarkin (2014) mukaan näkemys luotettavasta toimijasta perustuu edeltäviin kokemuksiin. Kansalaisten ja uhrien näkemys Vastaamosta luotettavana palveluna muuttui sillä hetkellä, kun tietomurto tuli ilmi. Vastaamo oli psykoterapiaa tarjoavana yrityksenä päätynyt yksinkertaisten ja helposti korjattavien tietoturvapuutteiden takia vuotamaan kiristäjän kautta potilaiden salassa pidettäviä tietoja. Mikään kriisiviestinnän keino ei voinut korjata tapahtunutta vahinkoa.

Sztompka (1999) ja Van Dijck (2014) nostavat esille institutionaalisen luottamuksen, sekä suhteen luottajan ja luotettavan välillä. Suomessa on tutkitusti tapana luottaa yhteiskunnan instituutioihin ja tahoihin, joten niiden toimintaan liitetään myös odotuksia ja vastuunottoa. Koska Vastaamo on yksityinen yritys, joka on saanut ”siunauksen” tekemällä yhteistyötä isompien

yhteiskunnallisten toimijoiden kanssa (Kela ja Valvira), myös luottamuksen menetys ja pettymys odottamattomasta toiminnasta olivat merkittäviä. Vastaamon tietomurrossa syntyi monien tahojen verkosto, joiden väliset luottamussuhteet katkesivat. Tärkein luottamussuhde oli asiakkaiden ja Vastaamon välillä. Tämän luottamuksen menetys johti laajempaan luottamuksen verkoston hajoamiseen (Sellnow & Seeger, 2013). Asiakkaat, asiakkaiden läheiset, Vastaamon henkilökunta sekä uutisten vastaanottajat joutuivat kriisissä uudelleen miettimään ja kyseenalaistamaan sitä, mitkä heitä ympäröivistä tahoista ovat oikeastaan luotettavia. Jos psykoterapiapalveluita tuottavaan yritykseen ei voi luottaa yksityisyyden ja tietoturvan kannalta, niin voiko luottaa esimerkiksi pankkiin tai julkiseen terveydenhuoltoon? Tietomurto oli paljon kriisiviestintää ja tietoturvaa laajempi tapahtuma, jossa luottamusta koeteltiin yhteiskunnallisella tasolla.

7.2 Tietomurron uhkakuvat – hallitsemattomuus digitaalisessa riskiyhteiskunnassa

Uutisista paljastui miten erilaisia ja laajalle ulottuvia huolia tietomurto toi tullessaan. Tilanteen epäselkeys, neuvottomuus ja epävarmuus olivat tietomurron uhkia, jotka koettelivat koko yhteiskuntaa. Riskiyhteiskunnan piirteisiin kuuluvat ihmisten itsensä aiheuttamat riskit, jotka toteutuessaan saavat aikaiseksi mittavia vahinkoja (Beck, 1992). Niistä ollaan yleensä tietoisia, mutta Vastaamon tapauksessa tietomurto tuli yllättäen; tietomurrot eivät itsessään ole uusi uhka, mutta oletuksena on, että julkisen sektorin, tässä tapauksessa terveydenhuollon, tietokannat ovat turvassa (Gaskell & Gottweis, 2011; Van Dijck, 2014). Tietomurto häiritsi vahvana pidettyjä oletuksia ja yhteiskunnallisia rakenteita luottamuksen puutteen takia. Digitaalisessa ympäristössä tapahtunut tietomurto vaikutti luottamuksen, valtion ja kansalaisten väliseen dynamiikkaan, heikentäen näitä rakenteita ja hallinnan tunnetta, sekä lisäämällä epäilystä ja turvattomuuden tunnetta. Turvattomuuden tunne uhkaa yhteiskunnallista järjestystä, sillä se heikentää luottamusta ja muuttaa käsitystä luotettavista tahoista (Sztompka, 1999; Sellnow & Seeger, 2013). Suurimman osan uhista pystyi asettamaan yhteiskunnalliseen kehykseen. Uudet uhkat nähtiin osana digitaalista kehitystä, joka toi mukanaan tietomurrot ja uudet rikollisuuden muodot. Tämä tarkoitti tarvetta uusille suojautumisen keinoille (Beck, 1992; Bauman, 1993). Tietomurto

osoitti, etteivät viranomaiset olleet valmistautuneita vastaavanlaiseen tapahtumaan, eikä toimivia ratkaisukeinoja tilanteeseen ollut heti saatavilla. Tietomurto ei paljastanut pelkästään potilastietojärjestelmien heikkouden, vaan koko digitaalisen yhteiskunnan ongelmakohdat alkaen digitaalisten palveluiden järjestämisestä ja sääntelystä valtion tasolla ja loppuen sen käyttäjiä koskeviin vaikutuksiin. Kriisin laajuus teki Vastaamon tietomurrosta jotain laajempaa — siitä tuli kansallisen luokan digitaalinen suuronnettomuus.

Tietomurrosta löytyi useampia Beckin (1992) ja Giddensin (1990) mainitsemaa riskiyhteiskunnalle tyypillisen uhkan piirteitä. Tietomurto sai alkunsa ihmisten luomasta teknologiasta: internetistä ja sen mahdollistamasta infrastruktuurista. Tietomurrolla ei ollut rajoja ajan tai paikan suhteen, rikollinen on voinut yhtä lailla tehdä murron Suomesta tai ulkomailta. Uhreja yhdisti Vastaamon asiakkuus tai työskentely yhtiössä, mutta muuten heidän taustansa, ikänsä ja maantieteellinen sijaintinsa oli voinut olla hyvin erilainen. Tietomurto osui riskiyhteiskunnan ytimeen: tämä tapaus olisi voinut tapahtua mille tahansa yhtiölle tai organisaatiolle ja koskettaa ketä tahansa. Se ei ollut aistein havaittavissa (Giddens, 1990), sitä ei näkynyt tai kuulunut, eikä se välttämättä olisi koskaan tullut julkisuuteen, ellei rikollinen olisi lähestynyt Vastaamoaa kiristysviestillä tai murrosta tienneet henkilöt olisivat tuoneet asiaa julkisuuteen. Tietomurron aiheuttamat riskit olivat yksilön kannalta intiimejä ja henkilökohtaisia. Yksilöt olivat verrattain avuttomia riskien edessä, eivätkä he pystyneet vaikuttamaan tapahtumien kulkuun. Kriisin aiheuttamien riskien arvioiminen ja torjuminen jäi kuitenkin heidän tehtäväkseen. (Beck, 1992; Bauman, 1993). Tästä muodostui Beckin (1992) ja Baumanin (1993) mainitsema markkinarako: tilanteen voittajia olivat vakuutusyhtiöt ja luottokieltopalvelut (Yle, 2020).

Tietomurto pakotti eri toimijoita Beckin (1992) mainitsemaan itsekritiikkiin ratkaisujen löytämiseksi. Todelliseen refleksiivisyyteen ei kuitenkaan ulotuttu, sillä ongelmia ratkaistiin pintapuolisesti ja lyhyellä tähtämellä, ottaen käyttöön uutta teknologiaa. Giddensin (1994) mukaan riskejä aiheuttavaa teknologiaa saatetaan pyrkiä ratkaisemaan luomalla uutta teknologiaa. Tässä tapauksessa asia saatiin ”ratkaistua” tehostamalla Valviran B-järjestelmän toimijoiden valvontaa ja liittämällä A-järjestelmään enemmän suuria organisaatioita. Lisäksi tietomurto kiihdytti

erilaisten palveluiden ja järjestelmien siirtymistä vahvaan tunnistautumiseen. Nämä ratkaisut toimivat myös (riski)yhteiskunnan palautumisen keinoina, jotka tarjoavat tavan minimoida niitä riskejä, joita ei voida enää välttää (Beck, 1992; Bauman, 1993). Yksityisten yritysten tietoturvasääntelyyn ei kuitenkaan tullut merkittäviä muutoksia, minkä lisäksi uhrit joutuivat ratkaisemaan tietomurron tuomat huolet pitkälti itsenäisesti ja omakustanteisesti, ilman varmuutta korvauksista. Baumanin (1993) mukaan teknologiaa tulisi ajatella pitkällä tähtäimellä, mutta Vastaamon tietomurron jälkeiset ratkaisut tulevat todennäköisesti vanhentumaan suhteellisen nopeasti, jolloin tulee jälleen tarve uudistaa niitä. Vahvempaan tunnistautumiseen siirtyminen ei myöskään ole ongelmatonta. Se toteutetaan useimmiten pankkitunnistautumisen kautta, mikä vahvistaa pankkien asemaa henkilötietojen portinvartijoina ja syrjii henkilöitä, joilla ei ole suomalaisia pankkitunnuksia (esimerkiksi maahanmuuttajat ja paperittomat), jolloin ihmisiä jää palveluiden ulkopuolelle. Myös pankkeihin kohdistuu jatkuvasti tietomurtoja- ja vuotoja, eikä mikään takaa tietojen pysyvän pankkien tietokannassa turvassa loputtomasti.

Tietomurto kosketti yhteiskunnan eri sektoreita ja vaati laajaa sektoreiden välistä yhteistyötä, jota Beck (1992) ja Giddens (1990, 1991) ovat painottaneet osana riskiyhteiskunnan toimintaa. Giddensin (1991) mainitsemat asiantuntijajärjestelmät olivat löydettävissä osana tietomurron jälkipuintia. Tietomurron laajuus ja seuraukset olivat vaikeasti arvioitavissa, jolloin asiantuntijajärjestelmien merkitys korostui ja tyypillisesti valvontaa harjoittavan Valviran toiminta oli tehotonta. Kun asiantuntijatkaan eivät tieneet miten toimia, voimisti se epäluottamusta ja epävarmuutta (Giddens, 1991; Sztompka, 1999). Luottamus ei horjunut pelkästään teknologian suhteen, vaan myös auktoriteettien, joiden tehtävänä oli valvoa järjestelmän turvallisuutta ja säädellä yritysten tietoturva vaatimuksia. Asiantuntijatieto petti odotukset, kun paljastui että tietomurtoon oli johtanut tietoturvan laiminlyönti, sääntelyn puute ja valvonnan olemattomuus. Nämä asiat myös aiheuttivat järjestelmän haavoittuvuuden. Luottamus perustavanlaatuisen digitaalisten palveluiden järjestämiseen sai kolhuja ja tietoisuus järjestelmän haavoittuvuuksista nousi julkisuuteen. Vaikka asiantuntijoilla ei ollut heti ratkaisuja saatavilla, he olivat kuitenkin merkittävin taho, jonka puoleen käännettiin, mikä vahvisti asiantuntijatiedon asemaa entisestään.

Tietomurto oli medioitunut kriisi: sitä käsiteltiin päivittäin mediassa, muokaten ja luoden sen merkityksiä (Giddens, 1990; Beck, 1992). Tuomalla kriisi julkisuuteen, paljasti se uusia uhkia kansalaisille. Samalla se loi yhteisöllisyyttä uhrien keskuudessa ja synnytti yleisempää keskustelua terapiaan liittyvästä stigmasta. Uutisten analyysin perusteella uhrien todellisuus monien kuukausien päästä tietomurrosta oli edelleen vahvasti huolen ja itsenäisesti asioiden selvittämisen värjäämä. Median jakama tieto keskittyi vahvasti kertomaan uhreille erilaisia suojautumisen keinoja, mikä yksilöllisti riskit uhrien velvollisuudeksi (Bauman, 1993). Siinä missä Vastaamon kriisiviestintä epäonnistui ja päättyi yrityksen konkurssiin, valtion ponnistus johti yhteiskunnalliseen palautumiseen. Beckin (1992) ja Giddensin (1990) riskiyhteiskuntateoriaa soveltaen, tätä käsitystä normaaliin palautumisesta muokkasi osaltaan media. Luottamusta yhteiskunnalliseen järjestelmään rakennettiin Sztompkan (1999) mainitseamalla tavalla, eli poliittisen päätöksen- teon ja linjausten asettamisten avulla. Tietomurto oli elänyt uutissyklinsä ja tapahtuma saatiin päätökseen Vastaamon saadessa seuraamusmaksun ja sääntelyn muuttuessa valvonnan suhteen. Uhka kansalaisille, joita tietomurto ei koskettanut vaikutti olevan ohi, sillä nyt sääntelyyn ja ongelmakohtiin oltiin puututtu. Se ei kuitenkaan estä tulevia tapauksia, joten ratkaisu on pitkällä tähtäimellä katsottuna hetkellinen. Loppujen lopuksi tietomurto ei saanut ihmisiä lopettamaan terapiassa käyntiä ja digitaalinen yhteiskunta jatkaa kehittymistään. Tietomurto saattoi olla kolhu luottamukseen digitaalista yhteiskuntaa kohtaan, mutta se ei sitä rikkonut. Uhrien kan- nalta tapahtuma ei kuitenkaan saanut päätöstä.

Vastaamon tietomurto konkretisoi Pinkin ym. (2018) käsittelemiä ihmisten huolia digitaalisessa ympäristössä. Tässä tapauksessa uhrit eivät itse olleet tehneet mitään väärää, eikä kyse ollut heidän osaamattomuudestaan tai puutteellisista digitaidoista. Etenkin alussa huolet johtuivat siitä, etteivät uhrit tienneet mitä tietoja heistä on kirjoitettu ylös ja vuodettu. Uhrien haastatte- luissa toistui huoli siitä, ettei heillä ole mitään mahdollisuutta kontrolloida heistä liikkuvia tie- toja. Uutisissa uhrit toistivat yksimielisesti, ettei heille tarjottu tarpeeksi nopeasti ja selvästi neuvoja siitä, miten kannattaa toimia tietomurron jälkeen. Toisaalta uhrit, jotka kaipasivat ta- kuuvarmaa suojaa esimerkiksi henkilötunnusta vaihtamalla, joutuivat kohtaamaan uuden uh- kan, jossa toimenpide saattaisi johtaa tietojen katoamiseen kansallisissa järjestelmissä, jättäen

heidät palvelujen ulkopuolelle. Luottamuksen menetys ja puute aiheuttivat haasteita jatkaa tavallista arkea tietomurron jälkeen, joka oli etenkin uhreille erilaisten riskien täyttämää. Tiedot ovat edelleen saatavilla verkossa, eivätkä uhrin voi tehdä asialle mitään. Kyseisessä tilanteessa luottamuksesta muodostuu tärkeä työkalu, joka Luhmannin (2017) mukaan auttaa sujuvoittamaan arkea ja käsittelemään riskejä. Riskin ja luottamuksen välillä vaikuttaakin oleva perustavanlaatuisen yhtymäkohta: ne molemmat toimivat keinona käsitellä epävarmuutta.

Riskiyhteiskunnan näkökulmasta tietomurto lisäsi epäilyä moniin eri yhteiskunnan tahoihin, mikä saattaa vaikeuttaa luottamuksen rakentamista tulevaisuudessa (Sztompka, 1999; Luhmann, 2017). Luhmann (2017) sekä Beck, Giddens ja Lash (1994) esittävät modernisaation piirteisiin kuuluvan epäilyksen yleistymisen ja luottamuksen puutteen (Beck, 1992). Vastaamon tapauksessa kyse oli monesta tuhannesta haavoittuvassa asemassa olevasta ihmisestä, jotka koki viranomais tiedon pettäneen. Työn kirjoittamishetkellä uhrin ovat edelleen keskellä korvausprosessia ja poliisin tutkinta on kesken. Tietomurrosta on mennyt melkein puolitoista vuotta, mutta uhrien kannalta tilanne on edelleen yhtä epävarma. Tapausta ei olla vielääkään saatu selvitettyä, eikä uhreilta voi vaatia tilanteen pitkittymistä ja siihen palaamista loputtomiin.

8 Lopuksi – miten luottaa hallitsemattomaan?

Tarkastelin tässä työssä Vastaamon tietomurtoa luottamuksen, riskiyhteiskunnan ja kriisiviestinnän näkökulmista. Digitaalisen teknologian tuoma hallitsemattomuus ja laajamittaiset, pitkäkestoiset seuraukset nousivat työn keskeisiksi tuloksiksi. Vastaamon tietomurto osoittautui digitaalisesti suuronnettomuudeksi, joka nähtiin yhteiskunnallisella tasolla merkittävänä ja uhkaavana tilanteena. Vaikka kyseessä on tapaustutkimus, jossa näkökulma rajoittuu vain yhteen tapaukseen, näen että saamani tulokset voidaan yleistää tarkastelemaan digitaalisen yhteiskunnan ongelmakohtia laajemmin. Eri järjestelmät muodostavat monimutkaisen ja haavoittuvan verkoston, jossa monet eri kytkökset saattavat pettää. Uhkakuvat tiivistyvät digitaalisen ympäristön hallitsemattomuuteen. Kun tilanne kerran karkaa käsistä, ei paluuta enää ole.

Digitaalisen ympäristön hallitsemattomuus ei anna varaa käyttäjille luottaa kerran epäonnistuneeseen alustaan, jolloin luottamuksen uudelleen rakentaminen vaikeutuu. Uhkana on, että taphtuma toistuu muissakin yrityksissä. Riski joutua tietomurron uhriksi on todellinen niin yksityisen henkilön, yrityksen, kuin julkisen organisaation kohdalla. Tämän takia on tärkeää, että jokainen organisaatio ottaisi tietoturvakysymykset vakavasti. Valvonta on edelleen jaettu A- ja B- luokan järjestelmiin, joissa yksityistä puolta valvotaan vähemmän, jos ollenkaan. Koska uhka joutua tietomurron kohteeksi on sama siitä huolimatta, onko kyseessä julkinen vai yksityinen toimija, tulisi sääntelyn koskea niitä yhdenvertaisesti. Yksityisen puolen valvonnan ja sääntelyn laiminlyönti vaarantaa kansalaisten tietoja. Heidän ei kuuluisi pelätä henkilökohtaisten tietojensa puolesta asioidessaan missään palvelussa, etenkin jos kyse on terveydenhuollosta. Palvelujen tarjoajilla on vastuu taata tietoturva. Todennäköisesti moni tietomurto ei tule julkisuuteen ollenkaan, eikä uhreilla ole mitään mahdollisuutta vaikuttaa yksityisten tietojensa näkyvyyteen, tai edes tietää onko tietoja vuodettu. Vähintä, mitä vastuullinen yritys voisi tehdä, on ilmoittaa mahdollisimman aikaisin tietomurron tai tietovuodon sattuessa.

Luottamukseen liittyy kuitenkin myös paljon ristiriitaisuuksia. Se, että Vastaamon tietomurto tapahtui, ei saanut suurinta osaa ihmisistä lopettamaan internetin käytön tai tietojensa kertomisen terveydenhuollossa asioidessaan. Ihmisillä ei myöskään ole vaihtoehtoja: jos palveluja haluaa käyttää, vaatii se yleensä jonkinlaista tiedon luovuttamista. Digitaalinen yhteiskunta on rakennettu periaatteelle, jonka mukaan kansalaisista on tietoja monessa eri tietokannassa. Vaikka yksittäisten kansalaisten käyttäytymiseen tietomurto ei välttämättä vaikuttanut, oli tietomurrolla vaikutuksia poliittiseen päätöksentekoon, ainakin hetkellisesti. Tietoturvakysymyksiä käsiteltiin jo ennen tietomurtoa hallituksessa, mutta sen jälkeen kyseisen aiheen painoarvo nousi. Tämä nousi esille uutisten analyysissä, jossa mainittiin valtion hallituksen kokoontumiset tietomurron jälkeen, sekä ministeriön muodostama asiantuntijaryhmä, jonka tarkoituksena oli selvittää tietoturvan tilaa yhteiskunnan kriittisillä toimialoilla. Aikaansaadut muutokset ja päätökset eivät kuitenkaan pitkällä tähtäimellä tuoneet merkittäviä muutoksia, vaan ne antoivat

hetkellisen ratkaisun. Digitaalinen yhteiskunta ei muuttunut perustavanlaatuisesti, vaan se on edelleen yhtä riskialtis ja hallitsematon kuin ennen tietomurtoa.

Koska digitalisaatio on niin kaiken kattava ja nopea kehitykseltään, on sitä myös vaikea säädellä. Lainsäädäntö on usein liian kankea ja hidas pysymään mukana digitalisaation kehityksessä, mikä puolestaan muodostaa mahdollisuuksia väärinkäyttää olemassa olevaa sääntelyä tai muodostaa käytäntöjä, jotka voidaan huomata vasta jälkepäin haitallisiksi tai yksityisyyttä rikkoviksi. Lainsäädäntö tyypillisesti laahaa perässä ja ongelmakohdat osataan usein korjata vasta, kun vahinko on jo tapahtunut. Vastaamon tietomurto synnytti paljon puhetta julkisuudessa mahdollisista tulevaisuuden ratkaisuista ja toisaalta siitä, miten tietomurto oli saattanut ylipäänsä tapahtua ottaen huomioon, kuinka arkaluontoista tietoa järjestelmissä pidettiin. Tietomurto olisi ollut tilaisuus ottaa opiksi ja vakauttaa se esimerkkinä, jossa tuhansia haavoittuvassa asemassa olevia kansalaisia joutui ahdinkoon. Harmia tapahtui niin henkisesti kuin rahallisesti. Puolentoista vuoden kuluttua tapahtuma on pitkälti unohdettu, mikä koskee myös tietomurron uhreja. Todellisia ratkaisuja ei saatu aikaiseksi, eivätkä uhrat ole saaneet vielääkään korvauksia. Heidän tietojansa voidaan väärinkäyttää monien vuosienkin päästä.

Tietomurto paljasti sen, kuinka luottamustamme digitaaliseen yhteiskuntaan jatkuvasti koetellaan. Hallitsemattomuuteen ja epävarmuuteen tarvitaan tukipilariksi luottamusta, mutta ne myös hajottavat sitä, mikä tekee digitaalisesta ympäristöstä dynaamisen ja alati muuttuvan. Tämä toimii kaikkien uhkakuvien taustalla. Ympäristön ollessa epävakaa on vaikea perustaa luotettavia rakenteita, joita ei kyseenalaisteta jatkuvasti.

Alun perin lähestyin tutkielman teemaa luottamuksen rakentamisen näkökulmasta. Sain kuitenkin pian huomata, että sen sijaan, että Vastaamo olisi pyrkinyt juuri luottamuksen rakentamiseen, kyseessä olikin laajempi ilmiö, nimittäin pyrkimys hallita käsistä karannutta tilannetta digitalisoituneessa ympäristössä. Tietomurrossa ei lopulta ollut aineistoni valossa edes kyse luottamuksen rakentamisesta tai menettämisestä. Kyse oli hallinnan menettämisestä. Hallinnan

menettivät niin yritys, asiakkaat, henkilökunta, viranomaiset, kuin lopulta itse rikollinenkin, joka päästi tiedot käsistään. Analyysi johdatti minut ajattelemaan tietomurron ydintä, joka on nimenomaan hallitsemattomuuden käsitteessä. Hallitsemattomuus tuo mukanaan riskiyhteiskunnalle ominaista epäilyä, joka korvaa luottamuksen. Syntyy tilanne, jossa luottamusta ei voi syntyä. Riskiyhteiskunnalle tyypilliseen tapaan kansalaiset luottavat “sokeasti” asiantuntijatahoihin ja viranomaisiin, sillä se on ainoa tapa ylläpitää arkea ja käsitellä sen kaoottisuutta. Digitaalisen ympäristön toimintatapa mahdollistaa tehokkuuden ja nopeuden, mutta sen kanssa tekemisissä olevat toimijat joutuvat jatkuvasti painimaan sen suhteen millaisia riskejä sen käyttöön liittyy.

Etenkin uutisten lähiluennassa olisin voinut ottaa lisää media-aineistoa tulkittavaksi. Tässä tutkielmassa otin huomioon vain uutisartikkelit, mutta olisi ollut mielenkiintoista tutkia myös esimerkiksi videomateriaalia ja vertailla uutislähteiden eroja tietomurron esittämisessä. Uutisten käsittelyssä olisi voinut käyttää myös lähiluennan sijaan kehysanalyysiä, mutta kyseinen asetelma voisi muodostaa itsenäisen kokonaisuuden. Sisällönanalyysin kohdalla on muistettava, että joku toinen saattaisi löytää hyvin erilaisia näkökulmia samaan aineistoon. Minulla oli jonkin verran taustatietoa tapahtumasta jo ennen kuin aloitin analyysin ja lähiluennan tekemisen, joten se saattoi vaikuttaa aineiston käsittelyyn. Vaikka kyseessä on tapaustutkimus, voidaan siitä löytää yleistettävissä olevia piirteitä, kuten organisaation harjoittama kriisiviestintä ja digitaalisen suuronnettomuuden piirteet. Näiden piirteiden tutkiminen lisää ymmärrystä ja tietoa digitaalisesta ympäristöstä, mikä aineistoni valossa osoittautui yhdeksi yhteiskunnalliseksi kehityskohteeksi. Samaan aiheeseen voisi olla myös mielekästä syventyä esimerkiksi haastatteleamalla tietomurron uhreja tai Vastaamon henkilökuntaa, ottaen näkökulmaksi tavat, joilla he käsitelivät kriisin aiheuttamaa epävarmuutta ja huolta.

Tutkielman viimeistelyvaiheessa Ylellä julkaistiin uusi uutinen helmikuussa 2022 liittyen Vastaamon tietomurron tutkintaan. Tunteamattomasta syystä johtuen poliisin tietokannasta oli kadonnut uhrien tekemiä tuhansia rikosilmoituksia. Sähköisen lausuntolomakkeen täyttämistä varten uhreilla tuli olla ensin rikosilmoitus tehty poliisin tietojärjestelmässä. Ilman sitä uhrin

eivät voi saada vahingonkorvauksia ja edetä oikeusprosessissa. Asianosaisille ei ilmoitettu asiasta, minkä takia lausuntoja oli kertynyt vain kymmenes uhrien kokonaismäärästä. Päätin mainita tämän uutisen työni lopussa, sillä se kiteyttää itseensä digitaalisen yhteiskunnan luonteen. Uhrit, joiden arkaluontoiset tiedot vietiin ja jotka kaipasivat selkeää tiedotusta ja toimintaa, ovat saattaneet tietämättään jäädä poliisin sähköisen järjestelmän ulkopuolelle täysin odottamattoman teknisen vian takia. Poliisin mukaan vika saattoi johtua rikosilmoitusten suuresta määrästä. Teknologia petti ja aiheutti sidosryhmien välisen viestinnän katkoksen. Poliisi pelkäsi suoran yhteydenoton uhreihin aiheuttavan enemmän haittaa, sillä aikaisemmin uhrit olivat saaneet villillisiä kuulustelukutsuja sähköpostitse. Tilanteessa ei osattu toimia, minkä johdosta kymmenet tuhannet tietomurron uhrit eivät välttämättä saa ansaittuja vahingonkorvauksia.

Vastaamon tietomurto on varoittava esimerkki siitä, millaisia haasteita digitaaliseen yhteiskuntaan kuuluu. Siitä olisi voinut ottaa opiksi paljon enemmän asioita, sen sijaan, että tapaus unohdettaisiin heti kun sille on näennäisesti löydetty ratkaisu. Opittavaa ja korjattavaa oli etenkin sen saralla, miten yksityisten palvelujen tietoturvan valvonta on järjestetty ja miten sääntely on ylipäänsä voinut luoda aukon, jossa tällaiselle digitaaliselle suuronnettomuudelle oli mahdollisuus. Opittavaa oli myös siitä, miten ja millaista tietoa tietomurron uhreille on saatavilla ja millaisia tarpeita syntyy näin laajan tietomurto tapahtuessa.

Digitaalisen yhteiskunnan palvelut vaativat luotettavan järjestelmän, jossa kansalaisten tiedot pysyvät turvassa. Digitaaliset suuronnettomuudet eivät ole yleisiä, mutta niillä on merkittävä vaikutus digitaalisten alustojen luotettavuuteen ja uskottavuuteen. Koska digitalisaatio on leviytynyt lähes kaikille elämän osa-alueille, on todennäköistä, että vaikka käyttäjien luottamusta rikottaisiin, ei heillä ole muita hyviä tai realistisia vaihtoehtoja toiminnalle, joten kansalaiset jatkavat palveluiden käyttöä. Se ei kuitenkaan tarkoita, etteikö digitaalisesta ympäristöstä voitaisi tehdä turvallisempaa ja oikeudenmukaisempaa käyttäjiä kohtaan. Yhteiskunnan, digitaalisen ympäristön ja luottamuksen välillä on jatkuvasti muuttuva dynamiikka, jota tulee ylläpitää

ja ottaa huomioon teknologian kehittyessä. Tulemme tarvitsemaan entistä vahvempaa ymmärrystä ja tietoa toimintatavoista vastaavissa tilanteissa. Tämän työn avulla olen ottanut askeleen kyseiseen suuntaan.

Lähteet

- Bauman, Z. (1993). *Postmodern Ethics*. Blackwell. Oxford.
- Beck, U. (1992). *Risk society: Towards a new modernity*. Sage.
- Beck, U., Giddens, A., and Lash, S. (1994). *Reflexive Modernization*. Cambridge, England: Polity Press.
- Benoit, W. L., & Dorries, B. (1996). Dateline NBC's persuasive attack on Wal-Mart. *Communication Quarterly*, 44(4), 463–477.
- Benoit, W. L. (2014). *Accounts, Excuses, and Apologies, Second Edition: Image Repair Theory and Research*. State University of New York Press.
- Brummett, B. (2018). *Techniques of Close Reading*. SAGE Publications.
- Caplan, Pat (2000). *Introduction: Risk Revisited*. In Caplan, Pat (ed.). *Risk Revisited*. London: Pluto Press. pp. 1–28.
- Carr, L. J. (1932). Disaster and the Sequence-Pattern Concept of Social Change. *The American Journal of Sociology*, 38(5), 207.
- Coombs, W. T., & Holladay, S. J. (2010). *The handbook of crisis communication*. Wiley-Blackwell.
- Clark, D. (2014). *The Role of Trust in Cyberspace*. In R. Harper (Ed.), *Trust, Computing, and Society* (pp. 17-37). Cambridge: Cambridge University Press. doi:10.1017/CBO9781139828567.005
- Corbin, J., & Strauss, A. (2012). *Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory*. SAGE E-Books.
- Eurobarometer (2009). *Patient Safety and quality of healthcare*. Special Eurobarometer 327. http://ec.europa.eu/public_opinion/archives/eb_special_339_320_en.htm#327
- Gaskell, G., & Gottweis, H. (2011). *Biobanks need publicity*. *Nature* 471 (10): 159-160.
- Giddens, A. (1990). *The Consequences of Modernity*. Polity Press, Cambridge.
- Giddens, A. (1991). *Modernity and Self-Identity. Self and Society in the Late Modern Age*. Polity Press, Cambridge.
- Giddens, A. (1994). *Beyond Left and Right. The Future of Radical Politics*. Polity Press, Cambridge.

- Harper, R. H. R. (Toim.). (2014). *Trust, Computing, and Society*. Cambridge University Press. <https://doi.org/10.1017/CBO9781139828567>
- Korpiola, L. (2011). *Kriisiviestintä digitaalisessa julkisuudessa*. Infor.
- Kouvo, A., & Kankainen, T., (2009). *Sosiaalista pääomaa rakentamassa vai purkamassa? Suomalaiset hyvinvointipalvelut ja yleistynyt luottamus*. *Yhteiskuntapolitiikka* 74 (6): 585–602.
- Lahti, V.-M. (1998). *Riskiyhteiskunta vesilasissa*. Yliopistopaino.
- Laine, M., Bamberg, J. & Jokinen, P. (2007). *Tapaustutkimuksen taito*. Gaudeamus.
- Lindell, M., & Perry, R. (2004) *Communicating Environmental Risk in Multiethnic Communities*. Thousand Oaks, Calif. SAGE.
- Luhmann, N. (1993). *Risk: a sociological theory*. Walter de Gruyter, Berlin.
- Luhmann, N., King, M. & Morgner, C. (2017). Uudistettu painos, alkuperäinen 1973. *Trust and Power: Vsk. English edition*. Polity. <https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1619159&site=ehost-live&scope=site>
- Pink, S., Lanzeni, D., & Horst, H. (2018). *Data anxieties: finding trust in everyday digital mess*. *Big Data & Society*, 5(1), 2053951718756685.
- Pöysä, J., Järviluoma, H., & Vakimo, S. (2010). *Vaeltavat metodit*. Suomen kansantietouden tutkijain seura.
- Sellnow, T. L. & Seeger, M. W. (2013). *Theorizing Crisis Communication*. John Wiley & Sons, Incorporated. <http://ebookcentral.proquest.com/lib/helsinki-ebooks/detail.action?docID=1110724>
- Simons, H. (2009). *Case Study Research in Practice*. SAGE Publications. <http://ebookcentral.proquest.com/lib/helsinki-ebooks/detail.action?docID=743724>
- Steedman, R., Kennedy, H. & Jones, R. (2020) *Complex ecologies of trust in data practices and data-driven systems*, *Information, Communication & Society*, 23:6, 817-832, DOI: 10.1080/1369118X.2020.1748090

- Suomalaisen Työn Liitto. (2022). Haettu 5. tammikuuta 2022 osoitteesta <https://suomalainen-tyo.fi/yrityksille/yhteiskunnallinen-yritys/>
- Sztompka, P. (1999). *Trust: A Sociological Theory*. Cambridge University Press. <http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=72916&site=ehost-live&scope=site>
- Valtioneuvosto (2019). *Pääministeri Sanna Marinin hallituksen ohjelma 10.12.2019: Osallistava ja osaava Suomi – sosiaalisesti, taloudellisesti ja ekologisesti kestävä yhteiskunta*. Haettu 1. maaliskuuta 2022, osoitteesta <http://urn.fi/URN:ISBN:978-952-287-808-3>
- Valvira (2021). *Sosiaali- ja terveydenhuollon tietojärjestelmät*. Haettu 14. lokakuuta 2021 osoitteesta <http://www.valvira.fi/terveydenhuolto/sosiaali-ja-terveydenhuollon-tietojarjestelmat>
- Van Dijck, J. (2014). *Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology*. *Surveillance & Society*, 12(2), 197–208. <https://doi.org/10.24908/ss.v12i2.4776>
- Yle Uutiset. (2017). *Joku julkaisi 16 000 suomalaisen henkilötunnukset netissä kuusi vuotta sitten – nyt niillä tehtaillaan tuhansia rikoksia vuodessa*. (2017, marraskuuta 5). Haettu 1. maaliskuuta 2022 osoitteesta <https://yle.fi/uutiset/3-9914817>
- Yle Uutiset (2020). *Identiteettivarkauden uhri voi saada apua myös kotivakuutuksesta, jos tietojen avulla on tehty vaikka verkko-ostoksia*. (2020, lokakuuta 29). Haettu 14. syyskuuta 2021 osoitteesta <https://yle.fi/uutiset/3-11617224>
- Yle Uutiset (2021). *Huijari voi esiintyä sinuna, jos tietää sinusta kolme asiaa – Ylen selvitys näyttää, miten suosittujen verkkokauppojen suojaus vuotaa*. (2021, tammikuuta 11). Haettu 1. maaliskuuta 2022 osoitteesta <https://yle.fi/uutiset/3-11690670>
- Yle Uutiset (2022). *Poliisi hukkasi Vastaamosta tehtyjä rikosilmoituksia – tietomurron uhri: "En ymmärrä, miksi he eivät ole tiedottaneet asiasta jälkikäteen"*. (7. helmikuuta 2022). Haettu 11. huhtikuuta 2022 osoitteesta <https://yle.fi/uutiset/3-12303576>

Liitteet

Liite 1. Lista Vastaamon tiedotteista

Tiedotteet haettu 6. huhtikuuta 2021, <https://vastaamo.fi/ajankohtaista/>

Tiedote	Julkaisupäivä	Viite tekstissä
Vastaamoon kohdistettu tietomurto ja kiristys	21.10.2020	T1
Vastaamoon kohdistettu tietomurto ja kiristys (päivitetty)	22.10.2020	T2
Kiristäjä lähestyy murron uhreja suoraan sekä tarkentunutta tietoa tietokantaan tunkeutumisesta	24.10.2020	T3
Vastaamon tuki kiristyksen uhreille	25.10.2020	T4
Vastaamon tietomurron selvitystyöt edenneet – taustalla puutteita tietoturvassa	26.10.2020	T5
Nyt voi hakea hyvitystä Asiakastiedon turvapalveluiden ostamisesta. Tietojen toimitukset omien rekisteritietojen tarkastuspyynnön tehneille myös alkaneet.	30.10.2020	T6
Heini Pirttijärvi Vastaamon hallituksen puheenjohtajaksi	9.11.2020	T7
Vahva sähköinen tunnistautuminen käyttöön potilastietojen tarkastuspyynnöille – asiakirjojen toimitus suojatulla sähköpostilla mahdollistuu noudon sijaan	16.11.2020	T8
Valvira: Vastaamo on tehnyt tarvittavia korjauksia tietoturvaan	18.11.2020	T9
Kela päättänyt jatkaa uusien asiakkaiden ohjausta Vastaamoon	20.11.2020	T10
Suuret kertaluontoiset kuluerät rasittaneet Vastaamon taloutta	27.11.2020	T11
Vastaamo on keskittynyt tietomurron selvittämiseen, tietoturvan vahvistamiseen ja tietoturvaloukkauksen uhrien tukemiseen	27.11.2020	T12
Tietomurron kohteena olleita pyydetään hakemaan Vastaamolta hyvitystä Asiakastiedon turvapalveluista 15.1.2021 mennessä	11.12.2020	T13
Joulunajan asiakaspalvelu, tarkastuspyynnöt sekä turvapalveluiden hyvitysten hakeminen	11.12.2020	T14
Hyvää joulunodotusta sekä kiitos tietoturvaloukkauksen uhreille annetusta tuesta	15.12.2020	T15
Vastaamon hallitus on kutsunut yhtiökokouksen 28.1. päättämään jatkotoimista	9.1.2021	T16
Tuhannet tietomurron kohteena olleet ovat käyttäneet rekisteritietojen tarkastusoikeutta ja hakeneet hyvityksiä Suomen Asiakastiedon turvapalveluista	18.1.2021	T17
Vastaamo on asetettu selvitystilaan	29.1.2021	T18

Vastaamon toiminta jatkuu selvitystilan ajan	29.1.2021	T19
Psykoterapiakeskus Vastaamo on haettu konkurssiin ja liiketoiminta siirtyy Verveen	11.2.2021 (päivitetty 18.2.)	T20
Psykoterapiakeskus Vastaamon toiminta on päättynyt 1.3.2021	2.3.2021	T21

Liite 2. Lista käytetyistä Ylen uutisista

Tiedotteet haettu 14. syyskuuta, 2021

Uutinen	Julkaisupäivä	Linkki	Viite tekstissä
Useat tahot tutkivat psykoterapiakeskus Vastaamon tietoturtoa ja kiristystä – Kyberturvallisuuskeskus pitää tapausta poikkeuksellisenä	21.10.2020	https://yle.fi/uutiset/3-11605223	U1
Oysin psykoterapian palvelutoimittaja Vastaamo on joutunut tietomurron kohteeksi – Oysin potilastiedot ovat turvassa	21.10.2020	https://yle.fi/uutiset/3-11606242	U2
Näin Psykoterapiakeskus Vastaamo lähestyi asiakkaitaan tietomurron jälkeen: "Todennäköiset seuraukset voivat vaihdella paljon"	22.10.2020	https://yle.fi/uutiset/3-11608906	U3
Valvira: Kukaan ei valvo yksityisiä psykoterapeutteja aloitusilmoituksen jälkeen – Nyt Valvira selvittää terapiakeskus Vastaamon tietoturtoa	22.10.2020	https://yle.fi/uutiset/3-11607115	U4
Psykoterapiakeskus Vastaamon kiristäjä julkaisi yöllä lisää erittäin arkaluontoisia potilaskertomuksia	22.10.2020	https://yle.fi/uutiset/3-11606925	U5
Psykoterapiakeskus Vastaamo tietomurrosta: Olemme pahoillamme, toiminta jatkuu normaalisti – hallituksen puheenjohtaja vastaa 5 kysymykseen	22.10.2020	https://yle.fi/uutiset/3-11608182	U6
Toimi näin, jos epäilet joutuneesi tietovuodon uhriksi	22.10.2020	https://yle.fi/uutiset/3-11608585	U7
Psykoterapiakeskus Vastaamon tietomurto voi koskea myös TAYSin nuoria asiakkaita	22.10.2020	https://yle.fi/uutiset/3-11607842	U8
Vastaamon tietomurto ei tämän hetkisen tiedon mukaan koske KYS:n potilastietoja	23.10.2020	https://yle.fi/uutiset/3-11611575	U9

Vastaamon tietomurto ei osu Päijät-Hämeeseen? – julkisuuteen vuotaneet potilastiedot ovat ajalta ennen hyvinvointiyhtymän os-topalvelua	23.10.2020	https://yle.fi/uutiset/3-11610783	U10
Psykoterapiakeskuksen tietomurron uhreja saattaa olla myös Luoteis-Pirkanmaalla – Kolmostien terveydellä on yhteistyötä Vastaamon kanssa	23.10.2020	https://yle.fi/uutiset/3-11609599	U11
Psykoterapiakeskus Vastaamon tietomurto voi koskea myös Kanta-Hämeen keskussairaalan potilaita	23.10.2020	https://yle.fi/uutiset/3-11609729	U12
Yle seurasi Vastaamon tietomurtotapausta: Vastaamo on ollut myös Kelan palvelutuottaja, kiristäjän verkkosivu palasi nettiin, HUSin, Tyksin, Taysin ja Kanta-Hämeen keskussairaalan asiakastietoja voinut vuotaa	23.10.2020 (Päivitetty 25.10.2020 10:34)	https://yle.fi/uutiset/3-11610267	U13
Analyysi: Vastaamon tietomurto on kuin lento-onnettomuus – hirveä tilanne, josta kaikki voivat oppia jotain	23.10.2020	https://yle.fi/uutiset/3-11611291	U14
Psykoterapiakeskus Vastaamon tietomurron uhrien joukossa mahdollisesti 49 Tyksin asiakasta	23.10.2020	https://yle.fi/uutiset/3-11609976	U15
Lapin sairaanhoitopiireillä ei sopimuksia tietomurron kohteeksi joutuneen Vastaamon kanssa	23.10.2020	https://yle.fi/uutiset/3-11610887	U16
Vastaamon kiristäjän sivu ilmestyi takaisin nettiin – kiristäjä julkaisi yöllä lisää potilastietoja, mutta sitten sivu katosi useiksi tunneiksi	23.10.2020	https://yle.fi/uutiset/3-11609503	U17
"Onneksi tyttärelläni on vihainen äiti, jolla on energiaa selvittää tätä asiaa" – nyt puhuvat Vastaamon tietovuodon uhri ja omainen	23.10.2020	https://yle.fi/uutiset/3-11609797	U18
Vastaamon tietomurto moninkertaisti yhteydenotot Rikosuhripäivystykseen – lisääpua värvätty uhrien auttamiseksi	24.10.2020	https://yle.fi/uutiset/3-11611857	U19
Vastaamon asiakkaat saavat nyt kiristysviestejä sähköposteihinsa: viesteissä vaaditaan 200–500 euron arvosta bitcoineja – Poliisi: Vaatimuksiin ei tule suostua	24.10.2020	https://yle.fi/uutiset/3-11612183	U20
Sisäministeri Ohisalo: Avainministerit pikaisesti koolle pohtimaan Vastaamon tietovuotovyhtiä – "Kyseessä on erittäin vakava tietomurto"	24.10.2020 (Päivitetty 25.10.2020 00:32)	https://yle.fi/uutiset/3-11612258	U21
F-Securen Hyppönen Vastaamon asiakkaiden kiristämisestä: Kansainvälisestikin poikkeuksellinen tapaus	24.10.2020	https://yle.fi/uutiset/3-11612224	U22
Mitä terapiakäynneistä kirjataan, entä mitä ei saa kirjata? Psykoterapeutit vastaavat viiteen ydinkysymykseen	25.10.2020	https://yle.fi/uutiset/3-11612496	U23
Vastaamon tietojärjestelmään on saatettu tehdä yhden sijaan kaksi murtoa – tietomurron uhreille tarjolla keskusteluapua	25.10.2020	https://yle.fi/uutiset/3-11612331	U24
Kyberturvallisuuden työelämäprofessori Jarno Linnéll Ylen erikoislähetyksessä: "Ministerien kokoontuminen antaa viestin siitä, kuinka merkittävästä asiasta on kysymys"	25.10.2020	https://yle.fi/uutiset/3-11612588	U25

KRP tiedotti Vastaamon tietomurtojutusta – Anastettuja tietoja voi olla kymmeniätuhansia, tuhannet tehneet rikosilmoituksen, Yle seurasi hetki hetkeltä	25.10.2020	https://yle.fi/uutiset/3-11612452	U26
Tietomurto on kolaus digitaaliselle yhteiskunnalle, sanoo työelämäprofessori: "Meillä on ollut luottamus, että arkaluontoiset asiat pysyvät oikeissa käsissä"	25.10.2020	https://yle.fi/uutiset/3-11612420	U27
Vastaamon tietomurto sai uhrin tuskalliseen tilanteeseen – Mieli ry: Koeta välttää ajatusten noidankehää, älä jää kauhukuvien kanssa yksin	25.10.2020	https://yle.fi/uutiset/3-11612444	U28
Presidentti Niinistö Vastaamon tietomurrosta: Tämä koskettaa meitä kaikkia	25.10.2020	https://yle.fi/uutiset/3-11612492	U29
Yle seurasi Vastaamon tietomurtoa: Näin kiristäjä ilmestyi Torverkon foorumille, poliisi pyytää harkintaa asiaan liittyvien yksityiskohtien julkaisemisessa	25.10.2020 (Päivitetty 2.11.2020 12:03)	https://yle.fi/uutiset/3-11612399	U30
Paljastaako pilkutus jotakin Vastaamon kiristäjästä? Miksi hän ei osaa teitillä suomeksi? Tämä tiedetään valtavasta kiristysvyyhdistä	26.10.2020	https://yle.fi/uutiset/3-11613667	U31
Kela odottaa selvitystä Vastaamolta: päätöksiä sen jälkeen – sairaanhoitopiiri jäädytti asioinnin psykoterapiakeskukseen	26.10.2020	https://yle.fi/uutiset/3-11613438	U32
Psykologi pelkää: Vastaamo-tietomurto rapauttaa luottamusta psykoterapiaan	26.10.2020	https://yle.fi/uutiset/3-11613978	U33
Mitä tehdä, jos törmää vuodettuun materiaaliin? Tietojen käsittelemisestä voi saada jopa vuoden vankeusrangaistuksen	26.10.2020	https://yle.fi/uutiset/3-11613689	U34
Vastaamon potkut saanut toimitusjohtaja: "Olen syvästi pahoillani vastaamolaisten ja heidän asiakkaidensa puolesta"	26.10.2020	https://yle.fi/uutiset/3-11614709	U35
Jo 180 rikosilmoitusta tehty Itä-Suomessa Vastaamon tietomurrosta	26.10.2020	https://yle.fi/uutiset/3-11613544	U36
Pirkanmaalla jo 3 000 rikosilmoitusta tietomurrosta – uhreina voi olla Tampereen perheneuvolan asiakkaita	26.10.2020	https://yle.fi/uutiset/3-11614314	U37
Myös kainuulaisten tietoja mennyt Vastaamon tietomurrossa	26.10.2020	https://yle.fi/uutiset/3-11613082	U38
Kaakkois-Suomessa tehty satoja rikosilmoituksia Vastaamon tietomurron ja kiristysviestien takia	26.10.2020	https://yle.fi/uutiset/3-11613630	U39
Tietoturvakandaalissa rypevän Vastaamon toimitusjohtajalle potkut – yhtiön hallituksen mukaan pimitti tietomurtoa 1,5 vuotta	26.10.2020	https://yle.fi/uutiset/3-11614453	U40
Vastaamon tietomurrosta jatkuvasti lisää rikosilmoituksia Lounais-Suomessa	26.10.2020	https://yle.fi/uutiset/3-11614356	U41
Asiantuntija penää yritysten johdon vastuuta tietoturvasta: "Nyt pitäisi herätä"	26.10.2020	https://yle.fi/uutiset/3-11610288	U42

Psykerapiakeskus Vastaamon tietomurtoon liittyen on tehty Keski-Suomessa jo yli 400 rikosilmoitusta	26.10.2020	https://yle.fi/uutiset/3-11613742	U43
Vastaamon tietomurron uhreja voi olla myös pohjalaismaakunnissa – EP:n sairaanhoitopiiri ostaa palveluja Vastaamolta, Vaasassa ja Soitella ei sopimusta tietomurtojen ajalta	26.10.2020	https://yle.fi/uutiset/3-11613751	U44
"Tämä on nyt henkilökohtaista": Tietoturvan huippuasiantuntijan omat tiedot vietiin Vastaamolta – auttaa jäljittämään rikollista	26.10.2020 (Päivitetty 30.10.2020 14:44)	https://yle.fi/uutiset/3-11613311	U45
Mitä väliä Vastaamon tietovuodolla on, jos se ei kosketa itseä? Tässä lyhyet vastaukset	26.10.2020	https://yle.fi/uutiset/3-11614519	U46
Mistä tiedän onko tietoni vuodettu? Uskaltaako terapiassa enää puhua? Haimme vastaukset 31 kysymykseen Vastaamon tietomurrosta	27.10.2020	https://yle.fi/uutiset/3-11615408	U47
Vastaamon tietomurto koskee viittätoista Kanta-Hämeen keskussairaalan potilasta	27.10.2020	https://yle.fi/uutiset/3-11615818	U48
Kiellot yhdeltä luukulta, hetu vaihtoon, terveystietoja valvottava tiukemmin – tässä keinoja tietomurron uhrien auttamiseksi ja vastaavien rikosten estämiseksi	27.10.2020	https://yle.fi/uutiset/3-11616144	U49
Tietovuodon ja kiristuksen kohteeksi joutunut kriisiviestinnän asiantuntija suomii Vastaamon viestintää: "Katastrofaalisen väärin"	27.10.2020	https://yle.fi/uutiset/3-11613976	U50
Vastaamo-kiristäjä teki pahan virheen perjantaina, sanoo F-Securen Hyppönen: "Hän päästi käsistään kaikkein tärkeimmän tietonsa"	27.10.2020 (Päivitetty 2.11.2020 10:18)	https://yle.fi/uutiset/3-11615644	U51
Vastaamo kannatti vielä äsken loistavasti – uusi johtaja ei halua arvioida kriisiyhtiön talousnäkyviä, pyytää anteeksi kärsimyksiä	27.10.2020	https://yle.fi/uutiset/3-11616707	U52
NörttipSYkologi koodasi ohjelman, jolla voi tarkistaa, onko omat Vastaamon tiedot julkaistu – siinä voi olla ongelma, mutta tietoturva-asiantuntija puoltaa palvelua	27.10.2020	https://yle.fi/uutiset/3-11613376	U53
Vuotaneilla henkilötiedoilla voi tehdä tilauspetoksia ja ottaa luottoa uhrin nimiin – Asiakastieto ja Vastaamo tarjoavat tietomurron uhreille maksuttomat turvapalvelut	27.10.2020	https://yle.fi/uutiset/3-11614893	U54
Vastaamon kiristysmurto on täysin ainutlaatuinen koko maailmassa – Harvat aiemmat potilaiden kiristämiset ovat liittyneet kauneusleikkauksiin	28.10.2020	https://yle.fi/uutiset/3-11615839	U55
Vastaamon tietomurrosta tehty 240 rikosilmoitusta Itä-Suomen poliisilaitoksen alueella	28.10.2020	https://yle.fi/uutiset/3-11618196	U56

Vastaamo on lähettänyt henkilötunnuksia sähköpostissa suojaamatta laskun mukana – asiantuntija: "Vastoin kaikkia sääntöjä"	28.10.2020	https://yle.fi/uutiset/3-11617763	U57
Bitcoin voi saada Vastaamo-kiristäjän kiikkiin – kryptovaluutalla on pimeä maine, mutta sen käytöstä jää aina jälki	28.10.2020	https://yle.fi/uutiset/3-11615795	U58
Onko siinä mitään järkeä, jos Vastaamon uhrit vaihtavat nyt henkilötunnustaan? Otimme selvää	28.10.2020	https://yle.fi/uutiset/3-11618730	U59
Vastaamo-kiristäjä pysyi piilossa vaikka lunnaiden maksuaika umpeutui – nyt uhkana uhrien identiteettivarkaudet	28.10.2020 (Päivitetty 2.11.2020 10:17)	https://yle.fi/uutiset/3-11618253	U60
Vastaamo on alan yrityksistä suurimpia, mutta kuuluu vähemmän valvottuihin – viranomainen selvittää ylimääräistä tarkastuskierrosta	28.10.2020	https://yle.fi/uutiset/3-11617359	U61
Marin toivoo, että Vastaamon tietomurron uhrit voisivat muuttaa henkilötunnustaan nopeasti – hallitus pui tietomurtoa iltakouluksaan	28.10.2020	https://yle.fi/uutiset/3-11617366	U62
Asiantuntijat: Vastaamon sisällä riidellään miljoonista – yksityisyytensä menettäneet joutuvat odottamaan korvauksia vuosia	28.10.2020 (Päivitetty 30.10.2020 08:42)	https://yle.fi/uutiset/3-11616028	U63
Psykoterapiakeskus Vastaamoon liittyviä rikosilmoituksia on tehty Keski-Suomessa noin 600 – Poliisi: Täysin poikkeuksellinen rikosilmoitustulva	28.10.2020	https://yle.fi/uutiset/3-11617147	U64
Marinin hallitus ottaa tänään kantaa Vastaamon tapaukseen – hallituksen pöydällä ainakin identiteettivarkaudet ja terveystyritysten valvonta	28.10.2020 (Päivitetty 30.10.2020 13:29)	https://yle.fi/uutiset/3-11616890	U65
Tietoturva-asiantuntija Sami Laihon sähköposti täyttyy huolestuneista viesteistä: "Hoitajat kirjautuvat lääkäreiden puolesta järjestelmiin"	29.10.2020	https://yle.fi/uutiset/3-11617870	U66
Yksityinen psykoterapeutti: Valviran valvonta on 0,1 – Valviran ylijohdaja: Totta kai valvonnan lisääminen olisi hyvä potilasturvallisuudelle	29.10.2020	https://yle.fi/uutiset/3-11616308	U67
Analyysi: Sopu turvallisuuspolitiikasta kestää yli hallitusvaihdosten, mutta pienet näkemuserot hiertävät johtavia poliitikkoja	29.10.2020	https://yle.fi/uutiset/3-11620941	U68
F-Securen Hyppönen: Ainakin 14 ihmistä on maksanut Vastaamon kiristäjälle ensimmäisen kiristyssumman – "ransom_man" aktivoitui viime yönä	29.10.2020	https://yle.fi/uutiset/3-11620064	U69
Identiteettivarkauden uhri voi saada apua myös kotivakuutuksesta, jos tietojen avulla on tehty vaikka verkko-ostoksia	29.10.2020	https://yle.fi/uutiset/3-11617224	U70
16 000 suomalaisen henkilötiedot varastettiin 2011 – rikosta tutkineiden mukaan Vastaamon tietomurrossa on sekä samoja että ihan uusia piirteitä	30.10.2020	https://yle.fi/uutiset/3-11621691	U71

Vastaamon tietomurrosta satoja rikosilmoituksia Hämeestä	30.10.2020	https://yle.fi/uutiset/3-11621816	U72
Vastaamo kehuu itseään "yhteiskunnallisen hyvän tuottamisesta" – saattaa menettää tästä kertovan diplomin	30.10.2020	https://yle.fi/uutiset/3-11622387	U73
Yksi heistä on kiristäjä	31.10.2020 (Päivitetty 21.12.2020 12:00)	https://yle.fi/uutiset/3-11616210	U74
Ex-tietosuojavaltuutettu Reijo Aarnio jyrähtää vielä kerran: Vastaamon tietomurto on digitaalista väkivaltaa ja verinen vääryys	1.11.2020	https://yle.fi/uutiset/3-11615577	U75
Pankit tiedottaneet ja rauhoitelleet tietoturvasta huolestuneita asiakkaitaan – tietoisuus huijausyrityksistä kohentunut	2.11.2020	https://yle.fi/uutiset/3-11623516	U76
Vastaamon tietovuotorikos työllistää vapaaehtoisia tukijoukkoja Etelä-Karjalassa	3.11.2020	https://yle.fi/uutiset/3-11629085	U77
Vastaamon tietomurto aiheutti vyöryn: viikossa tehty yli 10 000 rekisterikieltopyyntöä, tavallisesti koko vuonna alle 300	3.11.2020	https://yle.fi/uutiset/3-11628308	U78
Vastaamon omistajat tienasivat miljoonia psykoterapiakeskuksen myynnistä	3.11.2020	https://yle.fi/uutiset/3-11626190	U79
Psykoterapiakeskus Vastaamon palvelut ostokieltoon Helsingissä – apulaispormestari Vesikansa: Emme ohjaa enää yhtään uutta asiakasta Vastaamoon	4.11.2020	https://yle.fi/uutiset/3-11631359	U80
Vastaamon ehdinko jatkuu: Kela lopetti uusien asiakkaiden ohjaamisen yritykseen toistaiseksi, osa asiakkaista ja terapeuteista on lähtenyt	5.11.2020	https://yle.fi/uutiset/3-11632200	U81
Kuluttaja-asiamies saanut Vastaamon tietomurron jälkeen huolestuneita yhteydenottoja – nettiostoihin tarjottava luotto voi olla tietosuojariski	6.11.2020	https://yle.fi/uutiset/3-11631588	U82
JAMK alkaa opettaa terveydenhuollon väelle, miten tietoturvaohjelma voi välttää - ensimmäinen koulutus Jyväskylässä syksyllä	6.11.2020	https://yle.fi/uutiset/3-11635011	U83
Työryhmä selvittämään kriittisten toimialojen tietoturvaa	9.11.2020	https://yle.fi/uutiset/3-11638974	U84
Vastaamon hallituksen uudeksi puheenjohtajaksi Heini Pirttijärvi – toiminut aiemmin Esperin johdossa	9.11.2020	https://yle.fi/uutiset/3-11638020	U85
Vastaamon tietomurrosta poliisille jo 25 000 rikosilmoitusta	9.11.2020	https://yle.fi/uutiset/3-11637719	U86
Analyysi: Vastaamon uhrien henkilötunnuksen vaihto olisi huono reaktio vakavaan oireeseen – hallituksella olisi kyky nujertaa myös koko tauti	10.11.2020	https://yle.fi/uutiset/3-11627838	U87

Tietomurron uhrin elämä voi mullistua hetkessä, mutta henkilötunnuksen vaihto on piinallista – “Minulle ilmoitettiin, ettei sinua ole olemassakaan”	10.11.2020	https://yle.fi/uutiset/3-11635095	U88
Vastaamon tietomurron uhrina yksi Päijät-Hämeen hyvinvointiyhtymän asiakas	11.11.2020	https://yle.fi/uutiset/3-11642117	U89
Uusi tieto: Vastaamo arvioi uhrien määrän aluksi rajusti alakanttiin – piti asiakkaille ilmoittamista "kohtuuttoman" työläänä	11.11.2020	https://yle.fi/uutiset/3-11642774	U90
Kysyimme poliisilta Vastaamo-tutkinnasta: Rikollisia etsitään nyt ympäri maapallon, mutta "tekijä voi asua vaikka lähikorttelissa"	11.11.2020	https://yle.fi/uutiset/3-11642360	U91
Vastaamon uhreilta parisataa rikosilmoitusta Pohjanmaan poliisille	12.11.2020	https://yle.fi/uutiset/3-11644066	U92
Vastaamon hallituksen uusi puheenjohtaja Heini Pirttijärvi ensi kertaa laajassa haastattelussa – Lue tästä, miten hän kommentoi yhtiön toimia tietomurtokriisin aikana	12.11.2020	https://yle.fi/uutiset/3-11643516	U93
Tietomurron uhreilta kiitosta ja kritiikkiä hallituksen suunnitelmille: "Pitäisi keskittyä henkilötunnusten suojaamiseen eikä niiden vaihtamiseen"	12.11.2020	https://yle.fi/uutiset/3-11645268	U94
Hallitus yrittää avittaa Vastaamon tietomurron uhreja: henkilötunnuksen vaihtamista helpotetaan, pesukonetta ei voisi ostaa enää pelkällä hetulla	12.11.2020	https://yle.fi/uutiset/3-11643743	U95
Tuhannet asiakkaat ovat pyytäneet tietojaan Vastaamolta, mutta noutopaikkoja on koko maassa vain viisi – tietojen toimittaminen salatulla sähköpostilla tekeillä	13.11.2020	https://yle.fi/uutiset/3-11644744	U96
Lounais-Suomen poliisi saanut noin 2 500 rikosilmoitusta Vastaamon tietomurtoon liittyen	13.11.2020	https://yle.fi/uutiset/3-11645850	U97
Puolueet kannattavat nykyistä vahvempaa tunnistautumista verkkokaupassa – “Ei ole kohtuullista, että toisen henkilötunnuksilla voi ottaa velkaa”	13.11.2020	https://yle.fi/uutiset/3-11647611	U98
Vastaamon asiakkaat voivat nyt saada pyytämänsä asiakirjat suojatulla sähköpostilla tai postitse – aiemmin tiedot oli haettava paikasta päältä	16.11.2020	https://yle.fi/uutiset/3-11649827	U99
Valvira teki tarkastuskäynnin Vastaamon Helsingin-toimipisteeseen – ei havainnut puutteita	18.11.2020	https://yle.fi/uutiset/3-11653641	U100
Kun yritys on kriisissä, tämä nainen ei pelkää astua johtoon: Heini Pirttijärvi selvittää Vastaamon sotkua ja puhuu eniten luotamuksesta	22.11.2020	https://yle.fi/uutiset/3-11655451	U101

Rikosilmoitusvyyhti psykoterapiakeskus Vastaamon tietomurrosta kasvanut – Itä-Suomesta lähes 300 tutkintapyyntöä	26.11.2020	https://yle.fi/uutiset/3-11667274	U102
KRP tutkii, syyllistyikö osa Vastaamon työntekijöistä tietosuojarikokseen	10.12.2020	https://yle.fi/uutiset/3-11690960	U103
Uutta tietoa Vastaamon tietomurrosta: Poliisi tehnyt kotietsintöjä ja laite-etsintöjä törkeistä rikoksista epäillyn tekijän jäljittämiseksi	18.12.2020	https://yle.fi/uutiset/3-11704977	U104
Presidentti Niinistö muistuttaa "sivistysvaltion dilemmasta": "Mitä annetaan turvaa ihmisille, joiden varalta joudutaan turvaamaan muita"	1.1.2021	https://yle.fi/uutiset/3-11721108	U105
HS: Vastaamon uusi omistaja teki poliisille tutkintapyynnön yrityskaupasta	5.1.2021	https://yle.fi/uutiset/3-11725094	U106
Kela purkaa sopimuksia Vastaamon kanssa – osa terapeuteista ei täyttänyt asetettuja vaatimuksia, joissain sopimuksissa ollut puutteita alusta alkaen	20.1.2021	https://yle.fi/uutiset/3-11746075	U107
Uudet tiedot: Vastaamon potilaiden tiedot olivat ehkä jopa vuosia suojaamatta netissä – tietoturva-asiantuntija: "Älyvapaata"	22.1.2021	https://yle.fi/uutiset/3-11750220	U108
Uskalletaanko terapeutille kertoa jatkossa kaikesta? Kokenut psykoterapeutti pelkää että ei, koska pian käynnin tiedot näkyvät Omakannassa	26.1.2021	https://yle.fi/uutiset/3-11750061	U109
Vastaamon uusi toimitusjohtaja on eronnut tehtävästään, yhtiökoukous tulossa	26.1.2021	https://yle.fi/uutiset/3-11755889	U110
Vastaamon potilaskertomukset ovat jälleen Tor-verkossa – Itä-Suomen poliisi ei ole saanut uusia rikosilmoituksia	27.1.2021	https://yle.fi/uutiset/3-11757920	U111
Ehkä jopa 32 000 Vastaamon potilaan tiedot ilmestyivät viime yönä Tor-verkkoon – poliisi: "Emme tiedä, monenko käsissä tietokanta on"	27.1.2021	https://yle.fi/uutiset/3-11757676	U112
Vastaamon omistajat asettivat yhtiön selvitystilaan, terapiatoiminta jatkuu toistaiseksi – selvitysmies: Ensimmäinen tehtävä on löytää ostaja ja turvata palvelut	29.1.2021	https://yle.fi/uutiset/3-11762440	U113
Vastaamon selvitystila tai konkurssikaan ei vapauta korvausvastuusta – uhreilla useita mahdollisia väyliä saada korvauksia	29.1.2021	https://yle.fi/uutiset/3-11762624	U114
Vastaamon tietomurto: joku yrityksen avainhenkilöistä ei puhu totta maaliskuun 2019 tapahtumista	9.2.2021	https://yle.fi/uutiset/3-11774478	U115

Tietomurron kohteeksi joutunut psykoterapiakeskus Vastaamo on haettu konkurssiin – selvitysmies jatkajasta: "Kiinnostuneita ta- hoja oli monta"	11.2.2021	https://yle.fi/uutiset/3-11784072	U116
"On moraalitonta jättää haittojen torjunta rikoksen uhrille", sanoo tutkija – henkilötunnuksen muuttaminen ei poista mahdollisuutta identiteettivarkauteen	12.2.2021	https://yle.fi/uutiset/3-11782128	U117
Psykoterapiakeskus Vastaamo asetettiin konkurssiin	15.2.2021	https://yle.fi/uutiset/3-11790537	U118
Vastaamon tietomurrosta on kuukausia, ja uhrin ovat yhä kuin löysässä hirressä: "Tämä on elinikäistä – tiedot on jo verkossa"	17.2.2021	https://yle.fi/uutiset/3-11784431	U119
Vastaamo-tapauksesta tehty sata uutta rikosilmoitusta – tietomurto tuli julkisuuteen 4 kuukautta sitten, eikä Sofia, 25, vielä- kään tiedä, mitä hänestä netissä kerrotaan	20.2.2021	https://yle.fi/uutiset/3-11790633	U120

Liite 3. Lisäksi aikajanassa käytetyt Ylen uutiset

Uutinen	Julkaisupäivä	Linkki
Käräjäoikeus määräsi Vastaamon perustajan ja hänen vanhempiensa omaisuutta takavarikkoon lähes 10 miljoonan euron edestä	24.3.2021, haettu 14.9.2021	https://yle.fi/uutiset/3-11853348
Psykoterapiakeskus Vastaamon asiakkaat voivat saada potilastietoa- jaan Kelasta	10.5.2021, haettu 14.9.2021	https://yle.fi/uutiset/3-11924531
Vastaamon tietomurto näkyy huimana nousuna viime vuoden rikos- tilastoissa – yksityiselämää loukkaavasta tiedon levittämisestä yli 21 000 ilmoitusta	12.5.2021, haettu 14.9.2021	https://yle.fi/uutiset/3-11927434
Valvira: Psykoterapiakeskus Vastaamon toiminnassa useita puutteita – johtaja laiminlöi tehtäviä ja yhtiön omavalvonta petti	19.5.2021, haettu 14.9.2021	https://yle.fi/uutiset/3-11938127
Asiantuntijat näkevät Suomen hajanaisessa kyberpuolustuksessa Vastaamon kaltaisia aukkoja suurillekin iskuille	13.6.2021	https://yle.fi/uutiset/3-11979008
Vastaamo-tietomurron uhrin voivat hakea vahingonkorvauksia oman harkinnan mukaan - "Uhrin kannalta haastavaa ja monimutkaista"	20.6.2021, haettu 14.9.2021	https://yle.fi/uutiset/3-11990992
Vastaamon tietomurron uhrin tehneet 25 000 rikosilmoitusta kirjistyks- sestä – poliisi toivoo silti lisää ja aloittaa kuulemiset syksyllä	23.6.2021, haettu 14.9.2021	https://yle.fi/uutiset/3-11995066
KRP tutkii Tor-verkkoon ilmestynyttä hakukonetta, jolla voi etsiä tietoja Vastaamon asiakkaista – Poliisi: En olisi kovin huolissani	18.8.2021, haettu 14.9.2021	https://yle.fi/uutiset/3-12063432
Korkein oikeus linjasi: Poliisi ei saa tutkia Vastaamon asiakastietoja	6.10.2021, haettu 18.12.2021	https://yle.fi/uutiset/3-12130302

Vastaamon entiset potilaat vaativat jopa 10 000 euron korvauksia tietomurrosta – konkurssipesä pitää 2 500:aa euroa ylärajana	9.10.2021, haettu 18.12.2021	https://yle.fi/uutiset/3-12134525
Poliisi alkaa pian kuulla Vastaamo-tietomurron tuhansia uhreja – "Ratkaiseva tekijä voi olla jo nurkan takana", sanoo tutkinnanjohtaja	21.10.2021, haettu 18.12.2021	https://yle.fi/uutiset/3-12152682
Voisiko Vastaamon kaltainen tietomurto toistua? Maanantaina voimaan tuleva laki tekee siitä erittäin epätodennäköistä, sanovat asian-tuntijat	27.10.2021, haettu 18.12.2021	https://yle.fi/uutiset/3-12162669
Vastaamo-tietomurrossa on merkittävä Euroopan ulkopuolelle suuntautuva tutkintalinja: "On liian aikaista sanoa, ketkä ovat epäiltyjä"	27.10.2021, haettu 18.12.2021	https://yle.fi/uutiset/3-12161474
Vastaamon tietomurron vahingonkorvaukset uhreille ovat jäämässä laihoiksi: "Tuntuu ihan naurettavalta saada alle 100 euroa"	17.11.2021, haettu 18.12.2021	https://yle.fi/uutiset/3-12192745
Tietosuojavaltuutettu määräsi Psykoterapiakeskus Vastaamolle 600 000 euron seuraamusmaksun erittäin vakavista tietoturvallisuuspuutteista	16.12.2021, haettu 18.12.2021	https://yle.fi/uutiset/3-12232962