Avoimien tietolähteiden hyödyntäminen taustatarkistuksissa

Jari Stolt

2022 Laurea

Laurea-ammattikorkeakoulu

Avoimien tietolähteiden hyödyntäminen taustatarkistuksissa

Jari Stolt

Turvallisuusjohtamisen koulutus

Opinnäytetyö

Kesäkuu 2022

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusjohtamisen koulutus
Ylempi AMK

Jari Stolt

Avoimien tietolähteiden hyödyntäminen taustatarkistuksissa

Vuosi 2022 Sivumäärä 55

Tässä opinnäytetyössä tarkasteltiin mahdollisuuksia hyödyntää avoimien tietolähteiden tiedustelua rekrytointitilanteissa ja taustatarkistuksissa sekä miten lainsäädäntö rajoittaa tätä toimintaa. Työssä on käyty läpi esimerkkitapausten avulla keskeiset syyt taustatarkistusten tekemiseen. Tulevaisuuden kehitystä on pohdittu tekoälyn ja koneoppimisen kautta, potentiaaliset haasteet syntyvät erityisesti läpinäkyvyydessä ja tulosten perustelussa.

Opinnäytetyössä tutkittiin kotimaisia ja ulkomaisia kirjallisuuslähteitä sekä millaisia ohjeistoja (engl. guidelines) tai eettisiä ohjeita muualta löytyy. Avoimien tietolähteiden suhteen nousee esille Euroopan unionin tietosuoja-asetus eli englanniksi General Data Protection Regulation (GDPR) sekä Suomen tietosuojalainsäädäntö. Erityisesti olennaista on, kuinka paljon tietosuojalainsäädäntö ja GDPR rajoittavat avoimien tietolähteiden tiedustelua. Opinnäytetyössä pohdittiin lainsäädännön, etiikan ja ohjeiden merkitystä tiedustelua suorittavalle palveluntarjoajalle ja heidän työntekijöilleen.

Tehokkaan kansallisen sääntelyn puute ja teknologian nopea kehitys haastavat tulevaisuudessa yksityisyydensuojan. Koneoppimisen ja tekoälyn mahdollisuudet luovat haasteen lainsäädäntötyölle, mikä tuo erityisesti painetta alan sisäiselle sääntelylle. Alan sisäinen sääntely voisi tarkoittaa eettisiä ohjeita, yhtenäisiä toimintaohjeita, määritelmän hyväksytyistä tietolähteistä sekä vaatimuksen myös tarkastuksen kohteen etujen suojelemisesta sekä taustatarkistusprosessin läpinäkyvyydestä.

Avointen tietolähteiden hyödyntäminen ei taustatarkistuksen tai luotettavuuden arvioinnin työkaluna ole poissuljettu, mutta laillisten edellytysten tulee täyttyä täysimääräisesti. Tällä hetkellä merkittävimmät toimintaa määrittelevät säädökset ovat Euroopan unionin tietosuoja-asetus, laki yksityisyyden suojasta työelämässä sekä tietosuojalaki, jotka määrittelevät tarkastuksen kohteen oikeuksia sekä minkälaista tietoa kohteesta voidaan kerätä.

Tavoitteena oli myös ohjata kehittämään taustatarkistusprosessiin avoimuutta ja toimintaa harjoittavia yrityksiä laatimaan ohjeistukset ja eettiset ohjeet tutkintaa suorittaville työntekijöilleen. Näillä parannetaan taustatarkistuksen kohteen yksityisyyden suojaa ja oikeusturvaa sekä luodaan luottamusta taustatarkistusprosessiin.

Asiasanat: avoimet tietolähteet, tiedustelu, rekrytointi, taustatarkistus, OSINT

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security Management
Master of Business Administration

Jari Stolt

Using Open-source Intelligence in Background Check

Year 2022 Pages 55

Open-source intelligence has risen in the media in several different contexts. In the context of crises, it forms a means of creating a situation picture, as well as a holistic understanding of events. Many master's theses have dealt with intelligence-related technology, opportunities, and technical solutions to search for information. Significantly less discussed are ethical or legislative restrictions on an open source intelligence, for example, the legality of the availability of sources is situated. Thesis reviews the possibilities of utilizing the inquiries of open data sources in recruitment situations and background checks, and how much legislation limits the action.

The thesis presents domestic and foreign literature sources and explores what kind of guidelines or ethical guidelines exist. With regard to open sources of information, the European Data Protection Regulation, i.e. General Data Protection Regulation (GDPR), and Finland's data protection legislation are also discussed. It is essential to note how much data protection legislation and GDPR limit the intelligence of open sources of information. The thesis considers the importance of legislation, ethics and guidelines for the service provider and their employees.

The possibilities of machine learning and artificial intelligence create a challenge for legislative work, which specifically brings pressure on intra-sector regulation. Legislation is not likely to bring a rapid and clear solution. Internal regulation in the field could mean ethical guidelines, uniform guidelines, the definition of approved sources of information, also the requirement to protect the interests of the inspection item and the transparency of the background inspection process.

The thesis is intended to provide an understanding of possible risks of action to various parties and, on the other hand, to bring out the benefits of background checks. The aim is also to guide the development of transparency in the background inspection process and to guide the activities carried out by companies to draw up guidelines and ethical guidelines for their investigations. These improve the privacy and legal protection of objects of the background check and create confidence in the background check process.

Keywords: open source intelligence, intelligence, recruiting, background check, osint

Sisällys

1 Johdanto

Viime vuosina avoimien tietolähteiden tiedustelu eli englanniksi Open Source Intelligence (OSINT) on ollut voimakkaasti esillä. Monissa tutkimuksissa, opinnäytetöissä, pro graduissa ja seminaareissa on tuotu esille sen mahdollisuudet muun muassa rekrytoitavien taustatarkistuksen laatimisessa. Hyvin vähän on pohdittu toimintaa esimerkiksi eettisistä tai lainsäädännön näkökulmista tai sen suhteen, millaisia riskejä tällaisesta toiminnasta voi olla eri toimijoille. Erityisesti yrityksille voi potentiaalisesti syntyä merkittävä imagoriski ja muita mahdollisia lainsäädännöllisiä seuraamuksia avoimien lähteiden väärinkäytöksistä tai henkilötietojen lainvastaisesta käytöstä.

Loshe ja Viitanen (2018) mukaan avoimiksi tietolähteiksi luokitellaan yleisesti kaikki tietolähteet, joiden tieto on kaikille saatavilla. Tietolähde voi olla ilmainen tai maksullinen, mutta olennaista on, että se on julkisesti saatavilla. Työnantajalle saattaa syntyä mielikuva, että työnantaja voi etsiä avoimista tietolähteistä ja sosiaalisesta mediasta tietoja rekrytoitavasta henkilöstä, mutta laki yksityisyyden suojasta työelämässä (2004/759) säännökset 3 §, 4 § ja 5 § määrittävät olennaiset rajoitteet. Ensimmäinen on tarpeellisuusvaatimus, jonka mukaan työnantaja saa käsitellä vain työsuhteen kannalta tarpeellista tietoa. Toinen on lain neljännessä pykälässä määritellyt tietojen keräämisen edellytykset, missä todetaan, että työnantajan on kerättävä työntekijää koskevat henkilötiedot ensi sijassa työntekijältä itseltään. Toissijaisesti tietoja voidaan kerätä työntekijän antamalla kirjallisella suostumuksella, ennalta määritellyistä lähteistä. Suostumus ja sen merkitys on käsitelty myöhemmin luvussa 5.2.

Viranomaisen resurssit ovat vähentyneet jatkuvasti, ja samalla on turvallisuusselvityksen edellytyksiä tulkittu yhä tiukemmin. Tämä on johtanut siihen, että yhä useampi turvallisuusalan yritys on ryhtynyt tarjoamaan taustatarkistuspalveluita. Palveluntarjoajina on vartiointiliikkeitä, yksityisetsiväpalveluita sekä turvallisuuskonsultteja, mutta myös rekrytointiin erikoistuneita yrityksiä. Turvallisuusalan yritysten toiminta perustuu pitkälti rikosten paljastamistoimintaan, joka on määritelty laissa yksityisistä turvallisuuspalveluista. Laki yksityisistä turvallisuuspalveluista (2015/1085) määrittelee vartioimistehtävät seuraavasti: vartioimistehtävällä tarkoitetaan omaisuuden vartioimista, henkilön koskemattomuuden suojaamista sekä vartioimiskohteeseen tai toimeksiantajaan kohdistuneen rikoksen paljastamista sekä näiden tehtävien valvomista. Vartiointitehtävän on katsottu sisältävän myös ennalta tapahtuvan seurannan rikoksen paljastamiseksi. Viimeisessä kohdassa rikoksen ei ole tarvinnut vielä tapahtua, vaan siinä pyritään selvittämään, kohdistuuko toimeksiantajaan mahdollisesti rikollista toimintaa. Avoimien lähteiden tiedustelua voidaan

hyödyntää näissä tehtävissä, mutta samalla on huomioitava, mitä henkilötietojen käsittelystä on erikseen säädetty muualla lainsäädännössä.

Taustaselvityksistä puhuttaessa usein sekoitetaan kaksi termiä, poliisiviranomaisen suorittama turvallisuusselvitys ja turvallisuusyrityksen suorittama taustatarkistus. Merkittävimpänä erona näissä termeissä on, että turvallisuusselvityksen pääasialliset tietolähteet on määritelty Turvallisuusselvityslaissa (2014/726) sekä siihen liittyvässä asetuksessa, kun taas yksityisen toimijan tietolähteitä ei ole määritelty lainsäädännössä. Palvelujen markkinoinnissa helposti sekoittuvat termit taustatarkistus ja taustaselvitys on puolestaan määritelty suomenkielisessä standardissa, SFS-EN 15602 Turvallisuusalan toimittaja, terminologia.

Taustatarkistuksen suorittamiselle ei ole lainsäädännöllistä tai standardissa määriteltyä sisältöä, ja myöskään tietolähteitä ei ole sen suhteen määritelty. Tämän vuoksi onkin tärkeää, että tarkastuksia tekevillä olisi käytössä toimeksiantajan ohjeistus tai määritelmä niistä periaatteista, joilla taustatarkistus laaditaan. Toimeksiantajalle voi syntyä erityinen riski, jos taustatarkistuksen suorittava palveluntarjoaja syyllistyy rikokseen tietoja hankkiessaan. Mikäli palveluntarjoaja esimerkiksi käyttää laittomia menetelmiä, kuten tietokoneen tai puhelinten hakkerointia, pimeään verkkoon (engl. dark web) vuodettujen laittomien tietojen hyödyntämistä tai salassa pidettävän tiedon käyttöä, voi toimeksiantajalle syntyä merkittävä imagoriski. Lisäksi voi toiminnalla olla myös rikosoikeudellisia seurauksia toimeksiantajalle.

Kun tutkitaan kotimaisia ja ulkomaisia kirjallisuuslähteitä sekä millaisia ohjeistoja (engl. guidelines) tai eettisiä ohjeita muualta löytyy, on Suomessa nojauduttava vain lainsäädäntöön. Suomalaisista lähteistä ei ole löydettävissä tähän aihepiiriin liittyvää eettistä pohdintaa ainakaan laajemmalla foorumilla. Keskeisimmät toimintaa määrittävät lait ovat Euroopan unionin (EU) tietosuoja-asetus eli englanniksi General Data Protection Regulation (GDPR) sekä Suomen tietosuojalainsäädäntö ja laki yksityisyyden suojasta työelämässä. Erityisen olennaista on kaikille osapuolille ymmärtää, kuinka paljon tietosuojalainsäädäntö ja GDPR rajoittavat avoimien tietolähteiden tiedustelutiedon hyödyntämistä. Opinnäytetyössä pohdin lainsäädännön, etiikan ja ohjeiden merkitystä tiedustelua suorittavalle toimeksiantajalle, palveluntarjoajalle ja heidän työntekijöilleen.

Opinnäytetyön keskeinen kysymys on, ovatko yksityisen sektorin laatimat taustatarkistukset sekä eettisesti että lainsäädännöllisesti hyväksyttäviä. Opinnäytetyössä on kysymystä käsitelty voimassa olevan lainsäädännön puitteissa sekä eettisiin että ihmisoikeusarvoihin peilaten, ja lisäksi on kartoitettu tulevaisuuden teknologisen kehityksen tuomia haasteita. Yksityisen sektorin suorittaessa taustatarkistuksia tulee aina lähteä oikein toimimisen periaatteesta. Tämä tarkoittaa käytännössä, että taustatarkistusta laadittaessa tulee noudattaa lakia ja

eettisiä arvoja. Tämän lähtöolettaman vuoksi on työssä pyritty tuomaan esille niitä lähtökohtia, joiden tulee toteutua myös käytännön elämässä.

Opinnäytetyön lopputuloksena on tarkoitus lisätä ymmärrystä toiminnan mahdollisista riskeistä toimeksiantajalle sekä toisaalta avata toiminnasta saatavia hyötyjä. Avoimien tietolähteiden toimintaa voidaan hyödyntää esimerkiksi kyberturvallisuuden parantamisessa tai yritykseen kohdistuneiden uhkauksien selvittämisessä. Tarkoituksena on myös ohjata toimeksiantajia vaatimaan palveluntarjoajilta avoimuutta taustatarkistusprosessiin sekä toimintaa harjoittavia yrityksiä laatimaan ohjeistukset ja eettiset ohjeet tutkintaa suorittaville työntekijöilleen.

Opinnäytetyö on suunnattu kaikille, jotka hyödyntävät työssään avoimia tietolähteitä. Tähän ryhmään kuuluvat sekä yritysturvallisuuden parissa työskentelevät, yksityisellä turvallisuusalalla rikosten paljastamistehtävissä toimivat kuin avoimia tietolähteitä hyödyntävien palveluntarjoajien asiakasyritykset. Opinnäytetyössä tuodaan esille niitä eettisiä ongelmia, jotka liittyvät avoimista tietolähteistä kerättyyn tietoon sekä tiedon analysointiprosessiin taustatarkistuksen laatimisessa. Samoin tuodaan esille niitä lainsäädäntöön liittyviä haasteita, joita tulevaisuudessa, teknologian kehittyessä voi syntyä tiedon käyttämisen suhteen.

2 Tutkimuskysymys ja menetelmät

Opinnäytetyön tavoitteena on lisätä ymmärrystä hyödyistä ja haitoista, joita voi esiintyä, kun käytetään avoimia tietolähteitä yritysturvallisuuden taustatarkistuksiin joko rekrytoinnissa tai luotettavuuden selvittämisessä. Opinnäytetyössä on käytetty hyväksi laadullista tutkimusmetodia, jossa teoriaa on hyödynnetty tulkintojen tekemiseen kerätystä aineistosta. Aineistonkeruumenetelmissä on hyödynnetty kirjallisuustutkimusta. Yksilöhaastattelussa haastateltiin F-Securen Mikko Hyppöstä liittyen tulevaisuuden teknologiseen kehitykseen – keskittyen lähinnä tekoälyyn ja koneoppimiseen liittyviin näkemyksiin. Lisäksi tehtiin sähköpostikysely eri asiantuntijoille, jolla selvitettiin mahdollisia näkemyseroja asiantuntijoiden välillä.

Pertti Alasuutari toteaa kirjassaan *Laadullinen tutkimus 2.0.*, että metodin tulee olla sopusoinnussa tutkimuksen teoreettisen viitekehyksen kanssa. Jos aineisto koostuu pienestä joukosta yksilöhaastatteluita, sen pohjalta ei voi yrittää vastata kysymykseen siitä, miten vaikka tamperelaiset tai peräti kaikki suomalaiset suhtautuvat ulkomaalaisiin ja mitkä tekijät suhtautumistapoihin vaikuttavat. (Alasuutari 2011)

Tämän vuoksi opinnäytetyössä haastatteluja on käytetty pääasiassa kuvaamaan eri asiantuntijoiden näkemyseroja. Asiantuntijoiden näkemykset auttavat myös ymmärtämään,

missä määrin asiat nähdään yksimielisesti. Haastattelupyyntöihin ei vastannut oikeusoppineet tai tietosuojaan perehtyneet juristit, jonka vuoksi heidän näkemyksiään ei ole käytettävissä. Teoreettinen kehys nojaa tulkintaan lainsäädännön säädöksistä sekä miten niitä on tulkittu eri hallinto-organisaatioissa. Tällaisia toimivaltaisia hallinto-organisaatioita ja lähteitä ovat Suomessa oikeusasiamiehen toimisto, tietosuojavaltuutetun toimisto, oikeusministeriö sekä hallituksen esitykset perusteluineen. Eurooppalaisista säädöksistä merkittävin on Euroopan unionin tietosuoja-asetus sekä sen tulkintaan liittyen EU:n tietosuojaviranomaisten yhteistyöelin, tietosuojatyöryhmä (engl. European Data Protection Board). Kun yhdistellään sekä haastateltavien että hallinto-organisaatioiden näkemyksiä, voidaan opinnäytetyössä tehdä yleistäviä johtopäätöksiä kansallisen ja Euroopan unionin tason toiminnan laillisuudesta sekä eettisen pohdinnan tarpeesta.

Jotta aineistossa olevat havainnot voidaan erottaa tutkimuksen tuloksista, tarvitaan selkeä tutkimusmetodi. Metodi koostuu niistä käytännöistä ja operaatioista, joiden avulla tutkija tuottaa havaintoja, sekä niistä säännöistä, joiden mukaan näitä havaintoja voi edelleen muokata ja tulkita niin, että voidaan arvioida niiden merkitystä johtolankoina. (Alasuutari 2011)

Tutkimusmetodin avulla on opinnäytetyössä pyritty tuottamaan yhtenäinen kuva tutkimuskysymyksestä eli onko avointen tietolähteiden tiedustelun käyttäminen laillista taustatarkistuksien laatimisessa. Opinnäytetyössä keskitytään lähtökohtaisesti kahteen työelämän tilanteeseen, joissa taustatarkistuksia yleensä suoritetaan, eli rekrytoitavan taustantarkastamiseen sekä työntekijän luotettavuuden arviointiin työtehtävän vaihtuessa. Sisällöllisesti nämä kaksi tilannetta ovat lähes samanlaiset, minkä vuoksi esimerkkinä käytetään pääasiassa rekrytointia.

Opinnäytetyössä ei ole pyritty laatimaan käsikirjaa tai ohjeistusta taustatarkistuksien toteuttamiseen, vaan avaamaan niitä näkökulmia, mitä taustatarkistusta laatiessa tulisi huomioida. Vaikka monet esimerkit pohjautuvat empiiriseen kokemukseen, on niitä pyritty arvioimaan tieteellisin menetelmin. Kaikkia tässä työssä esitettyjä haasteita tai ongelmia on pyritty avaamaan sekä lainsäädännöllisestä että eettisestä näkökulmasta. Työssä on tietoisesti yhdistetty samankaltaisia tapauksia siten, etteivät ne ole yksilöitävissä yhteenkään asiakkaaseen tai henkilöön. Vain mediassa julkisuutta saaneet tapaukset on esitetty siten, kuten ne on mediassa uutisoitu.

Kirjallisuustutkimusta on työssä hyödynnetty lainsäädännön lisäksi myös eettisten näkemyksien pohdinnassa sekä teknisten määritelmien yhdenmukaistamisessa. Kirjallisuuslähteistä on pyritty analysoimaan avointen tietolähteiden käyttöön ja tiedusteluun liittyviä rajoitteita sekä nostamaan esille eettisiä kysymyksiä.

Kirjallisuustutkimuksessa tarkastellaan valittua ilmiötä kokoamalla ja analysoimalla tätä ilmiötä koskevaa tutkimuskirjallisuutta. On hyvä huomata, että koska tutkimuskirjallisuus edustaa ilmiötä – kuten jäkälätutkijalle ilmiötä edustavat luonnosta kerätyt jäkälänäytteet – ei eroa tutkimusaineiston ja lähdeaineiston välillä tyypillisesti tehdä suoraan. Poikkeuksen muodostavat sellaiset tutkimukset, joissa tutkittavana ilmiönä on jokin tutkimus, teoria tai muu lähestymistapa. (Aalto-yliopisto 2021)

Tutkimuskirjallisuus on sisältänyt tieteellisiä tutkimuksia ja artikkeleita. Tämän lisäksi on tutkimusta varten käyty läpi taustatarkistuksiin erikoistuneiden eurooppalaisten lakitoimistojen artikkeleita liittyen yksityisyyden suojaan ja due diligence (engl.) -palveluihin sekä koottu yhdysvaltalaisista lähteistä taustatarkistusten kuluttajansuojaan liittyviä aineistoja. Erityisesti taustatarkistuksien kuluttajansuoja on mielenkiintoinen aihepiiri, sillä EU:n alueelta en löytänyt tähän liittyen tutkimuksia tai viranomaisten kannanottoja. Yhdysvalloissa taas kuluttajansuojajärjestöt ovat nostaneet kanteita taustatarkistuspalveluita tarjoavia yrityksiä vastaan, johtuen lähtökohtaisesti epäluotettavista tai paikkansa pitämättömistä taustatarkistusraporteista. Kuluttajansuojajärjestöt ovat näissä kanteissa edustaneet lähtökohtaisesti taustaselvityksen kohteena ollutta henkilöä.

Lähteiden analysointia on tehty vertaamalla aineistoja lainsäädäntöön sekä viranomaisten tulkintaan laista. Haastattelujen sisältöjä on työssä käytetty sellaisinaan eli kuten asiantuntijat ovat vastanneet kysymyksiin. Asiantuntijoiden näkemyksille on pyritty löytämään vahvistus lainsäädännöstä tai tieteellisestä tutkimuksesta. Tässä on hyvä kuitenkin huomata, että asiantuntijat vastaavat sekä oman lainsäädännön tulkinnan näkemyksensä että empiirisen kokemuksensa perusteella. Laintulkinnan osalta on asiantuntijoilla hyvin yhtenäinen näkemys, mutta empiirinen kokemus, esimerkiksi avointen tietolähteiden tiedustelusta, voi aiheuttaa eroja näkemyksiin.

3 Avoimet tietolähteet ja tiedustelu

Avointen lähteiden tiedustelu (engl. open source intelligence) on tavanomaisoikeuden perusteella sallittu tiedustelulaji. Avointen lähteiden sisältämä informaatio on kaikille tarkoitettu ja se on myös jokaisen saatavilla. Avointen lähteiden tiedustelutieto on siis kaikkien saatavilla olevista lähteistä hankittua informaatiota. Avointen lähteiden tiedustelu ei puutu perus- ja ihmisoikeuksiin, ja siksi siitä ei ole ollut tarpeen säätää laissa. (Lohse ym. 2019)

Määritelmän mukaan voivat avoimet tietolähteet olla ilmaisia tai maksullisia, mutta olennaista on, että ne sisältävät yleisesti saatavilla olevaa tietoa. Avoimia tietolähteitä ovat esimerkiksi Suomen Asiakastieto Oy:n maksulliset yritystietoraportit tai Spokeo-

verkkopalvelusta ostetut henkilöraportit. Spokeo on yhdysvaltalainen palvelu, josta voi ostaa henkilöraportteja. Raporteista ilmenee laajasti eri rekistereistä löytyviä tietoja henkilöstä, kuten yhteystietoja, osoitetietoja, sosiaalisen median tilejä sekä muuta kyseiseen henkilöön yhdistettyä tietoa. Palvelusta löytyy pääsiassa Yhdysvaltojen kansalaisten tietoja sekä maassa pitkään oleskelleiden henkilöiden tietoja.

Hallituksen esitys eduskunnalle laiksi sotilastiedustelusta sekä eräiksi siihen liittyviksi laeiksi määrittelee, että tyypillisiä avoimia tiedonlähteitä ovat muun muassa kirjallisuus, tilastot, kartat, lehdet, yksityisten ja viranomaisten julkaisut, viranomaisten julkiset rekisterit ja tietokannat, yleisölle suunnatut televisio- ja radiolähetykset sekä tietoverkon ja sosiaalisen median sisällöt. Internetiä ei avointen lähteiden tiedustelussa käsitetä omana tiedonlähteenään, vaan kanavana, josta tietoa hankitaan. Avointen lähteiden tiedustelu voidaan jakaa tiedonhankintaan sekä mediaseurantaan, jonka pääasiallisena tarkoituksena on tukea tiedustelutilannekuvan muodostamista. Määritelmä ei ole muuttunut valiokuntakäsittelyssä. (HE 203/2017)

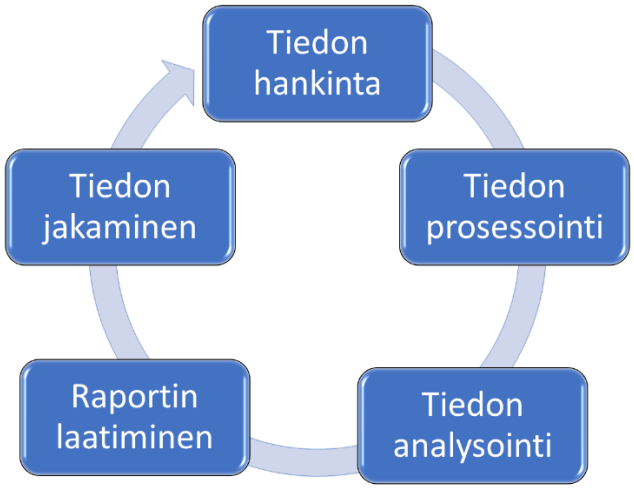
Sosiaalisen median tiedustelulla (engl. social media intelligence, SOCMINT) tarkoitetaan julkisista sosiaalisen median profiileista suoritettavaa tietojen keruuta ja analysointia. SOCMINT voidaan määritellä sosiaalisen median verkostoissa olevan tiedon analyyttiseksi hyödyntämiseksi. Määritelmä tunnistaa sosiaalisen median sisällön mahdollisuutena ja haasteena avoimen lähdekoodin tutkimuksille (Trottier 2015).

Sosiaalisen median tiedustelua ei kaikkialla pidetä osana avoimen tietolähteen tiedustelutoimintaa, koska sosiaalisen median profiilit voivat olla julkisia tai yksityisiä. Haasteelliseksi nousee esimerkiksi sellaisen sosiaalisen median käyttäjän profiilin katsominen, joka on yksityinen. Profiilin näkemiseen tarvitaan käyttäjän hyväksyntä, ja luvan saamista tilin omistajaa harhauttamalla ei voida pitää avointen lähteiden tiedusteluna. Toisin sanoen, jos tiedustelua suorittava harhauttaa profiilin omistajaa luulemaan häntä muuksi kuin tiedustelija todellisuudessa on, toiminnan ei voida katsoa olevan avointen tietolähteiden tiedustelua. SOCMINT-tiedustelu on hyväksytty tiedustelun muoto monissa maissa, mutta Suomessa on katsottu, että harhauttamalla suoritettu tiedustelu viranomaisen suorittamana on kyseenalaista.

Tiedustelutoiminnalla yleisesti tarkoitetaan tiedon hankintaa eri keinoilla, tiedon prosessointia ja analysointia sekä tiedon jakamista asiakkaalle. Tiedustelu jaetaan osa-alueisiin tiedonhankintatavan perusteella, kuten avoimien tietolähteiden tiedustelu, sosiaalisen median tiedustelu, signaalitiedustelu, teletiedustelu, henkilötiedustelu, geo- ja paikkatiedustelu sekä tekninen tiedustelu. Näistä yksityisen sektorin käytettävissä ovat laillisesti vain avoimien tietolähteiden tiedustelu, sosiaalisen median tiedustelu, geo- ja paikkatiedustelu ja henkilötiedustelu. (Loshe & Viitanen 2019)

Määritelmän mukaan henkilötiedustelu (engl. human intelligence, HUMINT) on henkilökohtaiseen kanssakäymiseen taikka henkilön tai henkilöryhmän havainnointiin perustuvaa tiedonhankintaa, kuten tarkkailua. Geo- ja paikkatiedustelussa on kyse tiettyyn paikkaan tai laajempaan alueeseen ja siinä vallitseviin olosuhteisiin kohdistuvasta tiedonhankinnasta. Geotiedustelulla (engl. geospatial intelligence, GEOINT) tarkoitetaan tiedon hankkimista alueellisesta toimintaympäristöstä ja sen olosuhteista. Avoimien lähteiden ja sosiaalisen median tiedustelu on käsitelty laajemmin muualla tässä työssä. (Loshe & Viitanen 2019)

Tiedusteluprosessin kulku on hyvin yksinkertainen. Se muistuttaa paljon tieteellisen tutkimuksen prosessia, joskaan prosessi ei ole yhtä tarkka ja säännelty kuin tieteellisessä tutkimuksessa. Yleensä lähtökohtana on jokin tutkimuskysymys eli on tarve tietää syvemmin henkilöstä, asiasta tai kohdealueesta. Tämän johdosta ryhdytään keräämään tietoa eri lähteistä, arvioiden aina lähteen luotettavuutta ja tiedon jakamisen motiiveja. Kun tietoa on kerätty runsaasti, voidaan tietoa ryhtyä prosessoimaan. Prosessoiminen voi olla tiedon järjestämistä eri luokkiin, esimerkiksi tiedon lähteen tai lähteen luotettavuuden perusteella. Tiedon analysoinnissa pyritään aktiivisesti tunnistamaan, järjestämään ja sanoittamaan tehtyjä havaintoja. Analysoinnissa tehdyistä johtopäätöksistä, kuten trendi- ja muista havainnoista, laaditaan asiakkaalle raportti. (Loshe & Viitanen 2019)



Kuva 1. Tiedusteluprosessin kehä. Kuvassa on kuvattu kehällä tiedusteluprosessin kulku eri vaiheineen. Tiedon jakaminen saattaa nostaa uusia kysymyksiä, jolloin kehä käynnistyy uudelleen.

Avoimien tietolähteiden tiedustelu on siis laillista, kaikille avoimen tiedon hyödyntämistä. Kuten tiedustelussa yleisestikin on yksittäinen avoimen lähteen tieto usein merkitykseltään vähäinen, mutta avoimista tietolähteistä kootun tietomassan analysointi voi tuottaa tarkan profiilin henkilöstä tai auttaa luomaan selkeän tilannekuvan kriisitilanteessa.

4 Avointen tietolähteiden tiedustelun työkalut ja työmenetelmät

”Perinteinen OSINT:in kirous on se, että kun lähteet ovat ilmaisia, ala on aliarvostettu ja aliresursoitu. Avointen lähteiden tiedustelu vaatii osaamista, resursseja ja työkaluja”, sanoo suojelupoliisin erikoistutkija Veli-Pekka Kivimäki. (Vainio 2021)

Avointa tietoa on saatavilla yhä helpommin. Yli 4,6 miljardia ihmistä käyttää internetiä, pääosin älypuhelimella, ja lataa päivittäin verkkoon sisältöjä 2,5 kvintiljoonaa tavua. Verkossa olevan datan määrän odotetaan vain kasvavan lähivuosina. Avoimia lähteitä hyödyntävät niin amatöörit, järjestöt kuin yksityiset organisaatiot, ja usein ne haastavat jopa valtioiden tiedusteluorganisaatiot. Samaan aikaan monimutkaiset sekä eri aloihin vaikuttavat uhat ja teknologian jatkuva kehitys lisäävät tarvetta tehokkaammalle tiedustelutiedon keräämiselle ja analysoinnille. Tämä on tuonut mukanaan uuden ilmiön, jossa valtiolliset organisaatiot ovat yhä riippuvaisempia yhteistyöstä yritysten kanssa. (Vainio 2021)

Yhä useammin valtiolliset tiedusteluorganisaatiot ovat riippuvaisia myös palveluntarjoajien kanssa tehtävästä yhteistyöstä, mitä on pyritty esimerkiksi Yhdysvalloissa mahdollistamaan lainsäädännön avulla. Valtiolliset tiedustelupalvelut hyödyntävät muun muassa Googlen, Applen, WhatsAppin, Twitterin sekä muiden haku- ja sosiaalisen median palveluntarjoajien tietokantoja omassa toiminnassaan. Samoin tiedusteluorganisaatiot pyrkivät vaikuttamaan salausohjelmien valmistajiin, jotta niissä voitaisiin purkaa esimerkiksi sähköpostien salauksia tarvittaessa.

Vuoteen 2018 asti Yhdysvaltain keskustiedustelupalvelu (engl. Central Intelligence Agency, CIA) omisti salaa useiden valtioiden käyttämän salausohjelman valmistajan Crypto AG:n. CIA loi salausohjelmaan useita takaportteja (engl. backdoors), joiden avulla voitiin tarkkailla eri valtioiden salaista tiedonvaihtoa. Operaatio tuli tunnetuksi nimellä Rubicon, ja se oli sekä luonteeltaan röyhkeä että laajuudeltaan ennennäkemätön. Operaatiossa tiedustelutietojen keräämisen kohteena olivat sekä viholliset että liittolaiset. Washington Post -lehden lainaaman CIA:n raportin mukaan Operaatio Rubicon oli "vuosisadan tiedusteluvallankaappaus". (Winder 2020)

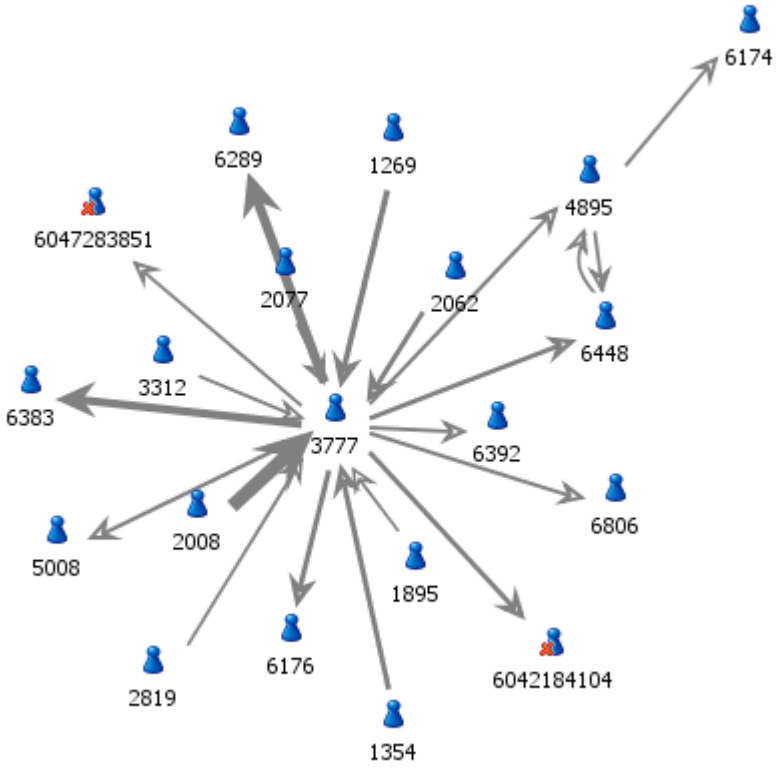
Siinä vaiheessa, kun valtiollinen tiedusteluorganisaatio ryhtyy valmistamaan ja markkinoimaan tietoturvaan liittyviä ohjelmia, on asiakkaan vaikea tietää, ovatko tiedot turvassa vai kyseisen organisaation hyödynnettävissä. Vielä ongelmallisempaa on, jos kyseisen organisaation tehtävänä on myös tukea oman maan yritysten kilpailukykyä ja hankkia kilpailuetua globaaleilla markkinoilla. Vaarana onkin, että hyödyntämättömästä tiedustelutiedosta tulee myyntituote, jota tarjotaan tiedustelupalveluita tarjoaville yksityisille tiedusteluyrityksille.

On usein sanottu, että hakupalveluiden ja sosiaalisen median käyttämien algoritmien ansiosta ja käyttäjien verkkotoiminnasta kerättyjen profiilien johdosta tuntevat yhtiöt käyttäjänsä

paremmin kuin käyttäjät itse luulevat tuntevansa itsensä. Tämä voi pitää paikkansakin, sillä algoritmit ja koneoppimisessa tietokone eivät pyri miellyttämään suurta yleisöä. Ne toimivat juuri siten, kuten ne on ohjelmoitu toimimaan, ja keräävät kaikista käyttäjän suorittamista toiminnoista tietoa. Tämän tiedon pohjalta rakennetaan käyttäjäprofiili, jota hyödynnetään markkinoinnin kohdentamisessa tai parhaiden hakutulosten tuottamisessa.

Avointen tietolähteiden tiedusteluun on tarjolla sekä kaupallisia että ilmaisia open source (engl.) -työkaluja. Hakukoneilla, kuten Google-palvelulla, voidaan suorittaa laaja-alaista tiedustelua sekä löytää monia olennaisia tietolähteitä. Sosiaalisen median tiedustelussa ovat käytettävissä yleisimmät sovellukset, kuten LinkedIn, Twitter, Facebook, Instagram, PIPL, Peek You, Name Chk ja muut vastaavat palvelut. Lisäksi sosiaalisen median tiedusteluun on kehitetty monia ohjelmia, jotka hyödyntävät sosiaalisen median heikkouksia tiedonkeruussa. Yksi tällainen ja kohua herättänyt palvelu oli vuonna 2013 julkaistu hollantilaisen hakkerin tekemä Stalkscan-sivusto, jonka avulla oli mahdollista etsiä Facebookista sen käyttäjien tietoja.

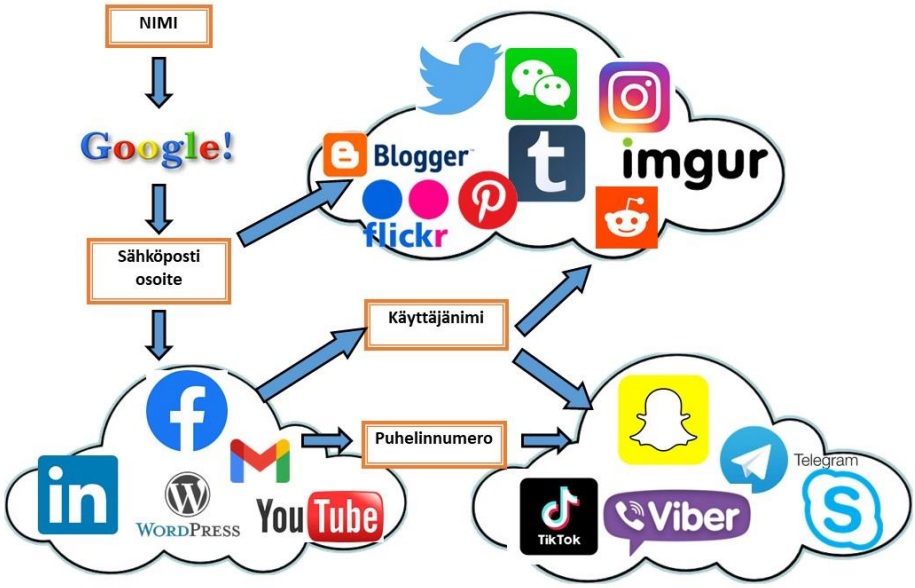
Toinen, varsinkin sosiaalisen median avulla luotava tiedon lähde on verkostoanalyysi eli suhdeverkostokartta. Verkostoanalyysi on graafinen esitys yksilön suhteista eli keitä ihmisiä tämä tuntee. On olemassa useampia ohjelmistoja, joiden avulla on mahdollista yhdistää sosiaalisen median kontaktit graafiseksi esitykseksi. Tästä prosessista käytetään englanninkielisiä termejä Social Network Analysis tai Human Network Analysis, joiden avulla on mahdollista luoda kuvaus siitä, kuka tuntee kenetkin.



Kuva 2. Esimerkki Social Network Analysis -kaaviosta. (themainstreamseer)

Yksi kaupallisista toimijoista, eteläafrikkalainen Maltego, on kasvattanut suosiotaan OSINT-kentällä. Maltego on avoimen lähdekoodin tiedustelu- ja graafinen analyysityökalu, jota käytetään tiedon keräämiseen ja tietojen yhdistämiseen tutkintatehtäviä varten. Maltego on Java-sovellus, joka toimii Windowsissa, Macissa ja Linuxissa. Maltegoa käytetään laajasti, aina turvallisuusalan ammattilaisista oikeuslääketieteellisiin tutkijoihin, tutkiviin toimittajiin ja tutkijoihin. Muun muassa Bellingcat-yhteisön tiedetään käyttäneen Maltego-sovellusta Ukrainassa alas ammutun Malaysia Airlinesin lennon 17 tutkinnan yhteydessä.

Alla on esitetty kuvassa 3, miten yksinkertaisimmillaan avoimien tietolähteiden tiedustelu toimii. Syöttämällä Google-hakupalveluun henkilön nimen, voidaan löytää henkilön sosiaalisen median tili tai sähköpostiosoite. Sähköpostiosoitteen tai sosiaalisen median tilin kautta voidaan löytää henkilön puhelinnumero. Sosiaalisen median käyttäjänimellä voidaan löytää useampia eri tilejä sosiaalisen median muilta alustoilta. Myös puhelinnumerolla voidaan löytää erilaisia tilejä, joiden luomisessa käytetään puhelinnumeroa.



Kuva 3. Kuvaus avoimien tietolähteiden tiedustelun prosessin etenemisestä.

Edellä kuvatuilta sosiaalisen median alustoilta voidaan löytää paljon tietoa henkilöstä, vaikka henkilön tili ei olisikaan julkinen. Näiden tietojen avulla voidaan tehdä johtopäätöksiä henkilön verkostoista, asuinpaikasta, matkustelusta, harrastuksista, kiinnostuksen kohteista sekä perhesuhteista. Yhdenvertaisuuslaissa (2014/1325) määritellään tietoja, jotka ovat syrjintäkiellon alaisia, kuten ikä, alkuperä, kansalaisuus, kieli, uskonto, vakaumus, mielipide, poliittinen toiminta, ammattiyhdistystoiminta, terveydentila, vammaisuus tai seksuaalinen suuntautuminen. Myös näitä tietoja on kuitenkin usein mahdollista hankkia sosiaalisen median avulla. Sosiaalisen median tilien avulla voidaan löytää tietoa henkilön nettikäyttäytymisestä, kuten muun muassa siitä kuinka avoimesti henkilö jakaa tietoa yksityiselämästään. Analyysia voidaan tehdä myös erilaisten julkisten keskustelufoorumien, videoblogien, blogien, kuvien ja videoiden jakopalveluiden sekä muiden vastaavien lähteiden avulla.

Foorumien, sosiaalisten verkostojen tai median laaja käyttö sekä olemassa olevan tiedon suuri määrä tekevät OSINT-toiminnasta seuraavan internetin kultakaivoksen. Tiedon hankkiminen julkisista lähteistä on tapa ratkaista olemassa olevia ongelmia erilaisesta ja innovatiivisesta näkökulmasta. Erityisesti kyberturvallisuus ja kyberpuolustus voivat hyötyä suuresti tuloksista, joita tämäntyyppinen älykkyys voi tarjota. Tämän johdosta olisikin hyvä ottaa käyttöön automatisoidut OSINT-prosessit, jotka pystyvät viemään tutkimukset internetin kaikkiin osiin ja laajentamaan mieliä verkon kautta. (Pastor-Galindo ym. 2020)

Pastor-Galindo ja muut tutkijat näkevät suurena mahdollisuutena sen, että avointen tietolähteiden tiedustelussa hyödynnetään laajasti sosiaalista mediaa, internetin käyttöä ja keskustelufoorumien sisältämää dataa. Tutkijat pitävät tekoälyn ja koneoppimisen hyötyjä

merkittävinä juuri tiedonkeruulle ja analysoinnille. Samalla, kun tämä on nähtävä suurena mahdollisuutena, se saattaa olla myös Pandoran lippaan avaamiseen rinnastettava teko. Teknologiaa voidaan käyttää hyödylliseen tarkoitukseen, esimerkiksi kyberhyökkäyksien torjumiseen, mutta sillä on laajat mahdollisuudet tulla käytetyksi myös rikolliseen toimintaan. Tekoälyn ja koneoppimisen ongelmallisuutta käsitellään opinnäytetyön luvussa 9.

5 Kansainvälinen ja EU-lainsäädäntö

Taustatarkastuksien osalta on olennaista ymmärtää, että yksityisyydensuojan taso vaihtelee merkittävästi eri maissa. Kansainvälisellä näkökulmalla alla tarkoitetaan Euroopan unionin ulkopuoleisia maita, pois lukien Iso-Britannia, jossa lainsäädäntö on Euroopan unionin Tietosuoja-asetusta vastaava. Eurooppalaisella lainsäädännöllä viitataan Euroopan unionin alueeseen, jossa Euroopan unionin Tietosuoja-asetus määrittelee yksityisyydensuojan ja henkilötietojen käsittelyn hyvin tarkkarajaisesti.

5.1 Avoimien tietolähteiden tiedustelu ja lainsäädäntö — kansainvälinen näkökulma

Monesti eri foorumeilla esitetään kysymys siitä, miten laillista avointen tietolähteiden tiedustelu on. Vastaus ei ole aivan yksinkertainen, sillä laillisuus riippuu muun muassa sen maan lainsäädännöstä, missä tiedustelua tehdään sekä suorittavasta tahosta ja käyttötarkoituksesta. Avoimien tietolähteiden tiedustelu sinällään ei ole laitonta toimintaa, mutta kerättyjen tietojen muodostamat rekisterit sekä henkilötietojen käyttö voivat muodostua laittomiksi. Myös tiedon käyttötarkoituksella on merkittävä syy-yhteys, kuten sillä kerätäänkö tietoa estämään valtiollisen toimijan hirmutekoja vai pyritäänkö yksilöimään joidenkin henkilöiden taustatietoja ja poliittista suuntautumista esimerkiksi päätöksentekoa varten. Opinnäytetyön luvussa kuusi käsitellään avoimien tietolähteiden hyödyntämisen rajoitteita Euroopan maissa, mutta myös kansainvälisesti on käyty keskustelua tähän liittyvistä eettisistä kysymyksistä sekä vaikutuksista ihmisoikeuksien toteutumiseen.

Avoimen tietolähteen tiedustelun työkaluja on käytetty enenevissä määrin yksityisellä turvallisuussektorilla sekä myös valtiollisten toimijoiden, kuten tiedusteluviranomaisten tai poliisien, keskuudessa. Uuden tiedonkeruumenetelmän vaikutuksia tulisikin lisääntyvän käytön johdosta pohtia ja miettiä mahdollisuuksia käyttää menetelmää vastuullisella tavalla sekä teoriassa että käytännössä. Esimerkiksi voidaan nostaa, että useimmissa länsimaisissa yhteiskunnissa on jo olemassa tiukkaa lainsäädäntöä puhelimien tai internetliikenteen salakuunteluun liittyen, mutta sosiaalisen median sivustoilta tai sovelluksilla kerättävään dataan ei ole yhtä ilmiselvää sääntelyä olemassa.

Monet turvallisuusviranomaiset eivät luultavasti näe tarvetta lisätä OSINT-toiminnan vastuullisuutta. Viranomaiset voivat esimerkiksi esittää, että sosiaalisen median sivustojen

tieto on julkista ja kuka tahansa voi käyttää niitä. Erona satunnaisen käyttäjän ja turvallisuusviranomaisen välillä on kuitenkin, että OSINT-toiminnalla voidaan välillisesti tai suoraan vaikuttaa tiedustelun kohteen yksityiselämään tai tulevaisuuden mahdollisuuksiin. Ihmisoikeuksien näkökulmasta tulisi erityisesti näiden sivuvaikutusten olla oikeassa suhteessa. (Eijkman & Weggemans 2013)

Eijkman ja Weggeamans ottavat tieteellisessä artikkelissaan kantaa avoimista tietolähteistä kerätyn tiedon lopulliseen käyttötarkoitukseen. Tutkijoiden mukaan on eroa, käyttääkö sosiaalisen median profiilista saatua tietoa profiilin omistajan oma kontakti saadakseen tietää omistajan viimeisimmät kuulumiset vai yksityinen yritys profiloidakseen tai arvioidakseen rekrytoitavan henkilön luotettavuutta ja sopivuutta yritykseen työntekijäksi. On myös huomioitava tilanteet, joissa valtiollinen tiedusteluorganisaatio pyrkii seulomaan sosiaalisen median profiilien avulla tietyn mielipiteen omaavia kansalaisia ja kohdistamaan heihin laajamittaista tiedustelutoimintaa.

Kun tarkastellaan asiaa eettisestä näkökulmasta, avointen lähteiden tiedustelun ongelmakohtana voidaan pitää ihmisoikeuksien ja yksilön tietosuojan toteutumista. OSINT on hyvä työkalu paljastamaan valtioiden sortotoimia vähemmistöjä kohtaan, mutta sitä voidaan käyttää myös näiden sortotoimien kohteiden määrittelyyn ja tiedon keräämiseen halutuista henkilöistä. Valtio voi kartoittaa esimerkiksi toisinajattelijoita sosiaalisen median tai viestipalveluiden kautta, jolloin yksilönvapaus on uhattuna merkittävässä määrin.

5.2 Lainsäädännön rajoitukset Euroopassa

Avoimien tietolähteiden hyödyntäminen yritysturvallisuudessa on lainsäädännön puitteissa yksinkertaista, kunnes toiminnassa ryhdytään käsittelemään luonnollisen henkilön henkilötietoja. Tällöin mukaan tulevat rajoitukset Euroopan yleisestä tietosuoja-asetuksesta sekä sitä täydentävästä tietosuojalaista. EU:n tietosuojalain mukaisesti henkilötiedoilla tarkoitetaan kaikkia tietoja, jotka koskevat tunnistettua tai tunnistettavissa olevaa henkilöä. Toisin sanoen kyseessä on tieto, jonka perusteella henkilö voidaan yksilöidä suoraan tai välillisesti yhdistämällä eri tietoja yhteen.

Käytännön tasolla on esimerkiksi henkilön luotettavuuden selvittämisessä tai taustatarkistuksen laatimisessa kyse tällaisesta toiminnasta. Henkilöstä kerätään tietoa eri avoimista tietolähteistä, joita voivat olla yritysrekisterit, oikeusistuinten tuomiot, mediassa esiintyneet artikkelit, matrikkelit, tieteelliset julkaisut, haastattelut ja organisaatioiden tiedotteet. Näiden kerättyjen tietojen pohjalta laaditaan raportti toimeksiantajalle. Tässä prosessissa selvityksen kohteena olevan henkilön anonymisointi on mahdotonta, jolloin selvityksen tekijä joutuu käsittelemään henkilötietoja.

EU:n tietosuojasääntely edellyttää, että tietoja käsitellään asianmukaisesti ja lainmukaisesti, tiettyä ja laillista tarkoitusta varten. Yrityksen on huolehdittava siitä, että käsitelläkseen henkilötietoja sen toiminta täyttää jonkin seuraavista ehdoista:

- yritys on saanut asianomaisen henkilön suostumuksen
- yritys tarvitsee henkilötietoja täyttääkseen sopimusvelvoitteen henkilön kanssa
- yritys tarvitsee henkilötietoja laillisen velvoitteen täyttämiseksi
- yritys tarvitsee henkilötietoja suojellakseen henkilön elintärkeitä etuja
- yritys käsittelee henkilötietoja yleisen edun mukaisen tehtävän suorittamiseksi
- yritys toimii oikeutetun etunsa puitteissa niin kauan, kun sillä ei ole vaikutusta tietojen käsittelyn kohteena olevan henkilön perusoikeuksiin ja -vapauksiin. Jos henkilön oikeudet ohittavat yrityksen edut, henkilötietoja ei voida käsitellä. (EU 2016)

Nath Solicitors Limited on lakitoimisto Lontoossa, joka on erikoistunut henkilön yksityisyydensuojaan ja EU:n tietosuoja-asetuksen vaatimusten täyttämiseen. Yritys on myös laatinut listan siitä, mitkä ovat tärkeimmät GDPR-periaatteet OSINT-tiedustelua käyttävien yritysten kannalta:

- yrityksen on ymmärrettävä, milloin se on rekisterinpitäjä tai tietojenkäsittelijä
- yrityksellä on oltava oikeusperusta henkilötietojen käsittelyyn
- yrityksen on noudatettava tiettyjä periaatteita henkilötietojen käsittelyssä
- yrityksen on ymmärrettävä ja kunnioitettava rekisteröityjen erityisiä yksityisyyden- ja tietosuojaoikeuksia.

Lähtökohta toiminnalle on aina, että kohdehenkilön suostumuksella voidaan suorittaa taustatarkistus tai luotettavuuden arviointi. Suositusten mukaan suostumuksen tulee olla kirjallinen ja suostumuksen antajan tulee ymmärtää, mihin hän suostuu. Suostumuksen tulee olla vapaaehtoinen, yksilöity, ja sen tulee olla suostumuksen antajan tietoinen aktiivinen päätös. Tämä sulkee pois esimerkiksi rekrytointilomakkeessa tai työsopimuksessa olevan sanallisen ilmaisun, jolla annetaan työnantajalle oikeus seurata henkilön sosiaalista mediaa. On tärkeää huomioida, että koska kyseessä on niin sanottu ”loukatun suostumus”, voi suostumuksen antaja peruuttaa suostumuksensa milloin tahansa. Suostumuksen peruuttaminen tarkoittaa, että henkilötietojen käsittely tulee keskeyttää välittömästi. Tämän lisäksi kaikki kerätyt tiedot on tuhottava, sillä laillista perustetta henkilötietojen käsittelyyn ei enää ole.

Jos sosiaalisessa mediassa julkaisun tarkoitus on ainoastaan journalistinen, kirjallinen tai taiteellinen, siihen ei sovelleta useimmissa tapauksissa GDPR:n velvoitteita. Monilla sosiaalisen median alustoilla on käyttäjä hyväksynyt käyttöehdoissa muun muassa tietojen

käyttämisen muuhun tarkoitukseen, kuten niiden kopioimisen ja julkaisun muilla alustoilla. Tässä on tärkeää huomioida, että tietoja palvelun ulkopuolelle tallennettaessa tietosuoja tulee voimaan. Muun muassa EU:n työryhmä, Data protection working party 2013, on linjannut, että on muistettava kaikkien tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvien tietojen, julkisesti saatavilla olevien ja muiden, olevan henkilötietoja. Lisäksi pelkästään se, että tällaiset tiedot on asetettu julkisesti saataville, ei johda vapautukseen tietosuojalaista. Avoimia tietolähteitä käytettäessä on hyvä myös huomioida, että esimerkiksi yksilöitävä käyttäjätunnus on sosiaalisessa mediassa julkinen, mutta kun tuodaan käyttäjätunnus esimerkiksi taustatarkistusraporttiin, se muuttuu GDPR:n mukaan henkilötiedoksi.

Erityisen vaikeaa on rajanveto sen välillä, missä roolissa taustatarkistusta laadittaessa toimitaan eli määritelläänkö taustatarkistuksen laatija tietojen käsittelijäksi vai rekisterin pitäjäksi. Käsittelyn aikana henkilötiedot saattavat myös kulkea useiden yritysten tai organisaatioiden kautta. Euroopan yleisen tietosuoja-asetuksen (EU 2016/679) mukaan henkilötietojen käsittelyssä on aina kaksi toimijaa, jotka hoitavat henkilötietojen käsittelyä:

- Rekisterinpitäjä - päättää henkilötietojen käsittelytarkoituksesta ja -tavasta.
- Henkilötietojen käsittelijä - säilyttää ja käsittelee tiedot rekisterinpitäjän puolesta.

Roolit eivät eroa merkittävästi tietosuojan, salassapidon ja tietojen turvallisen säilyttämisen näkökulmasta, sillä samat vaatimukset koskevat molempia. Rekisterinpitäjällä on oikeus määritellä, mitä tietoja kerätään, miksi ja miten niitä käytetään, ja henkilötietojen käsittelijällä on velvollisuus noudattaa rekisterinpitäjän määräyksiä. Vastuiden selkeyttämiseksi tämän roolijaon tulisi olla selvä työn tilaajan ja palveluntarjoajan välillä.

Lakitoimisto Nordic Law on keskittynyt liikejuridiikkaan ja yritysjärjestelyihin, ja yrityksen palveluihin kuuluvat muun muassa due diligence (engl.) -palvelut yrityskauppojen yhteydessä. Lakitoimiston verkkoartikkelissa, joka koskee due diligence -prosessia ja EU:n yleisen tietosuoja-asetuksen vaikutuksia siihen, todetaan, että prosessissa ainut varteenotettava tietojen käsittelyperuste on rekisteröidyn antama suostumus. Mikään muu peruste ei tässä tilanteessa voi tulla lainmukaisesti sovellettavaksi. Tällöinkin on tosin huomattava tietosuoja-asetuksen suostumukselle asettamat tiukat kriteerit, minkä takia suostumuksen käyttäminen käsittelyperusteena on hyvin herkästi lain vastainen. Lisäksi on huomattava, että harvemmin syntyy sellaista mahdollisuutta, jossa yrityskaupan osapuolet voisivat due diligence -vaiheessa tiedustella rekisteröityjen suostumuksen perään, sillä due diligence -vaihe on käytännössä aina luottamuksellinen. (Nordic Law 2019)

Tämä sama käsittelyperiaate koskee myös avoimien tietolähteiden tiedustelua silloin, kun kohteena on luonnollinen henkilö. Esimerkiksi rekrytoitavan henkilön taustatarkistusta tehtäessä henkilön suostumus on ainoa lain mukainen käsittelyperuste. Siinäkin on

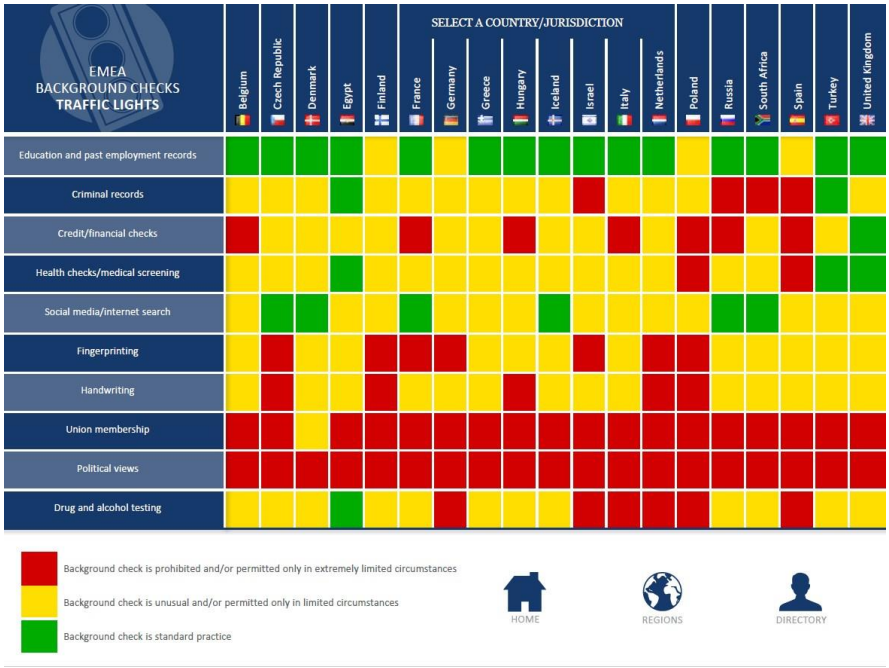
huomioitava, että luonnollinen henkilö voi koska tahansa peruuttaa suostumuksensa. Mikäli henkilö peruuttaa suostumuksensa, on prosessi keskeytettävä välittömästi sekä kerätyt henkilötiedot on tuhottava. Kuten aiemmin on todettu, suostumus tarkoittaa vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua, jolla luonnollinen henkilö suostuu taustatarkistusprosessiin. Prosessista tulee antaa kohteelle selkeä selvitys, mitä tietoja käsitellään sekä mitä tietolähteitä selvityksessä käytetään.

Toinen henkilötietojen käsittelyperuste, joka voi tulla kyseeseen, on lainmukainen käsittelyperuste. Tässä tapauksessa rekisterinpitäjän tulee yksiselitteisesti kyetä osoittamaan lainmukainen peruste ja laillinen tarkoitus, ja pääsääntöisesti tällöin on kyseessä sopimus tai muu oikeutettu etu. Mikäli henkilötietojen käsittelyltä puuttuu asianmukaisuus ja lainmukaisuus, on henkilötietojen käsittely lainvastaista.

Mayer Brown on globaali lakitoimisto, jolla on toimintaa 26 eri maassa ympäri maailmaa. Lakitoimisto on erikoistunut muun muassa yritysjuridiikkaan, pankki- ja talouselämään, tietosuojaan ja kyberturvallisuuteen, yritysturvallisuuden sekä kansainvälisen kaupan juridiikkaan. Lakitoimiston tietosuojaosaamista pidetään yleisesti erittäin luotettavana, minkä vuoksi yrityksen julkaisemia materiaaleja voidaan pitää korkealaatuisina.

Mayer Brow -lakitoimiston infograafista (kuva 4) voidaan havaita, että myös EU-maiden välillä on eroja, vaikka niissä kaikissa noudatetaan samaa EU:n yleistä tietosuoja-asetusta. Esimerkiksi työnhakijan luottotietojen selvittäminen on kiellettyä Belgiassa, Ranskassa, Unkarissa, Italiassa, Puolassa ja Espanjassa. Suomessa selvitys voidaan tehdä vain hyvin rajatuissa tilanteissa, mikä käytännössä tapahtuu poliisin laajamuotoisen turvallisuusselvityksen yhteydessä. Toisaalta esimerkiksi Englannissa luottotietojen selvittäminen on aina ollut ja on edelleen osan normaalia rekrytointiprosessiin liittyvää taustaselvitystä. Englanti erosi Euroopan unionista vuonna 2020, mutta heidän tietosuojalainsäädäntönsä on yhteneväinen EU:n tietosuoja-asetuksen kanssa.

Mayer Brown julkaisee vuosittain päivittyvää *A Global Guide Background Checks* -julkaisua, joka käsittelee eri maiden lainsäädäntöä taustaselvityksiä koskien. Julkaisu on valittu voittajaksi vuoden 2017 MPF (Managing Partners' Forum) *Awards for Management Excellence* -kilpailussa, jossa se oli mukana sarjassa Best provision of know-how to clients. Julkaisusta lainattu Mayer Brownin liikennevaloinfograafi (kuva 4) toimii hyvänä esimerkkinä taustatarkistuksia laatimisesta eri EMEA-alueen eli Euroopan, Lähi-idän ja Afrikan maissa. Infograafissa vihreä väri tarkoittaa, että selvitettävä tieto kuuluu maassa normaaliin prosessiin. Keltainen väri tarkoittaa, että tiedon selvittäminen on harvinaista tai kielletty tai se voidaan sallia vain tietyissä olosuhteissa. Punainen väri tarkoittaa, että kyseisen tiedon selvittäminen on kielletty, mutta äärimmäisen harvinaisissa tilanteissa selvitys voi tulla kysymykseen.



Kuva 4. Kuvaruutukaappaus Mayer Brown -sivuston EMEA-alueen taustatarkistuksista, liikennevalo infograafi ilmaisee, mitkä tiedot taustaselvityksessä voidaan selvittää. (Mayer Brown 2017)

Mayer Brown -lakitoimiston liikennevaloinfograafissa (kuva 4) on esitetty mahdollisia taustatarkistuksessa selvitettäviä asioita, jotka voivat tulla kyseeseen globaalisti toimivien organisaatioiden toimeksiannoissa. Suomessa ainoastaan viranomaisilla on pääsy useimpiin näistä tiedoista, jolloin yksityisen sektorin toimijalla ei ole mahdollista suorittaa taustatarkistusta. Näitä tietoja ovat esimerkiksi koulutus- ja työtodistukset (engl. education and past employment records), jolla tarkoitetaan tietojen varmentamista oppilaitoksesta ja aiemmilta työnantajilta. Rikosrekisteri (engl. criminal records) eli rikosrekisteritiedot voidaan tarkastaa vain, mikäli kohdehenkilö suostuu toimittamaan rikosrekisteriotteen. Taloustilanne ja luottotiedot (engl. credit/financial check) voidaan Suomessa tarkastaa eri palveluiden avulla, mutta lain mukaan henkilöluottotietoja saa käyttää vain luoton myöntämistä ja luoton valvontaa varten. Terveystietojen tarkastaminen (engl. health and medical screening) voidaan toteuttaa rekrytoitavalle ainoastaan työterveystarkastuksessa. Sosiaalisen median ja internetin haut (engl. social media/internet search) voidaan toteuttaa ainoastaan henkilön omalla suostumuksella. Sormenjälkiä (engl. fingerprinting) voidaan kerätä ainoastaan biometrisenä tunnisteena työsuhteen alettua. Käsialanäytteitä (engl. handwriting) ei juuri nykyään kerätä Euroopassa. Ammattiliittojen jäsenyys (engl. union membership) kuuluu erityisiin henkilötietoihin, ja sen käsittelystä säädetään EU:n yleisessä tietosuoja-asetuksessa. Poliittisen kannan (engl. political views) kerääminen ja käyttäminen henkilön arviointiin on

kielletty lainsäädännöllä. Huumausaine- ja alkoholitestit (engl. drug and alcohol testing) ovat mahdollisia työnantajalle tiettyjen edellytysten täyttyessä työterveydenhuollon toimesta.

Euroopan unionin ja EU-maiden kansallinen tietosuojalainsäädäntö rajoittaa yksilön henkilötietojen keräämistä ja niiden käyttämistä voimakkaasti. Tämän vuoksi esimerkiksi yhdysvaltalaisten avoimien tietolähteiden tiedustelun ja taustatarkistusohjeiden mukaiset toimintaohjeet eivät sovellu käytettäväksi Euroopan alueella. Tilanne on sama myös monien EU:n ulkopuolisten maiden rekrytointitoimintaan annettujen tarkastusohjeiden osalta. Näissä maissa on pääsääntöisesti yksilön tietosuoja merkittävästi heikompi kuin mitä se on EU:n alueella.

Perustuslakivaliokunta on lausunnossaan (PeVL 14/2018 vp) pohtinut Euroopan unionin tietosuoja-asetuksen perustuslaillisia näkökulmia. Perustuslakivaliokunta kiinnittää erityistä huomiota sääntelytarpeeseen silloin, kun henkilötietoja käsittelee viranomainen. Samalla Perustuslakivaliokunta korostaa, että lainsäätäjän tulee turvata yksityiselämän ja henkilötietojen suoja tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa. Perustuslakivaliokunta painottaa, että yksityiselämän ja henkilötietojen suojalla ei ole etusijaa muihin perusoikeuksiin nähden. Arvioinnissa on kyse kahden tai useamman perusoikeussäännöksen yhteensovittamisesta ja punninnasta. (Perustuslakivaliokunta 2018)

Euroopan unionin tietosuoja-asetuksen valiokuntakäsittelyissä on otettu kantaa henkilötietojen ja julkisuusperiaatteen väliseen suhteeseen. Muun muassa Hallintovaliokunta toteaa lausunnossaan (HaVL13/2018), että julkisuusperiaate on yksi keskeinen hallinnon periaate Suomessa. Perustuslain mukaan viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta. (Hallintovaliokunta 2018)

Kaikissa Eduskunnan valiokuntien käsittelyssä ei ole huomioitu yksityisen sektorin suorittamien taustatarkistusten laillisuutta tai suhdetta tietosuoja-asetukseen. Lausunnoissa painotetaan, että henkilötietojen käsittelyn tulee olla lainmukaista ja rekisteröidyn kannalta läpinäkyvää.

Suomessa Tietosuojavaltuutetun toimisto on ottanut kantaa tietojen keräämiseen julkaisussa Työelämän tietosuojan käsikirja (2022). Työnantajan on kerättävä työntekijää/työnhakijaa koskevat henkilötiedot ensisijaisesti työntekijältä/työnhakijalta itseltään. Jos työnantaja kerää henkilötietoja muualta kuin työntekijältä itseltään, työntekijältä on hankittava suostumus tietojen keräämiseen. Suostumus ei kuitenkaan ole tarpeen silloin, kun viranomainen luovuttaa tietoja työnantajalle tämän laissa säädetyn tehtävän suorittamiseksi tai jos tietojen keräämisestä tai

saamisesta laissa erikseen nimenomaisesti säädetään. Tietosuojavaltuutetun painottaa erityisesti, terveydentilatietojen kerääminen internetistä ei täytä työelämän tietosuojalain 3 §, 4 § ja 5 § vaatimuksia. (Tietosuojavaltuutetun toimisto 2020)

Azets on taloushallinnon ja palkanlaskennan osaamista sekä HR-asiantuntemusta ja ohjelmistoratkaisuja tarjoava Euroopan laajuinen yritys. Azets ohjeistaa verkkosivuillaan seuraavasti, ”Googlaaminen” eli työnhakijan tietojen etsiminen Internetin syövereistä on juridisesti hieman epäselvällä pohjalla. Elinkeinoelämän keskusliitto EK katsoo sen olevan sallittua, kunhan tietoa ei talleteta mihinkään eli ei muodosteta rekisteriä. Tietosuojavaltuutettu puolestaan ei pidä työnhakijan ”googlettamista” suotavana. Ei edes silloin kun työnhakijalta kysyttäisiin siihen lupa. Luvan antamatta jättäminen, kun voisi varsin todennäköisesti johtaa siihen, että työsuhdetta ei synny. Googlaamisen haasteena on myös se, että jos työnhakijan nimi on vähänkään yleisempi, niin voiko siinä mennä henkilöt keskenään sekaisin? (Azets 2022)

LinkedInin käyttö puolestaan katsotaan sallituksi. Tätä tulkintaa voi puoltaa ns. asemavaltuutuksen kautta. Koska kysymyksessä on alusta, jolla lähtökohtaisesti henkilöt antavat ennen kaikkea ammatillista tietoa itsestään, niin LinkedIn –tilin perustaminen voidaan katsoa sisältävän henkilön antaman luvan sille, että kuka tahansa voi näitä tietoja katsoa. (Azets 2022)

6 Avoimien tietolähteiden tiedustelun hyödyntäminen yritysturvallisuudessa

Saattaa olla vaikea luoda eroa tiedonhankkimiselle ja avointen tietolähteiden tiedustelulle, sillä molemmat käsittävät järjestelmällistä tiedon keräämistä ja analysointia. Usein tiedustelu mielletään jopa eräänlaiseksi ”agenttitoiminnaksi”, mutta loppujen lopuksi se eroaa vain hyvin vähän normaalista tiedonhankinnasta. Tarkoituksena on kerätä mahdollisimman paljon tietoa asiasta, minkä jälkeen tieto analysoidaan ja sen merkitys arvioidaan. Tämän jälkeen voidaan muodostaa tilannekuva, joka auttaa päätöksenteossa tai tulevien toimenpiteiden suunnittelussa. Yritysturvallisuuden eri osa-alueilla avointen tietolähteiden tiedustelua voidaan hyödyntää monilla tavoin tilannekuvan luomisessa tai täydentämisessä.

Tilannekuva määritellään päättäjien ja heitä avustavien henkilöiden ymmärryksenä tapahtuneista asioista, niihin vaikuttaneista olosuhteista, eri osapuolten tavoitteista ja tapahtumien mahdollisista kehitysvaihtoehdoista. Tilannekuva on koottu kuvaus vallitsevista olosuhteista, käsillä olevan tilanteen synnyttäneistä tapahtumista, tilannetta koskevista taustatiedoista ja tilanteen kehittymistä koskevista arvioista sekä eri toimijoiden toimintavalmiuksista. Tilannekuva voidaan käsittää myös suppeammin tarkoittamaan vain

esimerkiksi karttaa ja suullista tai kirjallista tietoa esillä olevasta tilanteesta. (TEPA-termipankki)

Avoimien tietolähteiden tiedustelua on käytetty apuna kyberturvallisuudessa tilannekuvan luomiseksi eri tilanteissa, kuten puolustajien kerätessä tietoa hyökkäysmetodeista tai hyökkääjien eri järjestelmien haavoittuvuuksista. OSINT-menetelmillä on saatu tietoa eri ryhmittymien aktiivisuudesta verkossa, heidän hyökkäysmetodeistaan sekä ryhmien mahdollisesta sijainnista. Esimerkiksi useiden aktiivisten hakkeriryhmien toimintaa on paikallistettu Venäjän tai Pohjois-Korean alueille, ja parhaimmillaan on kyetty nimeämään yksittäisiä ryhmään kuuluvia henkilöitä.

Kilpailutilanteen kartoittamisessa toimialalla on avoimien tietolähteiden tiedustelua käytetty pitkään, osin tietoisesti ja osin tiedostamatta. Hyvään johtamiseen kuuluu, että toimialan ja kilpailijoiden kehitystä seurataan aktiivisesti. Tämä auttaa muodostamaan käsityksen siitä, mihin suuntaan toimiala on kehittymässä ja miten kehityksen tulisi vaikuttaa oman yrityksen päätöksentekoon. Toimialaseurannassa ei riitä, että seurataan vain kotimaisia kilpailijoita, vaan on seurattava myös globaaleja trendejä. Monesti globaalit trendit jalkautuvat kotimaahan hieman myöhemmin, jolloin niistä perillä olevalla yrityksellä on mahdollisuus hyödyntää muuttuva markkinatilanne ennen kilpailijoita.

Ulkomailla toimittaessa pyritään luomaan kohdealueen tilanteesta tarkka tilannekuva, joko liiketoiminnan laajentuessa alueelle tai toiminnan jatkuvuuden varmistamiseksi. Esimerkkinä voidaan olettaa, että yritys on laajentamassa toimintaansa Afrikan alueelle. Tällöin toimintaympäristön PESTLE-analyysin laatiminen on enemmän kuin suositeltavaa. Analyysissa kartoitetaan taloudellisia, sosiaalisia, teknologisia, ekologisia, lainsäädäntöön liittyviä ja poliittisia tekijöitä, mitkä tulee ottaa huomioon tai mitkä vaikuttavat toimintaan. Tiedonkeruu jokaisesta näistä osa-alueesta vastaa todellisuudessa avointen tietolähteiden tiedustelua, sillä niissä lähteinä ovat usein paikallinen media, sosiaalinen media, internetin lainsäädäntösivustot, kohdevaltion viralliset sivustot, muiden kokemukset alueella toimimisesta ja niin edelleen. On hyvä huomata, että tilannekuvan luomiseen eivät riitä ainoastaan viralliset sivustot, koska niiden sisältö saattaa olla hyvin kaukana todellisuudesta. Esimerkiksi, jos löydetään yhdestä lähteestä maininta korruptiosta alueella, tulee puolestaan muista lähteistä selvittää, onko kyseinen maininta yksittäinen mielipide, yksittäistapaus vai maan tapa.

Yritykseen kohdistuvien uhkien tai riskien kartoittamisessa eli riskienhallinnassa avointen tietolähteiden tiedustelu on yleistä, vaikka sitä ei sellaiseksi aina mielletäkään. On hyvin tavanomaista etsiä tietoa vastaavanlaisiin, saman toimialan yrityksiin kohdistuneista uhkista tai toteutuneista tapahtumista, ja arvioida niiden todennäköisyyttä omassa yrityksessä. Pinnallisesti tarkastellessa yksittäinen riski saattaa tuntua epätodennäköiseltä, mutta syvempi

analysointi voi osoittaa sen olevan varteen otettava riski. Esimerkiksi sisäinen väärinkäyttö saattaa vaikuttaa vähäiseltä riskiltä, mutta laajan tietoaineiston keruun ja analysoinnin avulla voidaan huomata, että sisäinen väärinkäyttö nouseekin yrityksessä todelliseksi ja riskienhallinnassa huomioitavaksi uhaksi. Tässä toiminnassa lähteinä voidaan käyttää vakuutusyhtiöiden tilastoja, rikostilastoja, vahinkotilannetietoja tai muita tutkimuksia aiheesta.

Yllä esitetyt tilanteet ovat vain muutamia esimerkkejä siitä, kuinka avoimen tietolähteen tiedustelua voidaan hyödyntää yritysturvallisuudessa. Toimittajat ovat kautta aikojen hyödyntäneet avoimien tietolähteiden tiedustelua artikkelien kirjoittamisessa. Yksi merkittävä esimerkki on Bellingcat, joka on tutkivan journalismin kollektiivi. Kollektiivi ylläpitää Bellingcat-verkkosivustoa sekä tarjoaa koulutusta avoimen tietolähteen tiedusteluun. Bellingcat-verkkosivusto tarjoaa paljon oppaita ja aiheeseen liittyvää materiaalia julkisesti hyödynnettäväksi. (Bellingat 2022)

Toimittajakollektiivi itse määrittelee toimintansa seuraavasti: Bellingcat on riippumaton kansainvälinen tutkijoiden ja kansalaistoimittajien kollektiivi, joka koostuu ydinhenkilöstöstä ja tuhansista vapaaehtoisista. Käytämme todennettavissa olevaa digitaalista tietoa tutkiaksemme monenlaisia aiheita, vahvistaaksemme tosiasiat ja paljastaaksemme väärinkäytöksiä. Käytämme todisteisiin perustuvaa menetelmää mahdollisimman avoimesti ja julkaisemme havainnot oikeudenmukaisuuden ja vastuullisuuden edistämiseksi. Teemme yhteistyötä muiden kanssa, jaamme tietoa ja rakennamme näyttöön perustuvien tutkijoiden verkostoja. (Bellingcat 2022)

7 Taustatarkistukset rekrytoinnissa

Käytäntö on osoittanut, että taustatarkistusten laatimisella on tärkeä rooli rekrytoinnissa. Suomestakin löytyy useita esimerkkejä rekrytoinneista, joissa taustatarkistus olisi estänyt merkittävien taloudellisten, imagoriskien tai liikesalaisuuksien vuotojen toteutumisen. Tapauksia on mediassa käsitelty vain vähän, sillä usein varsinainen rikosnimike on arkipäiväisempi, mutta rekrytoinnissa tehty virhe on mahdollistanut rikoksen toteuttamisen.

Alle on koottu muutamia mediassa esillä olleita esimerkkejä tapauksista, joissa taustaselvityksen laatimisella olisi voitu estää virheellinen rekrytointi. Osassa tapauksia on väärennetyillä tutkintotodistuksilla erehdytetty työnantajaa maksamaan korkeampaa palkkaa, mutta pahimmillaan on seurauksena tapahtunut potilasturvallisuuden laiminlyöminen, mikä on johtanut jopa kuolemantapauksiin.

Ilman lääkärin tutkintoa yli kymmenen vuotta lääkärinä toiminut ja vuonna 2011 kiinni jäänyt Esa Laiho vältteli vastuuta ja päätöksiä. Laiho pärjäsi vaativassa työssään myös siksi, että hän erikoistui vanhusten hoitoon, missä potilaat voivat ikänsä tai kuntonsa johdosta olla jo lähellä kuolemaa. Laihon vuonna 1994 Venäjältä, pietarilaisesta Pavlovin yliopistosta saadut tutkintotodistukset samoin kuin kaikki muut hänen Pietarista saamansa asiakirjat osoittautuivat lopulta väärennöksiksi. (Helsingin Sanomat 2014)

Vuonna 2010 paljastui Karkkilan terveysaseman vuodeosaston lääkäri valelääkäriksi. Hän oli rekrytointivaiheessa esittänyt väärennetyt tutkintotodistukset, joiden mukaan hän oli kandivaiheessa oleva lääkäriopiskelija. Henkilö työskenteli vuoden työssään väärennetyillä todistuksilla, ja rikostutkinnassa selvisi, että hän oli tuona aikana kirjoittanut useita potilasturvallisuuden vaarantavia reseptejä. Kiinnijäämisen jälkeen henkilö onnistui vielä tekemään työsopimuksen Karjaalla sijaitsevan yksityisen lääkäriaseman kanssa, mutta tuolloin hän jäi lopulta kiinni rikoksesta Terveydenhuollon ammattihenkilörekisterin ansiosta. (Helsingin Sanomat 2010)

Terveydenhuollon alalla on paljastunut myös useita valehoitajia, joista osalla on ollut väärennetty tutkintotodistus, osalla tutkintotodistus on puuttunut kokonaan ja osalta on väärinkäytösten vuoksi peruttu oikeus harjoittaa ammattiaan.

Lahdessa paljastui vuonna 2013 koulutusalan yrityksessä tradenomin tutkintotodistuksen väärennös. Paljastunut naishenkilö väärensi tradenomin tutkintotodistuksen kopioimalla internetistä Tampereen ammattikorkeakoulun tutkintotodistuksen. Hän keksi todistukseen oppilaitoksen edustajien nimet ja tekaisi siihen myös allekirjoitukset. Todistusväärennöksen tarkoituksena oli hankkia oikeudetonta hyötyä ammattikorkeakoulututkinnosta saatavan palkanlisän saamiseksi. (Ilta-Sanomat 2012)

Nämä edellä kuvatut tapaukset ovat julkisuudessa käsiteltyjä tapauksia, mutta todellisuudessa väärennetyillä tutkintotodistuksilla tai työhistorialla on päästy yrityksissä merkittäviin asemiin. Toimihenkilö voi olla asemassa, jossa hän voi aiheuttaa yritykselle merkittäviä taloudellisia tappioita. Kun rikos paljastuu, voi taloudellisen vahinkojen ohella imagohaitta olla jopa vahinkoja vakavampi riski. Taloudelliset vahingot ovat yleensä korvattavissa, mutta imagohaitan korjaaminen usein ylittää moninkertaisesti taloudelliset vahingot. Pahimmillaan, kun luottamus yritykseen on kerran mennyt, sitä voi olla hyvin vaikea saavuttaa uudelleen.

Suomessa on ollut tilanteita, joissa yrityksen hallintoon rekrytoitu henkilö on syyllistynyt edellisessä työpaikassaan esimerkiksi kavallukseen. Uuteen tehtävään rekrytoinnin yhteydessä ei hänen taustaansa ole tarkastettu, jolloin kyseinen rikos on jäänyt havaitsematta. Henkilön syyllistyessä samaan rikokseen uudessa tehtävässään usein todetaan, ettei tilannetta olisi voitu estää ennakkoon. Tarkemmin tarkasteltaessa voidaan kuitenkin todeta tapahtuneen

kaksi virhettä, jotka huomioimalla olisi voitu vaikuttaa rikoksen ennalta estämiseen tehokkaasti. Ensimmäinen ja merkittävin virhe on taustatarkistuksen laiminlyöminen rekrytoinnissa, ja toinen virhe on hyvään hallintotapaan kuuluva tehokkaan sisäisen valvonnan puute.

Helsingin Sanomat -sanomalehti kirjoitti jo vuonna 2005 artikkelin väärennetystä tutkintotodistuksista. Artikkelin mukaan suomalaisten korkeakoulujen väärennettyjä tutkintotodistuksia kaupataan esimerkiksi internetissä. Todistusväärennöksiin erikoistuneella sivustolla myydään lehden mukaan esimerkiksi Teknillisen korkeakoulun, Helsingin yliopiston ja Tampereen yliopiston väärennettyjä todistuksia noin 300 eurolla. Maailmalla liikkuvien väärennösten vuoksi ulkomaiset yliopistot ottavat usein yhteyttä suomalaiskorkeakouluihin, kun ne haluavat tarkistaa hakijoidensa aiempien tutkintojen todenperäisyyttä. (Helsingin Sanomat 2005)

Internetistä löytyy useita palveluita, joista voi ostaa ulkomaalaisten yliopistojen tutkintotodistuksia. Samoin löytyy palveluita, jotka tarjoavat tutkintotodistuksen lisäksi niin kutsutun opintotoimistopalvelun. Tämä tarkoittaa, että valeyliopisto tarjoaa sähköpostin ja puhelinnumeron, jotka todistuksen ostaja voi antaa työnantajalleen. Valeyliopiston opintotoimisto vahvistaa tutkintotodistuksen ostajan opinnot, mikäli työnantaja suorittaa taustatarkistuksia.

Vaikka edellä mainitut tapaukset ovat räikeitä ja saaneet mediassa paljon huomiota, ne ovat vain jäävuoren huippu. Taustatarkistuksia laatiessa on opinnäytetyön tekijän omassa työhistoriassa tullut vastaan paljon erilaista vilppiä rekrytoitavien henkilöiden osalta. Yleisimpiä ovat olleet jonkin työpaikan ilmoittaminen työhistoriaan, vaikka henkilö ei ole ollut kyseisen yrityksen palveluksessa. Toisaalta usein tulee myös esille huijaamisia vastuualueiden, työtehtävien tai -projektien kohdalla. Henkilö on esimerkiksi työhakemuksessaan voinut kertoa olleensa vastuuhenkilönä merkittävässä projektissa, mutta taustatarkistuksessa on selvinnyt, ettei tämä tieto pidä paikkaansa. Tämän vuoksi on taustatarkistuksen tekeminen rekrytoitaessa erityisen tärkeää, varsinkin liittyen vastuunalaisiin tehtäviin tai työhön, johon liittyy erityinen luotettavuuden vaatimus. Ensisijaisesti tulisi aina harkita poliisin suorittamaa taustaselvitystä, mutta mikäli tämä ei ole mahdollista, on toissijaisesti hyvä miettiä taustatarkistuksen teettämistä yksityisellä toimijalla.

Valviran ylläpitämä JulkiTerhikki palvelu on Sosiaali- ja terveydenhuollon ammattihenkilöiden keskusrekisteri, jonka avulla esimerkiksi terveydenhuollon henkilökunnan pätevyys voidaan varmistaa. JulkiTerhikkiä ei opinnäytetyössä käsitellä syvemmin, mutta se toimii yhtenä avoimena tietolähteenä Sosiaali- ja terveydenhuollon laillistettujen tai nimikesuojattujen ammattihenkilöiden varmentamisessa. (JulkiTerhikki 2022)

7.1 Avoimien tietolähteiden tiedustelun hyödyntäminen rekrytoinnissa

Avoimia tietolähteitä voidaan hyödyntää taustatarkistuksen yhteydessä rekrytoinnissa hyvin rajatuin edellytyksin, sillä taustatarkistuksessa tulee toteutua lainsäädännön asettamat vaatimukset. Luvussa kuusi käsitellään tarkemmin näitä edellytyksiä ja minkälaisia rajoitteita EU:n alueella niiden osalta on.

Avoimien tietolähteiden tiedustelua voidaan hyödyntää rekrytoinnissa monilla tavoin, kuten oikeiden rekrytoitavien etsimisessä tai rekrytoitavan henkilön soveltuvuuden ja luotettavuuden arvioinnissa. Tyypillisin taustatarkistustoimeksianto on kuitenkin rekrytoitavan henkilön koulutustodistusten ja aiempien työpaikkojen varmentaminen. Monet oppilaitokset kuitenkin vaativat, että taustatarkistuksen kohteena olevalta henkilöltä on saatava kirjallinen lupa taustatarkistuksen suorittamiseen oppilaitoksen rekistereistä. On huomioitava, että ulkomaalaiset oppilaitokset vaativat englanninkielisen luvan tietojen luovuttamiseen eli englanniksi niin kutsutun Weiver- tai Consent-lomakkeen. Weiver-lomakkeen virallinen englanninkielinen nimi on Background Check Pre-Employment Waiver, toisin sanoen lupa taustatarkistuksen suorittamiseen työnhakijan osalta. Consent-lomake tunnetaan nimellä Pre-Employment Screening Consent and Release Form. Molemmista lomakkeista löytyy internet-haulla useita mallipohjia, joita voidaan tilanteissa hyödyntää. Niiden käytössä on huomioitava, että lomakkeen tulee olla Euroopan unionin alueelle tarkoitettu eikä esimerkiksi Yhdysvaltojen lainsäädännön mukainen.

Tilanteissa, joissa myönnetään lomakkeessa lupa tietojen luovuttamiseen, tulee luvan myöntäjän selkeästi ymmärtää, mihin ja missä laajuudessa hän myöntää luvan lomakkeella. Hyvä tapa lomakkeen luonnissa on, että siinä on selvitetty, mihin tarkoitukseen ja milloin lupa on myönnetty sekä kuinka kauan lupa on voimassa. Hyvin laaditussa lupalomakkeessa on selitetty henkilötietojen käsittelyn perusteet ja mitä tietoja henkilöstä käsitellään. Lisäksi tulisi lomakkeessa olla selkeä kuvaus tietojen säilytyksestä, arkistoinnista ja hävittämisestä, kuten kuinka pitkään tietoja säilytetään, mihin tiedot on tallennettu sekä miten tiedot hävitetään määräajan umpeuduttua. Tässä yhteydessä on hyvä antaa taustatarkistuksen kohteelle myös rekisterinpitäjän yhteystiedot, jotta taustatarkistuksen kohteena oleva henkilö voi tarkastaa, käsitelläänkö hänen tietojaan edelleen. Tietosuoja-asetuksen periaatteiden mukaisesti rekisteröidyllä on oikeus saada rekisterinpitäjältä vahvistus siitä, käsitteleekö tämä häntä koskevia henkilötietoja. Näin rekisteröidyllä on mahdollisuus arvioida ja varmistaa käsittelyn lainmukaisuus. Jos rekisteröidyn tietoja käsitellään, on rekisterinpitäjän toimitettava rekisteröidylle jäljennös käsiteltävistä henkilötiedoista. Jos rekisteröity esittää pyynnön sähköisesti, on tiedot toimitettava yleisesti käytetyssä sähköisessä muodossa, paitsi rekisteröidyn toisin pyytäessä.

Avoimien tietolähteiden tiedustelua voidaan hyödyntää rekrytoitavan henkilön taustatarkistuksen laatimisessa, mutta erityistä painoarvoa on tässä toiminnassa asetettava yksityisyydensuojalle ja toiminnan eettisyydelle. Erityisen olennaista on eettinen pohdinta taustatietoja kerätessä ja raportoidessa, kuten koostetaanko kaikki tieto, johon on annettu suostumus ja johon lainsäädäntö antaa mahdollisuuden. Vaihtoehtoisesti voidaan toimia eettisesti oikein ja kerätä vain tietoa, joka on rekrytoitavan tulevien tehtävien kannalta olennaista. Jos esimerkiksi taustatarkistuksen aikana tulee tietoon rekrytoitavan mahdollinen parisuhdeongelma, on mietittävä, onko tarpeen raportoida tieto edelleen tulevalle työnantajalle, mikäli sillä ei ole merkitystä työtehtävien hoitamisen kannalta.

8 OSINT, SOCMINT ja etiikka

Avoimien tietolähteiden tiedustelu ja erityisesti sosiaalisen median tiedustelu eivät ole täysin ongelmattomia. Yhden merkittävimmän ongelman tuo erottelu yksityisen (engl. private) ja julkisen (engl. public) tiedon välillä. Tieto, jonka käyttäjä jakaa Facebookissa, on kaikkien luettavissa, mutta tämän tiedon käyttäminen esimerkiksi henkilön profilointiin tai muuhun vastaavaan tarkoitukseen ilman lupaa loukkaa yksilön tietosuojaa.

Lohse ja Viitanen (2018) ovat pohtineet viranomaisen suorittamaa siviilitiedustelua eettisestä näkökulmasta kirjassaan *Johdatus tiedusteluun*. Tutkijat pohtivat, saako virkamies liikaa valtaa suorittaessaan tiedustelua, ja toteavat, että poliisi toimii virkavastuulla ja tämän toiminta on laillisuusvalvonnan kautta valvottua. Myös eduskunnan perustuslakivaliokunta on tiedustelutoiminnan valvontalakiesitystä koskevassa mietinnössään korostanut, että valvonnan toimivuutta on syytä tarkoin seurata.

Siviilitoimijoiden, kuten yritysten, yhteisöjen sekä yksityishenkilöiden, suhteen ei toistaiseksi ole virkavastuuta, julkista valvontaa tai tietolähteiden käyttöä määritelty. Tämä korostaa tarvetta toiminnan eettisten sääntöjen kehittämiselle. Vaikka lainsäädäntö jo määrittelee tietojen käyttöä, tulisi toimijoiden pohtia tietolähteiden käyttöä myös eettisestä näkökulmasta. Tämä koskee erityisesti henkilötiedon tai arkaluontoisen tiedon keräämistä, arkistointia sekä kerätyn tiedon hävittämistä.

Yksityisellä sektorilla tiedonkeruu kulminoituukin pääsääntöisesti kolmeen merkittävään tekijään, joita ovat läpinäkyvyys, tiedon oikeellisuus ja kohteen yksityisyyden suojan kunnioittaminen. Taustatarkistuksia tehdessä tulisi aina ymmärtää, kenen etu on etusijalla.

8.1 Läpinäkyvyys

Läpinäkyvyys on yksi olennainen osa avoimien tietolähteiden tiedustelua, kun sitä käytetään henkilö luotettavuuden arviointiin tai rekrytoitavan taustatarkistuksen tekoon. Läpinäkyvyys

tarkoittaa, että kohteena olevan henkilön tulee saada tieto prosessissa kerättävistä tiedoista ja käytetyistä tietolähteistä. Lisäksi hänelle tulisi olla selvää myös tiedon käyttötarkoitus ja säilytys.

EU:n tietosuojatyöryhmä toteaa marraskuussa 2017 julkaistussa mietinnössään, että luonnollisille henkilöille tulisi olla läpinäkyvää, miten heitä koskevia henkilötietoja kerätään ja käytetään sekä miten niihin tutustutaan tai niitä käsitellään muulla tavoin. Luonnollisen henkilöiden tulisi myös olla selvillä siitä, missä määrin henkilötietoja käsitellään tai on määrä käsitellä. Läpinäkyvyyden periaatteen mukaisesti kyseisten henkilötietojen käsittelyyn liittyvien tietojen ja viestinnän on oltava tietojen käsittelyn kohteen helposti saatavilla ja ymmärrettävissä, ja viestinnässä on käytettävä selkeää ja yksinkertaista kieltä. Tämä periaate koskee erityisesti tietoja rekisterinpitäjän identiteetistä ja tietojen käsittelyn tarkoituksista. Vaatimus koskee myös lisätietoja, joilla varmistetaan luonnollisia henkilöitä koskevan tietojen käsittelyn asianmukaisuus ja läpinäkyvyys, sekä luonnollisten henkilöiden oikeutta saada vahvistus ja ilmoitus heitä koskevien henkilötietojen käsittelystä.
(EU 2016)

Toisaalta on tärkeää, että prosessi on avoin ja läpinäkyvä myös toimeksiantajan suuntaan. Toimeksianto voi olla joko yrityksen sisäinen tai ulkoistettu kolmannelle osapuolelle. Lähtökohdista huolimatta toimeksiantajan on kyettävä tarkastelemaan koko prosessia laillisuus- ja vaikutusten arvioinnin toteuttamista varten. On tärkeää, että toimeksiantaja ymmärtää, millaisista tietolähteistä tietoa on kerätty, jotta toimeksiantaja voi arvioida niiden käytettävyyttä. Esimerkiksi tilanteissa, joissa tietoja on kerätty tietolähteistä, joiden käyttämiseen kohteena oleva henkilö ei ole antanut suostumustaan, on tietojen käyttäminen tietosuoja-asetuksen vastaista henkilötietojen käsittelyä.

8.2 Tiedon oikeellisuus

Taustatarkistuksen kohteen oikeusturvan kannalta on tärkeää, että tiedot ovat oikein ja ne on hankittu lainmukaisen oikeutusperusteen mukaisesti. Yhtä tärkeää on, että kerätty tieto on ajantasaista, paikkansapitävää ja koskee tarkastuksen kohteena olevaa henkilöä. Taustatarkistusprosessissa ei saa olla sellaista sekoittumisen mahdollisuutta, jossa tietoa ei varmuudella voida liittää kohdehenkilöön, ja jos sekaantumisen mahdollisuus on, ei tietoa tule käyttää.

The national consumer law center (NCLC) on yhdysvaltalainen kuluttajaoikeusjärjestö, joka toiminnallaan pyrkii vahvistamaan kuluttajien oikeuksia. NCLC on vuonna 2019 julkaissut Ariel Nelsonin laatiman julkaisun nimeltä *Broken Records Redux*, jossa tuodaan esille ongelmia, joita syntyy virheellisesti laadituista taustaselvityksistä. Yhdysvalloissa on yleistä, että taustaselvitys laaditaan työnhakijoista, vuokralaisista tai potentiaalisista

yhteistyökumppaneista. NCLC nostaa esille haasteena tässä sen, että toimiala ei ole säädeltyä ja selvityksen laatimisessa ei ole vakioituja toimintamalleja. (Nelson A, 2019)

Broken Records Redux -julkaisussa on tuotu esille useita tapauksia, joissa työpaikka, laina tai asunto on jäänyt saamatta, koska taustaselvitys on ollut virheellinen. Esimerkiksi julkaisussa on kuvailtu oikeusjuttu *Henderson v. CoreLogic National Background Data*, jossa Tyrone Henderson -nimisen henkilön taustaselvitysraporttiin oli otettu mukaan virheellisesti rikosrekisteritietoja. Tarkemmin oikeudenkäynnissä oli kyse Tyrone Hendersonin taustaselvityksessä esiin tulleista rikosrekisterimerkinnöistä, jotka estivät useampaan kertaan Hendersonin työpaikan saannin. Taustalla asiassa oli, että taustaselvitykseen oli lisätty samannimisen toisen henkilön rikosrekisterietoja, missä toisen henkilön henkilötunnus kuitenkin poikkesi taustaselvityksen kohteen henkilötunnuksesta. (Nelson A 2019)

NCLC nostaa merkittävimmiksi ongelmiksi taustaselvityksissä tietojen sekoittumisen toisen henkilön tietoihin, salassa pidettävien tietojen käyttämisen, datan käyttämisen erehdyttävällä tavalla, epäeettiset tiedonkeräämiskeinot sekä sen, että asiakkaalla ei ole mahdollisuutta oikaista hänestä kerättyä virheellistä tietoa. NCLC on myös tuonut esille, että nämä ongelmat eivät poistu tekoälyä tai automaattista päätöksentekoa hyödyntävissä taustaselvityksissä. Samaan aikaan on Euroopassa tuotu esiin nimenomaan prosessin läpinäkyvyys taustaselvityksen kohteen suojakeinoksi sekä korostettu mahdollisuutta korjata vääriä tietoja. (Nelson A 2019)

8.3 Kohteen oikeusturva ja yksityisyyden suoja

On huomioitava, että Suomen oikeusjärjestys antaa laajan tietosuojan henkilölle ja hänen yksityisyydelleen. Suomessa lähtökohta on, että perustuslaillisiin oikeuksiin, kuten yksityisyyden suojaan, ei saa puuttua ilman laissa säädettyä perustetta.

Myös Euroopan ihmisoikeussopimuksen kahdeksannen artiklan perimmäisenä tarkoituksena on suojata yksilöä viranomaisten mielivaltaiselta puuttumiselta yksityis- ja perhe-elämään. Artiklan mukainen yksityiselämän suojaaminen edellyttää muun muassa sitä, että yksityiselämän suojan piiriin kuuluvien henkilötietojen keräämisestä, käyttämisestä ja säilyttämisestä säädetään riittävän täsmällisesti. (Pitkänen, Tillikka & Warma 2013)

Edellä mainittu tuo viranomaisille tarkkarajaisen vaatimuksen siitä, ettei yksityisyyden suojan piiriin kuuluvia tietoja voida kerätä tai käyttää viranomaisen toimesta mielivaltaisesti. Lain analogian puitteista on siis johdettavissa, ettei samaa oikeutta voi myöskään olla yksityisellä toimijalla. Lain analogia tarkoittaa, että kahta arvioitavaa tilannetta pidetään suhteessa samanlaisina, minkä johdosta niitä tulee arvioida samalla tavalla. Tämä koskee toimeksiantojen osalta niin toimeksiantajaa kuin toimeksiannon saanutta yritystä ja sen

työntekijöitä. Yhtä lailla vaatimus koskee myös työnantajia sekä sitä, millaista tietoa nämä työntekijöistään keräävät.

Työnantaja ei voi olettaa, että tällä olisi automaattisesti oikeus työntekijöidensä henkilötietojen käsittelyyn. Myöskään henkilön sosiaalisen median profiili tai mikä tahansa muu tieto, joka on julkisesti saatavilla, ei synnytä automaattista oikeutta kerätä tai käsitellä kyseistä tietoa. Henkilötietojen käsittely vaatii aina laillisen perusteen, joka voi olla oikeutettu etu tai henkilön suostumus. Sosiaalisessa mediassa tai internetissä julkisesti saatavilla olevien tietojen osalta on yritystenkin otettava huomioon, liittyvätkö hakijasta löytyvät tiedot hänen työtehtäväänsä vai ovatko tiedot tarkoitukseltaan yksityisiä. Tietosuojavaikutusten arviointi on syytä suorittaa aina ennen tällaisten henkilötietojen käsittelyä.

Tietosuojavaltuutetun kannan mukaan työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työnantajan työntekijöille tarjoamiin etuuksiin taikka johtuvat työtehtävien erityisluonteesta. Tarpeellisuusvaatimuksesta ei voida poiketa työntekijän suostumuksella. (Tietosuojavaltuutetun toimisto 2022)

Myös Elinkeinoelämän keskusliitto on lausunnossaan 6.9.2021, että työntekijästä kerättävien henkilötietojen pitää aina olla työsuhteen kannalta tarpeellisia. Tärkeä periaate sisältyy sekä GDPR:ään että Suomen lainsäädäntöön. Lisäksi työnantajan on informoitava työntekijöitä henkilötietojen käsittelystä. Työnantaja ei saa siis nytkään kerätä työntekijöiden henkilötietoja ilman, että he tietävät mitä tietoja heistä kerätään ja mistä niitä kerätään. (EK 2022)

8.4 Kenen etu on ensisijalla?

Lainsäädäntö asettaa ehdottoman vaatimuksen siitä, että rekisteröidyn edun tulee olla aina etusijalla. Rekisteröidyllä on ehdoton oikeus päättää henkilötietojensa käsittelystä, ellei rekisterinpitäjällä ole lakisääteistä perustetta tietojen käsittelemiselle. Tämän määrittävät sekä yleinen tietosuoja-asetus että tietosuojalaki, ja poikkeukset tästä periaatteesta koskevat lähinnä viranomaisia.

Moni asiantuntija, joiden kanssa opinnäytetyön tekijä on keskustellut aiheesta, on tuonut esille näkökulmansa edusta. Tarkemmin tällä tarkoitetaan sitä, kumman etu on ensisijainen, työnantajan vai rekrytoitavan. Lähes kaikki asiantuntijat lähtevät siitä tulkinnasta, että rekrytoitavan etu on aina asetettava ensisijalle eli että taustatarkistuksen tulee olla laillista, läpinäkyvää ja siihen tulee olla rekrytoitavan suostumus.

Muutama haastatelluista asiantuntijoista toi esille poikkeustilanteita, joissa työnantajan etu voisi nousta etusijalle. Nämä kriittiseen infrastruktuuriin sekä merkittävien yrityksen tai asiakkaiden tietoihin pääsemiseen liittyvät työtehtävät ovat kuitenkin poikkeuksia toimeksiannoissa. Yleensä ne liittyvät työtehtäviin, jotka oikeuttavat yritystä teettämään viranomaisen laatiman taustaselvityksen. Näissä tilanteissa viranomaisen laatimaa taustaselvitystä voidaan usein pitää tarkoituksenmukaisempana kuin yksityisen toimijan laatimaa taustatarkistusta.

9 Asiantuntijoiden näkemykset aiheesta ja tulevaisuuden kehityksestä

Opinnäytetyötä varten haastateltiin tietosuojaan liittyviä asiantuntijoita ja tietosuojalainsäädännön valvonnasta vastaavia viranomaisia. Asiantuntijoiden esittämissä näkemyksissä näkyi eroa lähinnä operatiivisen ja juridisen näkemyksen painotuksissa. Viranomaisten kannat olivat luoteeltaan enemmän ohjaavia, ja muun muassa EU:n tietosuojatyöryhmä toimitti opinnäytetyön tekijälle asiaan liittyviä työryhmämuistioita ja ei haastattelussa ottanut kantaa suoraan.

Opinnäytetyötä varten lähetettiin haastattelupyyntöjä myös tietosuojaan erikoistuneille juristeille ja oikeustieteilijöille, mutta haastattelupyyntöihin ei vastattu tai niistä kieltäydyttiin. Tämän vuoksi asiantuntija haastattelussa ei ole oikeustieteen edustajia, jotka ovat perehtyneet tietosuojaan. Sama tilanne ilmeni myös etiikkaan ja eettisiin kysymyksiin perehtyneiden asiantuntijoiden osalta, haastattelupyyntöihin ei vastattu tai ilmoitettiin kohteliaasti, etteivät he ole käytettävissä.

Opinnäytetyöhön haastateltu professori Jarno Limnéll Aalto-yliopistosta keskittyi vastauksissaan yleisellä tasolla avoimien tietolähteiden ja sosiaalisen median tiedusteluun, erityisesti lähteiden luotettavuuden näkökulmasta sekä lähdekriittisyyden vaatimuksesta. Limnéll kertoi, ettei edellä mainittuun ole hänen mielestään yhtä selkeää vastausta. Professori painotti näkemyksessään, että vaikka sosiaalisen median lähteitä voidaan hyödyntää, tulee näistä lähteistä saatavat tiedot kyetä aina varmistamaan myös toisesta lähteestä ennen tiedon käyttöä ja johtopäätösten tekoa niistä.

Oikeustieteen tohtori Eelis Paukku totesi haastattelussa, että käytännössä avointen tietolähteiden käyttö taustatarkistuksessa on kiellettyä. Nämä tiedot ovat lähes aina EU:n yleisen tietosuoja-asetuksen mukaisia henkilötietoja. Näiden käsittelyn elinkeinotoiminnassa on perustuttava lakiin, käytännössä tietosuoja-asetuksen kuudenteen artiklaan, jossa on kuusi perustetta tietojen käsittelylle. Käytännössä näistä voi yksityisten välisissä oikeussuhteissa useimmiten soveltua vain rekisteröidyn suostumus, joka tilaajan tulisi hankkia.

Turvallisuusasiantuntija Hannu Huttunen HPH Consulting Oy:stä totesi haastattelussa, että jos hakijasta halutaan selvittää tietoja muutenkin kuin hänen lähettämästään hakemuksesta, ja käyttää tietoja hyödyksi esimerkiksi rekrytoinnin yhteydessä, tarvitaan tähän hakijan suostumus. Omatoiminen tiedonhankinta esimerkiksi rekrytoinnin yhteydessä hakemuksessa annettujen tietojen lisäksi, ilman hakijan suostumusta, ei Huttusen mukaan ole mahdollista.

Opinnäytetyötä varten kysyttiin myös EU:n tietosuojatyöryhmän kannanottoa, mutta työryhmä ei ottanut suoraan kantaa, koska EU:n yleisen tietosuoja-asetuksen tulkinta kuuluu kunkin jäsenmaan lainvoimaiselle viranomaiselle. Tietosuojatyöryhmä kuitenkin toimitti Data Protection Working Party -työryhmän muistioita, joissa on käsitelty taustaselvityksien laatimista rekrytointi- ja luotettavuudenarviointitilanteissa. Näissä todetaan, että yleinen tietosuoja-asetus asettaa laillisuusvelvoitteen tietojen käsittelijälle. Tietojen käsittelijä vastaa sekä käsittelyn laillisuudesta että käsittelyn tietoturvallisuudesta. Kunkin jäsenmaan tietosuojasta vastaava viranomainen puolestaan ohjeistaa ja valvoo, että yksittäiset toimijat noudattavat annettuja säännöksiä.

Vastauksessaan EU:n tietosuojatyöryhmä toteaa, että GDPR asettaa uuden ja rajat ylittävän vastuuvelvollisuuden periaatteen. Tämä tarkoittaa sitä, että jokaisen organisaation on analysoitava oma tilanteensa ja toteutettava omassa tapauksessaan tarvittavat organisatoriset ja tekniset toimenpiteet. Tähän tarvitaan tapauskohtainen analyysi, jossa arvioidaan organisaation henkilötietojen aiheuttama riski yksilön tietosuojalle.

Tietosuojavaltuutetun toimiston haastateltu asiantuntija ei näe estettä esimerkiksi rekrytointivaiheessa tehtävälle taustatarkistukselle, kunhan GDPR:n ja tietosuojalain vaatimukset huomioidaan toiminnassa. Tietosuojavaltuutetun toimiston haastateltavan mukaan toimistossa pidetään taustatarkistustoimintaa toistaiseksi niin vähäisenä, ettei sitä varten ole katsottu tarpeelliseksi laatia erillistä ohjeistusta. Keskustelun aikana asiantuntija kuitenkin totesi olevan mahdollista, että ohjeistuksia saattaa tulla myöhemmin.

Kaikki opinnäytetyötä varten haastellut asiantuntijatahot olivat sitä mieltä, että useimmissa tapauksissa taustatarkistusta suorittava taho toimii rekisterinpitäjän roolissa. Tämä tuo taustatarkistuksen laatijalle merkittävän vastuun. Monessa taustatarkistuksia markkinoivassa yrityksessä Euroopassa on otettu käytännöksi, että kaikki tiedot tarkistettavasta henkilöstä poistetaan järjestelmästä taustatarkistusraportin luovuttamisen jälkeen. Tällä pyritään välttämään henkilörekisterin kertymistä sekä estämään mahdollisen tietovuodon syntymistä tai ainakin minimoimaan sen vaikutuksia. Keskimääräinen taustatarkistuksen laatimisaika on alle viisi päivää, joten tiedot ovat palveluntarjoajan tietojärjestelmässä yleensä noin viikon ajan.

Tällä hetkellä monet palveluntarjoajat tuottavat palveluita, joissa tieto kerätään pääasiassa henkilötyönä ja enintään osittain automaattisesti. Tulevaisuuden teknologia tulee haastamaan

tämän, kun tarjolle tulee tekoälyyn perustuvia palveluita. Tämän vuoksi tulisikin laatia kansallisesti selkeät pelisäännöt ja valmistella ja hyväksyä lainsäädäntöä, ennen kuin tekoälyyn perustuvat palvelut tulevat voimakkaammin markkinoille.

Tiukka tietosuoja saattaa johtaa tilanteeseen, jossa taustaselvityksiä tilataan Euroopan unionin ulkopuolelta. Esimerkiksi Venäjällä, Yhdysvalloissa ja Aasiassa on useita yrityksiä, jotka tarjoavat taustatarkistuksia avoimista tietolähteistä. Tämä tarkoittaa usein myös kontrollin katoamista sekä taustaselvityksen kohteen yksityisyydensuojan merkittävää heikentymistä. Vaikka näitä EU:n ulkopuolisista maista tilattuja taustatarkistuksia ei käytetä virallisesti rekrytoinnissa tai luotettavuuden arvioinnissa, saatetaan niitä käyttää ilmoittamatta. Tällöin ne voivat vaikuttaa rekrytointiprosessiin, mutta ne eivät samaan aikaan ole taustatarkistuksen kohteen tiedossa. Tämä voi johtaa tilanteeseen, jossa henkilöllä ei ole tiedossa, mikä vuoksi työpaikan saaminen ei onnistunut tai mihin tietoihin päätös on tosiasiassa perustunut.

Tekoäly on jatkuvassa kehityksessä, ja sen osalta olisi tarpeen luoda sääntelyä tai vähintään vahva eettinen säännöstö. Siinä, missä tekoälyn teknologiaa voidaan hyödyntää monella tavoin kehittämään globaalia turvallisuutta tai paikallisten ratkaisujen toteuttamiseksi, voidaan samaa teknologiaa käyttää myös rikollisiin tai lainvastaisiin tarkoituksiin. Tältä osin jää monia avoimia kysymyksiä, esimerkiksi kumpi osapuoli on syyllinen laittomuuteen, palveluntarjoaja vai käyttäjä. Monissa tilanteissa tähän ei löydy juridisesti selkeää vastausta, ja pahimmillaan esimerkiksi yksityisyydensuojan loukkaamisessa voi olla haastavaa määrittää, kuka lakia on lopulta rikkonut. Toisaalta, jos teko tapahtuu kolmannessa maassa, on huomioitava myös tuomiovaltaan liittyvät kysymykset.

Taustatarkistuksien laatiminen on ollut pitkään niin sanottua käsityötä, jossa laatijan osaaminen ja kontaktiverkosto on ollut merkittävässä roolissa. Tämä on korostunut erityisesti silloin, kun tietoa haetaan ulkomaisista lähteistä. Käsityönä tehtävissä tarkistuksissa on haasteita tuonut luotettavan tiedon löytäminen, etenkin tilanteissa, joissa jo kielikysymys on usein ollut haaste. Toisaalta toiminnan etuna on ollut se, että taustatarkistuksen laatija on tehnyt inhimillisiä, juridisia ja eettisiä päätöksiä suorittaessaan tutkimusta, esimerkiksi käytetäänkö tietoa vai ei, mikäli tieto ei liity rekrytoitavan työtehtävään tai tapahtumasta on kulunut pitkä aika.

Tekoäly tuo taustatarkistuksen tekemiseen merkittävää hyötyä, jotka liittyvät sen kykyihin käydä läpi useita eri lähteitä lyhyessä ajassa sekä koostaa niistä selkeä raportti. Järjestelmä on mahdollista ohjelmoida suorittamaan useita eri hakuja erilaisista lähteistä, kuten viranomaisen rekistereistä, avoimista lähteistä sekä sosiaalisen median lähteistä. Tiedonkeruulle voidaan asettaa tekoälyn osalta myös erilaisia suodattimia, rajoituksia ja määritelmiä.

Merkittävimpänä ongelmana toisaalta voidaan pitää mahdollisuutta käyttää tekoälyä niin sanotun raa'an logiikan mallilla. Tämä tarkoittaa tarkemmin, että kaikki tekoälyn löytämät tiedot hyödynnetään raakadatana raportissa. Erityisen ongelmalliseksi tilanne muuttuu, jos tiedonkeruussa ryhdytään hyödyntämään laittomia lähteitä tai keinoja. Yhtenä tällaisena laittomana keinona voidaan pitää esimerkiksi hakkerointia tai hakkeroitujen tietojen hyödyntämistä.

Haastattelin opinnäytetyötä varten videoyhteydellä Suomen kansainvälisesti tunnetuinta tietoturva-asiantuntijaa, F-Securen tutkimusjohtaja Mikko Hyppöstä. Haastattelussa keskusteltiin tekoälyn käytöstä taustatarkistuksien laatimisessa sekä tähän liittyvistä ongelmista ja haasteista. Hyppönen omaa vahvan työhistorian tietoturvallisuuden alalla jo usealta vuosikymmeneltä, minkä lisäksi hänet tunnetaan laaja-alaisena tietotekniikan osaajana, joka kykenee esittämään vaikeitakin asiakokonaisuuksia alalta kansantajuisesti.

Haastattelussa Hyppönen toi esille haasteita, joita voi nousta, jos tekoälyn käyttö lisääntyy taustatarkistuksien laatimisessa. Mikko Hyppönen avasi ongelmaa:

> *"Kun näkyvyys häviää… kun mustalaatikko antaa vastauksia, niitä on vaikea haastaa tai vaikea riitauttaa. Jos ihminen päätyy jostain syystä mustalle listalle, tai vähän joka firman automatiikka hylkää sun työhakemuksen, etkä oikeestaan tiedä miksi. Tämä helposti johtaa Kafkamaiseen limboon, sä et tiedä mikä sun rikos on, etkä tiedä mistä sut on tuomittu, etkä tiedä mihin sä voit valittaa."*

Hyppönen näki tilanteen ongelmalliseksi oikeusturvan ja ihmisoikeuksien kannalta, koska välttämättä ei tiedetä, minkä takia laitteisto tai algoritmi tekee tiettyjä päätöksiä. Hyppönen toi esille samassa yhteydessä myös tahattomien virheiden mahdollisuuden eli esimerkiksi tilanteet, joissa järjestelmä ei osaa erotella kahta samannimistä henkilöä. Mainittu tilanne ei ole poissuljettu edes nykyisten manuaalisten taustatarkistusten kohdalla, mutta haastavammaksi ongelma ja sen havaitseminen voivat muuttua täysin automatisoidussa järjestelmässä ja loppukäyttäjän ajatellessa, että järjestelmä toimii virheettömästi. Työnantajan tulisi voida luottaa siihen, että taustatarkistusraportti on paikkansa pitävä.

Haastattelussa opinnäytetyön tekijä esitti Hyppöselle myös kysymyksen siitä, kuinka todennäköistä on, että koneäly oppii hakemaan tietoa esimerkiksi hakkeroiduista tiedostoista, jotka on jaettu pimeään verkkoon. Esimerkkinä tilanteesta voidaan pitää Psykoterapiakeskus Vastaamon vuonna 2019 hakkeroitua terveystietokantaa, jonka sisältämiä tietoja jaettiin pimeässä verkossa. Hyppösen mukaan on vaikea antaa vastausta tähän kysymykseen. Hyppösen mukaan tämä olisi periaatteessa teknisesti jo mahdollista, mutta vielä tällaista tekoälyn kykyä ei tiettävästi ole olemassa. Toisaalta koneoppiminen ja tekoäly kehittyvät

Hyppösen mukaan niin nopeasti, että tänään asia voi olla kaukaista tulevaisuutta, mutta huomenna sama asia onkin jo olemassa olevaa teknologiaa.

Hyppönen näki kuitenkin, että vaikka terveystiedot ovat selkeästi yksi kiinnostuksen kohde, niin niiden merkitys taustaselvityksessä on kuitenkin vähäinen. Lisäksi tällaisen tiedon käyttämiseen liittyy merkittävä rikosoikeudellinen riski sekä tiedon kerääjälle että loppukäyttäjälle.

Paljon merkittävämpänä asiana Hyppönen toi esille tekoälyn tai koneoppimisen hyödyntämisen erilaisten keskustelufoorumien seurannassa ja tiedonkeruussa henkilöiden verkkokäyttäytymisestä. Keskustelufoorumeilla niiden käyttäjät keskustelevat muiden kanssa ja ottavat kantaa asioihin, ja keskusteluissa ihminen tyypillisesti usein edustaa omaa itseään ja näkemyksiään. Tähän pohjautuva tiedonkeruu mahdollistaisi erittäin tarkan profiilin luomisen henkilöstä. Vuodetut terveystiedot eivät ole paras lähde, mutta Hyppösen mukaan vaikka kymmenen vuoden sosiaalisen median ja internetkäyttäytymisen historia kertoo jo merkittävästi tarkemmin henkilön todellisesta persoonallisuudesta.

Mikko Hyppönen toi esille myös laillisten järjestelmien haitallisen käytön, kuten mustamaalaamisen tai ongelmien tuomisen ihmisille, joista joku ei pidä. Hän totesi, että järjestelmien yleistyessä ja tietoisuuden lisääntyessä siitä, että niiden kautta löytyy muista henkilöistä myös negatiivista tietoa, voidaan tätä käyttää rikollisessa tai haitallisessa tarkoituksessa. Henkilö voi esimerkiksi esiintyä toisena henkilönä keskustelufoorumeilla ja jakaa mielipiteitä olettaen, että tieto päätyy edellä mainittuun tietokantaan. Toisin sanoen järjestelmää voidaan manipuloida tietoisesti, ja näin aiheuttaa ongelmia toiselle osapuolelle.

Ongelmaksi nousee myös prosessin läpinäkyvyys eli mistä tieto on alun perin saatu ja onko tiedon käyttöön hyväksyntä. Hyppönen totesi haastattelussa, että mitä pidempään oppimisjärjestelmää on opetettu, sitä vaikeampaa on vastata kysymykseen, miksi kone antoi siltä saadun vastauksen. EU-direktiivissä todetaan, että koneen antama päätös tulee aina pystyä perustelemaan. Tämä on helppo sanoa, mutta käytännössä asian toteutus voi olla vaikeaa. Jo pelkästään tavanomaisen Google-haun antamien vastausten perusteleminen on liki mahdotonta, koska haussa on taustalla jo noin 15–20 vuotta koneoppimista. Hyppösen mukaan ei ole mahdollista vastata kysymykseen, miksi ohjelma tuntee käyttäjänsä niin hyvin, että osaa päätellä kuka tämä, missä tämä on, mikä kellonaika on ja mitkä ovat käyttäjän mieltymykset. Hyppönen totesikin, että vaikka ohjelma tekisi, mitä se on ohjelmoitu tekemään, ei tämä tarkoita, että ymmärrettäisi, mitä ohjelma todellisuudessa tekee. Toisin sanoen, vaikka ohjelma noudattaa ohjelmointia, ei ihminen enää välttämättä kykene selittämään ohjelman tuottamia vastauksia.

Haastattelun lopuksi kävimme vapaata keskustelua tekoälyn ohjaamisen haasteista, nimenomaan etiikan, politiikan ja lainsäädännön puitteissa. Hyppönen nosti merkittävimmäksi

ongelmaksi sen, että lainsäätäjillä ja poliitikoilla ei ole riittävää ymmärrystä tekoälystä ja koneoppimisesta. Esimerkkinä Hyppönen toi esille sen, mitä voidaan todellisuudessa toteuttaa ja miten sinällään yksinkertaiselta kuulostava toiminto voi todellisuudessa vaikuttaa tiedon määrään. Vaikka eettiset näkemykset usein ohjaavatkin lainsäädäntöä ja poliittista päätöksentekoa, vaaditaan Hyppösen mukaan näiden ohelle kuitenkin laaja-alaista ymmärrystä teknisistä mahdollisuuksista.

Anderson ja Anderson (2011) ovat teoksessaan *Machine Ethics* viitanneet myös teknologian eettisiin haasteisiin. Järjestelmien ei tulisi tutkijoiden mukaan olla mustia laatikoita, joiden antamia vastuksia kukaan ei kykene selittämään. Algoritmien ja niiden antamien tulosten tulisi olla läpinäkyviä ja toimintalogiikan perusteltavissa. Tutkijat ovat tulleet johtopäätökseen, että ohjelmoijien tulisi toimia eettisesti kestävien periaatteiden mukaan, ja samalla lainsäädäntö voi antaa vain puitteet toiminnalle. Samuel Lo Piano (2020) toteaa artikkelissaan, että todennäköisesti tulevaisuudessa ajaudutaan poliittisiin ongelmiin, kun edessä on kompromissi yhteiskunnan vaatiman oikeudenmukaisuuden ja esimerkiksi yksityisen toimijan vaatiman algoritmisen tarkkuuden välillä.

Turun kauppakorkeakoulun työelämäprofessori ja filosofi Maija-Riitta Ollila käsittelee aiheen ongelmaa kirjassaan *Tekoälyn etiikka* (2019). Ollilan mukaan aluksi on luotava kehikko tekoälyjärjestelmien selitettävyyden parantamiseksi. Tämä koskee Ollilan mukaan erityisesti niitä tilanteita, joissa tekoälyjärjestelmät tekevät sosiaalisesti merkittäviä päätöksiä ja päätöksillä saattaa olla ei-toivottuja seurauksia. Eri toimialoja varten saatetaan tarvita erilaisia kehikoita, joten prosessiin on otettava mukaan eri alojen, kuten tieteen, liike-elämän, juridiikan että etiikan, edustajia. Ollilan mukaan on kehitettävä oikeudellisia menettelyitä, jotka soveltuvat tekoälyyn liittyvien ongelmien käsittelyyn ja parannettava oikeuslaitosten kykyä käsitellä algoritmin tekemiä päätöksiä.

Ollila viittaa tällä siihen, että lainsäädäntö kehittyy teknologiaan nähden hyvin hitaasti. Ennen kuin teknologian tai algoritmin tuoma epäkohta päätyy toimivaltaisessa ministeriössä lain valmistelun kohteeksi, on teknologia kehittynyt jo niin paljon, ettei säädetty laki enää vastaa uuteen ongelmaan. Tämän vuoksi tekoälyn ja koneoppimisen osalta lainsäädäntötyön tulisi olla ennakoivaa, mutta tässä haasteena on Mikko Hyppösen haastattelussaan esille tuoma ongelma. Hyppösen mukaan lainsäätäjiltä ja poliitikoilta puuttuu riittävä tekninen osaaminen ymmärtää koneoppimista ja tekoälyä, jotta lainsäädännöllä voitaisiin vastata ongelmaan. Tämän vuoksi algoritmien, tekoälyn ja koneoppimisen kehittäjien tulisi olla ensisijaisesti vastuussa eettisesti kestävän teknologian luomisesta.

Opinnäytetyötä varten haastateltujen asiantuntijoiden näkemyksissä oli havaittavissa vähäisiä eroja, mikä selittyy haastateltavien taustoilla, kuten juridisella ja operatiivisella näkökulmalla. Juridista näkökulmaa edustavat haastateltavat toivat esille tiukan näkemyksen,

kun taas operatiivista näkökulmaa edustavat olivat tulkinnoissaan hiukan väljempiä. Juristit painottivat nimenomaan lainsäädännöllisiä rajoitteita, kuten yksityisyyden suojaa työelämässä sekä EU:n tietosuoja-asetusta, jotka asettavat merkittäviä rajoitteita henkilötietojen keräämiselle sekä niiden käsittelylle. Operatiivisen näkökulman edustajat ymmärsivät käyttötarpeen, mutta korostivat lainsäädännön noudattamista kaikissa tilanteissa. Kaikki korostivat vaatimusta siitä, että tiedot on saatava työnhakijalta itseltään tai taustatarkistukseen on oltava hakijan nimenomainen ja yksiselitteinen suostumus.

10 Johtopäätökset

Opinnäytetyötä varten tutkittiin useita avoimien tietolähteiden tiedustelun oppaita sekä aihepiiristä kirjoitettuja muita teoksia. Huomiota herätti opinnäytetyön tekijässä erityisesti se, miten vähän niissä on otettu kantaan toiminnan eettisyyteen tai laillisuuteen. Teokset käsittelevät pääsääntöisesti tiedustelutekniikoita, teknisiä ratkaisuja, käytettäviä sovelluksia sekä strategisia näkökulmia. Sama tilanne oli havaittavissa myös palveluiden markkinoinnissa, jossa kyllä mainostetaan palveluita, mutta niiden lainsäädännöllisiä rajoitteita ei tuoda ilmi. Tämä antaa toimeksiantajalle helposti väärän mielikuvan, että kaikki toimeksiannossa hankittu tieto olisi lainmukaista. Tämä puolestaan voi johtaa siihen, että toimeksiantaja saattaa joutua edesvastuuseen lain rikkomisesta.

Myös toimialan eli palveluita tuottavien yritysten kannanotot vastuullisuuteen, yksityisyyden suojaan, lainsäädäntöön tai eettisiin kysymyksiin puuttuvat lähes kokonaan. Tämä on vallitseva tilanne nykyhetkessä, jossa palveluiden tuottajat toimivat ilman selkeää lainsäädännöllistä ohjausta tai valvontaa. Teknologian kehitys moninkertaistaa nämä haasteet, sillä tekoäly ja koneoppiminen kehittyvät jatkuvasti. Vaikuttaa siltä, ettei taustatarkistusten suhteen tulla asettamaan yksityistä sektoria koskevaa lainsäädäntöä, ja näin ollen ei tulevaisuudessakaan voida vastata teknologian kehityksen mukanaan tuomiin monikertaistuviin haasteisiin. Tämä johtaa ongelmalliseen tilanteeseen, jossa lainsäädäntö tulee jatkuvasti teknologisen kehityksen perässä. Käytännössä tämä tarkoittaa, että tulevalla lainsäädännöllä pyritään jatkuvasti ”sammuttamaan paloja, kun niitä huomataan”. Ennaltaehkäisevään ja kehittyvän teknologian käytön ohjaamiseen tapahtuvaa lainsäädäntöä ei opinnäytetyön tekijän selvitysten pohjalta vaikuta olevan tulossa.

EU:n tekoälyasetuksen luonnos on pyrkinyt vastaamaan tähän haasteeseen, mutta asetus on asiantuntijoiden näkemyksen mukaan riittämätön. Suurimpana haasteena on se, etteivät lainsäätäjät itse ymmärrä teknologiaa, jonka käyttöä pyritään rajoittamaan yksityisyyden suojan, eettisyyden tai prosessin läpinäkyvyyden puitteissa. Maija-Riitta Ollila toteaakin, että tulevaisuudessa on kehitettävä oikeudellisia menettelyitä, jotka soveltuvat tekoälyyn

liittyvien ongelmien käsittelyyn. Ollilan mukaan on myös parannettava oikeuslaitosten kykyä käsitellä algoritmin tekemiä päätöksiä sekä tekoälyä. (Tekoälyn etiikka 2019)

Euroopan parlamentin tekoälysäädös kieltää esimerkiksi suuririskiset järjestelmät, jotka katsotaan selkeäksi uhkaksi kansalaisille. Tällaiseksi suuren riskin teknologiaksi on määritelty muun muassa tekoälyjärjestelmät, joita käytetään työllistämisessä, henkilöstöhallinnossa ja itsenäisen ammatinharjoittamisen mahdollistamisessa. Erityisesti järjestelmät, jotka liittyvät henkilöiden rekrytointiin ja valintaan, uralla etenemistä ja työsuhteen päättämistä koskevien päätösten tekemiseen sekä tehtävien jakamiseen työhön liittyvissä sopimussuhteissa oleville henkilöille ja heidän seurantaansa tai arviointiinsa, olisi luokiteltava suuririskisiksi. Nämä järjestelmät voivat vaikuttaa merkittävästi henkilöiden tuleviin uranäkymiin ja toimeentuloon. (Euroopan parlamentin tekoälysäädös 2021)

Taustatarkistuksille on nyt ja tulevaisuudessa yhä suurempi tarve onnistuneen rekrytoinnin toteuttamisessa tai alihankintaprojektien vastuullisuuden ja due diligence (engl.) kysymysten selvittämisen yhteydessä. On kuitenkin tiedostettava, että lainsäädäntöprosessit ovat hitaita, ja ne ovat usein kompromisseja yksityisyydensuojan ja yritysten tavoitteiden välillä. Tämän takia toimialan sisällä tapahtuvan eettisen keskustelun, eettisten ohjeiden ja sisäisen säännöstelyn merkitys on huomattavan tärkeää. Mitä paremmin toimiala pystyy itsenäisesti ohjaamaan palveluntarjoajien toimintaa, sitä luotettavampi ja myös läpinäkyvämpi prosessista tulee. Samalla onnistuessaan tämä sääntely toimisi hyvänä pohjana lainsäädäntötyölle, ja liiketoimintaa merkittävästi haittaavia kieltoja ei tarvitsisi tehdä poliittisessa päätöksentekoprosessissa alan huonon julkisuuskuvan vuoksi.

Yritysturvallisuuden kannalta työnhakijoille suoritettavan taustatarkistuksen avulla voidaan vaikuttaa kokonaisturvallisuuteen sekä estää esimerkiksi väärennettyjen työ- tai tutkintotodistusten käyttäminen työnhaussa. Läpinäkyvä ja lainmukainen taustatarkistusprosessi on omiaan luomaan molemminpuolista luottamusta työnantajan ja työntekijän välille. Myös avoimien tietolähteiden käyttäminen tässä tarkastelussa on mahdollista rekrytoitavan luvalla. Vaatimukset hyvälle taustatarkistusprosessille ovat selkeät: läpinäkyvyys, yksityisyydensuojan ja kohteen oikeusturvan kunnioittaminen sekä rekrytoivan edun huomioiminen. Koska taustatarkistuksen merkitys rekrytointiprosessissa on tärkeä, sen tulisi olla luonnollinen osa yritysturvallisuutta ja henkilöstöjohtamisprosessia.

Avoimien tietolähteiden hyödyntäminen ei ole poissuljettu taustatarkistuksen tai luotettavuuden arvioinnin työkaluna, mutta laillisten edellytysten tulee täyttyä täysimääräisesti. Tällä hetkellä merkittävimmät toimintaa määrittelevät säädökset ovat EU:n tietosuoja-asetus, laki yksityisyyden suojasta työelämässä sekä tietosuojalaki, jotka määrittelevät tarkastuksen kohteen oikeuksia sekä minkälaista tietoa voidaan kohteesta kerätä. EU:n yleinen tietosuoja-asetus edellyttää, että tietoja käsitellään asianmukaisesti ja

lainmukaisesti, tiettyä ja laillista tarkoitusta varten. Se määrittelee henkilötiedoksi myös kaiken tiedon, jonka perusteella henkilö voidaan yksilöidä suoraan tai välillisesti yhdistämällä eri tietoja yhteen.

Taulukossa 1 esitetään opinnäytetyön tekijän johtopäätöksiä ja havaintoja opinnäytetyön aiheeseen liittyen sekä materiaaleja, joiden avulla näihin johtopäätöksiin on tultu.

Johtopäätös/havainto	**Lähde**
Turvallisuusselvityksen laatimisen lähteet viranomaisen toiminnassa	Turvallisuusselvityslaki
Työntekijän tai rekrytoitavan yksityisyydensuoja	Laki yksityisyydensuojasta työelämässä
Rekisteröidyn oikeudet, oikeus päättää henkilötietojen käsittelystä, henkilötietojen määritelmä	Euroopan unionin tietosuoja-asetus Tietosuojalaki Tietosuojavaltuutetun toimisto
Taustatarkistuksen ja taustaselvityksen määritelmä	SFS-EN 15602 Turvallisuusalan toimittaja, terminologia
Lainsäädäntö rajoittaa taustatarkistuksien laatimista	Euroopan unionin tietosuoja asetus Laki yksityisyydensuojasta työelämässä Data protection working party, pöytäkirjat
Tiedon oikeellisuus ja luotettavuus ovat taustatarkistuksen kivijalkoja	Euroopan ihmisoikeussopimuksen 8. artikla Euroopan unionin tietosuoja-asetus The National consumer law center, *Broken Records Redux* -julkaisu
Taustatarkistuksen kohteen yksityisyydensuoja on keskeinen lähtökohta	Euroopan unionin tietosuoja-asetus Laki yksityisyydensuojasta työelämässä Data protection working party, pöytäkirjat
Prosessin läpinäkyvyys on tärkeä tekijä kaikkien osapuolten oikeusturvan kannalta	Data protection working party, pöytäkirjat
Tulevaisuuden kehitys ja tekoäly tuovat uusia riskejä	Haastattelu Mikko Hyppönen

Taulukko 1. Opinnäytetyön johtopäätökset sekä lähteitä, joiden avulla johtopäätöksiin on tultu.

Taustatarkistuksen kohteen oikeuksien toteutuminen voi edelleen vaarantua, mikäli taustatarkistuksia ryhdytään toteuttamaan EU:n ulkopuolella. Erityisesti näin voi käydä siinä vaiheessa, kun tekoälyyn ja koneoppimiseen perustuvat palvelut alkavat yleistyä. Rekrytoitavan on tällöin mahdotonta tietää, onko esimerkiksi hylkäävä rekrytointipäätös perustunut tosiasialliseen pätevyysvertailuun hakemuksen perusteella vai onko työnantaja käyttänyt EU:n ulkopuolista taustatarkistuspalvelua työnhakijan tietämättä ja perustanut päätöksensä palvelun tuottamaan raporttiin.

Yhteenvetona voidaan todeta, että edellä mainittu alan sisäinen sääntely Euroopan unionin alueella olisi tärkeää. Tällä voitaisiin mahdollistaa tarkastuksen kohteen yksityisyydensuojan ja lakisääteisten oikeuksien toteutuminen sekä samalla vaikuttaa tulevaan lainsäädäntöön. Yleensä maan tapa on voinut muuttua lainsäädännöllä vahvistetuksi toiminnaksi, mikäli ala on omatoimisesti kyennyt toteuttamaan sisäisen ohjeistuksen ja toimijat ovat myös noudattaneet ohjeistusta. Tällä hetkellä on selvää, ettei lainsäädäntö ole tuomassa nopeaa ja selkeää ratkaisua tilanteeseen. Alan sisäinen sääntely voisi tarkoittaa eettisiä ohjeita, yhtenäisiä toimintaohjeita, määritelmän hyväksytyistä tietolähteistä ja vaatimuksen tarkastuksen kohteen etujen suojelemisesta sekä taustatarkistusprosessin läpinäkyvyydestä.

10.1 Opinnäytetyön reflektio ja luotettavuus

Opinnäytetyössä käsitelty aihepiiri on erittäin laaja, minkä vuoksi avoimien tietolähteiden tiedustelua on käsitelty suppeasti, rajattuna taustatarkistuksen näkökulmaan. Aiheesta löytyy varmasti useita erilaisia näkemyksiä ja tulkintoja, minkä vuoksi työssä on hyödynnetty yleisesti hyväksyttyjä näkemyksiä. Lähdeaineiston osalta on pyritty säilyttämään hyvä lähdekriittisyys. Haasteita toi, että aihetta on käsitelty hyvin vähän Suomessa joko juridiselta tai eettiseltä kannalta. Kansainvälisesti arvostettuja lähdeteoksia löytyy runsaasti, mutta niiden heikkous on, etteivät opit sovellu sellaisenaan eurooppalaiseen toimintaan. Pääsääntöisesti tämä johtuu kansallisista eroista henkilösuojassa, yksityisyyden suojassa sekä rekistereiden julkisuudessa.

Opinnäytetyö vastaa saatavilla olevista lähteistä kerätyn tiedon osalta nykytilannetta. Avoimien tietolähteiden tiedustelun ja tiedon käyttämisen osalta elämme jatkuvan muutoksen aikaa, minkä vuoksi opinnäytetyössä esitetyt näkemykset saattavat muuttua lyhyessäkin ajassa vanhentuneiksi. Tähän voi myös vaikuttaa, jos toimintaa ryhdytään sääntelemään

viranomaismääräyksin, kansallisen lainsäädännön tai Euroopan unionin säädöksien avulla. Eettisen pohdinnan osalta tilanne tulee tuskin muuttumaan merkittävästi, mutta globaalien tilanteiden muutokset saattavat vaikuttaa eettisiin arvoihin. Esimerkiksi Venäjän Ukrainassa tekemän sotilaallisen hyökkäyksen yhteydessä ei länsimaissa ole katsottu venäläisten sotilaiden tietojen julkaisemista verkossa merkittäväksi henkilötietojen käsittelyksi.

Keskeisenä teemana opinnäytetyössä on ollut Suomessa ja Euroopassa tehtävät yksityisen sektorin toimesta laaditut taustatarkistukset. Työssä on pyritty keskittymään lainsäädännön rajoitteisiin ja eettiseen pohdintaan. Opinnäytetyön tiedon hankinnassa on nojauduttu pääasiassa henkilötietojen käsittelyä määrittävään, voimassa olevaan lainsäädäntöön ja niiden perusteluihin. Työssä esitetyt näkemykset ja tiedot on pyritty vahvistamaan useammasta lähteestä, pois lukien asiantuntijoiden haastatteluissa lausumat näkemykset.

Työn tuloksien hyödyntäminen riippuu lukijan taustasta. Jos ajattelumallin mukaan tarkoitus pyhittää keinot, voi ajattelumallin muuttaminen olla vaikeaa. Suurin merkitys opinnäytetyöllä on organisaatioille ja taustaselvityksiä laativille toimijoille, jotka haluavat pohtia oman toimintansa eettisyyttä ja lainmukaisuutta. Eettisesti ja lainsäädännöllisesti opinnäytetyössä käsiteltyjä teemoja voidaan hyödyntää toimintaohjeiden ja -mallien luomisessa sekä laillisen ja eettisen tarkastelun kestävän toimeksiannon suunnittelussa.

Lähteet

Painetut

Alasuutari, P. 2011. Laadullinen tutkimus 2.0. Vastapaino: Tampere.

HE 203/2017 vp, Hallituksen esitys eduskunnalle laiksi sotilastiedustelusta sekä eräiksi siihen liittyviksi laeiksi.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2013. Tutki ja kirjoita. 18. painos. Helsinki: Tammi.

Lohse, M. & Viitanen, M. 2018. Johdatus tiedusteluun. Helsinki: Alma Media.

Lohse, M., Honkanen, K., Meriniemi, M., Honkanen, K. & Meriniemi, M. 2019. Tiedustelumenetelmät. Helsinki: Alma Talent.

Ollila, M-R. 2019. Tekoälyn etiikka. Helsinki: Kustannusosakeyhtiö Otava.

Pitkänen, O, Tiilikka, P. & Warma, E. 2013. Henkilötietojen suoja. Helsinki: Talentum.

Tietosuojavaltuutetun toimisto 2022. Työelämän tietosuojan käsikirja. Viitattu: 31.5.2022. https://tietosuoja.fi/documents/6927448/10594424/Ty%C3%B6el%C3%A4m%C3%A4n+tietosuojan+k%C3%A4sikirja+tietosuojavaltuutetun+toimisto.pdf/81dc78c3-6915-2893-5a19-62e3bc82988b/Ty%C3%B6el%C3%A4m%C3%A4n+tietosuojan+k%C3%A4sikirja+tietosuojavaltuutetun+toimisto.pdf?t=1600239849254

Trottier, D. 2015 “Open source intelligence, social media and law enforcement: Visions, constraints and critics”, European Journal of Cultural Studies, 18. SAGE Publications

Trottier D. 2015. Coming to terms with social media monitoring: Uptake and early assessment. Crime, Media, Culture: An International journal. Sage Publications

SFS.2008. SFS-EN 15602 Turvallisuusalan toimittaja, terminologia. Helsinki: Suomen Standardoimisliitto.

Sähköiset

Aalto Yliopisto. Kirjoita asiantuntevasti. Kurssimateriaali. Aalto Yliopisto: Espoo Viitattu: 2.1.2022
https://mycourses.aalto.fi/mod/book/view.php?id=688064&chapterid=5302&lang=fi

Anderson, M & Leigh Anderson, S. 2011. Machine Ethics. Cambridge University Press. https://ebookcentral.proquest.com/lib/laurea/detail.action?docID=691859.

Azets 2020. Mitä tietoja työnhakijasta voidaan selvittää? Azets verkkosivut. Viitattu: 31.5.2022
https://www.azets.fi/blogi/mita-tietoja-tyonhakijasta-voidaan-selvittaa/

EK 2021. Lausunto yksityisyyden suojasta työelämässä annetun lain 4 §:n muuttamisesta. Elinkeinoelämän keskusliitto. Viitattu 31.5.2022.
https://ek.fi/lausunnot/lausunto-yksityisyyden-suojasta-tyoelamassa-annetun-lain-4-%C2%A7n-muuttamisesta/

EU 2016. ARTICLE 29 DATA PROTECTION WORKING PARTY. 2016. 17/EN/WP260 rev.01. Viitattu 18.6.2021.
https://ec.europa.eu/newsroom/article29/redirection/document/51025

EU 2013. ARTICLE 29 DATA PROTECTION WORKING PARTY. 2013. 00569/13/EN WP203. Viitattu 18.6.2021.
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Bellingcat. Bellingcat-kotisivut. Viitattu: 30.12.2021
https://www.bellingcat.com/about/

Bellingcat annual report 2020. 2020. Bellingcat järjestön vuosirapotti.
https://www.bellingcat.com/app/uploads/2021/05/Bellingcat-Annual-Report-2020-1.pdf

Eijkeman, Q & Weggemans, D. 2013. Open Source Intelligence and Privacy Dilemmas: Is it Time to Reassess State Accountability?. Tieteellinen artikkeli. Reseachgate.
https://www.researchgate.net/publication/256057526_Open_Source_Intelligence_and_Privacy_Dilemmas_Is_it_Time_to_Reassess_State_Accountability/citations

EU 2016. Euroopan yleinen tietosuoja-asetus (EU) 2016/679. Viitattu 22.6.2021.
https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI

Euroopan parlamentin ja Neuvoston asetus tekoälyä koskevista yhdenmukaistetuista säännöistä (tekoälysäädös) ja tiettyjen unionin säädösten muuttamisesta. Säädösehdotus. 2021. Viitattu 17.3.2021.
https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0007.02/DOC_1&format=PDF

Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi HE 9/2018. Viitattu 10.6.2021.
https://www.finlex.fi/fi/esitykset/he/2018/20180009

Hallintovaliokunta. Valiokunnan mietintö HaVM 13/2018 vp. Viitattu 30.5.2022
https://www.eduskunta.fi/FI/vaski/Mietinto/Sivut/HaVM_13+2018.aspx

Huuskonen, M. 2005. Yliopistojen vääriä tutkintotodistuksia kaupataan internetissä. Artikkeli. Helsingin Sanomat. Viitattu 11.11.2021.
https://www.hs.fi/kotimaa/art-2000004307539.html

Iltasanomat.2012. Nyt löytyi valetradenomi - työnantaja antoi potkut ja perään laskun. Artikkeli. Viitattu 11.11.2021.
https://www.is.fi/kotimaa/art-2000000476068.html

Juntunen, E & Huuskonen, M. 2009. Valelääkäri vei luottamuksen Karkkilan terveyspalveluilta. Helsingin Sanomat. Viitattu 11.11.2021.
https://www.hs.fi/kotimaa/art-2000004703919.html

JulkiTerhikki. 2022. Tietoa rekisteristä. Valvira. Viitattu: 29.5.2022
https://www.valvira.fi/valvira/rekisterit/terveydenhuollon_ammattihenkilot/julkiterhikki

Jyväskylän yliopisto. 2021. Laadullinen analyysi. Verkkosivut. Viitattu: 2.1.2022
https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineiston-analyysimenetelmat/laadullinen-analyysi

Nath Solicitors Limited. 2020. Open Source Intelligence (OSINT) Solicitors London. Viitattu 10.6.2021.
https://www.nathsolicitors.co.uk/open-source-intelligence-osint-solicitors-london/

Nelson, A. 2019. Broken Records Redux. Boston: The National Consumer Law Center. Julkaisu. Viitattu 22.11.2021.
https://temeculaconsumerattorneys.com/wp-content/uploads/2019/12/NCLC-report-on-background-checks.pdf

Nordic Law. 2019. Yrityskauppa – henkilötietojen luovuttaminen ja huomioiminen due diligence -vaiheessa. Nordic Law verkkosivut. Artikkeli. Viitattu 22.6.2021.
https://nordiclaw.fi/yrityskauppa-henkilotietojen-luovuttaminen-ja-huomioiminen-due-diligence-vaiheessa/

Maltego. Yrityksen kotisivut. Viitattu: 3.1.2022
https://www.maltego.com/product-features/

Mayer Brown. 2016. A Global Guide to Background Checks. Lontoo: The Mayer Brown Practices. Viitattu 1.7.2021.

https://www.mayerbrown.com/en/perspectives-events/publications/2016/04/a-global-guide-to-background-checks

Moilanen, H. 2014. Valelääkärin entiset työkaverit: Esa Laiho hurmasi itsevarmuudellaan. Artikkeli. Helsingin Sanomat. Viitattu 11.11.2021. https://www.hs.fi/kaupunki/art-2000002703218.html

Laki yksityisistä turvallisuuspalveluista 2015/1085. Viitattu 20.5.2022. https://www.finlex.fi/fi/laki/ajantasa/2015/20151085?search%5Btype%5D=pika&search%5Bpika%5D=laki%20yksityisist%C3%A4%20turvallisuuspalveluista

Laki taustatarkastuksista 2014/726. Viitattu 30.5.2022. https://www.finlex.fi/fi/laki/ajantasa/2014/20140726?search%5Btype%5D=pika&search%5Bpika%5D=laki%20turvallisuusselvityksist%C3%A4

Lo Piano, S. 2020. Ethical principles in machine learning and artificial intelligence: cases from the field and possible ways forward. Humanities & Social Science Communication. https://doi.org/10.1057/s41599-020-0501-9

Ollila, M-R. 2019. Tekoälyn etiikka. E-kirja. Helsinki: Kustannusosakeyhtiö Otava.

Pastor-Galindo, J., Nespoli, P., Gómez Mármol, F. & Martinez Pérez, G. 2020. The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. IEEE: New York. Viitattu: 30.12.2021 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8954668

Perustuslakivaliokunta. Valiokunnan lausunto PeVL 14/2018 vp. Viitattu 30.5.2022. https://www.eduskunta.fi/FI/vaski/Lausunto/Sivut/PeVL_14+2018.aspx

TEPA-termipankki. Erikoisalojen sanastojen ja sanakirjojen kokoelma. Sanastokeskus TSK. Viitattu: 20.12.2021 https://termipankki.fi/tepa/fi/

Vainio, K. 2021. Tiedustelun renessanssi – järjestöt ja yritykset haastavat tiedustelupalveluiden monopolin. Ulkopolitiikka-lehti. 2/2021. Verkkoartikkeli. Helsinki: Ulkopoliittinen instituutti. Viitattu: 29.5.2021. https://ulkopolitiikka.fi/lehti/2-2021/tiedustelun-renessanssi/

Vilkka, H. 2014. Tutki ja mittaa. Määrällisen tutkimuksen perusteet. Viitattu 8.9.2016. http://hanna.vilkka.fi/wp-content/uploads/2014/02/Tutki-ja-mittaa.pdf

Winder, D. 2020. CIA Secretly Owned Global Encryption Provider, Built Backdoors, Spied On 100+ Foreign Governments: Report. Artikkeli. Forbes. https://www.forbes.com/sites/daveywinder/2020/02/12/cia-secretly-bought-global-encryption-provider-built-backdoors-spied-on-100-foreign-governments/?sh=491885ba580a

Yleinen tietosuoja-asetus. 2021. Yleinen tietosuoja-asetus. Euroopan unioni. Viitattu 11.6.2021. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

Julkaisemattomat

European Data Protection Board. Sähköposti vastaus kirjalliseen kysymykseen. 15.6.2021.

Professori Jarno Limnéll. Sähköposti vastaus kirjalliseen kysymykseen. 16.6.2021.

Oikeustieteen tohtori Eelis Paukku. Sähköposti vastaus kirjalliseen kysymykseen. 1.7.2021.

Turvallisuusasiantuntija Hannu Huttunen, HPH Consulting Oy. Sähköposti vastaus kirjalliseen kysymykseen. 12.7.2021.

Tietosuojavaltuutetun toimisto. Puhelinhaastattelu. 8.7.2021

Kuvat

Taulukot

Liitteet

Liite 1: Rekrytoitavan henkilön henkilötietojen käsittelyn perusteet

Tietolähteenä on pääsääntöisesti rekrytoitavan ilmoittamat tiedot ansioluettelossa ja työhakemuksessa.

Käsittely on tarpeen kolmannen osapuolen tai rekisterinpitäjän etujen suojaamiseksi perustetta käytettäessä tulee kyetä kiistattomasti osoittamaan merkittävä etu, jonka suojaamiseksi on välttämätöntä tarkastaa tämä henkilötieto.

Käsiteltävä henkilötieto	*peruste*	*peruste*
Nimi	Sopimus	Suostumus
Asuinpaikka	Sopimus	Suostumus
Yhteystiedot	Sopimus	Suostumus
Edelliset työnantajat	Suostumus	Käsittely on tarpeen kolmannen osapuolen tai rekisterinpitäjän etujen suojaamiseksi.
Ilmoitetut tutkinnot (oppilaitokset)	Suostumus	Käsittely on tarpeen kolmannen osapuolen tai rekisterinpitäjän etujen suojaamiseksi.
Ammattipätevyyden tarkastus	Suostumus	Käsittely on tarpeen kolmannen osapuolen tai rekisterinpitäjän etujen suojaamiseksi.
Oikeuden lainvoimaset tuomiot, mikäli oikeutettu peruste.	Suostumus	Käsittely on tarpeen kolmannen osapuolen tai rekisterinpitäjän etujen suojaamiseksi.
Medialähteet	Suostumus	Käsittely on tarpeen kolmannen osapuolen tai rekisterinpitäjän etujen suojaamiseksi.
Poliittinen virka tai vaikutusvalta *Poliittinen virka tai vaikutusvalta toisessa valtiossa tulee kysymykseen yrityksen toiminnan laajentuessa ulkomaille tai ulkomaisen yhteistyökumppanin osalta.*	Suostumus	Käsittely on tarpeen kolmannen osapuolen tai rekisterinpitäjän etujen suojaamiseksi.

Lähde: Euroopan Unionin yleinen tietosuoja asetus

Liite 2: Muistilista merkittävimmistä vaatimuksista

Aihe	Selite
Henkilötieto	Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Henkilötietoja ovat esimerkiksi nimi, puhelinnumero, sijaintitiedot ja isovanhempien perinnöllisiä sairauksia koskevat tiedot.
Tiedon suojaaminen ja luottamuksellisuus	Vastuu kerättyjen henkilötietojen turvassa pitämisestä. Se, että tieto on kerätty avoimista lähteistä, on täysin merkityksetöntä tiedon suojaamisen kannalta. Muista: Mikäli et voi suojata dataa, älä kerää sitä.
Luotettavuus	Taustatarkistusprosessissa ei saa olla henkilöiden sekoittumisen mahdollisuutta, mikäli tietoa ei varmuudella voida liittää kohdehenkilöön, ei sitä tule käyttää.
Läpinäkyvyys	Rekisteröidylle on kerrottava: • mitä henkilötietoja hänestä kerätään • mihin tarkoitukseen hänen henkilötietojaan käsitellään • millä tavoin hänen henkilötietojaan käsitellään • millaisia oikeuksia hänellä on Muista: Ole vastuullinen, huomioi rekisteröidyn oikeudet.
Datan tarkoituksenmukaisuus	Tietoa, mitä kerätään yhteen tarkoitukseen, ei tule käyttää toiseen yhteensopimattomaan tarkoitukseen.
Datan oikeellisuus	Tietojenkäsittelyssä on velvollisuus varmistaa, että tiedot ovat oikein, ei käytetä vanhentuneita tietoja tai tietoja, joiden tiedetään olevan virheellisiä.
Datan minimointi	GDPR edellyttää, että käsiteltyjen henkilötietojen määrä minimoidaan siihen, mitä todella tarvitaan tietojenkäsittelyn tavoitteen saavuttamiseksi. Muista: Niin paljon kuin on tarpeen, niin vähän kuin mahdollista.

Datan säilytysajan minimointi	GDPR:n mukaan säilytysajan ei pitäisi olla "pidempi kuin tarvitaan". Tietojen säilyttämiskäytäntö ja -aika tulisi selkeästi olla määritelty ja rekisteröidyn tiedossa, pois lukien rikosprosessi tai merkittävän edun turvaaminen.
Säilytettävän datan minimointi	Henkilötietojen oikean määrän arvioimiseksi on selkeästi tunnistettava se syy, miksi kyseisiä henkilötietoja tarvitaan. Käyttötarkoituksen kautta pystytään määrittelemään, mitkä henkilötiedot ovat välttämättömiä käsittelyn tarkoituksen toteuttamiseksi.
Käsittelyn laillisuus	Tietosuoja-asetuksessa on kuusi eri perustetta, joilla henkilötietojen käsittely on mahdollista: • rekisteröidyn suostumus • sopimus • rekisterinpitäjän lakisääteinen velvoite • elintärkeiden etujen suojaaminen • yleistä etua koskeva tehtävä tai julkinen valta • rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu.
Kohteen oikeudet	Rekisteröity voi käyttää oikeuksiaan seuraavasti: • Oikeus saada pääsy henkilötietoihin • Oikeus tietojen oikaisemiseen ja käsittelyn rajoittamiseen • Oikeus tietojen poistamiseen • Oikeus kieltää tietojen siirtämisen järjestelmästä toiseen • Oikeus vastustaa henkilötietojen käsittelyä • Paitsi, jos rekisterinpitäjä voi osoittaa, että • Oikeus peruuttaa suostumus • Oikeus tehdä valitus valvontaviranomaiselle
Datan hävittäminen	Kerätty data tule hävittää välittömästi, kun laillinen peruste sen käsittelylle päättyy. Tämä voi johtua kohteen kieltäessä datan käsittely tai toimeksiannon valmistuttua.