

**Vähäinen rikos ja riittämätön rangaistus:
Identiteettivarkauden kriminalisointi digitaalisessa
yhteiskunnassa**

Oikeussosiologinen tutkielma identiteettivarkauden kriminalisointiprosessista Suomessa
2000-luvulla

Marja Järvinen
Kandidaatintutkielma
Turun yliopisto
Sosiaalitieteet
4.1.2025

Turun yliopiston laatujärjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu
Turnitin OriginalityCheck -järjestelmällä.

Oppiaine: Sosiaalitieteet

Tekijä: Marja Järvinen

Otsikko: Vähäinen rikos ja riittämätön rangaistus: Identiteettivarkauden kriminalisointi digitaalisessa yhteiskunnassa

Ohjaaja: YTT Heidi Elmgren

Sivumäärä: 39 sivua

Päivämäärä: 4.1.2025

Oikeussosiologisessa tutkielmassani käsittelemäni identiteettivarkauden kriminalisointiprosessia vuosien 2001–2015 aikana. Keskityn vuonna 2013 käynnistettyyn tietoverkkorikosdirektiivin täytäntöönpanohanketta koskevaan identiteettivarkauden kriminalisointiin, erityisesti lainvalmisteluprosessissa pidettyihin sidosryhmien ja valiokuntien kuulemisiin. Teoreettisena viitekehystenä käytän Tea Kangasniemen (2012) artikkelia, jossa hän kuvaa oikeudellisia haasteita identiteettivarkauden kriminalisointiin liittyen. Empiirinen aineistoni koostuu tietoverkkorikosdirektiivin täytäntöönpanohankkeessa annetuista lausunnoista liittyen identiteettivarkauden kriminalisointiin. Taustoitin lausuntoja niiden pohjana olevilla muilla lainvalmisteluasiakirjoilla.

Tutkielmassani selvitan, miten lainvalmisteluprosessiin osallistuneet lausunnonantajat oikeuttavat ja haastavat identiteettivarkauden kriminalisointia Kangasniemen (2012) esittämät haasteet huomioiden. Loin synteesin Kangasniemen (2012) esittämistä haasteista ja lausunnoissa esiin nostetuista kriminalisointiperiaateista. Kriminalisointiperiaatteet ovat kriminaalipoliittisia käsitteitä ja oikeusvaltiota määrittäviä arvoja, joiden keskinäisestä hierarkiasta neuvotellaan identiteettivarkauden kriminalisoinnissa. Keskeisimpiä Kangasniemen (2012) ja lausunnonantajien esiin nostamia haasteita ovat 1) identiteetin ja identiteettivarkauden moninaisuus yhdistettynä lainsäädännön tarkkarajaisuuden vaatimukseen, 2) rikostutkinnan mahdollisuudet selvittää rikos yhdistettynä identiteettivarkauden uhrin oikeusturvaan, 3) esitutkinnan pakkokeinojen käytön valtuudet yhdistettynä yksilön ja rikoksesta epäilyn oikeuksien suojaan viranomaisvallalta, sekä 4) rikosoikeuden roolin määrittäminen identiteettitiedon hallinnassa suhteessa rikosoikeuden viimesijaisuuden periaateeseen.

Lausunnoissa kriminalisointia perustellaan ja haastetaan usein kriminalisointiperiaateilla, mutta eri periaatteet saavat etusijan eri lausunnoissa. Identiteettivarkauden kriminalisointi näyttyy kriminaalipoliittisena neuvotteluna eri rooleja edustavien toimijoiden – identiteettivarkauden tekijä ja identiteettivarkauden uhri sekä kansalainen yleensä – oikeussuojista. Lopputuloksena on kriminaalipoliittinen kompromissi. Yhtäältä identiteettivarkauden uhri saa asianomistaja-aseman, mutta toisaalta yksilöiden suojan viranomaisvallalta vuoksi, säännös ei mahdollista telepakkokeinoja, joita esitutkintaviranomaiset tarvitsisivat identiteettivarkauksien selvittämiseen. Kriminalisoinnissa näyttää korostuvan identiteettivarkauden uhrin asema ja yksilöiden suoja identiteettivarkauden tekijän rangaistusvastuun ja rikoksen preventiovaikutuksen yli.

Avainsanat: oikeussosiologia, tietoverkkorikollisuus, identiteettivarkaus, kriminalisointiperiaatteet, lainsäädäntöprosessi

Sisällys

1	Johdanto	4
2	Käsitteet: rikosoikeudellinen sääntely ja digitalisaatio	6
2.1	Internet ja kyberrikollisuus	7
2.2	Identiteettitiedon omistus ja varastaminen	9
2.3	Identiteettivarkaudesta petokseen	10
3	Teoria: oikeudelliset haasteet identiteettivarkauden kriminalisoinnissa digitaalisessa yhteiskunnassa	12
3.1	Identiteettivarkauden tarkkarajaisuus ja moninaisuus	12
3.2	Rikostutkinnan ja rikostekniset haasteet	13
3.3	Yksilön oikeudet ja uhrin asema	14
3.4	Rikosoikeuden rooli henkilötietojen hallinnassa	14
4	Tutkimusasetelma	16
5	EMPIRIA	18
5.1	Lainvalmisteluprosessi identiteettivarkauden kriminalisoinnissa	18
5.2	Laillisuusperiaate - yksilön suoja, oikeasuhtaisuus ja tarkkarajaisuus	21
5.2.1	Rikossäännöksen tarkkarajaisuus ja identiteetin moninaisuus	24
5.3	Oikeushyvien suojeleminen	24
5.4	Kriminalisoinnin hyödyt ja haitat	26
5.5	Rikosoikeuden viimesijaisuus ja mihin se riittää	27
6	Yhteenveto: Identiteettivarkaus ja kansalliset tarpeet	31
	Lähdeluettelo	33
	LIITTEET	39

1 Johdanto

Rikosoikeusjärjestelmän toiminta ja toimivuus perustuvat kriminologisiin teorioihin rikollisuuden ilmenemisestä ja sen kontrolloinnista, teorioihin siitä, mitä rikollisuus on ja miten siihen reagoidaan. Oikeussosiologian ja kriminologian kentällä on oltu kiinnostuneita siitä, miten digitalisaatio ja tietojärjestelmät ovat vaikuttaneet näiden teorioiden pätevyyteen. Internetin käytön yleistyminen on luonnollisesti lisännyt verkossa tehtyjen petosten ja identiteettivarkauksien määrää, jotka ovat itsessään otollisia toteutettavaksi digitaalisessa ympäristössä. Tietojärjestelmien kehitys ja integrointi ihmisten jokapäiväiseen elämään ovat mahdollistaneet uusien rikostyyppien (esim. tietomurto) luomisen, tai vanhojen rikostentien muotojen (esim. identiteettivarkaus) siirtymisen digitaaliseen ympäristöön.

Vuonna 2001 julkaistussa Euroopan neuvoston tietoverkkorikollisuuden yleissopimusta (*Budapest Convention on Cybercrime ETS No. 185*) koskevassa raportissa esitettiin, että ”uudet teknologiat haastavat olemassa olevan lainsäädännölliset konseptit”. Valtioiden rajat eivät enää estä tiedonkulkua samalla, kun valtion sisäinen oikeus rajoittuu tiettyyn maa-alueeseen. Ilmenneet tietoverkkoympäristön ongelmat tulisi yleissopimuksen mukaan käsitellä kansainvälisen oikeuden tasolla. (Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus 2001.) Vuonna 2005 julkaistiin Euroopan neuvoston puitepäätös tietojärjestelmiin kohdistuvista hyökkäyksistä (Puitepäätös 2005/222/YOS), ja kaksi vuotta myöhemmin Suomi allekirjoitti tietoverkkorikollisuuden yleissopimuksen (Yleissopimus 60/2007). Muun muassa tämän yleissopimuksen pohjalta alettiin yhdenmukaistamaan Euroopan sisäistä tietoverkkorikollisuutta koskevaa lainsäädäntöä, johon identiteettivarkauden kriminalisointikin kuuluu.

Vuonna 2009 sisäministeri Holmlund oli valmis harkitsemaan identiteettivarkauden kriminalisointia, sillä se parantaisi ”internetiä käyttävän kansalaisen turvallisuutta” (Yle Uutiset, *Holmlund kriminalisoisi identiteettivarkaudet* 2009). Niin ikään vuonna 2009 tietosuojavaltuutettu korosti identiteettivarkauden uhrin heikkoa oikeusturvaa, kun taas Keskusrikospoliisin ylitarkastaja huomautti rikostutkinnan haasteista. Poliisi ei voi tutkia tietojen luvaton keräämistä ennen kuin kerättyjä tietoja käytetään rikolliseen tarkoitukseen. (Yle Uutiset, *Identiteettivarkaus on Suomessa toistaiseksi tuntematon rikos* 2009.) Identiteettirikollisuus tietoverkkoympäristössä on itsessään yhteiskunnallinen haaste, mutta sitä koskevissa kriminalisointiprosesseissa on myös omat ongelmansa. Samalla, kun

identiteettivarkauden uhrien oikeussuoja on todettu heikoksi, identiteettivarkauksien tutkinta oli ja yhä on haaste poliisitoiminnalle. Identiteettirikokset eivät sovellu poliisin rutinoituun toimintaympäristöön, eikä lainsäädäntö varmista poliisille aina riittäviä keinoja selvittää identiteettivarkauksia. Toisaalta pakkokeinojen käytön laajentaminen on ristiriidassa perusoikeuksien, kuten yksityisyydensuoja, kanssa.

Oikeussosiologisessa tutkielmassani tarkastelen dokumenttianalyysin keinoin, miten identiteettivarkauden kriminalisointiprosessi eteni vuosina 2001–2015 sen laiksi saattamiseen asti. Keskityn nimenomaan digitaalisessa ympäristössä tehtyihin identiteettivarkauksiin, mikä on myös aineistoni eli eduskunnan lainvalmisteluasiakirjojen sisällöllinen painopiste. Teoreettisena viitekehyksenä asiakirjojen analyysille hyödynnän Kangasniemen (2012) artikkelia, jossa kirjoittaja esittelee haasteita identiteettivarkauden kriminalisoinnille. Keskeisiä haasteita (em.) ovat muun muassa internetin luomat voimakeroivaikutukset identiteettirikollisuuden ilmenemiseen, henkilötietoihin liittyvät oikeushyvät (yksityisyys ja omaisuus), niiden suojaamiseen liittyvät ristiriidat suhteessa yksilön oikeuksiin (sananvapaus) ja ristiriidoista aiheutuvat tutkinnalliset haasteet. Identiteettivarkauden kriminalisointia koskevissa lausunnoissa haasteita käsitellään kriminalisointiperiaatteisiin vedoten, mikä on rikoslainsäädännön valmistelutyöltä odotettavaa. Tutkielman tavoitteena on selvittää, miten Kangasniemen (2012) esittämät haasteet ratkaistiin niin, että nähtiin perustelluksi säätää identiteettivarkaus uutena rikostyyppinä rikoslakiin kriminalisointiperiaatteet huomioiden.

2 Käsitteet: rikosoikeudellinen sääntely ja digitalisaatio

Rikosoikeudellisen sääntelyn tehtävät voidaan jakaa kahteen osaan. Kriminalisoinnilla säädellään niin yleistä käyttäytymistä kuin sitä, mitä pidetään paheksuttavana ja missä määrin. Uudelleenkriminalisoinnilla kohdennetaan yhteiskunnallinen vastuu uudestaan. (Hannu Takala 1973 ks. Kostiainen 2023, 1.) Lappi-Seppälän (2022) mukaan rangaistavuuden yksi olennainen tehtävä on täyttää odotukset, joita ihmiset asettavat oikeusturvansa toteutumiseksi. Tähän linkittyvät rangaistuksen yleinen preventiovaikutus ja erityispreventiovaikutus. Jotta rikosoikeusjärjestelmän yleispreventio eli rikollisuuden ennaltaehkäisevä vaikutus toimisi, ihmisten pitää hyväksyä maan normisto. Hyväksynnän saamiseksi rangaistusten tulee olla oikeasuhtaisia ja järjestelmän tasapuolinen. Erityispreventiota sovelletaan, kun tuomari arvioi yksittäistapauksessa esimerkiksi rikoksen tekijän soveltuvuutta johonkin rangaistukseen. Päätettäessä esimerkiksi yhdyskuntapalvelun ja vankeusrangaistuksen välillä, tuomari punnitsee rikoksen tekijän ”sosiaalista selviytymistä” rangaistuksesta sekä rangaistuksen rikollisuutta ehkäisevää vaikutusta. (Lappi-Seppälä 2022.)

Sääntelyn tutkimuksen pääperiaatteet rakentuvat sääntelyjärjestelmän vaikuttavuuden, vastaanottavuuden ja johdonmukaisuuden ympärille. Vaikuttavuudella tarkastellaan sääntelyn odotettuja ja odottamattomia vaikutuksia sosiaaliseen ympäristöön ja sitä, miten sääntely otetaan vastaan väestön toimesta. Vastaanottavuudella arvioidaan, miten uusi säännös sopii yhteen muiden sääntelymuotojen ja kontrollisysteemien kanssa. Johdonmukaisuudella tarkastellaan normien ja arvojen yhdenmukaisuutta sääntelyjärjestelmän sisällä, miten normit vaikuttavat toisiinsa luoden integroidun kokonaisuuden. (Crawford 2006.)

Rikosoikeusjärjestelmän johdonmukaisuutta pyritään ylläpitämään kriminalisointiperiaatteilla. Laillisuusperiaatteeseen sisältyy yhtäältä kielto menetellä viranomaistoiminnassa vastoin lakia tai lain rajat ylittäen ja toisaalta vaatimus viranomaistoiminnan laillisuudesta. Lisäksi lainsäädännön tulee suojata yksityisiä henkilöitä julkista valtaa vastaan ja rikossäännöksen on oltava tarkkarajainen. (Mäenpää 2020, 5–6.) Toisena periaatteena kriminalisoinnin tulisi suojella oikeushyviä. Kriminalisoinnista tulisi olla myös enemmän hyötyä kuin haittaa ja sen tulisi olla käytännön tasolla toimiva. Ultima ratio -periaatteen mukaan rikosoikeudellista järjestelmää ja kriminalisointia on käytettävä viimesijaisena keinona, kun ei ole muuta rikosoikeutta ”moraalisesti hyväksyttävämpää”, teholtaan ”kohtuullisissa määrin lähestyvää” ja kustannuksiltaan kohtuullista toimeenpantavissa olevaa järjestelmää. (Melander 2021, 27.)

2.1 Internet ja kyberrikollisuus

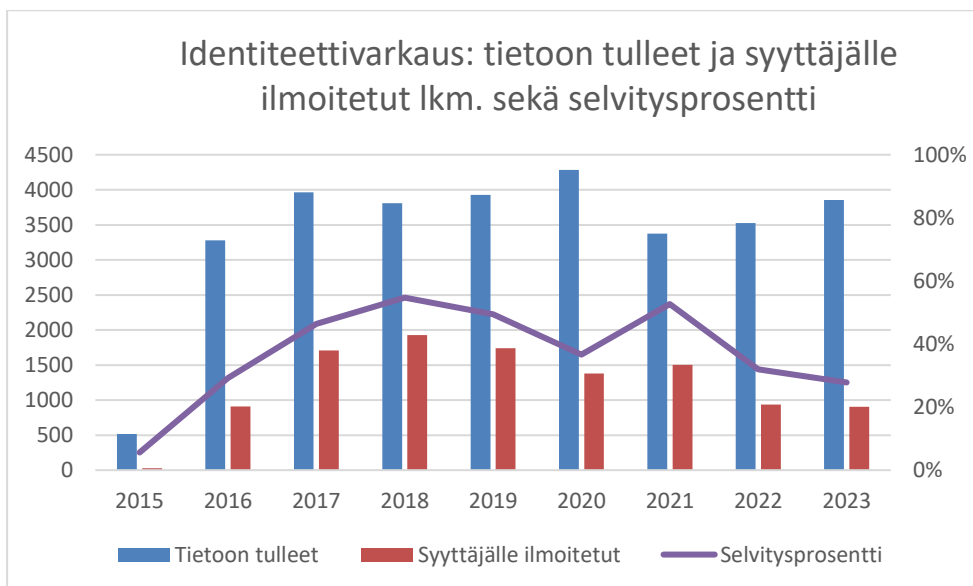
Kriminologiset teorit tarjoavat kriminaalipolitiikalle ja rikoslainsäädännölle teoreettisen pohjan rikollisuuden ja rangaistavuuden toimivuudesta ja oikeutuksesta. Voidaan nähdä, että rikollisuudessa on teknologisen kehityksen tuottaman ”ulkoisen muutosvirtauksen” (*external flux*, Murray 2008) myötä tapahtunut niin merkittävä muutos, että huomattavaa osaa rikollisuudesta ja kontrollimekanismeista ei voida välttämättä arvioida perinteisillä, fyysiseen ympäristöön rakennetuilla kriminologian teorioilla. Wall (2010) esittää, että tietoverkkoteknologiat toimivat voimakertoimina perinteisille rikosten teon muodoille kolmella tasolla. Ensinnäkin tekijä voi kohdentaa ja tehdä rikoksen etäältä vähentäen rikoksen teon riskiä verrattuna fyysisessä ympäristössä tapahtuvaan rikollisuuteen. Toiseksi tekijä voi anastaa pieniä määriä suurelta ihmisjoukolta, mikä vähentää yksilön ilmoitushalukkuutta ja korottaa viranomaisten tutkintakynnystä. Kolmanneksi rikoksen tekijä pystyy tavoittamaan lukemattoman määrän ihmisiä, informaatiota tai päätteitä samaan aikaan suhteellisen pienillä resursseilla. (Wall 2010.)

Wall (2010) viittaa tyypillisiin verkkopetoksiin termillä mikropetos (*micro-fraud*) korostaakseen niiden voimakeroivaikutuksia suhteessa petosten ilmenemiseen, mutta samat vaikutukset pätevät myös digitaalisiin identiteettivarkauksiin. Rikosten vaikutukset ovat laajoja ja mittavia yhteiskunnan tasolla, mutta näennäisen pieniä yksilön elämässä. Ansaintalogiikka perustuu toimintaan, jossa suureen ihmismassaan kohdistetaan suhteellisen pieniä varkauksia tai petoksia. Menetykset voidaan kokea niin vähäisiksi, etteivät monet uhrin halua hankkia varallisuutta takaisin. Lisäksi tapauksia ei tutkita aktiivisesti rikosoikeusjärjestelmän toimesta. (Wall 2010.) Kiinnijäämisriskiä pienentää myös petoksen uhrin kokema häpeä tai syyllistäminen, minkä vuoksi hän ei kerro tapahtuneesta muille (Cross 2015).

Tietojärjestelmät voivat olla rikoksen teon välineitä ja kohteita tai fasiliteetit tarjoavia alustoja. Esimerkiksi tietojenkalastelu-huijauksessa rikollinen yrittää saada uhrin jakamaan henkilökohtaisia tietojaan (Jewkes & Yar 2011). Väliintulohyökkäyksessä selaimen käyttäjän ja sivuston väliin tunkeutuu oikeudettomasti kolmas osapuoli, joka pyrkii väliintulollaan manipuloimaan osapuolten tietojenvaihtoa. (Mallik ym. 2019). Tietoverkossa toteutetun petoksen ja identiteettivarkauden kohdalla kyseeseen voi tulla myös hyvin yksilöity ja kohdennettu erehdyttäminen, jossa rikoksen tekijä käyttää enemmän aikaa rakentaakseen luottamuksellisen suhteen uhriin. Rikoksen tekijä pyrkii usein hyötymään toiminnallaan, mutta

niin kutsutuissa catfish-tapauksissa ihminen voi pyrkiä erehdyttämään toista ilman erityistä hyödyn tavoittelua.

ICF-konsulttiyhtiön Euroopan komissiolle teettämän tutkimuksen mukaan vuosina 2017–2019 31 % netin käyttäjistä EU:ssa ilmoitti joutuneensa erilaisten tietojenkalastelu-huijausten kohteeksi, ja suorat kokonaistappiot EU-kansalaisille on arvioitu 27 miljardin euron arvoiseksi. Vuosina 2017–2019 noin 32 miljoonaa EU-kansalaista oli joutunut identiteettivarkauden uhriksi tapauksissa, joissa tekijällä oli taloudellinen motiivi. Sen sijaan tapauksia, joissa tekijä oli esiintynyt oikeudettomasti uhrin henkilötietoja käyttämällä, oli noin 28 miljoonaa. (European Commission 2022, 15.) Näsin ja Tanskasen (2016, 154) mukaan digitalisaatio lisää rikoksen teon mahdollisuuksia, ja esimerkiksi petosrikosten suurta kasvua selittää osaltaan verkkopalvelujen käytön kasvu. Yhteiskunnan ja arkielämän palveluiden digitalisaatio altistaa nämä palvelut tietoverkkorikollisuudelle ja sen voimakeroainvaikutuksille. (Näsi & Tanskanen 2016.)



Kuva 1 Tietoon tulleet ja selvitetty identiteettivarkaudet Suomessa 2015–2023. Lähde: Tilastokeskus 2023

Digitaalisista identiteettirikoksista piirtyy kirjallisuudessa usein hyvin uhkaava kuva. Suomen kontekstissa ei kuitenkaan ole riittävää näyttöä tukemaan väitettä, että tietoverkkojen kehitys ja yhteiskunnan digitalisaatio johtaisi rikollisuuden suhteelliseen kasvuun verrattuna tietoyhteiskuntaa edeltäneeseen aikaan. Vaikka identiteettivarkaudet ovat lisääntyneet tilastoissa (kuva 2), määrän kasvusta ei voida johtaa selkeitä tai tyhjentäviä johtopäätöksiä ilmiön kehityksestä laajemmassa määrin (Näsi 2023). Identiteetti- ja tietoverkkorikollisuuteen

liitetty anonyymius ei kuvaa tietoverkkoympäristön todellisuutta kovin hyvin. Wall (2007; 2008) huomauttaa, että jokaisesta liikkeestä tai ”klikkauksesta” tietoverkossa jää jokin jälki, jota voi ainakin teoriassa seurata. ”Teoriassa” siinä mielessä, että paljon jää sen varaan, minkälaiset rahoitukselliset ja tietotekniset resurssit sekä valtuudet poliisitoiminnalle sallitaan jälkien seuraamiseksi. (Wall 2007, 2008.)

Wall (2013: 438) katsoo, että samalla kun yrityssektori vetäytyy vastuusta ennaltaehkäistä identiteettivarkauksia ja selvittää uhrin tilannetta, rikoksiin reagoiminen on jäänyt rikosoikeuden ja poliisin harteille. Reagointi on joskus ylimitoitettua kansalaisten toiveiden seurauksena, jolloin poliisitoiminnalla pyritään paikkaamaan kuilua sen välillä, mitä vaatimuksia yleisö poliisitoiminnalle asettaa identiteettirikosten kontrollissa ja mihin poliisi tosiasiallisesti kykenee. (Crawford 2006; Wall 2010.) Zedner (2003) katsoo, että rikosoikeusjärjestelmään ja etenkin ennaltaehkäisevään poliisitoimintaan liittyy paradoksi: jotta rikollisuuden riskien ennaltaehkäisy voitaisiin oikeuttaa, päättäjien ja viranomaisten on oletettava rikollisuuden olevan pysyvä osa yhteiskunnallista elämää.

Identiteettirikosten tutkinta on haaste perinteiselle poliisitoiminnalle ja sitä määrittävälle oikeuskäytännölle. Ensinnäkin identiteettirikosten alle menevistä moninaisista rikoksista puhutaan usein kuin ne olisivat keskenään yhdenmukaisia, eivätkä arkikieliset rikollisuuden käsitteet heijastu suoraan lakiin. (Wall 2013.) Identiteettivarkaus kattaa heterogeenisen joukon eri tavoin tehtyjä identiteettirikoksia ja niiden fasilitoimia muita rikoksia. Yhtäältä ihminen saattaa käyttää yksittäisen henkilön henkilötietoja valeprofiilin luomiseen sosiaalisessa mediassa kiusaamistarkoituksessa. Toisaalta rikollinen saattaa, useiden tietokoneohjelmien muodostaman ”bottiverkon” (tietojärjestelmistä koostuvan etähallinnoidun verkon) avulla huijata suurelta määrältä ihmisiä henkilötietoja saadakseen rikoshyötyä. (Komission ehdotus 2010; VN Kirjelmä 2010).

2.2 Identiteettitiedon omistus ja varastaminen

Suomen etymologisessa sanakirjassa identiteetti määritellään muun muassa sanoin ”(omin) olemus”, ”yksilöllisyys” ja ”henkilöys” (Kotimaisten kielten keskus 2024). Sisäministeriön identiteettiohjelman loppuraportissa (SM identiteettiohjelma 2010, 94) henkilöllisyyden synty ajoitetaan vaiheeseen, jossa henkilön tiedot viedään legitiimiin, ”julkista luotettavuutta” nauttivaan, väestötietojärjestelmään. Valtio takaa kansalaisten henkilöllisyyden, ja Pohjoismaiden väestötietojärjestelmien kattavuutta on pidetty maailmanlaajuisesti

poikkeuksellisena (Korhonen 2014). ”Varas”-sana puolestaan tarkoittaa henkilöä, joka ”ottaa luvottomasti ja salaa itselleen toisen omaisuutta” (Kotimaisten kielten keskus 2024). Rikoslain 28 luvun 1 §:n mukaan varkaudesta tuomitaan henkilö, joka on anastanut toiselta irtainta omaisuutta, rangaistuksena sakko tai enintään puolitoista vuotta vankeutta. Identiteettivarkautta ei ole sanakirjoissa, mutta rikoslaissa se määritellään seuraavasti:

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 (RL 38 luku 9 a §).

Henkilötieto ja tieto ylipäätään eroavat aineellisesta hyvästä muun muassa siten, että sen käyttäminen ei estä muita käyttämästä kyseistä tietoa eikä siihen liitetä aineelliseen hyvään kuuluvaa omistusoikeutta. Lainopillisesti *omistusoikeuden* kohteena voi olla vain aineellinen hyödyke, kun taas *omistus* tarkoittaa jonkin varallisuuskohteen kuulumista henkilölle. *Omaisuuuden* puolestaan nähdään koostuvan varallisuusosoikeuksista. Roomalaiseen oikeuteen perustuva aineettomien esineiden kategoria on Suomessa ”vanhastaan torjuttu”. (Kartio & Tammi-Salminen 2011.) Tietoa ei aineettomana hyödykkeenä sijoiteta omaisuuden tai omistusoikeuden käsitteiden piiriin, eikä henkilötietoja voi oikeudellisessa mielessä omistaa siten kuin esineitä ja varallisuutta (esimerkiksi osakkeet). Omaisuudensuoja ei kuitenkaan käsitä vain fyysisiä esineitä, mutta omaisuudelle pitää voida osoittaa ”jokin erityinen arvo” (Kangasniemi 2012, 230). Henkilötietojen käsittelyyn liittyy lisäksi oikeuksia, jotka perustuvat esimerkiksi EU:n yleiseen tietosuojasetukseen (GDPR) ja kansallisiin tietosuojaoikeuksiin. Henkilötiedot ovat kytköksissä erityisesti perusoikeuksiin, kuten yksityisyydensuojaan ja itsemääräämisoikeuteen, minkä turvin henkilöllä on tilannesidonnainen oikeus tietojensa poistoon tai tiedon käsittelyn rajoittamiseen (Asetus 2016/679/EU).

2.3 Identiteettivarkaudesta petokseen

Ennen identiteettivarkauden säätämistä rikoslakiin, sen alaan kuuluvia rikollisia tekoja käsiteltiin muun muassa petoksen, kunnianloukkauksen, kiristyksen ja tietomurron alla. Identiteettivarkaudella tarkoitetaan varsinaista ja välitöntä henkilötietojen, kuten luottokorttitietojen varastamista. Tämä voi edeltää ja fasilitoida petosta, jolla viitataan henkilön esiintymiseen tekaistulla tai muuten valheellisella identiteetillä. (Wall 2013, 439.) Varkauteen liittyy enemmän pakottavuus ja riistäminen (forceful crimes), kun taas petoksen keinot perustuvat erehdyttämiseen ja valheellisuuteen (Yar 2006, 80; David 2023). Taktiikoilla on eri

lähtökohdat: ensimmäisessä omaisuus anastetaan ilman suostumusta, toisessa erehdyttämisen ja valheellisen luottamuksen kautta saadulla suostumuksella.

Kun rangaistuksen laatua ja kesto/määrää mitataan, painoarvoa saa identiteettivarkaudella fasilitoitu muu rikollisuus, kuten petos. Petokseen syyllistyy se, joka on

toista erehdyttämällä hankkinut itselleen tai toiselle oikeudetonta taloudellista hyötyä taikka toista vahingoittaakseen, erehdyttämällä tai erehdystä hyväksi käyttämällä saa toisen tekemään tai jättämään tekemättä jotakin ja siten aiheuttaa taloudellista vahinkoa erehtyneelle tai sille, jonka eduista tällä on ollut mahdollisuus määrätä” (RL 36 luku 1 §).

Vuonna 2003 säädetyn tietoverkkorikollisuuden yleissopimuksen mukaan petokseksi katsotaan myös teko, jossa vääristetään tietojenkäsittelyn lopputulosta ja aiheutetaan taloudellista vahinkoa ”dataa syöttämällä, muuttamalla, tuhoamalla tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla” (RL 36 luku 1 §).

Petoksen motiivina on taloudellisen edun tai haitan (toiselle) tavoittelu. Säännös kohdistuu sen oikeuksien loukkaukselle, jota on erehdytetty väärillä henkilötiedoilla. Sen sijaan identiteettivarkauden säännöksessä identiteettivarkauden uhrin oikeudet saavat suuremman painoarvon. Petoksesta on säädetty lievä, perus ja törkeä muoto riippuen tavoitellun hyödyn taikka aiheutetun vahingon laadusta ja rikoksen tekijän taikka uhrin asemasta suhteessa toisiinsa. Petoksessa ainoastaan sen lievä muoto on asianomistajarikos. (RL 36 luku 1 §.) Identiteettivarkaus säädettiin asiaomistajarikokseksi ja ainoastaan lievässä muodossa (RL 38 luku 9 a §). Asianomistajarikoksissa syytteen nostamiseen tarvitaan asianomistajan pyyntö, kun taas perus tai törkeässä petoksessa syytteen nostamiseen ei tarvita asianomistajan pyyntöä. (Rikosuhripäivystys 2019).

3 Teoria: oikeudelliset haasteet identiteettivarkauden kriminalisoinnissa digitaalisessa yhteiskunnassa

Oikeussosiologisessa tutkielmassani tarkastelen kriittisesti identiteettivarkauden kriminalisointiprosessia. Tavoitteenani on selvittää, miten identiteettivarkauden kriminalisointiprosessi on edennyt vuosien 2001–2015 aikana. Oikeussosiologia paikantuu lähemmäksi sosiologiaa kuin oikeustieteitä painotuksessaan oikeuden sosiaalitieteelliseen ulottuvuuteen. Oikeussosiologian avulla voin tarkastella identiteettivarkauden kriminalisointia oikeustiedettä laajemmasta näkökulmasta, mikä sallii oikeuden tutkimisen lainopillisen tulkinnan ulkopuolelta sosiaalisena rakennelmana.

Aineiston teoreettisena viitekehyksenä hyödynnän Kangasniemen oikeustieteellistä artikkelia ”Identiteettivarkaudet – haasteita rikostutkinnalle ja -oikeudelle, paljon vaivaa ja harmia uhrille” (2012). Kirjoittaja käsittelee siinä identiteettivarkauden kriminalisoinnin oikeudellisia haasteita niin laintulkitsijan kuin rikoksen uhrin näkökulmasta. Haasteet voidaan jakaa neljään teemaan: 1) identiteettivarkauden monitulkintaisuus, 2) tutkinnalliset ja rikostekniset haasteet digitaalisten todisteiden jäljittämisessä, 3) näiden haasteiden suhde yhtäältä yksilön oikeuksiin, toisaalta uhrin oikeudelliseen asemaan identiteettivarkauden jälkeen, sekä 4) vastuun jakautuminen henkilötietojen hallinnassa. (Kangasniemi 2012.) Miten Kangasniemen esittelemiä haasteita on lainvalmisteluprosessin kuulemisissa ratkaistu niin, että identiteettivarkaus on nähty kriminalisoitavaksi sopivaksi kriminalisointiperiaatteiden mukaisesti? Seuraavaksi esittelen Kangasniemen käsittelemät haasteet.

3.1 Identiteettivarkauden tarkkarajaisuus ja moninaisuus

”Identiteettirikos” kattaa moninaisen kokoelman erilaisia ja eri vakavuustason rikoksia, joita yhdistää henkilötietojen luvaton käyttö sekä digitaalisen ympäristön mahdollistama massiivinen tietojenkeruu ja väärinkäyttö. Identiteettirikosta voi tarkastella kahdessa osassa: identiteettitietojen hankkimisena, esimerkiksi tietomurto, sekä niiden hyödyntämisenä. Identiteettivarkaudessa rikoksen tekijä *käyttää* oikeudettomasti toisen henkilötietoja eli identiteettiin liittyviä tunnisteita, kuten henkilötunnusta, käyttäjätunnusta tai maksukortin numeroa esimerkiksi tehdäkseen sopimuksia toisen nimissä. Rikokset tutkitaan usein erilaisten rikosnimikkeiden, kuten petoksen, maksuvälinepetoksen tai kunnianloukkauksen, kautta. Identiteettivarkaus on myös oikeudellisena käsitteenä harhaanjohtava, sillä henkilötietoja ei voi varastaa. Vaikka taloudellisen hyödyn tavoittelu motiivina on yleistä, sosiaalisen median

kontekstissa rikoksia tehdään myös loukkaamistarkoituksessa (Kangasniemi 2012), jolloin identiteettitieto ei ole pelkkä rikoksen teon väline, vaan sen kohde. Identiteettivarkaus ei ole vain käsitteenä oikeudellisesti epäselvä ja monitulkintainen, vaan se myös jättää ulkopuolelle monia vahingollisia petollisia ja identiteetin eheyttä loukkaavia tekoja (ks. ”catfish”, tämä tutkielma s. 8) riippuen siitä, mihin tekoihin se lainsäädännöllä on rajattu.

3.2 Rikostutkinnan ja rikostekniset haasteet

Se, että identiteettivarkauksia tutkittiin eri rikosnimikkeiden alla, teki esitutkinnasta haastavaa, sillä esitutkinta- ja pakkokeinovaltuudet vaihtelevat rikosnimikkeen mukaan. Tietoverkkorikosten tutkimisessa tarvitaan usein televalvontaa, jonka käyttöä kuitenkin rajoittavat perusoikeudet ja säännökset rikosten rangaistavuudesta. Perustuslakivaliokunta on painottanut, että televalvonnan käyttäminen ei saa rikkoa luottamuksellisen viestinnän suojaa ilman riittäviä perusteita (PeVL 66/2010; Kangasniemi 2012, s. 221). Tietoverkossa identiteettivarkauksien tutkintaa vaikeuttaa myös teknisten todisteiden lyhyt säilyvyys: rikoksen jäljet ovat usein hävinneet ennen tutkinnan aloittamista. Näyttöongelmat voivat johtaa tilanteisiin, joissa rikosilmoitukset eivät etene syytteiksi ja tuomioiksi.

Tietoverkkorikollisuuden, kuten identiteettivarkauksien kansainvälinen ulottuvuus haastaa rikoksen tutkintaa. Kansalliset lainsäädännöt vaihtelevat, minkä lisäksi kansainväliset oikeusapupyynnöistä seuraavat rikostutkinnan kustannukset voivat nousta liian suuriksi suhteessa koettuun hyötyyn rikoksen selvittämisestä. Yksityinen etu on heikossa asemassa, kun kansainvälisen virka-apupyynnön toteutuminen voi edellyttää huomattavaa rikosvahinkoa. (Kangasniemi 2012.) Sen lisäksi, että eri maiden kansalliset oikeuskäytännöt vaihtelevat, identiteettivarkaus itsessään on moninainen ilmiö, mikä tekee sen sääntelystä haastavaa rikoslain johdonmukaisuuden näkökulmasta. Identiteettivarkauksien tulkinnanvaraisuus sen aiheuttaman vahingon laadun perusteella (huom. ”vähäistä suurempaa haittaa” rikoslain 38 luvun 1 a §, tämä tutkielma s. 20) voi johtaa samankaltaisissa tapauksissa erilaisiin tuomioistuinten ratkaisuihin.

Kangasniemi (2012) käsittelee vuonna 2014 voimaan tullutta esitutkinta- ja pakkokeinolain muutosta. Lakimuutoksia koskevassa hallituksen esityksessä (HE 222/2010) todettiin, että aiempi sääntely liittyen televalvontaan tietoverkkorikollisuuden tutkinnassa ei vastannut rikostutkinnan tarpeita eikä se ollut johdonmukaista. Esityksessä ehdotettiin, että huomioiden digitalisaation kehitys ja sen vaikutus rikollisuuden muutokseen, televalvontalupa voitaisiin

laajentaa epäillyn telepäätelaitteen tai -osoitteen valvontaan rikoksissa, joissa tämän epäillään käyttäneen telepäätelaitetta rikokseen. Perustuslakivaliokunta kuitenkin katsoi, että perustuslain 10 §:n luottamuksellisen viestin salaisuuden kannalta televalvonta tulee rajata rikoksiin, jotka vaarantavat yksilön tai yhteiskunnan turvallisuutta. (Kangasniemi 2012.)

3.3 Yksilön oikeudet ja uhrin asema

Kangasniemen (2012) artikkelissa esitellään mahdollisuus identiteettivarkauden kriminalistointiin itsenäisenä rangaistussäännöksenä. Kriminalisointi parantaisi identiteettivarkauden uhrin asianomistaja-asemaa: jotta uhrilla olisi varsinainen asianomistaja-asema, tulee rikos voida todeta tapahtuneeksi. Identiteettivarkauden uhriksi joutuminen voi aiheuttaa merkittäviä taloudellisia ja sosiaalisia seurauksia. Uhri voi joutua vastaamaan luvattomasti tehdyistä sopimuksista, mikä voi johtaa taloudellisiin vaikeuksiin tai luottotietojen menetykseen. Identiteettivarkaus voisi johtaa jopa rikosepäilyyn identiteettivarkauden uhria vastaan, jonka nimissä toinen rikos on tehty. Sosiaaliseen mediaan toisen henkilötiedoilla luodut valeprofiilit (em., 228) voivat aiheuttaa merkittävää haittaa, mutta eivät välttämättä täytä rikoksen tunnusmerkistöä, ellei toimintaan liity kunnianloukkausta tai muita rangaistavia tekoja. Omaisuuden suoja ei kuitenkaan rajoitu fyysisiin esineisiin, vaan koskee myös aineetonta hyvää, jos niille voidaan osoittaa taloudellista arvoa. (Kangasniemi 2012.)

Lain säätäminen vaatii huolellista punnintaa perusoikeuksien, kuten yksityisyyden suojan ja sananvapauden, näkökulmasta. Toisinaan perusoikeudet ovat ristiriidassa, ja lainsäätäjän vastuulle jää tulkita perusoikeuksien hierarkia tapauskohtaisesti. Kangasniemi (2012) esittelee tähän liittyen Euroopan ihmisoikeustuomioistuimen tapausesimerkin *K.U. v. Suomi* 2.12.2008, jossa henkilö laittoi alaikäisen henkilön nimellä ”seksuaaliluonteisen seuranhakuilmoituksen” internetiin tämän tietämättä. Tapauksessa annettiin enemmän painoarvoa tietoliikennesalaisuudelle esimerkiksi maineen suojelun yli. Lainsäädännön aukko korjattiin myöhemmin lailla sananvapauden käyttämisestä joukkoviestinnässä. (Kangasniemi 2012, 230.)

3.4 Rikosoikeuden rooli henkilötietojen hallinnassa

Kangasniemi (2012) katsoo, että yksityisyyden suojan ala on laajentunut tietoverkkoympäristössä merkittävästi, sillä ihmiset jakavat sosiaalisessa mediassa ja eri internetin alustoilla yleensä paljon tietoa itsestään. Tietoa on saatavilla rajaton määrä, mutta

vastuu tiedon hallinnasta on epäselvä. Rekisterinpitäjällä on huolehtimisvelvollisuus henkilötiedoista, mutta sivuston käyttäjällä on myös vastuu tietojensa jakamisesta. Käyttäjä voi myötävaikutuksen vuoksi olla osaltaan vastuussa henkilötietojensa päätyemisestä rikolliseen toimintaan. Usein käyttäjän mahdollisuudet tai kyvyt estää henkilötietojensa kaappaaminen ja etenkin hyödyntäminen ovat todella pienet, ellei olemattomat. Tämän lisäksi säännöksistä huolimatta ihmisten on helppo kuluttaa ja jakaa oikeudettomasti levitettyä tietoa internetissä. (Kangasniemi 2012.) Uhrin asema voidaan jälleen todeta heikoksi samalla, kun rikoksella voi olla laajat ja pitkät seuraukset.

Lopuksi Kangasniemi (2012) esittää rikosoikeuden ulkopuolisia keinoja identiteettivarkauksien kontrollointiin. Kirjoittaja korostaa ihmisten valistamisen tärkeyttä etenkin liittyen tietojen hallintaan ja identiteettivarkaudesta ilmoittamiseen. Myös palveluntarjoajille voidaan säätää informointivelvollisuus henkilötietojen kaappauksesta. Ratkaisuksi identiteettivarkauksien selvittämisen ongelmaan on esitetty keskitettyä ilmoitusjärjestelmää, minkä kautta uhri voi ilmoittaa tapahtuneesta yksinkertaisemmin uhrin selvittelytaakkaa keventäen. Kangasniemi (2012) tuo myös esiin väestötietojärjestelmään säädetyin lain, joka mahdollistaa henkilötunnuksen vaihtamisen identiteettivarkauden uhrille. Kirjoittaja näkee, että ”näinkin radikaali mahdollisuus” on kannatettava identiteettivarkauden uhrin näkökulmasta, mutta samalla toteaa, että ”omasta henkilöllisyydestä luopuminen ... on raskas ratkaisu tehtäväksi”. (Kangasniemi 2012.)

4 Tutkimusasetelma

Tutkielmani tehtävänä on analysoida identiteettivarkauden kriminalisointia perehtymällä kriminalisointiprosessiin sisältyviin lainvalmisteluasiakirjoihin vuosilta 2001–2015. Tutkimuskysymykseni on:

- Miten digitaalisessa ympäristössä tehtyjen identiteettivarkauksien rikosoikeudellisesta kontrollista neuvotellaan Suomessa identiteettivarkauksia koskevassa kriminalisointiprosessissa vuosina 2001–2015?
 - o Miten kriminalisointia perustellaan ja haastetaan etenkin sidosryhmien ja valiokuntien lausunnoissa ja lakivaliokunnan mietinnössä?

Vastaan apukysymykseen hyödyntämällä identiteettivarkautta koskevan rikoslain uudistuksesta (HE 2014) annettuja lausuntoja ja lakivaliokunnan mietintöä (LaVM mietintö 2014). Pääasiallinen aineistoni kattaa seuraavat asiakirjat: lakivaliokunnan (LaVL lausunto 2010; LaVL lausunto 2011) ja hallintovaliokunnan (HaVL lausunto 2010; HaVL lausunto 2011) lausunnot; lausuntotiivistelmä identiteettivarkauden kriminalisoinnista (OM lausuntotiivistelmä 2013); tietoverkkorikosdirektiivin täytäntöönpanoa koskeva hallituksen esitys (HE 2014); edellisestä annetut lausunnot (OM lausuntokierros 2014); sekä lausuntojen pohjalta annettu lakivaliokunnan mietintö (LaVM mietintö 2014). Käsittelen muita lakihankkeeseen liittyviä lainvalmisteluasiakirjoja kontekstina lausunnoille, sillä lausunnoissa kommentoidaan niitä kyseisiä valmisteluasiakirjoja. Kaikki käsittelemäni asiakirjat ovat tutkielman liitteenä.

Rajaan analyysini lausuntokierroksiin ja lakivaliokunnan mietintöön, sillä niissä nimenomaan haastetaan ja puolletaan tietoverkkorikosdirektiivin sisältöä ja identiteettivarkauden kriminalisointia. Hallituksen esitys ja mietinnöt sen sijaan ovat tyyliltään muodollisia ja selostavia, sillä niissä lähinnä pyritään oikeuttamaan niiden sisältämät ehdotukset muun muassa lausuntopyynnön saaneille asiantuntijoille. Sidosryhmien keskenään erilaiset lausunnot eroavat tyyliltään valiokuntien lausunnoista, joiden rakenne on niin ikään muodollisempi ja yhtenäisempi (ks. Rantala & Alasuutari 2021: 75). Lausunnot ovat keskimäärin sivun tai muutaman sivun mittaisia, mutta identiteettivarkautta käsitellään usein korkeintaan muutaman kappaleen verran.

Kirjallisten lausuntojen antamiseen tulisi Oikeusministeriön kuulemisoppaan (OM Säädosvalmistelun kuulemisohje) mukaan varata aikaa vähintään kuudesta kahdeksaan viikkoa. Vuoden 2013 lausuntokierroksen kestosta ei ole ilmoitettu, mutta 2014 lausuntokierros kesti vajaa kaksi kuukautta, mikä vastaa lausuntokierroksen ideaalia vähimmäisaikaa (OM Säädosvalmistelun kuulemisohje). Valiokuntia kuultiin esivalmisteluvaiheessa, ja sidosryhmiä perusvalmistelun jälkeen. Kuulemisia järjestettiin useammassa vaiheessa, mutta kaikki lausuntopyynnön saaneet, kuten jotkin järjestökenttään kuuluvat tahot, eivät antaneet lausuntoa. Lisäksi kansalaisille ei avattu mahdollisuutta lausua asiasta. Saadut lausunnot eivät edusta laajuudeltaan kattavasti asiaan perehtyneiden monipuolista kenttää. Toisena aineistoon liittyvänä puutteena mainittakoon useassa kohtaa esiin tuotu oikeusministeriössä laadittu identiteettivarkautta koskeva arviomuistio (OM 4/41/2013), jota ei ole julkisesti saatavilla. Sen pohjalta annettu oikeusministeriön lausuntotiivistelmä (2013) on julkinen.

Tunnistin lausunnoista ja Kangasniemen (2012) artikkelista toistuvia haasteita ja hyötyjä, joilla kriminalisointia perusteltiin. Lausunnoissa haasteet ja hyödyt nimettiin kriminalisointiperiaatteiden mukaan. Sen sijaan Kangasniemi (2012) ei puhu sanalla sanoen kriminalisointiperiaatteista, vaan kirjoittaja käsittelee periaatteita kuvaamalla rikosoikeudelliset haasteet ja hyödyt auki. Kangasniemen (2012) artikkeli tulkintasuosituksineen vaikuttaa enemmän käytännölliseltä kuin teoreettiselta lainopilta, mikä voi selittää tyyllillisen eron. Selkeyttääkseni teoriaohjaavaa analyysiani, halusin luoda synteesin lausunnoista ja Kangasniemen (2012) artikkelista. Teemoittelin Kangasniemen esittämät haasteet lausunnoissakin toistuvien kriminalisointiperiaatteiden mukaan seuraavanlaisesti: 1) laillisuusperiaate – suojaako kriminalisointi yksityisiä henkilöitä julkista valtaa vastaan ja onko rangaistusuhka oikeasuhtainen tekoon nähden; kuinka yleisluontoinen tai tarkkarajainen rikoslain säännös on; 2) Oikeushyvien suojelun periaate – miten osittain vastakkain asettuvia oikeushyviä arvioidaan suhteessa viranomaisvaltaan ja kriminalisointiin; 3) hyöty-haitta-periaate eli mitkä ovat kriminalisoinnin hyödyt ja haitat sekä 4) ultima ratio -periaate – käytetäänkö rikosoikeutta viimesijaisena keinona eli onko muut keinot rikokseen reagointiin jo käytetty tai vähintäänkin arvioitu? Pyrin selvittämään, miten Kangasniemen (2012) esittelemiä haasteita on lausunnoissa perusteltu niin, että identiteettivarkaus on (tai ei ole) nähty tarpeelliseksi kriminalisoida kriminalisointiperiaatteiden mukaisesti ja osin ristiriidassa niihin.

5 EMPIRIA

Seuraavissa luvuissa esittelen identiteettivarkauden kriminalisointia koskevan lainvalmisteluprosessin Finlexin lainvalmistelun prosessioppaan (OM Lainvalmistelun prosessiopas) avulla, ja analysoin sidosryhmien ja valiokuntien kriminalisoinnista antamia lausuntoja. Aloitan kuvaamalla lainvalmisteluprosessin vaiheet tietoverkkorikosdirektiivin valmisteluprosessin näkökulmasta. Tämän jälkeen siirryn varsinaiseen analyysiin, jossa keskityn erityisesti vuosien 2010 ja 2011 hallinto- ja lakivaliokuntien lausuntoihin, 2013 ja 2014 lausuntokierroksiin sekä vuoden 2014 lakivaliokunnan mietintöön. Nämä kuulemiset on järjestetty tietoverkkorikosdirektiiviin liittyvien mietintöjen, raporttien, muistioiden ja hallituksen esityksen (HE 2014) pohjalta.

5.1 Lainvalmisteluprosessi identiteettivarkauden kriminalisoinnissa

Lainsäädäntöprosessi lähtee virallisesti käyntiin lakialoitteesta, joka voi syntyä esimerkiksi hallitusohjelman kirjauksena, kansalaisaloitteena tai EU-säädöksen velvoitteiden valmisteluna. Tietoverkkorikosdirektiivissä (Direktiivi 2013/40/EU) ja identiteettivarkauden kriminalisoinnissa on kyse juuri viimeisestä. Direktiivin taustalla on vuoden 2010 Euroopan komission esitys tietojärjestelmiin kohdistuvista hyökkäyksistä (Komission ehdotus 2010). Esityksen mukaan jäsenvaltion tulisi säätää rikosoikeudelliseksi seuraamukseksi vähintään viisi vuotta vankeutta, jos esimerkiksi laitton tietojärjestelmään tunkeutuminen ja/tai sen häirintä on tehty ”salaamalla rikosentekijän todellinen henkilöllisyys ja henkilöllisyyden oikealle omistajalle on aiheutettu vahinkoa”. (Komission ehdotus 2010, 4.) Vuoteen 2013 mennessä esityksen sisältöä muutettiin yleisluontoisemmaksi: tietoverkkorikosdirektiivissä (Direktiivi 2013/40/EU) esitetään, että EU:n jäsenvaltioissa henkilötietojen oikeudetonta käyttöä tulisi pitää raskauttavana tekijänä, kun rikos on laitton järjestelmän häirintä tai datan vahingoittaminen, ja rikos on tehty erehdyttämistarkoituksessa.

Valmistelun ensimmäisessä vaiheessa eli esivalmistelussa kerätään tietoa liittyen säädettävään lakiin ja päätetään lain säätämisen tarve. Tietoverkkorikosdirektiivi oli käsiteltävänä eduskunnassa vuosina 2010–2011, ja tällä kierroksella valmistuneita asiakirjoja hyödynnettiin tietoverkkorikosdirektiivin täytäntöönpanon toisella lainvalmistelukierroksella vuonna 2013. Yksi tällainen asiakirja on valtioneuvoston laatima muistio Euroopan komission valmistelemasta ehdotuksesta tietoverkkorikosdirektiiviksi (VN kirjelmä 2010). Siinä kuvataan lakihankkeen tausta, sisältö ja tässä tapauksessa EU-direktiivin vaikutukset Suomen

lainsäädäntöön. Identiteettivarkautta ehdotetaan rangaistavaksi muun rikoksen koventamisperusteena. Lakivaliokunnat antoivat vuosina 2010 ja 2011 ehdotuksesta lausuntonsa, joita analysoin tarkemmin alaluvussa 5.2. Myös sisäministeriön (SM) asettaman työryhmän valmistelemaa identiteettiohjelman loppuraporttia (SM identiteettiohjelma 2010) hyödynnetään vuoden 2013 lainvalmistelussa. Raportissa esitetään identiteettivarkauden kriminalisointia ratkaisuvaihtoehtona identiteettivarkauksiin. Kriminalisointia perustellaan digitalisaation mahdollistamalla toimintaympäristön muutoksella, jossa rikoksella on pienet kustannukset ja kiinnijäämisriski, suuri hyötypotentiaali sekä mahdollisuus rikollisen toiminnan automatisointiin. (SM identiteettiohjelma 2010.)

Esivalmistelun lopputuloksena tehdyssä hankesuunnitelmassa (OM hankesuunnitelma 2013) määrätään työryhmä valmistelemaan ehdotus hallituksen esitykseksi, ja valmisteluprosessin perusvalmistelu-vaihe alkaa. Ministeriön nimeämässä työryhmässä syvennetään tiedonkeruuta esimerkiksi tilaamalla selvityksiä ja tutkimusta sekä kuulemalla sidosryhmiä. Kuulemisessa tavoitteena on tuoda sidosryhmät ja kansalaiset osalliseksi lainvalmistelua tai saada heidän näkemyksensä kuulluksi lainvalmistelun aikana (OM Säädosvalmistelun kuulemisohje). Lainvalmisteluprosessissa järjestettiin erillinen identiteettivarkautta koskeva lausuntokierros, josta tehtiin tiivistelmä (OM lausuntotiivistelmä 2013). Lausuntoja pyydettiin oikeusministeriön arviomuistiota (ei saatavilla) koskevasta sisäministeriön laatimasta identiteettiohjelman loppuraportista (SM identiteettiohjelma 2010). Lausuntopyyntöjä lähetettiin 33 ja lausuntoja tuli 21. Niissä korostui kiusaamistarkoituksessa tehtyjen identiteettivarkauksien rikosoikeudellinen säätely uhrin aseman ja aineettomien oikeushyvien suojan näkökulmasta.

Hallituksen esityksen luonnos on tässä lakihankkeessa mietinnön muodossa. Oikeusministeriön laatimassa mietinnössä (OM mietintö 2014)) kriminalisoinnin toteuttamiseksi esitetään viittä vaihtoehtoa. Viimeiseksi esitetyssä vaihtoehdossa, jota esityksessä lopulta ehdotetaan toteutettavaksi, identiteettivarkaudesta laaditaan itsenäinen kriminalisointi rikoslain 38 lukuun 9 a §:ään. Rangaistavuuden ala laajenee, eikä sitä rajoiteta direktiivin vähimmäisvaatimukseen eli laittomaan järjestelmän häirintään ja laittomaan datan vahingoittamiseen. Identiteettivarkaudessa suojeluobjektina eli suojattavana oikeutena on identiteetin loukkaamattomuus, kun kahden muun suojeluobjektina on tietojärjestelmä tai data. Tekijä voidaan siis tuomita molemmista rikoksista rikosten tunnusmerkistöjen täytyessä, ja rangaistusseuraamus voi koventua yhteisen rangaistuksen mukaisesti. (OM mietintö 2014.)

Muita mietinnössä arvioituja kriminalisoinnin vaihtoehtoja ovat: 1) identiteettivarkauden liittäminen törkeisiin rikoksiin kvalifiointiperusteena, 2) rikoksen käsittely yleisenä taikka suunnitelmallisuuteen liittyvänä koventamisperusteena, tai 3) rangaistuksen mittaaminen rikoksen vahingollisuuden ja tekijän syyllisyyden perusteella. Kvalifiointiperuste tarkoittaa tunnusmerkistössä määriteltyä rikoksen vakavuuden luonnetta, minkä perusteella esimerkiksi datavahingontekoa (RL 35:3 a) tai tietojärjestelmän häirintää (RL 38:7 a) voitaisiin käsitellä törkeänä, jos rikoksen tekoon on käytetty identiteettivarkautta. Koventamisperuste sallii tuomioistuimelle liikkumavaraa määrätä ankarampi rangaistus rikoksen vakavuuden ja olosuhteiden perusteella, mutta se ei muuta rikoksen luonnetta perusmuodosta törkeäksi. Vaihtoehtoja pidettiin ongelmallisina muun muassa siksi, että ne voisivat sallia pakkokeinojen käytön identiteettivarkauden uhuriin tai rikosoikeuden oikeasuhtaisuuteen vedoten asettaa identiteettivarkauden liian korkealle rangaistusasteikolla. (OM mietintö 2014.)

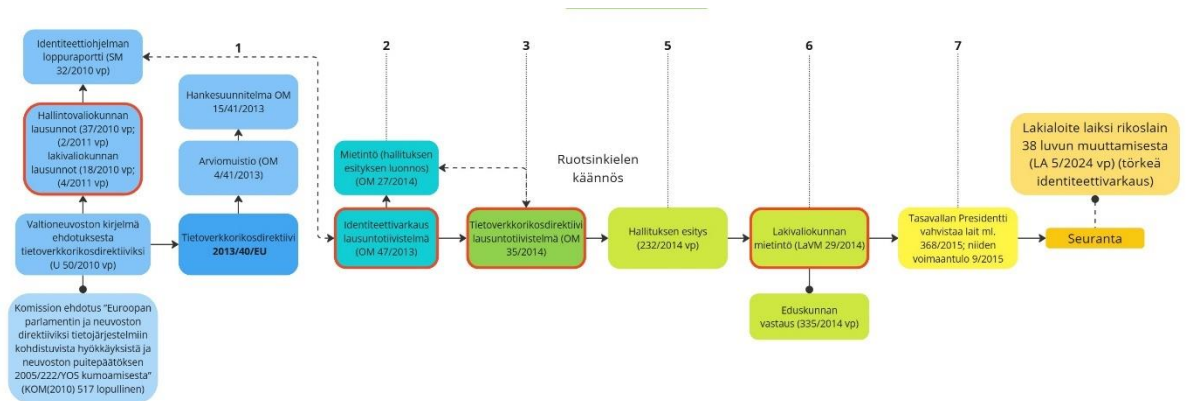
Kolmannessa vaiheessa eli lausuntomenettelyssä sidosryhmiltä pyydetään kirjalliset lausunnot HE-luonnoksesta, minkä jälkeen lausuntopalaute julkaistaan ja siitä tehdään lausuntotiivistelmä (esim. OM lausuntotiivistelmä 2014). OM:n tietoverkkorikosdirektiivin täytäntöönpanoa koskevasta mietinnöstä (OM mietintö 2014) lähetettiin 39 lausuntopyyntöä, ja lausuntoja saatiin 18. Lausuntokierroksella 2014 suuri osa lausunnonantajista katsoo, että identiteettivarkauteen sovellettavia pakkokeinovaltuuksia tulisi harkita mietinnön (em.) pohjalta uudelleen niin, että viranomaiset saisivat riittävät keinot tutkia identiteettivarkauksia.

Jatkovalmistelussa voidaan hallituksen esitysluonnoksen sisältöä lausuntopalauteen pohjalta ja esitysluonnos käännetään ruotsiksi. Prosessin viidennessä vaiheessa hallitus antoi esivalmistelun ja siihen liittyvien lausuntojen pohjalta esityksen (HE 2014) EU:n tietoverkkorikosdirektiivin kansalliseksi täytäntöönpanoksi. Esityksessä säädettäisiin identiteettivarkaus itsenäisenä rikoksena, mikä täyttäisi tietoverkkorikosdirektiivin velvoitteet. (HE 2014.) Identiteettivarkaussäännöksen mukaan

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 (RL 38 luku 9 a §).

Kuudennessa vaiheessa eduskuntakäsittelyssä valiokunnat kuulevat lakia valmistelleen ministeriön virkamiehiä ja asiantuntijoita. Esityksestä annetaan muutosehdotukset (esim.

LaVM mietintö 2014), ja eduskunta päättää hyväksytäänkö esitys. Eduskunta hyväksyi tietoverkkorikosdirektiivin täytäntöönpanon (2013/40/EU) esityksen ensimmäisellä kierroksella. Lopuksi tasavallan presidentti vahvistuksesta laki pannaan täytäntöön. Identiteettivarkaus lisättiin rikoslakiin syyskuussa 2015, ja vuoden loppuun mennessä siitä oli tehty 530 rikosilmoitusta (Suomen virallinen tilasto 2022). Kriminalisoinnin nähdään selkeyttävän identiteettivarkauden uhrin asianomistaja-asemaa oikeusprosessissa (HE 2014, 26). Kun laki astuu voimaan, alkaa vaikutusten seuranta. Lakivaliokunnan mietinnössä (LaVM mietintö 2014) kehoitettiin hallitusta seuraamaan identiteettivarkauden tutkintavaltuuksien riittävyttä ja tarvittaessa tehostamaan tutkintakeinoja.



Kuva 2 Tietoverkkorikosdirektiivin täytäntöönpanon lainvalmisteluprosessin vaiheet. Punaisella reunustetut tekstit ovat empiirisen aineistoni painopiste. Asiakirjat haettavissa esimerkiksi Turun yliopiston Lakitutka-palvelusta.

5.2 Laillisuusperiaate - yksilön suoja, oikeasuhtaisuus ja tarkkarajaisuus

Valmisteluasiakirjojen ja lausuntojen perusteella kriminalisoinnille nähdään laajasti olevan tarve, mutta kriminalisoinnista ja säännöksen sisällöstä on eriäviä mielipiteitä. Valtaosan lausunnonantajien näkemyksistä poiketen Suomen Lakimiesliitto ja Suomen Asianajajaliitto (OM lausuntotiivistelmä 2013) katsovat vuoden 2013 lausuntokierroksella, ettei identiteettivarkauksien yleistasoille kriminalisoinnille ole riittäviä perusteita, eikä se sovi yhteen kriminalisointiperiaatteiden kanssa. Oikeusministeriö (OM mietintö 2014) ja sisäministeriö (OM lausuntokierros 2014) lakia valmistelevalle tahoina ovat puolestaan olleet keskenään erimielisiä identiteettivarkauden esitutkintaan soveltuvista pakkokeinoista. Ensimmäinen ei näe telepakkokeinoille olevan riittäviä perusteita suhteessa niistä aiheutuviin haittoihin yksilön oikeuksien suojaan viranomaisvallalta. Lisäksi telepakkokeinojen käyttöön vaaditaan vähintään kahden vuoden vankeusuhka, minkä ei koeta olevan oikeasuhtainen teon vakavuuteen nähden. SM (OM lausuntokierros 2014) puolestaan katsoo, että telepakkokeinojen salliminen on edellytys toimivalle rikostorjunnalle ja siten identiteettivarkauden uhrin oikeusturvan toteutumiseksi.

SM:n (OM lausuntokierros 2014) mukaan tietoverkkorikosten, kuten identiteettivarkauksien, tutkinta ei ole mahdollista ilman televalvontaa. Kangasniemi (2012) havainnollistaa tietoverkkoon kohdistuvan tutkinnan haasteita vertaamalla sitä fyysisen ympäristön tutkintaan. Jälkimmäisen kohdalla perinteiset tutkintakeinot henkilöllisyyden selvittämiseksi koskevat esimerkiksi silminnäkijähavaintoja ja valvontakamerakuvia, jotka sijoittuvat usein julkisiin tiloihin. Tietoverkossa toteutetusta rikoksesta jää vain tietoteknisiä jälkiä (usein rikoksen tekijän omalle laitteelle) joiden tutkintaan telepakkokeinoja tarvitaan (Kangasniemi 2012.) Helsingin syyttäjänvirasto (OM lausuntokierros 2014) näkee ongelmana, etteivät säädetyt pakkokeinovaltuudet koske valeprofiileja sosiaaliselle medialle tyypillisinä identiteettivarkauksina (ks. myös Kangasniemi 2012, tämä tutkielma s. 14–15). Tehottomien tutkintakeinojen vuoksi tutkinnasta muodostuu raskas (OM lausuntokierros 2014 Helsingin syyttäjänvirasto), ja televalvonnan käyttö pakkokeinona helpottaisi esitutkintaviranomaisten työtä ja keventäisi tutkintaprosessia.

Kangasniemi (2012, 220) huomauttaa, että esitutkinnan keinot riippuvat siitä, ”minkä laatuista tai laajuista rikosta tutkitaan”: televalvonnan käyttö tutkinnassa edellyttää epäilyä rikoksesta, josta ankarin rangaistus on vähintään neljä vuotta vankeutta (pakkokeinolaki 10 luku 6 §) tai joka on kohdistunut automaattiseen tietojenkäsittelyjärjestelmään telepäätelaitetta käyttäen (Pakkokeinolaki 5 a luku 3 §). Koska pelkästä identiteettivarkauksesta tuomittaisiin lievänä rikoksena maksimissaan sakkorangaistus, tutkinnan voisi suorittaa suostumusperusteista televalvontaa käyttämällä. Kuitenkin hallituksen esityksessä (HE 2014) ja SM:n lausunnossa (OM lausuntokierros 2014) tunnustetaan tutkinnan kannalta haasteeksi rikokset, jotka on tehty useamman päätelaitteen kautta. Tällöin tietojen saantiin tarvittaisiin suostumus useammalta tiedonvälitysketjussa olevalta taholta, mikä hankaloittaa tutkinnan suorittamista. SM (OM lausuntokierros 2014) kokee epäoikeudenmukaiseksi sen, ettei esitutkintaviranomaisella ole ”mitään mahdollisuuksia” selvittää identiteettivarkaan todellista henkilöllisyyttä. Tästä syystä SM (em.) esittää OM:n mietinnöstä (2014) poiketen identiteettivarkauden lisättäväksi pakkokeinolain 10 luvun 6 §:n 2 momenttiin uudeksi televalvonnan perusterikokseksi.

Vuoden 2014 lausuntokierroksella muun muassa valtakunnansyyttäjänvirasto (VKSV), Helsingin syyttäjänvirasto ja Elinkeinoelämän Keskusliitto (EK) esittävät SM:n (OM mietintö 2014) tapaan identiteettivarkauden lisäämistä pakkokeinolakiin televalvonnan perusterikokseksi. Suomen Ammattiliittojen Keskusjärjestön (SAK) mukaan identiteettivarkauden kriminalisointi voi jäädä merkityksettömäksi, jos sen avulla ei taata

riittäviä tutkintakeinoja poliisille. Niin ikään Finanssialan Keskusliitto (FK) ja rikosoikeuden emeritusprofessori Asko Lehtonen katsovat, että sakko on riittämätön seuraamus rangaistuksen ennaltaehkäisevän vaikutuksen ja esitutinnan kannalta. FK ehdottaakin identiteettivarkaudesta säädettyä lisäksi sen törkeä muoto ja mahdolliseksi seuraamukseksi vankeusrangaistusta. (OM lausuntokierros 2014.)

Oikeussuojat, kuten yksityisyyden suoja ei kuitenkaan koske vain identiteettivarkauden uhrin oikeuksia, vaan myös rikoksesta epäillyn ja kansalaisen oikeuksien suoja viranomaisten heihin kohdistamilta tutkintatoimilta. Hallituksen esityksessä (HE 2014) huomautetaan perustuslaillisten suojien rajoituksista telepakkokeinojen käyttöön: viranomaisten pakkokeinoja rajoittavat muun muassa perustuslain 10 §:ssä säädetyt yksityiselämän ja luottamuksellisen viestinnän suoja. Perustuslakivaliokunta (PeVL 18/2014) katsoo, että televalvonnan käytön lisäksi, sähköisen viestinnän käyttöön liittyvät tunnistamistiedot ja niiden kokoaminen voivat olla ongelmallisia kyseisten suojien kannalta. (HE 2014, 7.) Kangasniemi (2012) huomauttaa, että valtuudet telepakkokeinoihin ovat olleet perustuslakivaliokunnan käsittelyssä jo vuonna 2010, jolloin valtioneuvosto esitti televalvonnan laajentamista telepäätelaitetta käyttäen tehtyihin rikoksiin. Perustuslakivaliokunta kuitenkin katsoi, että luottamuksellisen viestin suojan vuoksi, laajentaminen ei ole oikeasuhtaista rikoksen yhteiskunnalliseen vakavuuteen nähden. (Kangasniemi 2012, 221.)

Hallituksen esityksessä (HE 2014) itsenäinen identiteettivarkaus nähdään olevan lievä teko (vrt. Wall 2010, tämä tutkielma s. 14), ja tyypillisenä oheisrikollisuutena siitä tuomittava seuraamus olisi osa yhteistä rangaistusta. Lakivaliokunnan (LaVM mietintö 2014) mukaan vähäisenä rikoksena, ”joka toteutuu suhteellisen vähäisissä tilanteissa”, identiteettivarkauden rangaistusasteikon korottaminen ei olisi oikeasuhtaista. Kuitenkin rikoslainsäädännön puutteiden vuoksi erilliselle kriminalisoinnille on ”kansallistakin tarvetta” rikoslainsäädännön puutteiden vuoksi: on tilanteita, joissa vakavamman rikoksen tunnusmerkistö täyty, mutta tekoon voitaisiin soveltaa identiteettivarkauden tunnusmerkistöä. (LaVM mietintö 2014, 3–4.) Kangasniemi (2012) havainnollistaa ongelmaa jälleen fyysisen ja digitaalisen ympäristön sääntelyn eroavaisuuksilla oikeuskäytännössä. Ensinnäkin henkilön voi tuomita perus - tai törkeästä maksuvälinepetoksesta, jos hän anastaa ja syöttää fyysisen maksuvälinekortin automaattiin ilman tosiasiallista mahdollisuutta saada tililtä rahaa. Sen sijaan kopiaoidun korttitiedon luvattomassa hallussapidossa olisi kyse maksuvälinepetoksen valmistelusta, josta

tuomitaan enimmillään vuosi vankeutta. Tämänkaltainen ero tekemuotojen rangaistavuudessa on lainsäädännöllinen ja lainsoveltamisen ongelma. (Kangasniemi 2012.)

5.2.1 Rikossäännöksen tarkkarajaisuus ja identiteetin moninaisuus

Sosiaali- ja terveysministeriö (STM) ja tietosuojavaltuutettu (OM lausuntotiivistelmä 2013) sekä eduskunnan apulaisoikeusasiamies (OM lausuntokierros 2014) katsovat, että identiteettivarkaus-säännös on liian laaja ja tulkinnanvarainen täyttääkseen kriminalisointiperiaatteet. Helsingin syyttäjänvirasto (OM lausuntotiivistelmä 2013) puoltaa toisena esiintymisen kriminalisointia ilman vahingoittamis- tai hyötymistarkoitusta, jos tekijä mieltää väärän identiteetin käyttämisestä johtuvan vahingon olevan teon todennäköinen seuraus.

Rikossäännöksen tarkkarajaisuuden vaatimusta haastavat identiteetin käsitteen ja identiteettirikosten moninaisuus, minkä lisäksi digitalisaatio muovaa käsitystä identiteetistä. Vuoden 2013 lausuntokierroksella Nuotio (OM lausuntotiivistelmä 2013) yhdistää kiusaamisen identiteettivarkauden kontekstissa erityisesti internet-sukupolven nuorten kokemuksiin. Hän käsittää nuorten merkityksellistävän netin ja ”netti-identiteetin” eri tavalla kuin vanhempi sukupolvi, jolle internet on vain ”väline”; nuoret ”rakentavat omakuvaansa eläen tällä tavoin”. Nuotion mukaan kiusaaminen netissä voi olla nuorelle ahdistavampaa, koska se tulee ”lähelle”. (OM lausuntotiivistelmä 2013 Nuotio.)

Niin sanottujen valeprofiilien kaltaisten identiteettivarkauksien kohdalla voi usein täytyä myös kunnianloukkauksen tai yksityiselämää loukkaavan tiedon levittämisen tunnusmerkistöt, jolloin pakkokeinot määritellään niihin rikoksiin soveltuen (HE 2014). Varsinais-Suomen käräjäoikeus ja sisäministeriö (SM) katsovat, että vaikka valeprofiilin luominen voi täyttää kunnianloukkauksen tunnusmerkistön, on tavallista, että toisena esiintyminen tehdään tavalla, johon ei voida soveltaa kunnianloukkauksen tunnusmerkistöä. Identiteettivarkaus on käsitteenä oikeudellisesti monitulkintainen, mutta se myös jättää ulkopuolelle monia identiteetin eheyttä loukkaavia tekoja (ks. tämä tutkielma s. 13).

5.3 Oikeushyvien suojele

Identiteettivarkaudessa samalla teolla voidaan loukata useampaa oikeushyvää, jolloin rangaistavuutta arvioitaessa punnitaan oikeushyvien keskinäistä hierarkkisuutta. Vuoden 2013

lausuntokierroksella rikosoikeuden dosentti (nykyinen professori) Sakari Melanderin katsoo, että identiteettivarkaus voi loukata yksityisyyttä oikeushyväksi niin, ettei loukkaamiseen liittyä taloudellisen edun tavoittelua (OM lausuntotiivistelmä 2013 Melander).

Vuoden 2013 lausuntokierroksella sisäministeriö korostaa uhrin huonoa asemaa tietojensa suojaamisessa ja tietojensa koskevien loukkausten hoitamisessa. Toisena esiintyminen ja toisen henkilötiedoilla nettiin kirjoitetut tekstit säilyvät digitaalisessa ympäristössä, kun uhrin mahdollisuudet tiedon poistamiseen ovat olemattomat. (OM lausuntotiivistelmä 2013 SM.) Vuonna 2014 annetussa hallituksen esityksessä (HE 2014) todetaan, että kriminalisoinnissa merkityksellistä onkin identiteettivarkauden uhrin asianomistaja-aseman selkiyttäminen. Kun rikos voidaan todeta tapahtuneeksi itsenäisenä identiteettivarkautena, identiteettivarkauden uhri saa mahdollisuuden asianomistaja-asemaan (Kangasniemi 2012, ks. tämä tutkielma s. 14). Argumentointi itsenäisen kriminalisoinnin asianomistaja-asemaa parantavasta vaikutuksesta on osin ristiriitainen: pelkkä itsenäinen kriminalisointi ei paranna uhrin tosiasiallista asemaa ja oikeusturvaa, jos esitutkinnalla ei ole mahdollisuuksia selvittää rikoksia tehokkaasti. Tämän lisäksi asianomistajarikoksena vastuu syytteen nostamisesta on identiteettivarkauden uhrilla, joka ei välttämättä ole tietoinen oikeuksistaan identiteettivarkauden uhrina.

Lakivaliokunnan (LaVM mietintö 2014) mukaan asianomistajan oikeuksien turvaamiseksi viranomaisille on annettava riittävät tutkintakeinot ja -valtuudet identiteettivarkauksien tutkintaan. Kangasniemi (2012) antaa esimerkin tapauksesta, jossa asianomistajan oikeuksia ei turvattu esitutkinnassa televalvonnan puutteiden vuoksi. Tapausesimerkissä henkilön epäiltiin luoneen entisen kumppaninsa nimissä sosiaaliseen mediaan profiili ja ladanneen profiiliin entisen kumppaninsa alastonkuvia. Syyte yksityiselämää koskevan tiedon levittämisestä hylättiin. Vastaajan syyllisyys jäi epäselväksi muun muassa siksi, ettei asiassa ollut selvitetty IP-osoitetta, josta valeprofiili oli luotu. (Kangasniemi 2012, 228.) Joissain identiteettivarkauksissa loukattu oikeushyvä on omaisuudeksi tai ”välineeksi” (ks. OM lausuntotiivistelmä 2013 Nuotio, 28) rinnastettavat henkilötiedot, kun esimerkiksi edellä kuvatussa tapauksessa se on yksityisyys ja tiedollinen itsemääräämisoikeus (SM identiteettiohjelma 2010).

Vaikka omaisuudensuoja ei rajoitu vain fyysisiin esineisiin, omaisuuden haltijan pitää voida osoittaa omaisuudelleen ”jokin erityinen arvo” (Kangasniemi 2012, 230). Kun televalvontaan on rikoslainsäädännölliset valtuudet, sen oikeutusta pakkokeinona perustellaan Kangasniemen

(2012, 220–221) mukaan televalvonnan ”ratkaisevalla merkityksellä” tutkinnassa sekä rikoksen ”taloudellisella arvolla”. Vuoden 2014 lausuntokierroksella Lehtonen korostaa, että ihmis- ja perusoikeuksien, kuten yksityisyydensuojan valossa, taloudellisilla ja immateriaalisilla arvoilla pitäisi olla ”yhtäläinen rikosoikeudellinen suoja”. Finanssialan keskusliiton (FK) mukaan digitalisaation laajetessa identiteetin arvo haltijalleen kasvaa, ja samalla identiteettiin liitetään selkeämmin varallisuus oikeudellisia merkityksiä aineettoman oikeuden lisäksi. Etenkin varallisuus oikeuden myötä kysymykseksi nousee tiedon omistajuus ja hallintaoikeus/velvollisuus. (OM lausuntokierros 2014.) Niin viranomaisten kuin yksityishenkilöidenkin voi olla haastavaa hallita digitaalista tietoa: FK:n (em.) mukaan identiteettitiedon varastamisen ja käytön välillä kulunut aika voi olla pitkä, mikä rajoittaa esitutkinnan käynnistämistä. Lehtonen huomauttaa, että verkkoon julkaistujen tietojen poistaminen on yksityishenkilölle ”ylivoimainen tehtävä” (OM lausuntokierros 2014, 5; ks. myös Kangasniemi 2012, tämä tutkielma s. 15). Lisäksi Kangasniemi (2012, 227) huomauttaa, että ilman kriminalisointia pelkässä kiusaamistarkoituksessa tehdyissä identiteettivarkauksissa poliisi ei voi vaatia tuomioistuinta määräämään julkaistua tietoa poistettavaksi. Kriminalisoinninkin jälkeen tuomioistuin voi käyttää harkintavaltaansa tulkitessaan identiteettivarkaudella aiheutettua ”vähäistä suurempaa haittaa” (RL 38 luku 9 a §), jolloin tiedon poistaminen ei ole taattu.

Kuten huomautin laillisuusperiaatetta käsittelevässä alaluvussa (s. 22) kriminalisointi ja viranomaisten pakkokeinot kohdistuvat yksilöiden suojaan viranomaisten vallankäytöltä. Identiteettivarkaussäännöksen nähdään kaventavan perustuslain 12 §:ssä turvattua sananvapautta ”vähäisessä määrin” (HE 2014, 41). Hallituksen esityksessä (HE 2014) kavennus nähdään hyväksyttävänä, sillä se ei kohdistu sananvapauden ydinalueeseen (perusoikeuden keskeinen sisältö) eikä siinä puututa ennakkollisesti sananvapauden käyttöön. Sen sijaan identiteettivarkaudesta aiheutuva ”vähäistä suurempi haitta” (RL 38 luku 9 a §), voisi kohdistua henkilön sananvapauden suojaan: ”henkilöllä on oikeus omissa nimissään käyttää sananvapauttaan” (HE 2014, 37). Kriminalisoinnin pyrkimyksenä on suojata perustuslaissa turvattu oikeus yksityiselämään, johon liittyy myös oikeus henkilökohtaiseen identiteettiin (PeVL 25/2006 vp, 2; PeVL 16/2006 vp, 3; PeVL 59/2002 vp, 3, ks. HE 2014, 41).

5.4 Kriminalisoinnin hyödyt ja haitat

Kriminalisoinnista koituvat hyödyt ja haitat liittyvät olennaisesti eri rooleissa toimivien kansalaisten (uhri, rikollinen, kansalainen, viranomainen) oikeushyviin ja oikeussuojaan. Vuoden 2013 lausuntokierroksella Suomen Lakimiesliitto (OM lausuntotiivistelmä 2013)

katsoo, että kriminalisoinnista koituvat hyödyt ovat liian pieniä suhteessa kriminalisoinnista aiheutuvaan haittaan. Näkemystä voi kritisoida sillä, että vuonna 2013 ja tänä päivänäkin ihmisen voi olla todella haastavaa hallita yksityisyyttään ja julkisuuttaan. Yksilön tietojenhallinnan vaikeuden vuoksi netissä tehtyjen identiteetin loukkausten seuraukset voivat olla hyvinkin vahingollisia uhrin yksityisyyden suojalle ja omaisuuden suojalle. Identiteettiohjelman työryhmän (SM identiteettiohjelma 2010) mukaan identiteettivarkaudet loukkaavat kansalaisten yksityisyyden suojaa ja mahdollisuutta tiedolliseen itsemääräämisoikeuteen (henkilön oikeus omien tietojensa hallintaan), eikä loukkauksia tulisi sallia edes sananvapauden nimissä.

Hallituksen esityksessä (HE 2014) pyritään oikeuttamaan säädösehdotuksen kohtia, eikä sen sisällöllisiä haasteita avata yhtä tarkasti kuin sidosryhmien ja valiokuntien lausunnoissa. Esimerkiksi valeprofiilin, joka on luotu sosiaaliseen mediaan toisen henkilötiedoilla, poistaminen voi olla vaikeaa samalla, kun sen olemassaololla voi olla vahingollisia seurauksia uhrin sosiaalisissa verkostoissa (esim. OM lausuntokierros 2014 SM; OM lausuntokierros 2014 Lehtonen; Kangasniemi 2012). Professori Kimmo Nuotion sekä kuluttaja-asiamiehen (OM lausuntotiivistelmä 2013) mukaan identiteettivarkauden uhrin statuksen saaminen auttaisi uhria rikoksen seurausten selvittämisessä. Useiden lausunnonantajien mukaan identiteettivarkaus lievänä rikoksena ei kuitenkaan anna viranomaisille riittäviä tutkintakeinoja (esim. OM lausuntokierros 2014 SM, ks. tämä tutkielma s. 22–23).

5.5 Rikosoikeuden viimesijaisuus ja mihin se riittää

Ultima ratio -periaate on joiltain osin ristiriitainen kriminalisoinnin preventiovaikutuksen näkökulmasta: yhtäältä kriminalisoinnilla enenevissä määrin pyritään ennaltaehkäisemään rikosten tapahtumista, vaikka toisaalta rikosoikeuden tulisi olla viimesijainen keino rikolliseksi katsottuun toimintaan reagointiin. Kuten laillisuusperiaatetta koskevassa kappaleessa tuon esiin, monet lausunnonantajat puoltavat kriminalisointia. Myös Kangasniemen (2012, 225) mukaan identiteettivarkauden kriminalisoinnin tarve on tietoverkkorikollisuuden vaatimusten myötä ajankohtaistunut.

Vuonna 2010 identiteettiohjelman työryhmä (SM identiteettiohjelma 2010) toteaa, että identiteettitiedon käyttäminen väärin hyödyn hankkimiseksi tai kohteen vahingoittamiseksi on yleensä kriminalisoitu, ja lainsäädäntö takaa tältä osin riittävän suojan uhrille. Työryhmä viittaa tällä oletettavasti tilanteisiin, joissa identiteettitieto on ollut rikoksen teon väline, jonka avulla

pyritään saavuttamaan usein taloudellista arvoa osoittava rikoshyöty. Jos identiteettitieto käsitetään laajemmin kuin välineenä taloudellisen rikoshyödyn saavuttamiseen, rikollisuus voisi pitää sisällään myös loukkaamistarkoituksessa tehdyt teot (Kangasniemi 2012, ks. tämä tutkielma s. 14), joita ei ollut kriminalisoitu identiteettivarkauden alla ennen vuotta 2015. Identiteettitieto on näissä tapauksissa ensisijaisesti rikoksen teon kohde eikä väline.

Rikostutkinnan haasteet ja uhrin oikeudellinen asema ovat sidoksissa toisiinsa ja ne ovat korostetuimpia haasteita, joita lausunnoissa tuodaan esiin. Identiteettivarkauksia ja siitä aiheutuvia vahinkoja ei voida tutkia taikka estää tehokkaasti (Kangasniemi 2012), eikä vuoden 2010 identiteettiohjelman työryhmän (SM identiteettiohjelman 2010) mukaan pelkkä identiteettivarkauden kriminalisointi tarjoa riittävää keinovalikoimaa esitutkinnalle. Tietotekninen jälki todisteena rikoksen tekijästä on kadonnut, kun tiedon oikeudeton käyttäminen alkaa. (SM identiteettiohjelman 2010; ks. myös Wall 2007, 2008, tämä tutkielma s. 11.) Työryhmä kehottaa kiinnittämään huomiota rikostunnusmerkistön ja esitutkintaviranomaisten tutkintavaltuuksien väliseen epäsuhtaan, mikä rajoittaa rikosprosessin etenemistä. Hallituksen esityksessä (HE 2014, 7) todetaan, että rikoslaisissa on muitakin ”suhteellisen vähäisiä rikoksia”, joiden ratkaisemiseen poliisilla ei ole kaikkia salaisia pakkokeinoja. Esityksessä (em.) identiteettivarkauksista piirtyy kuva vääjäämättömänä pahana, jonka yhteiskunnalliset kustannukset ollaan valmiita hyväksymään, kenties rangaistuksen oikeasuhtaisuuden ja yksilön suojan viranomaisvallalta vuoksi.

Kangasniemi (2012) asettaa vastakkain pakkokeinojen laajentamisen identiteettivarkauteen ja identiteettivarkauden rangaistavuuden alan laajentamisen, jotka omilla tavoillaan vaikuttavat viranomaisten valtuuksiin käyttää telepakkokeinoja. Kysymykseksi nousee, onko se muoto, jossa kriminalisointi säädetään, viimesijainen suhteessa muihin muotoihin, kun huomioidaan kriminalisoinnin vaikutukset perusoikeuksien toteutumiseen. Identiteettivarkauden ajatellaan olevan yhteiskunnallinen uhka, kun se tapahtuu muun tietoverkkorikoksen yhteydessä, jolloin yhtenä vaihtoehtona olisi ollut säätää identiteettivarkaus koventamisperusteena jonkun muun rikoksen yhteydessä. Vuonna 2010 valtioneuvosto (VN muistio 2010) näkee ongelmallisena, että säännökset bottiverkoista ja henkilöllisyyden väärinkäytöstä olisivat rangaistavuuden alan laajentamisen sijaan koventamisperuste mainituille teoille. Kiinnijäämisriskin lisääminen esimerkiksi kansainvälisellä yhteistyöllä, ennaltaehkäisee rikoksia tehokkaammin kuin rangaistusasteikkojen tiukentaminen. (VN muistio 2010.) Myös lausunnoissa

identiteettivarkauden kriminalisointi koventamisperusteena pääosin tuomitaan vetoamalla laillisuusperiaatteen oikeasuhtaisuuden vaatimukseen.

Myöskään hallintovaliokunta (HaVL lausunto 2010) lausunnossaan identiteettiohjelman loppuraportista ei näe perusteita rangaistustason kasvattamiseksi: tietoverkkorikollisuudessa ongelmana on kiinnijäämisriskin pienuus, eikä seuraamusten ennaltaehkäisevän vaikutuksen puute. Rangaistustaso nähdään hyväksyttävänä, kun se on rajattu ”vakavampiin rikoksiin” (HaVL lausunto 2010) moninaisten identiteettirikosten joukossa. Näkemys voidaan haastaa, sillä rangaistuksen laajuus vaikuttaa tutkintavaltuuksiin ja rikosten selvittämiseen ja siten mahdollisesti ennaltaehkäisevään vaikutukseen. Koventamisperusteena kriminalisointi antaisi esitutkinnalle tehokkaammat keinot selvittää rikos, sillä telepakkokeinojen käyttö edellyttää rikokselta törkeää muotoa tai säädetyltä rangaistukselta vähintään kahdesta neljään vuotta vankeutta (Pakkokeinolaki 10 luku 3–6 §). Lakivaliokunnan mukaan (LaVL lausunto 2011) koventamisperuste voitaisiin panna täytäntöön laillisuusperiaatteen mukaisesti, mutta hallintovaliokunnan kantaa (HaVL lausunto 2011) mukailleen se näkee parempana vaihtoehtona identiteettivarkauden kriminalisoinnin erillisenä säädöksenä.

Oikeusministeriön johtama lainvalmistelutyö saa osakseen kritiikkiä. Käsitteen laaja-alaisuuden lisäksi, Suomen Lakimiesliitto ja sosiaali- ja terveysministeriö (STM) (OM lausuntotiivistelmä 2013) katsovat vuoden 2013 lausuntokierroksella, ettei identiteettivarkauden kriminalisointi täytä ultima ratio -periaatteen edellytyksiä rikosoikeuden viimesijaisuudesta. Asianajajaliitto toteaa, että suurin ongelma liittyy rikosten tutkintaan, mutta vuonna 2014 voimaan tulevien pakkokeinolain säädösten jälkeen poliisilla olisi riittävät keinot tutkia tietoverkkorikoksia Suomessa. (OM lausuntotiivistelmä 2013.) ”Riittävät keinot” on tulkinnanvarainen ilmaus, eivätkä Kangasniemen (2012, 221–222) mukaan kyseiset uudet säädökset kata kaikkia yhteiskunnan turvallisuuteen ja kotirauhaan kohdistuvia rikoksia; televalvonnan valtuudet koskevat rikoksia, joista on säädetty rangaistukseksi vähintään kaksi vuotta vankeutta. Vuoden 2014 lausuntokierroksella Helsingin syyttäjävirsto näkeekin ongelmana, etteivät säädetty pakkokeinovaltuudet koske valeprofiileja sosiaaliselle medialle tyypillisinä identiteettivarkauksina. Jos televalvonnan käyttö pakkokeinona käsitettäisiin yhtenä välineenä esitutkinnassa, sillä helpotettaisiin ja kevennettäisiin suhteellisen vähäiseksi katsotun rikoksen esitutkintaa ja rikosprosessia. (Helsingin syyttäjävirsto 2014.) Identiteettivarkauden kriminalisoinnissa voidaan katsoa noudatetun kriminalisointiperiaatteita

viranomaisvallalta suojelun näkökulmasta, mutta uhrin tiedollisen itsemääräämisoikeuden oikeushyvän kustannuksella.

Vuoden 2013 lausuntokierroksella Valtakunnansyyttäjänviraston (VKSV) (OM lausuntotiivistelmä 2013) mukaan oikeusministeriön näkökulmaa lainvalmistelussa leimaa kriminalisointiperiaatteiden korostaminen. VKSV katsoo, että vain laillisuusperiaatetta voidaan pitää yleisenä oikeusperiaatteena, kun ”ultima ratio” -periaatteen korostamisessa on kysymys ”kotimaisesta keksinnöstä”. VKSV pohtii, josko riittäisi, että kriminalisointi ennaltaehkäisee ”edes vähän” ei-toivottua menettelyä. (OM lausuntotiivistelmä 2013 VKSV.) Vuoden 2014 lausuntokierroksella Eduskunnan apulaisoikeusasiamiehen (OM lausuntokierros 2014) mukaan esitysluonnos vaikuttaa ”tekniseltä täytäntöönpanouudistukselta”. Suomen Lakimiesliiton ja STM:n vuoden 2013 lausuntoja (OM lausuntotiivistelmä 2013) mukailten, apulaisoikeusasiamiehen (OM lausuntokierros 2014) voidaan tulkita katsovan rikoslakia käytettävän ennemmin välineenä hallita ennaltaehkäisevästi ei-toivotun toiminnan seurauksia kuin ultima ratio -periaatteen tavoin viimesijaisena keinona kontrolloida asiaa. Ilmiössä voi tunnistaa piirteitä Zednerin (2003, ks. tämä tutkielma s. 8) paradokseista. Ultima ratio -periaatteen mukaan kriminalisoinnin tulisi olla viimesijainen keino vastata ongelmaan, jolloin kriminaalisoinnille tulisi olla yhteiskunnallinen tarve. Samalla yhteiskunnallinen tarve määrittyy rikosoikeusjärjestelmän preventiotehtävään nojaten, jolloin rikollisuuteen pyritään vastaamaan ennen kuin se on ehtinyt muodostua ongelmaksi, mikä on ristiriidassa ultima ratio -periaatteen kanssa.

Vuoden 2013 lausuntotiivistelmässä arvioidaan myös rikosoikeuden ulkopuolisia keinoja identiteettivarkauksien hallintaan. Tietosuojavaltuutetun (OM lausuntotiivistelmä 2013) mukaan kouluissa tehtävä ”yleinen kansanvalistus ja mediakasvatus” olisivat ainoita keinoja, joilla identiteettivarkauden kaltaista rikollisuutta voi torjua. Tuomariliitto ja kuluttaja-asiamies (em.) arvioivat, että ennaltaehkäisevät keinot eivät riitä uhrin oikeuksien suojaamiseen eikä identiteettivarkauksien ennaltaehkäisemiseen. Keskitetty ilmoitusjärjestelmä (Kangasniemi 2012) olisi rikosoikeuden ulkopuolisista vaihtoehdoista kenties konkreettisin apu identiteettivarkauden uhrille, koska se sallisi tiedon kulun yhdestä palvelusta eteenpäin muille viranomaisille. Rekisterinpitäjiä koskee huolehtimisvelvollisuus, minkä lisäksi on ehdotettu mahdollisuutta palveluntarjoajien informointivelvollisuuteen henkilötietojen hallintaan liittyen (Kangasniemi 2012). Yritysten vastuuta ei sen syvemmin käsitellä niin Kangasniemen artikkelissa (2012) kuin lausunnoissakaan (vrt. Wall 2013, ks. tämä tutkielma s. 11).

6 Yhteenveto: Identiteettivarkaus ja kansalliset tarpeet

Identiteettivarkauden kriminalisointi heijastaa oikeusjärjestelmän pyrkimystä mukautua yhteiskunnallisiin muutoksiin, kuten tietoverkkorikollisuuden yleistymiseen. Eritasoisista identiteettivarkauksista piiryy kuva vääjäämättömänä yhteiskunnan kiusana, jolloin syntyy tarve mahdollistaa uhreille mahdollisimman nopea ja sujuva siirtymä takaisin arkielämään rikoksen jälkeen. Lievänä ja vähäiseksi katsottuna oheisrikollisuutena (HE 2014), identiteettivarkauden rangaistukseksi voidaan asettaa vain sakkoa, mikä rajaa ulos mahdollisuuden televalvonnan käytön esitutkinnan pakkokeinona. Vuoden 2014 pakkokeinolain uudistuksesta huolimatta tutkintahaasteet näkyvät vielä tänä päivänä poliisin tilastoissa: vuonna 2023 vajaa 30 % identiteettivarkauksista selvitettiin, ja kriminalisoinnista lähtien tapauksista selvitettyjä oli parhaimmillaankin vain noin puolet (Tilastokeskus 2023, ks. tämä tutkielma s. 11).

Oikeudellisesti haastavaksi niin lausunnoissa kuin Kangasniemen (2012) artikkelissakin nähtiin kiusaamistarkoituksessa tehdyt identiteettivarkaudet, jotka esiintyvät usein sosiaalisessa mediassa itsenäisinä identiteettivarkauksina. Toisen henkilötiedoilla laittomasti kirjoitetut nettitekstit säilyvät digitaalisessa ympäristössä määrättömän ajan ja uhrin mahdollisuudet tiedon poistamiseen ovat pienet. Kriminalisointiperiaatteiden näkökulmasta kyseisen kaltaista tekoa on vaikea säätää johdonmukaisesti ja tarkkarajaisesti rikoslakiin, mistä syystä lainsäädännöllä ei kyetä turvaamaan henkilön tiedollista itsemääräämisoikeutta (ks. SM identiteettiohjelma 2010). Uusin käänne kriminalisointiprosessissa on kansanedustaja Harakan (sd) eduskunnalle tuoma lakialoite, jossa rikoslakiin lisättäisiin 38 luvun 9 b § törkeästä identiteettivarkauksesta, josta rangaistaisiin sakkoa tai enintään kolme vuotta vankeutta (LA 5/2024 vp). Törkeä muoto ja vankeusrangaistus voisivat sallia esitutkintaan telepakkokeinojen käytön.

Identiteettivarkauden kriminalisoinnista päätettäessä oikeudellinen problematiikka on keskittynyt kunkin osapuolen – identiteettivarkauden uhrin, rikoksesta epäilyn ja yleisesti kansalaisen – oikeuksien suojan väliseen arviointiin. Eri oikeuksien suojat rajoittavat viranomaisvallan ja valvonnan käyttämistä esitutkinnassa, mutta sujuva esitutkinta mahdollistaa rikosprosessin etenemisen ja vahvistaa rikoksen uhrin oikeudellista asemaa. Kriminalisoinnissa uhrin oikeudet (yksityisyyden suoja ja tiedollinen itsemääräämisoikeus) asianomistaja-asemassaan näyttävät korostuvan rikoksen tekijän rikosvastuun yli. Toisaalta

rikoksesta epäilyn sekä kansalaisen oikeuksien suojan (yksityisyyden ja luottamuksellisen viestin suoja) olivat eräitä perusteita esitutkintaviranomaisten pakkokeinojen rajaamiselle ulos rangaistussäännöksestä. Rikosoikeusjärjestelmän oikeasuhtaisuus ja viimesijaisuus sekä hyöty-haitta-punninta ovat kriminaalipoliittisia periaatteita ja tulkinnanvaraisia määritelmiä. Arviointi niiden merkityksestä rikoslainsäädännössä vaatii laajempaa yhteiskunnallista keskustelua siitä, milloin ja missä määrin yhteiskunnallista elämää halutaan hallita rikosoikeuden mekanismeilla (vrt. OM lausuntotiivistelmä 2013 VKSV). Sen sijaan, että kriminalisointiin olisi turvauduttu viimesijaisena keinona vastata identiteettivarkaus-ongelmaan, monista lausunnoista syntyy vaikutelma, että rikosoikeutta pyritään käyttää viimesijaisuuden sijaan ennemmin välineenä pakkokeinojen käytölle ja rikoksen uhria koskevien seurausten tehokkaalle hoitamiselle.

Vaikka uhrin ja kansalaisten oikeusturvaa korostettiin lainvalmistelussa, kansalaisille ei avattu mahdollisuutta lausua asiasta. Identiteettivarkaus voi loukata uhrin yksityisyyden suojaa ja tiedollista itsemääräämisoikeutta. Identiteettivarkauden kriminalisointi voi johtaa sananvapauden rajoituksiin, ja televalvontakeinot puolestaan yksityisyyden - ja luottamuksellisen viestin suojan heikennyksiin. Koska kyseinen kriminalisointi vaikuttaa etenkin identiteettivarkauden uhrin elämään, olisi uhrien tai heidän ääntään edustavien organisaatioiden näkemykset olleet tarpeellisia. Lausunnoissa toinen perusoikeus saa etusijan toiseen nähden, mikä korostaa oikeuslähteiden keskinäistä ristiriitaisuutta, jolta ei aina voi välttyä.

Lähdeluettelo

Tutkimusaineiston keräämiseen/rajaamiseen/analysointiin/... on käytetty Turun yliopiston [Lakitutka-palvelua](#). DOI: [10.5281/zenodo.6504432](https://doi.org/10.5281/zenodo.6504432)

Kirjallisuus

- Crawford, Adam (2006) Networked governance and the post-regulatory state?: Steering, rowing and anchoring the provision of policing and security. *Theoretical Criminology* 10(4), s. 449–479. Saatavilla: <https://doi.org/10.1177/1362480606068874> (Luettu: 19.10.2024).
- Cross, Cassandra (2015) No laughing matter: Blaming the victim of online fraud. *International Review of Victimology* 21(2), s. 187–204. Saatavilla: <https://doi.org/10.1177/0269758015571471> (Luettu: 9.10.2024).
- David, Mathew (2023) Networked Crime: Does the Digital Make the Difference? *Bristol University Press*. Saatavilla: ProQuest Ebook Central. (Luettu: 8.10.2024).
- European Commission (2022) European Commission Directorate-General for Migration and Home Affairs. Study on online identity theft and identity-related crime: final report. Publications Office of the European Union. Saatavilla: <https://data.europa.eu/doi/10.2837/197724> (Luettu: 1.1.2025).
- Jewkes, Yvonne & Yar, Majid (2011) *Handbook of Internet Crime (1. painos.)*. Willan. Saatavilla: <https://doi.org/10.4324/9781843929338> (Luettu: 1.9.2024).
- Kangasniemi, Tea (2012) Identiteettivarkaudet–haasteita rikostutkinnalle ja–oikeudelle, paljon vaivaa ja harmia uhrille. *Teoksessa Ervo, L., Lahti, R. & Siro, J. (toim.) Perus- ja ihmisoikeudet rikosprosessissa, Helsingin hovioikeuden julkaisuja*. Hakapaino Oy, Helsinki. Saatavilla: https://www.oikeus.fi/hovioikeudet/helsinginhovioikeus/material/attachments/oikeus_hovioikeudet_helsinginhovioikeus/julkaisut/ (Luettu: 16.10.2024).
- Korhonen, Rauno (2014) Sähköinen asiointi ja viestintä. *Teoksessa Tuominen, Tomi (toim.): Oikeus tänään*. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C. Rovaniemi.
- Kostiainen, Aura (2023) *Rationaalisuuden vallankumous: Oikeus, asiantuntijuus ja politiikka rikosoikeuskomitean (1972–1977) työskentelyprosessissa*. Suomalainen lakimiesyhdistys.

- Lappi-Seppälä, Tapio (2022) Seuraamusjärjestelmän pääpiirteet. *Teoksessa Rikosoikeus, Hakamies Kaarlo, Koskinen, Pekka; Martti Majanen, Sakari Melander, Kimmo Nuotio, Ari-Matti Nuutila, Timo Ojala, ja Ilkka Rautio*. Helsinki: SanomaPro.
- Mallik, Avijit & Ahsan, Abid & Shahadat, Mia Md. Zaglul & Tsou, Jia-Chi (2019) Man-in-the-middle-attack: Understanding in simple words. s. 77–92. Saatavilla: https://www.researchgate.net/publication/330249434_Man-in-the-middle-attack_Understanding_in_simple_words (Luettu: 8.10.2024).
- Melander, Sakari (2021) Johdatus rikosoikeuteen. *Oikeuden perusteet; Nro 32*. Helsingin yliopisto, oikeustieteellinen tiedekunta.
- Murray, Andrew D. (2008) Conceptualising the post-regulatory (cyber)state. *Teoksessa Brownsword, Roger & Yeung, Karen (Toim.) Regulating Technologies Legal: Futures, Regulatory Frames and Technological Fixes*. Hart Publishing, Oxford, UK, s. 287–316.
- Mäenpää, Olli (2020) *Julkinen valta ja oikeusvaltio*. (Oikeuden perusteet; Nro 2). Helsingin yliopiston oikeustieteellinen tiedekunta. Saatavilla: <https://unicontent.unigrafia.fi/#/reader/469b0a20-8848-11ea-bfb9-00155d64030a> (Luettu: 20.11.2024).
- Näsi, Matti (2023) Kyberrikollisuus. *Teoksessa Beuker, Aaro (Toim.) Rikollisuustilanne 2022: rikollisuuskehitys tilastojen ja tutkimusten valossa*. (Katsauksia; Nro 55/2023). Helsingin yliopisto, kriminologian ja oikeuspolitiikan instituutti. Saatavilla: <https://researchportal.helsinki.fi/fi/publications/rikollisuustilanne-2022-rikollisuuskehitys-tilastojen-ja-tutkimus> (Luettu: 20.11.2024).
- Näsi, Matti & Tanskanen, Maiju (2016) Kyberrikollisuus. *Teoksessa Niemi, Hannu & Danielsson, Petri (Toim.) Rikollisuustilanne 2015: Rikollisuuskehitys tilastojen ja tutkimusten valossa*. Helsingin yliopisto, Kriminologian ja oikeuspolitiikan instituutti.
- Rantala, Kati & Alasuutari, Noora (2021) Lainsäädäntötutkimus: esimerkkinä lainvalmistelun analyysi. *Teoksessa Kati Nieminen, & Noora Lähteenmäki (Toim.), Empiirinen oikeustutkimus* s. 70–91. Article 4 Gaudeamus. Saatavilla: <https://kauppa.gaudeamus.fi/sivu/tuote/empiirinen-oikeustutkimus/3275943> (Luettu: 7.12.2024).
- Rikosuhripäivystys (2019) Mitä tarkoittaa asianomistajarikos tai viralliseen syytteen alainen rikos? Saatavilla: <https://www.riku.fi/erilaisia-rikoksia/usein-kysyttya/mita-tarκοittaa-asianomistajarikos-ja-virallisen-syytteen-alainen-rikos/> (Luettu: 28.10.2024).

- Suomen virallinen tilasto (2022) Rikos- ja pakkokeinotilasto [verkkójulkaisu]. ISSN=2342-9151. 4. vuosineljännes 2021. Helsinki: Tilastokeskus, Saatavilla: https://www.stat.fi/til/rpk/2021/04/rpk_2021_04_2022-01-19_tie_001_fi.html (Luettu: 26.10.2024).
- Wall, David S. (2007) *Cybercrime: the transformation of crime in the information age*. Cambridge: Polity.
- Wall, David S. (2008) Cybercrime and the culture of fear. *Information, Communication & Society* 11(6), s. 861–884. Saatavilla: <https://doi.org/10.1080/13691180802007788> (Luettu: 11.12.2024).
- Wall, David (2010) ‘Micro-Frauds: Virtual Robberies, Stings and Scams in the Information Age’. *Teoksessa T. Holt, T., and B. Schell (2010) (toim.) Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications, Hershey, PA (USA): IGI Global*. Saatavilla: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1563626 (Luettu: 8.11.2024).
- Wall, David (2013) Policing identity crimes. *Policing and Society: An International Journal of Research and Policy* 23(4), s. 437–460. Saatavilla: https://heinonlineorg.ezphost.dur.ac.uk/HOL/Page?lname=&public=false&collection=journals&handle=hein.journals/pgsty23&men_hide=false&men_tab=toc&kind=&page=437 (Luettu: 5.12.2024).
- Yar, Majid (2006) *Cybercrime and society crime and punishment in the information age*. London: SAGE Publications.
- Zedner, Lucia (2003) Too much security?. *International journal of the sociology of law* 31(3), s. 155–184. Saatavilla: <https://doi.org/10.1016/j.ijsl.2003.09.002> (Luettu: 30.12.2024).

Virallislähteet

- Direktiivi 2013/40/EU, Euroopan parlamentin ja neuvoston direktiivi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta. Euroopan unionin virallinen lehti 14.8.2013. Saatavilla: <https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32013L0040> (Luettu: 5.11.2024).
- Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (2001) ETS No. 185, Convention on Cybercrime 23.11.2001. Saatavilla: <https://www.coe.int/en/web/cybercrime/the-budapest-convention> (Luettu: 24.9.2024).

- Asetus 2016/679/EU, Euroopan parlamentin ja neuvoston asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) III luku 3 jakso 16–18 artiklat. 27.4.2016.
- HaVL lausunto (2011) Hallintovaliokunnan lausunto HaVL 37/2010 13.1.2011. Lausunto Oikeusministeriön nettisivulla, osiossa hankkeet ja säädösvalmistelu. Saatavilla: <https://oikeusministerio.fi/hanke?tunnus=OM017:00/2013> (Luettu 5.11.2024).
- HaVL lausunto (2011) Hallintovaliokunnan lausunto HaVL 2/2011 20.5.2011. Lausunto Oikeusministeriön nettisivulla, osiossa hankkeet ja säädösvalmistelu. Saatavilla: <https://oikeusministerio.fi/hanke?tunnus=OM017:00/2013> (Luettu 5.11.2024).
- HE 222/2010 vp, Hallituksen esitys Eduskunnalle esitutkinta- ja pakkokeinolainsäädännön uudistamiseksi. Finlex-palvelussa, osiossa Hallituksen esitykset. Saatavilla: <https://finlex.fi/fi/esitykset/he/2010/20100222> (Luettu: 30.12.2024).
- HE (2014) 232/2014 vp Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräksi siihen liittyviksi laeiksi. Esitys Oikeusministeriön nettisivulla, osiossa hankkeet ja säädösvalmistelu. Saatavilla: <https://oikeusministerio.fi/hanke?tunnus=OM017:00/2013> (Luettu 5.11.2024).
- Komission ehdotus (2010) KOM(2010) 517 lopullinen, Euroopan parlamentin ja neuvoston direktiivi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS kumoamisesta 30.9.2010. Saatavilla: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:FI:PDF> (Luettu 5.11.2024).
- LaVL lausunto (2011) Lakivaliokunnan lausunto 18/2010 vp 20.1.2011. Lausunto Oikeusministeriön nettisivulla, osiossa hankkeet ja säädösvalmistelu. Saatavilla: <https://oikeusministerio.fi/hanke?tunnus=OM017:00/2013> (Luettu 5.11.2024).
- LaVL lausunto (2011) Lakivaliokunnan lausunto 4/2011 vp 7.6.2011. Lausunto Oikeusministeriön nettisivulla, osiossa hankkeet ja säädösvalmistelu. Saatavilla: <https://oikeusministerio.fi/hanke?tunnus=OM017:00/2013> (Luettu 5.11.2024).
- LaVM mietintö (2014) Lakivaliokunnan mietintö 29/2014 vp 27.2.2015. Julkaisu Oikeusministeriön nettisivulla, osiossa hankkeet ja säädösvalmistelu. Saatavilla: <https://oikeusministerio.fi/hanke?tunnus=OM017:00/2013> (Luettu 5.11.2024).

- OM hankesuunnitelma (2013) OM 15/41/2013, Asettamispäätös 27.9.2013. Julkaisu Oikeusministeriön nettisivulla, osiossa hankkeet ja säädösvalmistelu. Saatavilla: <https://oikeusministerio.fi/hanke?tunnus=OM017:00/2013> (Luettu: 1.12.2024).
- OM Lainvalmistelun prosessiopas. Oikeusministeriön Finlex-palvelussa. Saatavilla: <https://lainvalmistelu.finlex.fi/> (Luettu: 16.12.2024).
- OM lausuntotiivistelmä (2013) OMML 47/2013 vp 30.9.2013. Julkaisu Oikeusministeriön nettisivulla, osiossa hankkeet ja säädösvalmistelu. Saatavilla: <https://oikeusministerio.fi/hanke?tunnus=OM017:00/2013> (Luettu 5.11.2024).
- OM lausuntokierros (2014) Lausunnot Oikeusministeriön nettisivulla, osiossa hankkeet ja säädösvalmistelu. Saatavilla: <https://oikeusministerio.fi/hanke?tunnus=OM017:00/2013> (Luettu 5.11.2024).
- OM mietintö (2014) OMML 27/2014 vp 29.4.2014. Julkaisu Oikeusministeriön nettisivulla, osiossa hankkeet ja säädösvalmistelu. Saatavilla: <https://oikeusministerio.fi/hanke?tunnus=OM017:00/2013> (Luettu 5.11.2024).
- OM Säädösvalmistelun kuulemisohje. Oikeusministeriön Finlex-palvelussa, osiossa Säädösvalmistelun kuulemisopas. Saatavilla: <https://kuulemisopas.finlex.fi/ohje/kuulemisohje/#jakso-kuulemisohje> (Luettu: 16.12.2024).
- Pakkokeinolaki 22.7.2011/806 (2024) Pakkokeinolaki. Julkaisu Oikeusministeriön Finlex-palvelussa, osiossa Ajantasainen lainsäädäntö. Saatavilla: <https://finlex.fi/fi/laki/ajantasa/2011/20110806> (Luettu: 4.1.2025).
- PeVL 66/2010, Perustuslakivaliokunnan mietintö hallituksen esityksen esitutkinta- ja pakkokeinolainsäädännön uudistamiseksi johdosta.
- PeVL 18/2014, Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle tietoyhteiskuntaaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta 17.6.2014. Saatavilla: https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_18+2014.pdf (Luettu: 1.1.2025).
- Puitepäätös 2005/222/YOS, Neuvoston puitepäätös tietojärjestelmiin kohdistuvista hyökkäyksistä. Euroopan unionin virallinen lehti 16.3.2005. Saatavilla: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:FI:PDF> (Luettu: 5.11.2024).

RL 19.12.1889/39 (2024) Rikoslaki. Julkaisu Oikeusministeriön Finlex-palvelussa, osiossa Ajantasainen lainsäädäntö. Saatavilla: <http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001> (Luettu: 6.10.2024).

SM identiteettiohjelma (2010) Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti (SM092:00/2008) 15.12.2010.

VN kirjelmä (2010) U 50/2010 vp, Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS kumoamisesta 2.12.2010.

Yleissopimus 60/2007, Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus. Julkaisu Oikeusministeriön Finlex-palvelussa, osiossa Valtiosopimukset. Saatavilla: https://www.finlex.fi/fi/sopimukset/sopsteksti/2007/20070060/20070060_2 (Luettu: 10.11.2024).

Internet-lähteet

Kotimaisten kielten keskus (2024) Osiossa Suomen etymologinen sanakirja. Saatavilla: <https://www.kotus.fi/> (Luettu: 13.11.2024).

Yle Uutiset (2009) Holmlund kriminalisoisi identiteettivarkaudet, 30.7.2009. Saatavilla: <https://yle.fi/a/3-5293047> (Luettu: 26.10.2024).

Yle Uutiset (2009) Identiteettivarkaus on Suomessa toistaiseksi tuntematon rikos, 30.7.2009. Saatavilla: <https://yle.fi/a/3-5293044> (Luettu: 26.10.2024).

LIITTEET

Liite 1 Lainvalmistelun asiakirjat kronologisessa järjestyksessä

Lainvalmistelun asiakirjat	Lyhenne	Kuvaus	Päivämäärä
Komission ehdotus ”Euroopan parlamentin ja neuvoston direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS kumoamisesta”	KOM(2010) 517 lopullinen)	Komission ehdotus tietoverkkorikos-direktiiviksi	30.9.2010
Valtioneuvoston (VN) kirjelmä Eduskunnalle ehdotuksesta Euroopan parlamentin ja neuvoston direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS kumoamisesta	U 50/2010	VN:n kirjelmä eduskunnalle direktiiviehdotuksesta	2.12.2010
Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma), ryhmän loppuraportti	SM 32/2010	Identiteettiohjelman loppuraportti	15.12.2010
Hallintovaliokunnan lausunnot	HaVL 37/2010; HaVL 2/2011	Lausunnot asiakirjasta U 50/2010	13.1.2011; 20.5.2011
Lakivaliokunnan lausunnot	LaVL 18/2010; LaVL 4/2011	Lausunnot asiakirjasta U 50/2010	20.1.2011; 7.6.2011
Euroopan parlamentin ja neuvoston direktiivi tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta	2013/40/EU	Tietoverkkorikos-direktiivi	14.8.2013
Oikeusministeriön identiteettivarkautta koskeva arviomuistio	OM 4/41/2013	Asiakirja ei julkinen	Ei tietoa
Tietoverkkorikodirektiivin täytäntöönpanon hankesuunnitelma	OM 15/41/2013	Direktiivin kansallinen täytäntöönpanohanke	1.10.2013 – 10.4.2015
Identiteettivarkaus lausuntotiivistelmä	OM 47/2013	Lausunnot asiakirjasta SM 32/2010	30.9.2010
Tietoverkkorikodirektiivin täytäntöönpano	OM 27/2014	Hallituksen esityksen luonnos / OM mietintö	29.4.2014
Tietoverkkorikodirektiivi lausuntotiivistelmä	OM 35/2014	Lausunnot asiakirjasta OM 27/2014	26.8.2014
Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräksi siihen liittyviksi laeiksi	HE 232/2014	Tietoverkkorikodirektiivin täytäntöönpano	13.11.2014
Lakivaliokunnan mietintö hallituksen esityksestä	LaVM 29/2014	Mietintö HE:stä	27.2.2014