Ohjeet

Ohjeet perusturvat National Network to End Domestic violence -järjestön tuottamiin materiaaleihin.[1] Sisältöjä on päivitetty ja sovitettu Suomen olosuhteisiin yhdessä tietoturvan ja lainsäädännön asiantuntijoiden kanssa.

Naisten Linjan nettisivuilta löydät ajantasaiset tietoturvaohjeet ja digitaalisen väkivallan kokijalle hyödyllisen linkkikirjaston: naistenlinja.fi > Digitaalinen väkivalta > Näin suojaudut

Tietoturva-asetusten läpikäynti on työläs ja huolellisuutta vaativa prosessi, joten on viisasta tehdä se yhdessä luotetun ystävän tai ammattilaisen kanssa.

- Jos sinusta tuntuu siltä, että sinua vakoillaan teknologian välityksellä, on mahdollista, että niin tapahtuu. Väkivaltaisilla ja kontrolloivilla ihmisillä on voimakas tarve seurata kumppaninsa jokaista liikettä ja keskustelua. Tällaisessa tilanteessa on tärkeää pohtia tarkkaan, millaista tietoa väkivallan tekijällä voi olla vakoilun seurauksena.

- Tietokone, mobiililaitteet sekä erilaiset nettitilit ja -alustat tallentavat huomattavan määrän yksityistä tietoa toimistasi ja vuorovaikutuksestasi muiden kanssa: millaisilla sivuilla vierailet, mistä asioista haet tietoa, millaisia viestejä ja sähköposteja lähetät, millaisia nettivideoita katsot, mitä julkaiset sosiaalisessa mediassa, kenelle soitat, mitä teet nettipankissa, mitä ostat nettikaupoista ja niin edelleen.

- Jos väkivallan tekijä seuraa nettiaktiivisuuttasi tai laitteitasi, voi olla vaarallista lopettaa netin käyttö tai vaihtaa kaikki salasanat yhtäkkisesti. On luonnollista, että väkivallan kokija haluaa hankkiutua eroon laitteista tai sulkea nettitilejä, jotta väkivalta loppuisi. Voi olla kuitenkin hyvä idea jatkaa vanhan laitteen tai tilin käyttämistä ja hankkia rinnalle turvallinen laite tai luoda esimerkiksi uusi sähköpostitili.

- Jos epäilet, että tilejäsi seurataan, älä keskustele erosta tai sen tarkasta ajankohdasta viestittelemällä. Kasvokkainen tai puhelimen välityksellä käyty keskustelu on turvallisempi vaihtoehto.

- Huomioi, että jos olet yhteydessä väkivallan uhreja auttaviin tahoihin sähköpostitse, pikaviestipalveluiden kautta tai tekstiviesteillä, väkivallan tekijä saattaa

1 Lähteenä on käytetty lisäksi: Blue V, 2015; Laitinen J, 2017

päästä käsiksi tähän viestinvaihtoon. On turvallisempaa olla yhteydessä puhelimitse ja jos mahdollista käytä jonkun toisen puhelinta tai hankkia uusi puhelin, jossa on prepaid-liittymä.

Yksityisyyden suojaamisen ensimmäiset askeleet

- Ota tietoturva haltuun. Ryhdy opiskelemaan aihetta pikku hiljaa, vaikka se tuntuisikin aluksi vaikealta ja työläältä. Lähes kaikkiin kysymyksiin löytyy vastaus googlaamalla. Jos epäilet, että laitteessasi on vakoiluohjelma, käytä turvallista laitetta, kuten kirjaston tai ystävän konetta.
- Muista, että sinulla on oikeus olla jakamatta laitteitasi kenenkään kanssa.
- Suojaa kaikki laitteesi vahvalla suojakoodilla tai salasanalla, jonka vain sinä tiedät. Muista, ettei sormenjälkitunnistus ole välttämättä turvallinen tapa suojata laitteitasi, jos joudut esimerkiksi käyttämään voimakkaita unilääkkeitä. Suojakoodi on biometristä tunnistusta (esimerkiksi sormenjälki- tai kasvojentunnistusta) turvallisempi vaihtoehto laitteen lukituksen poistamiseen. Myös suojakuvioiden murtaminen saattaa onnistua helposti, jos eivät ole riittävän monimutkaisia.
- Vaihda salasanat ja ota käyttöön kaksivaiheinen tunnistautuminen kaikissa mahdollisissa palveluissa ja sovelluksissa. Huomioi, että luovuttaessasi puhelinnumerosi tai muita tietojasi johonkin palveluun, tilille murtautumisen yhteydessä myös näihin tietoihin pääsee käsiksi.
- Käytä eri tileillä eri kuvia ja käyttäjänimiä. Luo useampia sähköpostitilejä eri tilanteisiin.
- Ota käyttöön kirjautumisnotifikaatiot (ilmoitukset, jotka ilmoittavat, jos tileillesi on kirjauduttu uudesta laitteesta) kaikissa mahdollisissa palveluissa. Jos väkivallan tekijä on päässyt murtautumaan tilille ennen kirjautumisnotifikaatioiden aktivoimista, ilmoitusta uudesta laitteesta ei välttämättä tule.
- Käytä laitteidesi pääkäyttäjätiliä vain silloin, kun se on pakollista. Luo itsellesi erillinen tili, jota käytät päivittäin. Luo omat käyttäjätilit muille konetta käyttäville ihmisille.
- Tilien linkkaamiseen toisiinsa (esimerkiksi Pinterestiin kirjautuminen Google-tunnuksilla) liittyy riskejä. On parasta luoda erillinen sähköpostitili sisäänkirjautumisia varten. Varmista, ettei tämän tilin sähköpostiosoite tai salasana pidä sisällään mitään henkilökohtaisia tietojasi.
- Lataa laitteillesi kattava tietoturvaohjelma (esimerkiksi F-Securelta), pidä palomuuri päällä ja ota automaattiset päivitykset käyttöön.
- Voit myös suojata tietoliikenteesi VPN yhteydellä. Jos on riski, että yksityisyyttäsi on loukattu tai sitä yritetään loukata, kannattaa käyttää aina VPN yhteyttä. Sillä häivyttää tehokkaasti oman sijainnin tapauksissa, jos laitteessa ei ole vakoiluohjelmaa. Jos vakoiluohjelma on jo laitteella, VPN ei välttämättä auta, sillä ohjelma saattaa seurata laitteen toimintaa laajasti laitetasolla.
- Harkitse luotettavan salasanojen hallintaohjelman hankkimista. Tällöin sinun tulee muistaa vain yksi pääsalasana. Tallenna salasanat ohjelman avulla ainakin kahdelle eri laitteelle.
- Opettele hallinnoimaan selaimien selaushistoriaa ja surffaamaan netissä incogni-

to tai private browsing -moodissa. Käytä yksityistä selausta, jos käytät jonkun muun konetta kuin omaasi tai julkista tietokonetta esimerkiksi kirjastossa. Säädä selaimen historia-asetukset sellaisiksi, että selaushistoria ja keksit (engl. cookiet) pyyhkiytyvät pois oletuksena normaaliselaamisessa. Voi parantaa tietoturvaasi myös käyttämällä selaimessa scriptinestäjiä (engl. script blocker) (esimerkiksi NoScript). Scriptinestäjä voi tehokkaasti myös estää haittaohjelmien asentumisen tai haitallisen koodin ajamisen, jos on esimerkiksi sattunut klikkaamaan saastunutta linkkiä sähköpostissa.

- Suojaa oma verkkosi salasanalla, äläkä käytä avoimia verkkoja ilman VPN-suojausta. Puhelimen langattoman verkon jakaminen tietokoneelle voi olla turvallisin vaihtoehto.
- Kun käytät erilaisia nettipalveluita, anna itsestäsi niin vähän henkilökohtaisia tietoja kuin mahdollista. Älä anna nettisivuille tietoja sijainnistasi.
- Älä avaa linkkejä tai liitetiedostoja sähköposteista, joiden lähettäjä on sinulle tuntematon. Poista epäilyttävät sähköpostit, ja pidä mielessä, että sähköpostin väärentäminen on hyvin helppoa.

Miten muodostat vahvan salasanan?

- Turvallinen salasana on pitkä, vähintään 15–20 merkkiä. Salasanaa kannattaakin ajatella salalauseena. Salasanoja kräkätään tänä päivänä netistä ladattavien ohjelmien avulla, minkä vuoksi pituus on paljon olennaisempi turvallisen salasanan ominaisuus kuin esimerkiksi erikoismerkkien käyttö. Paras salasana tai -lause on sellainen, joka ei löydy sanakirjasta.
- Älä käytä salasanassa mitään henkilökohtaisia tietoja kuten lapsiin, asuinpaikkaan, syntymäaikaan, sosiaaliturvatunnukseesi tai puhelinnumeroosi liittyviä nimiä, sanoja tai numeroita.
- Älä jaa kriittisiä salasanojasi kenenkään kanssa. Varo salasanoja kalastelevia huijausviestejä.
- Käytä vähintäänkin tärkeimmissä laitteissa ja palveluissa eri salasanoja. Turvallisinta on käyttää aina eri salasanaa.
- Harkitse luotettavan salasanojen hallintaohjelman hankkimista. Tällöin sinun tulee muistaa vain yksi pääsalasana. Tallenna salasanat ohjelman avulla ainakin kahdelle eri laitteelle.
- Älä käytä turvakysymyksiä tunnistautumiseen ellei ole aivan pakko. Jos näin on, valehtele vastauksissa.
- Huomioi, että jos tallennat salasanasi selaimelle (esimerkiksi Chrome, Firefox, Safari), konettasi käyttävä ihminen saattaa päästä käsiksi kaikkiin selaimesi avainnippuun tallennettuihin salasanoihin.
- Jos käytät kumppanisi tai perheenjäsentesi kanssa yhteisiä tilejä (esimerkiksi jaettua Netflix-tiliä), varmista, ettet käytä samaa salasanaa missään muualla.
- Vaihda salasanasi säännöllisesti.

- Salasanat saattavat päätyä vääriin käsiin myös tietomurtojen yhteydessä. Have I Been Pwned -sivulta voit tarkistaa, onko tietojasi ollut tietomurroissa ja sivuilla voit myös asettaa hälytyksen, jos tietojasi leviää nettiin tulevaisuudessa.
- Muista, että yksinkertaisin tapa selvittää salasanasi saattaa olla kurkkiminen olan yli, kun kirjaudut sisään. Koneen näytön voi suojata näytön päälle laitettavalla tummennetulla kalvolla, jota kutsutaan tietoturvasuojaksi.

Näin käytät älypuhelinta turvallisemmin

- Suojaa kaikki laitteesi vahvalla suojakoodilla tai salasanalla, jonka vain sinä tiedät. Muista, ettei sormenjälkitunnistus ole välttämättä turvallinen tapa suojata laitteitasi, jos joudut esimerkiksi käyttämään voimakkaita unilääkkeitä. Suojakoodi on biometristä tunnistusta (esimerkiksi sormenjälki- tai kasvojentunnistusta) turvallisempi vaihtoehto laitteen lukituksen poistamiseen. Myös suojakuvioiden murtaminen saattaa onnistua helposti, jos kuviot eivät ole riittävän monimutkaisia.
- Laita puhelimesi sijaintipalvelut kokonaan pois päältä. Huomioi, että kaikki sovellukset eivät toimi ilman sijainnin jakamista. Jos sovellusta ei voi käyttää ilman sijainnin jakamista, se kannattaa ehkä jättää lataamatta laitteeseen. Varmista säännöllisesti, ettei sijainnin jakaminen ole mennyt takaisin päälle esimerkiksi päivitysten yhteydessä.
- On hyvä pohtia eri sovellusten kohdalla, miten laajoja oikeuksia haluaa kullekin ohjelmalle antaa. Mieti erityisen tarkkaan, onko sovelluksen perusteltua käyttää esimerkiksi kameraa ja mikrofonia. Poista turhat sovellukset puhelimestasi, ja jätä epäilyttävät sovellukset lataamatta.
- Sulje Bluetooth-yhteys silloin, kun se ei ole käytössä.
- Vieraile säännöllisesti omalla tililläsi puhelinoperaattorisi nettisivuilla, jotta tiedät, mitä turvallisuusasetuksia ja ominaisuuksia sinulla on käytössä. Huolehti myös operaattorin tilisi yksityisyydestä.
- Käytä virustorjunta- ja tietoturvaohjelmaa myös älypuhelimessasi.
- Kirjaudu ulos tileiltä, kun käytät erilaisia sovelluksia puhelimessa. Jos sovellus vaatii, että olet jatkuvasti sisäänkirjautuneena, voi olla parasta poistaa se puhelimestasi.
- Älä lataa puhelimeesi sovelluksia, joiden turvallisuudesta et ole täysin varma.
- Pohdi tarkkaan kenelle jaat puhelinnumerosi.
- Älä tallenna puhelimellesi arkaluontoisia tietoja kuten salasanoja, tunnuslukuja tai viestejä.
- Mikäli vain mahdollista, käytä vain itse ostamaasi uutta laitetta. Käytetyt laitteet saattavat olla alttiimpia vakoilu- ja haittaohjelmille.
- Ole varovainen, jos joudut siirtämään ohjelmia, kontakteja, tiedostoja tai SIM-kortteja eri puhelinten välillä, koska haittaohjelmat voivat siirtyä niiden mukana. Turvallisinta on tallentaa tiedot uuteen puhelimeen käsin.

- Suhtaudu erilaisiin turvallisuussovelluksiin kriittisesti. Sovelluksia kannattaa testata ystävien tai perheenjäsenten kanssa, jotta varmistut siitä, että todella toimivat kuten toivot.
- Ota selvää, mikä on yksinkertaisin tapa hälyttää apua puhelimellasi hädän hetkellä. Monilla puhelimilla voi hälyttää apua ilman, että tarvitsee näppäillä sisäänpääsykoodia.

Miten digitaalisen väkivallan kokemuksia kannattaa dokumentoida?

On tärkeää, että pidät kirjaa väkivallanteoista ja väärinkäytöksistä. Silloin sinulla on olemassa dokumentti tapahtumien kulusta, jota voit hyödyntää esimerkiksi rikostutkinnan tai oikeudenkäynnin yhteydessä. Dokumentointi voi antaa myös tietoa tilanteen eskaloitumisesta: tekojen määrän lisääntyminen saattaa kieliä vaaran kasvamisesta. Lisäksi se lisää ymmärrystä väkivallan tekijän tavoista väärinkäyttää teknologiaa ja mahdollistaa säännönmukaisuuksien etsimisen tekijän käytöksestä.

Luota omaan arviointikykyysi. Teknologiavälitteiset väkivallanteot saattavat kuulostaa uskomattomilta ulkopuolisen korviin. Jos sinusta tuntuu siltä, että sinua vakoillaan teknologian välityksellä, on mahdollista, että niin tapahtuu.

- Pidä kirjaa kaikista tapahtumista, myös niistä, joita et ole aikeissa raportoida viranomaisille.
- Kirjaa ylös 1) lyhyesti mitä tapahtui, 2) päivämäärä ja aika, 3) teknologia, jota väärinkäytettiin sekä 4) mahdollisten todistajien yhteystiedot.
- Tallenna kaikki mahdolliset tapahtumaan liittyvät todisteet, vaikka epämiellyttävien viestien poistaminen tuntuisikin houkuttelevalta.
- Ota ei-toivotuista tai uhkaavista viesteistä kuvakaappaukset. Kuvakaappaus kannattaa ottaa mahdollisimman nopeasti, koska joissain pikaviestipalveluissa (esimerkiksi WhatsAppissa) lähettäjä voi poistaa viestin lähettämisen jälkeen. Sosiaalisen median alustoilla viesti tai kuva kannattaa tallentaa kuvakaappauksella ennen kuin sen ilmiantaa palveluntarjoajalle, koska palvelusta poistamisen jälkeen, sitä voi olla mahdotonta saada enää takaisin.
- Jos mahdollista, ota kuvakaappaus siten, että siinä näkyy viestin lähettäjän tiedot ja lähettämisen ajankohta. Tallenna mieluiten koko kirjeenvaihto, ei vain yksittäisiä viestejä. Esimerkiksi WhatsApp keskustelun voi ladata erilliseksi tiedostoksi.
- Sähköpostit sisältävät lähettäjän IP osoitteen, joten on tärkeää, ettet poista sähköpostia. Myöskään eteenpäin välitetyssä viestissä ei näitä tietoja enää ole. Voit ottaa viesteistä esimerkiksi kuvakaappaukset, jos pelkäät, että väkivallan tekijä murtautuu sähköpostitilillesi.
- Tekstiviesteistä kannattaa ottaa varmuuskopio kuvakaappauksella. Tallenna viesti mielellään siten, että siinä näkyy lähettäjän puhelinnumero. Tekstiviesti- ja puhelutietoja on mahdollista saada myös operaattorilta.
- Häiritseviä tai uhkaavia puheluita on mahdollista nauhoittaa todisteeksi, mutta

soittajaa pitää informoida puhelun tallentamisesta, jos aiot käyttää tallennetta todisteena oikeudessa.

- Jos epäilet, että tilillesi on murtauduttu, tutki tallentaako palvelu kirjautumistietoja ja ota kuvakaappaus vieraista IP osoitteista, joista sivulle on kirjauduttu. Monet palvelut pitävät tallessa vain viimeisimmät kirjautumistiedot. Ota tämä huomioon.
- Varmista, ettei väkivallan tekijä pääse tuhoamaan todistusaineistoa murtautumalla tileillesi. Ota todisteista varmuuskopiot ja pidä niitä tallessa turvallisessa paikassa esimerkiksi pilvipalvelussa, jossa on vahva salasana ja käytössä kaksivaiheinen tunnistautuminen. Joissain tapauksissa USB-tikku tai ulkoinen kovalevy voi olla turvallisempi vaihtoehto.
- Jos epäilet, että puhelimessasi on vakoiluohjelma, toimita laite poliisille tutkittavaksi. Älä sulje puhelinta tai yritä poistaa ohjelmaa itse. Voit käyttää Faraday pussia, jos epäilet, että väkivallan tekijä seuraa sijaintiasi.
- Pidä kirjaa myös vahingonteon seurauksista (esimerkiksi fyysiset, psyykkiset, taloudelliset, sosiaaliset). Seurauksia on hyvä kirjata ylös, jotta ne ovat muistissa niin itseä varten kuin rikosilmoitusta tehtäessä. Ylös kirjaaminen auttaa selkeyttämään ja jäsentämään tapahtunutta. Jos asioit lääkärissä vahingonteon seurausten vuoksi (esimerkiksi ahdistuksen tai unettomuuden), voit pyytää lääkärintodistuksen rikosprosessin tueksi. Se ei kuitenkaan ole vaatimuksena sille, että rikoksen täyttyminen pystyttäisiin osoittamaan. Joidenkin rikostyyppien kohdalla (esimerkiksi identiteettivarkaus) teon seurausten osoittamisella on keskeinen merkitys rikosprosessissa. Yleensä rikosoikeudellisesta näkökulmasta tärkeintä on kuitenkin dokumentoida varsinaisen teon elementit, eli se mitä on tapahtunut.
- Laita turvallisuus etusijalle. Joissain tapauksissa väkivallan tekijä saa tiedon tapahtumien dokumentoinnista, mikä voi kasvattaa väkivallan uhkaa. Luota omaan arvioosi tilanteesta ja priorisoi turvallisuus.
- Tapahtumien kirjaaminen on raskasta ja herättää ikäviä tunteita. Pyydä tarvittaessa tukea luotetulta ystävältä tai ammattilaiselta.

Kuinka toimia, jos epäilet, että laitteitasi vakoillaan?

- Luota vaistoihisi. Jos sinulla on tunne siitä, että sinua vakoillaan, on mahdollista, että näin tapahtuu.
- Pohdi tarkkaan, millaista tietoa vakoilijalla tuntuu olevan ja mieti, mistä tämä tieto voisi olla peräisin. Onko väkivallan tekijällä ollut pääsy laitteisiisi tai puhelinoperaattorin hallussa oleviin tietoihin? Jos väkivallan tekijällä on tietoa sijainnistasi, käytätkö puhelimellasi sovelluksia, joissa on paikannusominaisuus? Onko sukulaisesi tai ystäväsi julkaissut esimerkiksi sosiaalisessa mediassa sinuun liittyviä kuvia tai tietoja?
- Käytä turvallista laitetta, johon väkivallan tekijä ei ole päässyt käsiksi tai saanut etäyhteyttä. Turvallinen laite voi olla esimerkiksi kirjaston tai ystävän tietokone.
- Jos sinulle herää epäilys vakoilusta, älä käytä kumppanisi laitteita. Jos kumppanin koneelle on asennettu esimerkiksi näppäilyntallennin, kaikki mitä teet ko-

neen näppäimistöllä (esimerkiksi salasanat ja kirjoittamasi viestit) päätyvät vakoilijan tietoon.

- Myös omissa laitteissasi saattaa olla vakoiluohjelma. Käytä turvallista laitetta (esimerkiksi kirjaston tai luotetun ystävän tietokonetta) riskialttiiseen toimintaan kuten salasanojen vaihtamiseen tai tiedon etsimiseen parisuhdeväkivallasta tai vakoiluohjelmista.
- Jos mahdollista, hanki uusi puhelin ja tietokone. Voit käyttää niitä vanhan laitteen rinnalla. Mitä yksinkertaisempi laite, sen hankalampi sitä on vakoilla. Turvallisinta on käyttää uudessa puhelimessa prepaid-liittymää. Jos hankit uuteen puhelimeen perinteisen liittymän, voi olla viisainta ottaa se uudelta operaattorilta kuin edellinen liittymäsi ja vaihtaa puhelinnumero.
- Jos joudut kuljettamaan mukanasi puhelinta, jota vakoillaan, voit estää vakoilun laittamalla laitteen Faraday pussiin tai hätä tapauksessa sulkemalla puhelimen, poistamalla akun ja käärimällä laitteen alumiinifolioon. Huomioi kuitenkin, että väkivallan tekijä saattaa saada tiedon, kun laitat puhelimen takaisin päälle.

Mitä on hyvä ottaa huomioon, kun käytät langatonta verkkoa?

- WLAN (lyhenne sanoista wireless local area network) on langaton lähiverkko, jonka tukiasemana toimii nettiin kytketty reititin. Tukiasema muodostaa ympärilleen mikroaaltokentän, joka mahdollistaa langattoman nettiyhteyden sen piirissä oleville laitteille. Wi-Fi on nimitys standardille, jonka mukaista tekniikkaa langaton verkko yleensä käyttää.
- Saman langattoman lähiverkon piirissä olevat laitteet voivat olla myös yhteydessä toisiinsa, mikä mahdollistaa joissain tapauksissa tietoliikenteen vakoilemisen.
- Kotitalouksissa WLAN:ia käytetään muun muassa verkottamaan langallinen internetyhteys langattomaksi, jottei asuntoihin tarvitse kaapeloida erillistä sisäverkkoa. Asuntoon tulevaan kiinteään tietoliikenneyhteyteen liitettyyn modeemiin kytketään langaton tukiasema, ja tietokoneeseen asennetaan tukiaseman kanssa radioteitse kommunikoiva lähetin-vastaanotin.
- Yritykset, kunnat tai kaupungit voivat myös tarjota avoimia verkkoja asiakkailleen tai asukkailleen ilmaiseksi tai maksua vastaan käytettäväksi.
- Tietoa WLAN-tukiasemien sijainnista voi hyödyntää paikannuksessa. Tarkkuus on tyypillisesti muutamia kymmeniä metrejä, joskus hivenen enemmän. Paikannus tapahtuu tukiaseman MAC-osoitetta hyödyntämällä. MAC-osoitteet on tallennettu tietokantoihin, joista osa on vapaasti hyödynnettävissä, mm. Googlen tietokanta "Google Location Services" -palvelun kautta. Tekniikka voi avustaa myös GPS-paikannusta.
- Suojaa lähiverkkosi vahvalla salasanalla. Ainoa turvallinen tapa tunnistaa verkkoa käyttävä laite on WPA2. Älä käytä WEP tai WPA autentikointiprotokollaa. Ainoa turvallinen salausmenetelmä on AES. Estä TKIP. Estä WPS kokonaan.
- Voit perustaa vieraidesi käyttöön oman vierasverkon, jonka salasana on simppelimpi kuin oman verkkosi.

- Jos käytät suojaamatonta avointa verkkoa, vieraile ainoastaan sivuilla, jotka käyttävät HTTPS-protokollaa. Sen tunnistaa nettiosoitteen alussa olevasta https-merkinnästä. Selain yleensä myös ilmaisee salatusta yhteydestä (esim. värittämällä osoitekentän tai näyttämällä suljetun lukon kuvaa).
- Kun käytät https-alkuisia sivuja, voit yleensä asioida turvallisesti nettipankissa, käyttää sähköpostia (esim. Gmailia) ja sosiaalista mediaa (esim. Facebook) sekä muitakin sivuja, jonne kirjaudutaan salasanalla. Sen sijaan hakukoneiden (esim. Google), karttapalveluiden (esim. Google maps) käyttöä ja monilla nettisivuilla vierailemista on helpompi seurata.
- Lähes kaikki langattoman verkon käyttämiseen liittyvät tietoturvariskit voi välttää käyttämällä VPN-yhteyttä. Sen voi ostaa sovelluskaupasta tai hankkia esimerkiksi tietoturvapaketin mukana. VPN-yhteys piilottaa laitteesi IP-osoitteen ja sijainnin.
- Muista huolehtia laitteidesi käyttöjärjestelmän, selaimien, tietoturvaohjelmiston ja muidenkin osien säännöllisestä päivittämisestä, koska uusia haittaohjelmia kehitetään ja haavoittuvuuksia löydetään jatkuvasti.
- Hanki kattava tietoturvaohjelmisto luotettavalta valmistajalta (esimerkiksi F-Secure). Haittaohjelmia saatetaan naamioida tietoturvaohjelmiksi tai virusten skannaamiseen, jotta käyttäjä haksahtaisi asentamaan ne koneelleen. Ole tarkkana.

Miten käytät sosiaalista mediaa turvallisemmin?

- Tutustu huolellisesti kaikkien käyttämiesi sosiaalisen median alustojen, yhteisöjen ja sovellusten tietoturva- ja yksiyisyysasetuksiin, jotta olet tietoinen esimerkiksi siitä, kuka näkee julkaisusi ja kuka ei.
- Monet sosiaalisen median alustat, verkkokaupat ja muut sivustot pyytävät henkilökohtaisia tietojamme esimerkiksi osoitteen tilausten toimittamista varten tai puhelinnumeron kaksivaiheista tunnistautumista varten. Huomaa, että tilille murtautuminen avaa pääsyn myös näihin tietoihin.
- Älä hyväksy epäilyttäviä tai epämiellyttäviä ihmisiä kavereiksesi. Vain sinulla on oikeus päättää kenen kaveri olet sosiaalisessa mediassa. Poista huoletta ja ilman syyllisyyttä sellaiset ihmiset kontakteista, joiden kanssa, et halua jakaa asioita.
- Jos olet huolissasi yksityisyydestäsi, varmista, etteivät ympärilläsi olevat ihmiset tai organisaatiot julkaise sinusta asioita ilman lupaa sosiaalisessa mediassa tai netissä laajemmin.
- Mieti tarkkaan, mitä informaatiota julkaisusi sisältää. Tunnistettavat paikat kuvissa kertovat, missä olet liikkunut. Jos olet jakanut sijaintitiedot kameralle, valokuvat saattavat myös sisältää hyvin tarkat koordinaatit paikasta, jossa kuva on otettu.
- Tilien linkkaamiseen toisiinsa (esimerkiksi Pinterestiin kirjautuminen Google-tunnuksilla) liittyy riskejä. On parasta luoda erillinen sähköpostitili sisäänkirjautumisia varten. Varmista, ettei tämän tilin sähköpostiosoite tai salasana pidä sisällään mitään henkilökohtaisia tietojasi.
- Ole myös varovainen sen suhteen, millaista tietoa jaat muista ihmisistä sosiaalisessa mediassa.

Mistä voin päätellä, että tililleni on murtauduttu?

- Monet sosiaalisen median tilit tai sähköpostiohjelmat tallentavat viimeisimmät kirjautumishistoriatiedot eli laitteen IP-osoitteen ja kirjautumisajan sekä mahdollisesti myös laitteen tyypin, jolla tilille on kirjaduttu. Huomioi, että jos kirjautuessa käytetään puhelimesta jaettua nettiyhteyttä tai VPN:n yhteyttä, IP-osoitteeseen liitetty paikkatieto voi heittää merkittävästi.

Miten tunnistan väärennetyn sähköpostiviestin?

- Sähköpostien lähettäjätietoihin ei valitettavasti voi luottaa. Netistä löytyy lukuisia ilmaisia ohjelmia, joiden avulla sähköpostin lähettäjätiedot (lähettäjän nimi ja sähköpostiosoite, mistä sähköposti näyttäisi tulevan) voi itse määritellä.
- Luota intuitioosi äläkä avaa epäilyttävien sähköpostien liitetiedostoja tai klikkaa linkkejä, varsinkaan omalla laitteellasi. Erityisesti, jos viesti sisältää linkkejä tai liitetiedostoja, voi olla hyvä idea ottaa viestin oletettuun lähettäjään yhteyttä ensin jotain muuta kautta, jotta varmistut sähköpostin aitoudesta. Väkivallan tekijä saattaa myös yrittää vaikuttaa esimerkiksi oikeudenkäyntiin lähettämällä viestin, jossa kerrotaan sovitun tapaamisen perumisesta tai siirrosta.

Mitä kautta vainoaja voi saada tietoa sijainnistani?

- Monet sosiaalisen median alustat, sovellukset ja laitteet tallentavat sijaintitietoja tai mahdollistavat sijaintitietojen jakamisen – myös käyttäjän tietämättä. Näin ollen pääsy näille tileille saattaa mahdollistaa käyttäjän paikantamisen. Sijaintitietoja tallentavat esimerkiksi: Google/Gmail, Facebook, Instagram, Twitter, WhatsApp. Käy käyttämiesi alustojen ja sovellusten asetukset huolellisesti läpi ja estä sijaintitietojen tallentaminen. Turhat tilit ja sovellukset kannattaa poistaa. Laita sijaintitietojen tallentaminen pois päältä myös puhelimesta.
- Erilaiset perhepaketit, jotka mahdollistavat perheenjäsenten sijainnin seuraamisen (esimerkiksi Applen Family Sharing, Google Families). Sijainnin jakaminen on saatettu aktivoida kumppanin tietämättä. Myös kadonneen puhelimen etsimiseen suunnitellut palvelut (esimerkiksi Find My iPhone) mahdollistavat paikantamisen. Sijaintisi saatetaan seurata myös lasten puhelinten kautta.
- Pääsy auton navigaattorin tietoihin paljastaa, missä olet liikkunut.
- Esimerkiksi kadonneiden avainten tai lemmikin paikantamiseen on kehitetty lukuisia sovelluksia (esimerkiksi Tile), joista osa on kooltaan kolikon kokoisia. Pieni paikannin on helppo piilottaa esimerkiksi käsilaukkuun, pyörään tai autoon, ja sen avulla voi seurata vakoilun kohteena olevan ihmisen liikkeitä reaaliaikaisesti ja päästä käsiksi myös sijaintihistoriatietoihin. Paikantaminen voi tapahtua myös ylimääräisen puhelimen avulla.
- Erilaiset vakoiluohjelmat mahdollistavat vakoilun kohteena olevan ihmisen sijainnin seuraamisen.
- Tietoja sijainnistasi voi levitä oman tai muiden sosiaalisen median kautta. Kuvat voivat sisältää tarkkojakin sijaintikoordinaatteja, jos paikkatiedot on jaettu ka-

meran kanssa, jolla kuva on otettu.

- Ole tietoinen omasta digitaalisesta jalanjäljestäsi, eli kaikesta tiedosta, jota sinusta löytyy netistä. Myös erilaiset organisaatiot (esimerkiksi koulut, yhdistykset, urheiluseurat, seurakunnat) julkaisevat jäsenistään tietoja.
- Paikannus lähietäisyydeltä voi onnistua myös wi-fin tai bluetoohin kautta. Käytä VPN-yhteyttä ja bluetoothia vain tarvittaessa.
- Tietoja saatetaan myös urkkia lähelläsi olevilta ihmisiltä ja ammattilaisilta mitä mielikuvituksellisin keinoin.

Mistä voin tietää, onko laitteessani vakoiluohjelma?

- Todennäköisintä on, että väkivallan tekijä saa tietonsa jotain muuta kautta esimerkiksi murtautumalla sähköpostiin, pikaviestipalveluiden tai sosiaalisen median tileille. Tyypillisin vaaranpaikka on heikko salasana. Jos tilejä on linkattu yhteen eli kirjaudut vaikkapa Pinterestiin Google-tunnuksilla, yhden salasanan avulla voi päästä käsiksi suureen määrään tietoa. Huomaa, että jos olet käyttänyt kumppanisi konetta, johon on asennettu näppäilyntallennin, hän on voinut saada käsiinsä suuren joukon salasanojasi.
- Jos arvioit tilanteen riittävän turvalliseksi, kannattaa aloittaa vaihtamalla tärkeimpien tilien salasanat turvallisella laitteella (esimerkiksi kirjaston tai ystävän koneella), ottaa käyttöön kaksivaiheinen tunnistautuminen ja estää sijainnin jakaminen puhelimesta.
- Seuraavaksi kannattaa miettiä, onko tekijällä ollut mahdollisuuksia asentaa laitteeseesi vakoiluohjelma. Onko tekijällä ollut pääsy laitteisiisi? Käytätkö tekijän laitteita tai teknologiaa, jonka sinä tai lapsesi ovat saaneet häneltä lahjaksi (näppäimistö mukaan lukien)? Onko tekijä auttanut sinua asentamaan ohjelmistoja laitteisiisi tai ratkomaan muita teknisiä ongelmia? Muistatko vastaanottaneesi epäilyttäviä sähköposteja, joissa on linkkejä tai liitetiedostoja?
- Vakoiluohjelmaa on syytä epäillä, jos tekijä tuntuu saavan salasanojen vaihtamisen jälkeenkin tietoja viesteistäsi, puhelinkeskusteluistasi, liikkeistäsi ja muusta teknologian käytöstäsi. Luota omiin vaistoihisi ja etsi säännönmukaisuuksia väkivallan tekijän käytöksestä.
- Joko väkivaltatyön ammattilaisen tai luotetun ystävän kanssa on hyvä ryhtyä systemaattisesti kartoittamaan, mitä vainoaja tietää ja mistä laitteesta, sovelluksesta tai muista lähteistä tämä informaatio voisi olla peräisin. Aina ei ole kyse teknologian välityksellä tapahtuvasta vakoilusta. Tietoa on mahdollista urkkia myös muilta ihmisiltä tai “perinteisillä keinoilla” kuten fyysisesti seuraamalla.
- Kun vakoiluohjelma on asennettu, se toimii niin sanotussa häivetilassa (engl. stealth mode), jolloin sitä on vaikea löytää ja poistaa. Laadukkaiden tietoturva- ja virustorjuntaohjelmien (esimerkiksi F-Securen tuotteet) pitäisi tunnistaa vakoiluohjelmat, mutta nekään eivät voi tarjota täyttä varmuutta, koska uusia ohjelmistoja kehitetään koko ajan. Virustorjuntaohjelma ei pysty esimerkiksi tunnistamaan erillisen näppäilyntallentimen välityksellä tapahtuvaa vakoilua.

- Tarkista säännöllisesti laitteen datankäyttö, virrankulutus, laitteeseen asennetut ohjelmat ja sovelluksille myönnetyt oikeudet. Poikkeuksellinen akun kuluminen tai piikki dataliikenteessä voi kieliä laitteeseen asennetusta vakoiluohjelmasta. Voit verrata tietoja dataliikenteen määrästä aikaisempaan, jos tietoja on saatavilla. Esimerkiksi vanhoista puhelinlaskuista löytää tiedon datankäytöstä. Kannattaa myös käydä läpi laitteeseen asennettuja ohjelmia ja niille myönnettyjä oikeuksia. Häivetilassa toimivia vakoiluohjelmia ei kuitenkaan välttämättä huomaa tällä tavalla.

Miten vakoiluohjelma asennetaan laitteeseen?

- Vakoiluohjelma voidaan asentaa laitteelle joko siten, että päästään laitteeseen fyysisesti käsiksi tai netin välityksellä esimerkiksi sähköpostiviestissä olevan linkin tai liitetiedoston kautta. Esimerkiksi Applen tuotteisiin vakoiluohjelman voi asentaa Apple ID-tunnuksilla. Ohjelma saattaa asentua itsestään myös pelkästään sähköpostin avaamalla. Asennusohjelma on voitu naamioida esimerkiksi peliksi tai onnitteluviestiksi. Myös laitetta käyttävä lapsi saattaa tietämättään asentaa vakoiluohjelman. Vakoiluohjelman asentuminen vaatii kuitenkin lähes aina käyttäjältä toimenpiteitä, kuten linkin klikkausta tai liitteen avaamista, joten älä klikkaa mitään vähänkään epäilyttävää.
- Vakoilu saattaa tapahtua myös fyysisen laitteen kuten koneen ja näppäimistön väliin asetettavan plugin välityksellä tai tallennusominaisuus saattaa olla näppäimistössä sisäänrakennettuna. Näppäimistön käytön tallentavia laitteita ja ohjelmistoja kutsutaan keyloggereiksi tai näppäilytallentimiksi.

Mitä teen, jos on syytä epäillä, että laitteessani on vakoiluohjelma?

- Älä poista vakoiluohjelmaa itse. Jos löydät laitteestasi vakoiluohjelman tai asiasta on vahva epäilys, ole yhteydessä väkivaltatyön ammattilaisiin tai poliisiin. Älä ryhdy itse poistamaan vakoiluohjelmaa esimerkiksi tehdasasetuksia palauttamalla. Tuhoat tärkeää todistusaineistoa. Pidä lähtökohtaisesti laite päällä kunnes esimerkiksi poliisi on toisin ohjeistanut. Laitteen sulkeminen saattaa tuhota todistusaineistoa. Huomioi, että puhelimen ollessa päällä väkivallan tekijä voi saada tiedon liikkeistäsi. Niin sanottu Faraday-pussi (ks. alempana) estää laitteen vakoilun, kun toimitat sen poliisille. Vakoilijan näkökulmasta laite ei ole verkossa, kun se on pussin sisällä. Kun laitteen ottaan pois pussista, vakoilija saattaa saada tiedon sijainnistasi.

- Käytä turvallisia laitteita. Mikäli on perusteltua epäillä, että laitteessa on vakoiluohjelma, on syytä olettaa, että tekijä pystyy seuraamaan kaikkea mitä laitteella teet. Hän saa tiedon esimerkiksi siitä, että etsit tietoa vakoiluohjelmista tai yrität poistaa ohjelman. Näin ollen väkivallan riskiä kasvattavat toimenpiteet (esimerkiksi tiedon hakeminen vakoiluohjelmista tai parisuhdeväkivallasta) kannattaa tehdä turvallisella laitteella kuten ystävän tai kirjaston tietokoneella.

- Priorisoi turvallisuus. Vakoiluohjelman poistaminen tai laitteen käytön lopettaminen saattaa joissain tapauksissa kasvattaa väkivallan riskiä. Luota omaan intuitioosi ja laita turvallisuutesi etusijalle. Joskus on parasta jatkaa laitteen käyttöä vakoilusta huolimatta ja käyttää rinnalla turvallisia laitteita.

- Jos mahdollista, hanki uusi turvallinen laite. Mitä vanhempi ja yksinkertaisempi malli, sitä vaikeampi sitä on vakoilla. Voit käyttää useampaa laitetta rinnakkain ja tehdä väkivallan riskiä kasvattavat toimenpiteet turvallisella laitteella. Ole varovainen, jos siirrät tiedostoja vanhalta koneelta uudelle (esimerkiksi sovelluksia, dokumentteja, kuvia, videoita), koska vakoiluohjelma saattaa asentua niiden kautta uudestaan.

- Huomioi lapset ja perheenjäsenet. On tärkeää, että myös lapset ja läheiset saavat tiedon vakoiluohjelmien vaaroista sekä niiltä suojautumisesta. Pyydä heitä olemaan avaamatta epäilyttäviä sähköposteja. Viattoman kuvan tai videon avaaminen tai sähköpostissa tai pikaviestipalvelussa olevan linkin klikkaaminen saattaa asentaa laitteelle vakoiluohjelman.

- Faraday Bag on pussi tai laukku, joka estää yhteyden saamisen, tiedonsiirron ja sijainnin jakamisen älypuhelimesta tai tietokoneesta, jossa on vakoiluohjelma tai jota vakoillaan jotain muuta kautta. Silloin vakoilija ei saa tietoa laitteen sulkemisesta, vaan ulospäin näyttää siltä, ettei laite ole verkossa. Pusseja löytyy eri valmistajilta.

AMMATTILAISELLE

Miten ryhdyn kartoittamaan tilannetta kokijan kanssa?

- Selvitä, mistä asioista kokija on tällä hetkellä eniten huolissaan ja mikä on hänen käsityksensä tapahtumien kulusta. Mitkä tilanteet ovat herättäneet hänessä eniten pelkoa viime aikoina? On tärkeää, että väkivallan kokija tulee kuulluksi, että häntä uskotaan ja että hänen intuitioonsa luotetaan.
- Kun yksityisyyttä on loukattu, lähtötilanteena on usein epämääräinen tunne siitä, että väkivallan tekijä tietää "liikaa." Kartoita kokijan kanssa järjestelmällisesti sitä, millaista informaatiota tekijällä tuntuu olevan ja mistä tämä tieto voisi olla peräisin. Väkivallan tekijällä saattaa olla tietoa esimerkiksi kokijan ja muiden ihmisten välisistä keskusteluista tai kokijan liikkeistä, mutta ei ole täyttä varmuutta, millä tavalla siihen on päästy käsiksi.
- Opasta kokijaa käyttämään turvallisia laitteita kuten kirjaston tietokonetta tai ystävän puhelinta.
- Auta kokijaa käymään läpi erilaisten laitteiden ja sovellusten turvallisuusasetuksia. On tärkeää käyttää turvallista laitetta (esimerkiksi kirjaston konetta), kun vaihdetaan salasanoja. Tilanne on syytä arvioida huolellisesti, koska joissain tapauksissa yksityisyyden lisääminen saattaa lisätä väkivallan uhkaa.
- Arvioi yhdessä kokijan kanssa erilaisten laitteiden, alustojen ja sovellusten käytön riskejä ja hyötyjä.
- Ohjeisteta kokijaa pitämään kirjaa väkivallanteoista ja tallentamaan digitaaliset vahingonteot.
- Päivitä yhdessä kokijan kanssa turvasuunnitelma miettien erityisesti teknologiaan liittyviä seikkoja. Auta kokijaa raportoimaan väärinkäytökset viranomaiselle tai palveluntarjoajalle, mutta pidä mielessä todistusaineiston tallentamiseen liittyvät seikat: loukkaavat viestit ja kuvat saatetaan poistaa nopeastikin sosiaalisen median alustoilta, joten ne on tärkeää tallentaa ne mahdollisimman pian esimerkiksi kuvakaappauksilla.

AMMATTILAISELLE

Miten voit avata keskustelun digitaalisen väkivallan tai vainon kokijan kanssa?

Voit kysyä esimerkiksi...

- Mistä asioista olet tällä hetkellä eniten huolissasi? Mitkä tilanteet ovat herättäneet sinussa epävarmuutta ja pelkoa viime aikoina?
- Arveletko, että väkivallan tekijä voi seurata liikkeitäsi? Mistä luulet tämän informaation olevan peräisin? Esimerkiksi: sovellukset ja alustat (Google, Facebook, Snapchat jne), erilaiset perhepaketit (Apple Family Sharing), auton navigointijärjestelmä, koiran tutkapanta, vakoiluohjelmat, GPS-paikannin

- Luuletko, että väkivallan tekijä seuraa sinun ja muiden ihmisten välisiä keskusteluja? Minkä välineen tai sovelluksen kautta tämä voisi tapahtua? Esimerkiksi: sähköposti, tekstiviestit, pikaviestipalvelut (WhatsApp, Messenger, Telegram), Facebook, Instagram
- Epäiletkö, että väkivallan tekijä on voinut kuunnella sinun ja muiden ihmisten välisiä puhelinkeskusteluja tai kasvokkaisia keskusteluja? Esimerkiksi: vakoiluohjelma puhelimessa, salakuuntelulaitteet, itkuhälyttimet
- Oletko huolissasi kuvista, dokumenteista tai informaatiosta, joita netissä on julkaistu sinuun liittyen? Osaatko sanoa, millä foorumeilla tai sivulla näitä asioita on levitetty? Huolestuttaako sinua joku muu netissä oleva sisältö?
- Herättääkö lastesi tai läheistesi teknologian käyttö sinussa huolta? Pohditko sitä, miten se vaikuttaa turvallisuuteesi? Liittyykö huoli joihinkin tiettyihin laitteisiin, sovelluksiin tai peleihin?
- Pohditko sitä, millä tavalla voit käyttää teknologiaa vaarantamatta turvallisuuttasi ja yksityisyyttäsi? Haluatko käydä läpi jonkun tietyn laitteen, sovelluksen tai sosiaalisen median alustan turvallisuusasetukset?
- Mitkä muut asiat huolettavat sinua yksityisyyteen ja turvallisuuteen liittyen?

Someturvan oikeudellinen arvio

Pyysimme Someturvan juristia kommentoimaan kyselyyn tulleita vastauksia rikosoikeudellisesta näkökulmasta. Someturva on sosiaalisessa mediassa tapahtuneisiin rikoksiin erikoistunut digitaalinen lakipalvelu (someturva.fi). On hyvä huomioida, että tapauksia arvioitiin hyvin suppean tiedon perusteella. Niiden pohjalta kuitenkin hahmottuu, missä kulkee rikollisen toiminnan raja digitaalisen väkivallan kohdalla.

"Mustasukkaisuus paheni koko ajan suhteen edetessä. Eksä luki tekstiviestini, eikä kokenut tekevänsä mitään väärää. Hänellä oli oikeus tietää kenen kanssa viestittelen ja mitä viestittelen. Minun piti nukkua puhelin tyynyn alla, ettei hän päässyt tutkimaan sitä."

Someturvan arvio: Jo perustuslaki takaa sen, että kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton (PL 2:10.2 §), joten toisen henkilön viestien lukeminen luvatta ei ole sallittua. Toisen henkilön viestien tutkimisessa ilman lupaa on kyse rikoksesta, jolloin puhutaan viestintäsalaisuuden loukkauksesta (RL 38:3).

"Entinen poikaystäväni on insinööri ja hän hallitsee hyvin teknologian käytön. Hän usein uhkaili, että tietää vakoiluohjelmia ja että kaikki sisältö mitä on minun puhelimessa voi hänen halutessaan latautua sekunneissa hänen puhelimelleen."

Tässä ei ole vielä tapahtunut rikosta, mutta jos puhelimen viestinvaihtoa luetaan esimerkiksi vakoiluohjelman avulla ilman lupaa, täyttyy rikoslain mukainen viestintäsalaisuuden loukkaus.

"Jos koulussa meni pitkään, viestejä ja soittoja tuli älytön määrä. Jos en pystynyt vastaamaan, tuli viestejä, joissa hän kehitteli skenaarioita ja syytteli: olin baarissa toisten miesten kanssa. Kotona sitten riideltiin. Hän sai minut aina tuntemaan syyllisyyttä, vaikken tehnyt mitään väärää. Minulla oli velvollisuus olla aina tavoitettavissa, jotta hän pystyi tarkastamaan mitä teen."

Tällaiset jatkuvat häiritsevät yhteydenotot voivat muodostaa rikoksen nimeltä viestintärauhan rikkominen (RL 24:1a). Edellytyksenä on, että toiminta (puhelut, viestit) on jatkuvaa ja sellaista, että se voi aiheuttaa kohteelleen huomattavaa häiriötä tai haittaa.

Lisäksi tällaisessa jatkuvassa yhteyden ottamisessa ja toisen tekemisten tarkkailussa voi tulla kyseeseen myös häirinnän vakavampi muoto, vainoaminen (RL 25:7a). Edellytyksenä on, että tilanne on jatkuva ja sellainen, että se voi aiheuttaa pelkoa tai ahdistusta kohteessaan.

Pelon ja ahdistuksen arvioinnissa on kyse ns. abstraktista vaarasta, eli edellytyksenä ei ole, että teot ovat aiheuttaneet pelkoa tai ahdistusta, vaikka näin on hyvin voinut tapahtua. Se, että teot ovat omiaan aiheuttamaan vainotussa pelkoa tai ahdistusta, tarkoittaa sitä, että pelko tai ahdistus on tuollaisen menettelyn tyypillinen seuraus.

"Entinen poikaystäväni, joka oli mustasukkainen ja väkivaltainen, piinasi minua puhelimen välityksellä. Hän lähetteli viestejä, jotka sisälsivät herjaavaa kieltä ja soitteli välillä taukoamatta. Hän suuttui, jos en vastannut ja käytti vastaa-

mattomuuttani ‘todisteena’ mustasukkaisille harhaluuloilleen.”

Myös tässä tapauksessa tulee kyseeseen edellä mainitut rikokset viestintärauhan rikkominen ja vainoaminen.

Lisäksi herjaavien viestien lähettäminen saattaa täyttää rikoksen nimeltä kunnianloukkaus (RL 24:9). Kunnianloukkauksen täyttymisessä arvioidaan sitä, millaisia herjaavat ilmaisut ovat ja miten loukkaavina niitä voidaan pitää. Esimerkiksi ”huora” ja ”lutka” ovat sellaisia ilmaisuja, joiden on voitu katsoa ylittävän kunnianloukkauksen rajan. Sen sijaan esimerkiksi ulkonäön kommentoinnin ei usein katsota täyttävän kunnianloukkauksen tunnusmerkistöä. Edellytyksenä kunnianloukkauksen täyttymisessä on, että teko aiheuttaa loukatulle kärsimystä tai häneen kohdistuvaa halveksuntaa.

“Ex avopuoliso suuttui joka kerta kun en vastannut puhelimeen, myös silloin kun olin töissä enkä pystynyt vastaamaan. Hän suuttui, jos en vastannut hänen viesteihinsä ja myös aina, jos sain viestin. Jos en vastannut puheluun, olin jonkun miehen kanssa ja jos itse sain viestin se oli hänen mukaansa aina joltain mieheltä. Jouduin aina näyttämään viestin. Silti siitä seurasi viikkojen mykkäkoulu, joka taas loppui huutamiseen ja riitaan.”

Mikäli henkilöä on painostettu väkivallalla tai uhkaamalla näyttämään viestit, voisi tässä täyttyä rikos nimeltä pakottaminen (RL 25:8).

“Eräs puolituttu mies on ollut minusta kiinnostunut ja hän on ottanut usein yhteyttä minuun. En kuitenkaan ole reagoinut mielestäni harmittomiin ‘mitä kuuluu?’ - viesteihin. Yhtenä iltana sain häneltä taas viestin. Mieheni suuttui silmittömästi, syytti minua yhteydenpidosta (jota ei ollut), otti puhelimeni väkisin ja soitti kyseiselle miehelle vastoin tahtoani käskien häntä lopettamaan yhteydenottonsa. Tämän jälkeen hän tarkasti Facebook - kontaktini, olenko hänen ystävänsä siellä.”

Tässä tapauksessa ei tämän kuvauksen perusteella ole kyse mistään sinänsä verkossa tapahtuneesta loukkauksesta. Asian arviointi ei siis kuulu palvelumme piiriin. Puhelimen riistäminen ja käyttäminen oikeudetta voisi mahdollisesti tulla arvoitavaksi rikoslain mukaisena luvattomana käyttönä (RL 28:7), mutta emme ota siihen sen enempää kantaa täyttyisikö kyseinen rikos.

“Lopulta puolisoni jossakin riidassa paljasti, että oli itse asiassa lukenut tekstiviestejäni koko meidän parisuhteen ajan ja jopa lähetellyt minun nimissäni joillekin ystäville sähköposteja sekä tekstiviestejä varmistaakseen, ettei minulla ollut/tulisi olemaan suhdetta heidän kanssaan.”

Viestien lukemisessa salaa on kyse viestintäsalaisuuden loukkauksesta.

Sähköpostien ja viestien lähettäminen toisen nimissä saattaa täyttää identiteettivarkauden (RL38:9a) tunnusmerkistön, edellyttäen että tekijä aiheuttaa kohteelle taloudellista vahinkoa tai vähäistä suurempaa haittaa. Kyseeseen voi tulla myös kunnianloukkaus, jos lähetettyjen viestien sisältö on sellaista, että se halventaa kohdettaan ja voi aiheuttaa hänelle ikäviä seurauksia.

“Koin suurta ahdistusta ja pelkoa, erityisesti, jos näin hänen soittaneen illalla ja puhelun menneen ohi. Tämä enteili yleensä sitä, että hän saattoi ilmoittamatta ilmaantua asuntooni esimerkiksi keskellä yötä tarkistamaan, olinko kotona. Näin yleensä tapahtui, vaikka olisin soittanut takaisin ja selittänyt, miksen vastannut.”

Myös tämä vaikuttaa tapaukselta, jossa voisi olla tulla kyseeseen vainoaminen. Vainoamisrikoksen täyttymisen edellytyksenä on muun muassa se, että toisen seuraaminen tai tarkkailu on toistuvaa ja että se on omiaan aiheuttamaan vainotussa pelkoa tai ahdistusta.

“Exäni latasi kännykkääni ohjelman, jolla saattoi seurata missä milloinkin liikun sekä ohjelman, jolla saattoi lukea lähettämiäni viestejä ja käymäni keskusteluja WhatsAppissa. En tiennyt asiasta mitään moneen kuukauteen. Suhteemme alussa en ollut kokenut tarvetta pitää kännykässäni lukkoa, joten ohjelmien asennukset tietämättäni olivat onnistuneet.”

Viestien lukemisessa on kyse rikoslain mukaisesta viestintäsalaisuuden loukkauksesta.

Toisen henkilön liikkumisen jatkuva tarkkailu ohjelman avulla viittaa myös vainoamisen tunnusmerkistön täyttymiseen. Edellytyksenä on, että tilanne voi aiheuttaa uhrissa pelkoa tai ahdistusta (em. abstrakti uhka).

"Seurustelukumppani oli 'auttanut' sähköpostin luomisessa. Eron jälkeen ymmärsin, että hän oli jotenkin onnistunut synkronoimaan sähköpostimme yhteen ja nähnyt kaikki viestini. Tämän lisäksi hän oli saanut käsiini kaikki salasanani mm. Facebookiin ja mahdollisiin muihin sähköposteihin ja tietoihini urkkimalla asunnossani."

Toisen henkilön sähköpostiviestien lukemisessa ilman lupaa täyttyy rikoslain mukainen viestintäsalaisuuden loukkaus.

"Minulla oli ollut lyhyt emotionaalinen suhde ex-rakastajani kanssa sosiaalisessa mediassa avioliittokriisin aikana. Lopetin suhteen, mutta mustasukkainen aviomieheni oli kirjautunut Facebook-tililleni lukemaan koko kirjeenvaihdon. Tämän seurauksena menetin yksityisyyteni ja ihmisarvoni vuosiksi."

Myös tässä on kyse viestintäsalaisuuden loukkauksesta (luettu kirjeenvaihto).

"Tiedoillani on tilattu mitä sattuu, voimakas epäily on ex kohtaan. Hirveästi hommaa selvitellä asioita ja todistaa, etten se minä ole ollut. Maksuhäiriöitä."

Toisen henkilön henkilötietojen tai tunnistamistietojen luvaton käyttäminen kolmatta osapuolta erehdyttääkseen (tässä myyjää) sillä tavalla, että siitä aiheutuu taloudellista vahinkoa sille, jonka tietoja käytetään, on rikoslain mukainen identiteettivarkaus (RL 38:9a).

"Exäni murtautui suhteemme aikana puhelimeeni, josta lähetteli nimissäni haukkumisviestejä ex-tyttöystävälleen, mustamaalasi minua julkisesti sosiaalisessa mediassa, jos tein jotain mistä hän ei pitänyt (jäin vaikka baariin vaikka hän oli käskenyt lähtemään), mustamaalasi minua ystävilleni ja urkki nettipankkitunnukseni ja tyhjensi tilini."

Mustamaalaaminen viittaa valheiden levittämiseen ja/ tai herjaamiseen, joten tilanteessa voi täyttyä kunnianloukkausrikos.

Viestejä on lähetetty toisen nimissä, joten kyseeseen voi tulla myös identiteettivarkaus, jos teosta on aiheutunut jotakin vähäistä suurempaa haittaa sille, jonka nimissä viestejä on lähetelty.

Tilin tyhjentämistä koskeva tapahtuma ei varsinaisesti kuulu Someturvan alaan, mutta asiaa voitaisiin arvioida mm. maksuvälinepetoksena.

"Erotessamme exäni poisti Dropboxistani kaikki vuoden takaiset kuvani. Profiilini oli jäänyt auki hänen kannettavalle tietokoneelleen. Pyysin kirjautumaan ulos profiilistani, mutta hän ei suostunut. Pyysin myös että saisin käydä hänen luonaan pelastamassa kuvani ja käydä kirjautumassa ulos Dropbox-tililtäni, mutta hän ei suostunut siihenkään."

Toisen omaisuuden oikeudeton hävittäminen, eli tässä kuvien poistaminen, on rikoslain mukainen vahingonteko. Tällainen ei kuitenkaan sinänsä kuulu Someturvan alaan.

"Kun kavereita tulossa kylään tai jos olin menossa autolla kavereiden luo kylään koiran tutkapanta saattoi olla kodinhoitohuoneen pöydällä tai jäi 'vahingossa' autoon. Ex aviopuoliso salakuunteli koiran tutkapannan avulla kotona ja autossa."

Tilanteessa täyttyy rikoslain mukainen salakuuntelu (RL 24:5). Salakuuntelu voi täyttyä kotirauhan suojaamassa paikassa tai myös muualla, jos puhetta ei ole tarkoitettu sitä salaa kuuntelevan/muun ulkopuolisen tietoon ja salakuuntelu tapahtuu sellaisissa olosuhteissa, joissa puhujalla ei ole syytä olettaa ulkopuolisen kuulevan hänen puhettaan.

"Kodistani josta heitin miehen pois löytyi tallentava mikrofoni ja autostani GPS-paikannin."

Tilanteessa voi täyttyä salakuuntelun tai salakuuntelun valmistelun tunnusmerkistö tallentavan mikrofonin osalta. GPS-paikantimen osalta saattaisi täyttyä vainoamisen tunnusmerkistö. Tunnusmerkistössä on mainittu yhtenä tekomuotona seuraaminen, joka edellyttää kuitenkin fyysistä seuraamista. Eräänä

toisena vainoamisen tekomuotona on mainittu tarkkaileminen, jossa voidaan hyödyntää myös teknisiä apuvälineitä.

"Hän jätti joitain kertoja oman läppärinsä kuvaamaan kotiamme webkameralla."

Kotirauhan suojaamassa paikassa ilman lupaa tapahtuva kuvaaminen täyttää rikoksen nimeltä salakatselu (RL 24:6) tunnusmerkistön.

"Ex-avopuoliso paikansi puhelintani eron jälkeen ja lähetti viestejä kenen kanssa milloinkin olin ja mitä tekemässä, väitti itse olevansa sattumalta paikalla. Puhelimeeni tuli monesti ilmoitus, että puhelimesi on löydetty. Meni pitkän aikaa ennen kuin tajusin mistä oli kyse. Tuntui etten päässyt jatkuvasta kontrollista eroon edes erottuani. Näin monesti painajaisunia tästä."

Tällainen toisen henkilön jatkuva tarkkailu mm. paikantamalla puhelinta voi myös täyttää vainoamisen tunnusmerkistön. Arvioinnissa otetaan huomioon mm. pelon ja ahdistuksen aiheutumisen mahdollisuus kohteelle (abstrakti vaara) ja toiminnan jatkuvuus.

"Puoliso luki tekstiviestit, työsähköpostini ja yritti murtautua sähköpostitilille, jossa oli valokuvat fyysisestä pahoinpitelystä. Seurasi minua Windows-phonen paikannuksen avulla kun tiesi tunnukseni (oli "auttanut" tekemään tunnukset käyttöönoton yhteydessä. Tyhjensi puhelimeni sivuhistorian, jotta ei jäisi kiinni tarkkailusta. Tarkkaili kotihälytysjärjestelmän avulla olenko kotona. Soitti ja laittoi tekstiviestejä koko ajan eikä uskonut, että olen palaverissa kun en vastannut. Vaati kuvaviestejä osoittamaan missä olen."

Myös tässä on jatkuvaa tarkkailua teknisen apuvälineen avulla, joten kyseeseen voi tulla vainoaminen.

"Eron jälkeen vainoaminen jatkui 24/7 reilun vuoden ajan ulottuen jopa työpaikallani ja esimieheni uhkailuun. Kun aloin selvittää kuinka vainoaminen mahdollistui niinkin laajassa mittakaavassa, paljastui taustalta teknologiaa. Puhelimeeni oli asennettu vakoiluohjelma, joka ilmoitti exän puhelimeen jokaisen saapuvan viestin sisältöineen sekä puheluista tiedot (mistä numerosta soitetaan, kumpi soittaa ja kauanko puhelu kestää). Vein tietokoneen huoltoon, josta löytyi vakoiluohjelma näppäimistön käytön tallentamiseen, josta selvisi myös hänen kirjautuneen tiedoilla Facebookiin ja sähköposteihini ja laittaneen uhkailuviestejä tutuilleni tietämättä."

Viestien lukemisessa täyttyy rikoslain mukainen viestintäsalaisuuden loukkaus.

Viestien ja puheluiden jatkuva seuraaminen viittaa myös sellaiseen toisen henkilön tarkkailuun, joka voisi täyttää vainoamisen tunnusmerkistön.

"Puolisoni valokuvasi kännykällä muun muassa vaatteiden vaihtoani (salaa) ennen kuin huomasin sen. Eron jälkeen alkoi viestien lähettely (myös kuvia sukupuolielimestä). Viestejä tuli niin työ kuin henkilökohtaiseen puhelimeen satoja. Ex-puolison lähettämiä sukupuolielin kuvia meni työpuhelimen kautta seuraajalleni työpaikallani. En usko, että niitä kovin mielissään katseltiin. Häirintää kesti melkein vuoden kunnes löysi uuden naisen itselleen."

Tällaisessa salaa tapahtuvassa kuvaamisessa on kyse rikoslain mukaisesta salakatselusta (RL 24:6). Kotirauhan suojaamassa paikassa, tai esimerkiksi pukuhuoneessa tai käymälässä tapahtunut kuvaaminen täyttää tunnusmerkistön.

"Miehen entisellä asunnolla oli kamerat, joista tiesin mutta en niiden sijaintia tai sitä että ne olivat päällä (piti nauhoittaa vain poissaollessamme). Videokuvaa minusta joutui miespuolisten ystäviensä arvosteltavaksi. Alusvaatteissa näytin kuulemma laudalta ja pojalta. Videokuvaa seksiaktista joutui yhden mieshenkilön käsiin. Tästäkin kommentit oli, että mieheni on homostellut pojan kanssa."

Koska henkilö ei ole ollut tietoinen kameroiden sijainnista tai siitä, että ne ovat päällä, tulee tässäkin tapauksessa kyseeseen salakatselu.

Sen lisäksi vähäpukeisuutta ja seksiaktia sisältävän videomateriaalin sisältöä voidaan pitää sellaisena yksityisyyden piiriin kuuluvana asiana, jonka levittäminen muille täyttää rikoslain mukaisen yksityiselämää loukkaavan tiedon levittämisen tunnus-

merkistön (24:8). Yksityiselämää loukkaavaa tiedon levittämistä koskevassa arvioinnissa oleellista on se, miten laaja joukko on levitetyn kuvan/ tiedon nähnyt. Usein vaatimuksena on kymmeniä ihmisiä.

Jos videomateriaalin levittämisen tarkoituksena on halventaa kohdettaan, voi tapaus tulla arvioitavaksi myös kunnianloukkauksena.

"Ex-poikaystävä kavereineen muokkasi kuvani pornosivulta napattuun screenshottiin ja jakoi sitä entisen kotipaikkakunnan sisällä erinäisissä keskusteluryhmissä."

Tapaus voisi tulla arvioitavaksi ainakin kunnianloukkauksena (muokattu, valheellinen kuva) ja arkaluontoisuutensa vuoksi myös yksityiselämää loukkaavana tiedon levittämisenä, jos kuva on levinnyt laajalle joukolle.

"Entinen kumppanini videokuvasi minua kännykällään seksin harrastamisen aikana. Olin tuolloin vasta 16-vuotias. Missään vaiheessa en ollut antanut lupaa kuvaamiseen, ja pyysin poikaystävääni lopettamaan useaan otteeseen. Jälkeenpäin hän valehteli poistaneensa videon samana päivänä, mutta olikin näyttänyt sen useammalle kaverilleen ja lähettänyt eteenpäin Facebookissa."

Kuvaaminen ilman lupaa täyttää salakatselun tunnusmerkistön. Lain mukaan esimerkiksi yksityisasunnossa saa kuvata ilman erikseen pyydettävää lupaa sosiaalisesti hyväksytyissä tilanteissa, mutta kuvaamisesta tulee rangaistava teko silloin, kun se tapahtuu oikeudettomasti ja varsinkin jos on kyse intiimistä tilanteesta.

Videon levittäminen voi täyttää muutamankin eri rikoksen tunnusmerkistön. Koska kohteena on ollut lain näkökulmasta lapsi eli alle 18-vuotias henkilö, kyseeseen saattaa tulla sukupuolisiveellisyyttä loukkaavan kuvan levittäminen. Levittämistä voidaan arvioida myös yksityiselämää loukkaavana tiedon levittämisenä, mikäli videota levitetään laajasti, taikka kunnianloukkauksena jos levittämisen tarkoituksena on ollut kohteen halventaminen.

"Ex poikaystävä uhkasi eron jälkeen myös jakaa internetissä alastonkuvani, jotka olin lähettänyt hänelle Whatsappissa suhteen hyvinä aikoina."

Yksityisyyden piiriin kuuluvat arkaluontoiset ja henkilökohtaiset asiat kuten juuri alastomuus. Siksi arkaluontoisen kuvan kuten alastonkuvan levittäminen ilman kuvassa olevan henkilön lupaa voi täyttää yksityiselämää loukkaavan tiedon levittämisen tunnusmerkistön. Tällöin edellytyksenä on, että kuvaa levitetään useiden ihmisten saataville. Lisäksi edellytyksenä on, että henkilö on tunnistettavissa kuvasta. Jos kuvan jakamiseen liittyisi halventamista (esim. haukkumista tms), voisi kyseeseen tulla myös kunnianloukkaus. Jos kuvassa oleva henkilö on alle 18-vuotias, voi kyseeseen tulla myös sukupuolisiveellisyyttä loukkaavan kuvan levittäminen.

"Olin kaukosuhteessa yli vuoden verran netin kautta erään ulkomailla asuvan miehen kanssa. Eron jälkeen mies oli laittanut minun alastonkuvani erääseen Facebook-ryhmään, jossa me kummatkin olimme. Myöhemmin rupesin saamaan viestejä tuntemattomilta miehiltä, eräs kysyi olenko minä tässä kuvassa (hän näytti alastonkuvaani minulle viestissä ja siinä oli linkki pornosivuille). Menin linkin kautta aikuissivuille ja siellä olivat minun alastonkuvani. Kasvoni näkyivät, koko nimeni ja missä maassa asuin oli näkyvillä. Kuvat olivat laitettu vielä pienellä 'esittelytekstillä', kuinka olen huora ja asun Suomessa ja panen muka kaikkia miehiä. Tuntui sanoinkuvaamattoman pahalta."

Toisena henkilönä esiintyminen Facebookissa voi olla identiteettivarkaus, jos teosta aiheutuu taloudellista vahinkoa tai muuta merkittävää haittaa sille, jonka tiedoilla profiili on tehty. Merkittävä haitta voi olla esimerkiksi se, jos asian selvittely tai profiilin poistaminen on vaatinut suurta vaivaa.

Lisäksi toisen henkilön kuvien käyttäminen Facebookissa voi olla rikoslain mukainen kunnianloukkaus, jos kuvien käyttämisellä ja tilin käytöllä on tarkoitus halventaa sinua. Erityisesti jos tilillä on lähetetty muille käyttäjille viestejä, voi viestien tarkemmasta sisällöstä riippuen henkilönä esiintyminen olla niin loukkaavaa, että kunnianloukkauksen raja ylittyy.

"Seurustelukumppani oli seurusteluaikana murtautunut tietokoneelleni, sähköposteihin, Whatsapp viesteihin, sosiaalisen median palveluihin. Eron jälkeen hän keksi tarinan minusta, jolla hän kiristi minua. Hän uhkasi, että kaikki lä-

heiseni, ystäväni, tuttavani ja työtoverini saisi tietää millainen huora minä olin. Hän uhkasi levittää keksimäänsä tarinaa sosiaalisen median kautta. Hän seurasi liikkeitäni, tekemisiäni, tapaamisia ja harrastuksiani. Hän lähettäminen uhkausviestejä työ- ja kotisähköpostiin sekä WhatsApin ja Facebookin välityksellä. Lopulta hän teki nimissäni Facebook-profiilin väittäen, että minulla on kaikenlaisia sukupuolitautеja. Profiili sisälsi yksityisiä vähäpukeisia kuvia minusta. Vainoamista, seuraamista ja uhkailua kesti reilun vuoden, seurustelu ei ollut kestänyt edes puolta vuotta."

Mikäli toimintaan sisältyy se, että tekijä pakottaa uhkauksella toisen tekemään, sietämään tai jättämään tekemättä jotakin, tilannetta voidaan arvioida pakottamisena. Rikoslain mukainen kiristäminen taas liittyy taloudelliseen etuun.

Jos uhkailija toteuttaisi uhkauksensa, voisi olla kyse kunnianloukkauksesta, sillä toisen maineen pilaaminen somessa voi täyttää tunnusmerkistön. Oikeudellisessa arvioinnissa otetaan tällöin huomioon muun muassa levitettävän valheen loukkaavuus ja kuinka suurelle ihmisjoukolle sitä levitetään.

"Minun poissaollessani exä oli tutkinut tietokoneeni läpikotaisin ja tallentanut koneeltani itselleen muun muassa valokuvia, missä esiinnyn jonkun entisen miesystäväni kanssa. Kun sitten lopulta erosimme ja aloitin uuden seurustelusuhteen, oli ex etsinyt Facebookista uuden miesystäväni ja tämän sähköpostiosoitteen ja lähetti näitä valokuvia hänelle."

Jos kuvat ovat vain tavanomaisia kuvia pariskunnasta, ja niitä on lähetetty ainoastaan tälle yhdelle henkilölle, ei kyseessä ole rikos.

Jos kyseessä olisi esim. intiimejä kuvia ja niitä levitettäisiin laajalle joukolle, voisi kyseeseen tulla yksityiselämää loukkaavan tiedon levittäminen.

Jos puolestaan kuvien jakamisen tarkoitus on herjata kuvassa olevaa henkilöä, voisi tapausta arvioida kunnianloukkauksena.

Lainsäädäntöä

1 a § (13.12.2013/879)
Viestintärauhan rikkominen

Joka häirintätarkoituksessa toistuvasti lähettää viestejä tai soittaa toiselle siten, että teko on omiaan aiheuttamaan tälle huomattavaa häiriötä tai haittaa, on tuomittava viestintärauhan rikkomisesta sakkoon tai vankeuteen enintään kuudeksi kuukaudeksi.

5 § (9.6.2000/531)
Salakuuntelu

Joka oikeudettomasti teknisellä laitteella kuuntelee tai tallentaa

1) keskustelua, puhetta tai yksityiselämästä aiheutuvaa muuta ääntä, jota ei ole tarkoitettu hänen tietoonsa ja joka tapahtuu tai syntyy kotirauhan suojaamassa paikassa, taikka

2) muualla kuin kotirauhan suojaamassa paikassa salaa puhetta, jota ei ole tarkoitettu hänen eikä muunkaan ulkopuolisen tietoon, sellaisissa olosuhteissa, joissa puhujalla ei ole syytä olettaa ulkopuolisen kuulevan hänen puhettaan,
on tuomittava salakuuntelusta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Yritys on rangaistava.

6 § (9.6.2000/531)
Salakatselu

Joka oikeudettomasti teknisellä laitteella katselee tai kuvaa

1) kotirauhan suojaamassa paikassa taikka käymälässä, pukeutumistilassa tai muussa vastaavassa paikassa oleskelevaa henkilöä taikka

2) yleisöltä suljetussa 3 §:ssä tarkoitetussa rakennuksessa, huoneistossa tai aidatulla piha-alueella oleskelevaa henkilöä tämän yksityisyyttä loukaten,
on tuomittava salakatselusta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Yritys on rangaistava.

7 § (9.6.2000/531)
Salakuuntelun ja salakatselun valmistelu

Joka sijoittaa 5 tai 6 §:ssä tarkoitetun laitteen salakuuntelussa tai -katselussa käytettäväksi, on tuomittava salakuuntelun valmistelusta tai salakatselun valmistelusta sakkoon tai vankeuteen enintään kuudeksi kuukaudeksi.

8 § (13.12.2013/879)
Yksityiselämää loukkaava tiedon levittäminen

Joka oikeudettomasti

1) joukkotiedotusvälinettä käyttämällä tai

2) muuten toimittamalla lukuisten ihmisten saataville
esittää toisen yksityiselämästä tiedon, vihjauksen tai kuvan siten, että teko on omiaan aiheuttamaan vahinkoa tai kärsimystä loukatulle taikka häneen kohdistuvaa halveksuntaa, on tuomittava yksityiselämää loukkaavasta tiedon levittämisestä sakkoon.

Yksityiselämää loukkaavana tiedon levittämisenä ei pidetä sellaisen yksityiselämää koskevan tiedon, vihjauksen tai kuvan esittämistä politiikassa, elinkeinoelämässä tai julkisessa virassa tai tehtävässä taikka näihin rinnastettavassa tehtävässä toimivasta, joka voi vaikuttaa tämän toiminnan arviointiin mainitussa tehtävässä, jos esittäminen on tarpeen yhteiskunnallisesti merkittävän asian käsittelemiseksi.

Yksityiselämää loukkaavana tiedon levittämisenä ei myöskään pidetä yleiseltä kannalta merkittävän asian käsittelemiseksi esitettyä ilmaisua, jos sen esittäminen, huomioon ottaen sen sisältö, toisten oikeudet ja muut olosuhteet, ei selvästi ylitä sitä, mitä voidaan pitää hyväksyttävänä.

8 a § (13.12.2013/879)
Törkeä yksityiselämää loukkaava tiedon levittäminen

Jos yksityiselämää loukkaavassa tiedon levittämisessä aiheutetaan suurta kärsimystä tai erityisen suurta vahinkoa ja rikos on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä yksityiselämää loukkaavasta tiedon levittämisestä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

9 § (13.12.2013/879)
Kunnianloukkaus

Joka

1) esittää toisesta valheellisen tiedon tai vihjauksen siten, että teko on omiaan aiheuttamaan vahinkoa tai kärsimystä loukatulle taikka häneen kohdistuvaa halveksuntaa, taikka

2) muuten kuin 1 kohdassa tarkoitetulla tavalla halventaa toista,
on tuomittava kunnianloukkauksesta sakkoon.
Kunnianloukkauksesta tuomitaan myös se, joka esittää kuolleesta henkilöstä valheellisen tiedon tai vihjauksen siten, että teko on omiaan aiheuttamaan kärsimystä ihmiselle, jolle vainaja oli erityisen läheinen.
Edellä 1 momentin 2 kohdassa tarkoitettuna kunnianloukkauksena ei pidetä arvostelua, joka kohdistuu toisen menettelyyn politiikassa, elinkeinoelämässä, julkisessa virassa tai tehtävässä, tieteessä, taiteessa taikka näihin rinnastettavassa julkisessa toiminnassa ja joka ei selvästi ylitä sitä, mitä voidaan pitää hyväksyttävänä.

Kunnianloukkauksena ei myöskään pidetä yleiseltä kannalta merkittävän asian käsittelemiseksi esitettyä ilmaisua, jos sen esittäminen, huomioon ottaen sen sisältö, toisten oikeudet ja muut olosuhteet, ei selvästi ylitä sitä, mitä voidaan pitää hyväksyttävänä.

10 § (13.12.2013/879)
Törkeä kunnianloukkaus

Jos 9 §:n 1 momentissa tarkoitetussa kunnianloukkauksessa aiheutetaan suurta kärsimystä tai erityisen suurta vahinkoa ja rikos on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä kunnianloukkauksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

7 § (21.4.1995/578)
Laiton uhkaus

Joka nostaa aseen toista vastaan tai muulla tavoin uhkaa toista rikoksella sellaisissa olosuhteissa, että uhatulla on perusteltu syy omasta tai toisen puolesta pelätä henkilökohtaisen turvallisuuden tai omaisuuden olevan vakavassa vaarassa, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa rangaistusta, laittomasta uhkauksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

7 a § (13.12.2013/879)
Vainoaminen

Joka toistuvasti uhkaa, seuraa, tarkkailee, ottaa yhteyttä tai muuten näihin rinnastettavalla tavalla oikeudettomasti vainoaa toista siten, että se on omiaan aiheuttamaan vainotussa pelkoa tai ahdistusta, on tuomittava, jollei teosta muualla laissa säädetä yhtä ankaraa tai ankarampaa rangaistusta, vainoamisesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

8 § (21.4.1995/578)
Pakottaminen

Joka oikeudettomasti väkivallalla tai uhkauksella pakottaa toisen tekemään, sietämään tai tekemättä jättämään jotakin, on tuomittava, jollei teosta muualla laissa säädetä ankarampaa rangaistusta, pakottamisesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

3 § (24.8.1990/769)
Kiristys

Joka muulla kuin 1 §:ssä tarkoitetulla uhkauksella pakottaa toisen luopumaan taloudellisesta edusta, johon rikoksentekijällä tai sillä, jonka puolesta hän toimii, ei ole laillista oikeutta, on tuomittava kiristyksestä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Yritys on rangaistava.

4 § (24.8.1990/769)
Törkeä kiristys

Jos kiristyksessä

1) uhataan vakavanlaatuisella rikoksella, joka vaarantaisi toisen hengen tai terveyden tai aiheuttaisi huomattavaa vahinkoa toisen omaisuudelle,

2) rikoksentekijä käyttää häikäilemättömästi hyväksi toisen erityistä heikkoutta tai muuta turvatonta tilaa,

3) taloudellinen etu, josta toinen pakotetaan luopumaan, on erittäin arvokas tai

4) aiheutetaan rikoksen uhrille tämän olot huomioon ottaen erityisen tuntuvaa taloudellista vahinkoa
ja kiristys on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästäkiristyksestä vankeuteen vähintään neljäksi kuukaudeksi ja enintään neljäksi vuodeksi.
Yritys on rangaistava.

3 § (10.4.2015/368)
Viestintäsalaisuuden loukkaus

Joka oikeudettomasti

1) avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka

2) hankkii tiedon televerkossa tai tietojärjestelmässä välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta,
on tuomittava viestintäsalaisuuden loukkauksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Yritys on rangaistava.

4 § (21.4.1995/578)
Törkeä viestintäsalaisuuden loukkaus

Jos viestintäsalaisuuden loukkauksessa

1) rikoksentekijä käyttää rikoksen tekemisessä hyväksi asemaansa sähköisen viestinnän tietosuojalaissa (516/2004) tarkoitetun teleyrityksen palveluksessa tai muuta erityistä luottamusasemaansa, (16.6.2004/517)

2) rikoksentekijä käyttää rikoksen tekemistä varten suunniteltua tai muunnettua tietojenkäsittelyohjelmaa tai teknistä erikoislaitetta tai rikos muuten tehdään erityisen suunnitelmallisesti taikka

3) rikoksen kohteena oleva viesti on sisällöltään erityisen luottamuksellinen taikka teko huomattavasti loukkaa yksityisyyden suojaa
ja viestintäsalaisuuden loukkaus on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä viestintäsalaisuuden loukkauksesta vankeuteen enintään kolmeksi vuodeksi.

Yritys on rangaistava.

Sähköisen viestinnän tietosuojaL 516/2004 on kumottu L:lla sähköisen viestinnän palveluista 917/2014.

8 § (10.4.2015/368)
Tietomurto

Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta

1) teknisen erikoislaitteen avulla tai

2) muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin
oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta tai datasta.

Yritys on rangaistava.

Tätä pykälää sovelletaan ainoastaan tekoon, josta ei ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta.

8 a § (10.4.2015/368)
Törkeä tietomurto

Jos tietomurto tehdään

1) osana 6 luvun 5 §:n 2 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa tai (8.5.2015/564)

2) erityisen suunnitelmallisesti
ja tietomurto on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä tietomurrosta sakkoon tai vankeuteen enintään kolmeksi vuodeksi.

Yritys on rangaistava.

9 a § (10.4.2015/368)
Identiteettivarkaus

Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava identiteettivarkaudesta sakkoon.