Aku Kettunen

TEKNOLOGIAN VAIKUTUS YKSITYISYYTEEN KIINASSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Kettunen, Aku
Teknologian vaikutus yksityisyyteen Kiinassa
Jyväskylä: Jyväskylän yliopisto, 2024, 30 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Halttunen, Veikko

Teknologian nopea kehitys on aiheuttanut merkittäviä yksityisyysongelmia erityisesti tietojen keräämisen ja sen käsittelyn osalta ja näihin ongelmiin on vaihtelevia reaktioita: Euroopan unioni pyrkii suojelemaan yksilön yksityisyyttä ja rajoittamaan yksityistä tietoa keräävien teknologioiden käyttöä, kun taas Kiina käyttää niitä luodakseen laajan valvontainfrastruktuurin. Koska yksityisyyden määritelmä vaihtelee kulttuurien ja kansojen välillä, tutkielmassa tarkasteltiin, kuinka yksityisyys määritellään Kiinassa ja kuinka tämä vaikuttaa sen tiedonkeruuseen ja teknologian käyttöön. Lisäksi tutkielmassa selvitettiin, mitä teknologioita tiedonkeräyksessä ja tarkkailussa käytetään ja miten kerättyä tietoa käytetään. Erityisesti tutkielmassa keskityttiin kansalaisen näkökulmaan, sekä mitä hyötyjä ja haittoja Kiinan lähestymistavasta heille on. Tutkimuskysymys oli seuraava: Onko yksityisyyden uhraaminen teknologian hyötyjen saamiseksi hyväksyttävä lähestymistapa? Aiheesta löytyy aiempaa tutkimusmateriaalia, mutta tutkimuskysymys ja ajankohta antavat tärkeän näkökulman aiheeseen ja tarjoavat vaihtoehtoisen näkökulman teknologian ja yksityisyyden suhteelle. Tutkielma toteutettiin systemaattisena kirjallisuuskatsauksena. Tutkielman aineistona oli 30 vertaisarvioitua englanninkielistä tutkimusta, jotka haettiin Google Scholar, Taylor & Francis, ja Elsevier – tietokantoja käyttäen hakutermejä kuten Data privacy in China, Social Credit System, ja Technology and privacy. Tutkielmaan käytettiin sekä kansainvälisiä, että kiinalaisia tutkimusartikkeleita. Tutkielmassa selvisi, että Kiinassa pääasiassa yhteisön etua arvostavan kulttuurin takia yksityisyyttä ei ole pidetty korkeassa arvossa. Kuitenkin yksilön yksityisyyden tärkeys on noussut etenkin uusien teknologioiden vaatiessa hyvin arkaluontoista informaatiota. Massadataa analysoimalla Kiina saa kerättyä suuren määrän yksityistä informaatiota ja arkaluontoisen informaation keräämiseen käytetään pääasiassa kasvojentunnistusteknologiaa ja GPS-jäljityssovelluksia. Kerättyä informaatiota käytetään etenkin sosiaaliseen luottoluokitusjärjestelmään. Kiinan lähestymistavasta yksityisyyteen on selkeitä hyötyjä kansalaisille, kuten korkeampi turvallisuus. Kuitenkin yksityisen informaation käyttö mm. vähemmistöjen syrjintään vahvasti kyseenalaistaa sen, voiko Kiinan tiedustelujärjestelmä olla kansalaisille eduksi.

Asiasanat: yksityisyys, yksityisyys verkossa, datankeräys, massadata, koneoppiminen, sosiaalinen luottoluokitusjärjestelmä

ABSTRACT

Kettunen, Aku
How technology affects privacy in China
Jyväskylä: University of Jyväskylä, 2024, 30 pp.
Information Systems Science, Bachelors' Thesis)
Supervisor: Halttunen, Veikko

The rapid development of technology poses significant privacy concerns, particularly regarding information collection and data privacy. Global reactions vary; the European Union aims to protect individual privacy and limit the use of private information collecting technologies, while China uses them to build extensive surveillance infrastructure. Given the cultural differences in defining privacy, this research investigates how privacy is defined in China, its influence on information gathering, and the use of technology. It examines what technologies are used for information collection and surveillance, and how the collected information is used. A specific focus was on the Chinese citizens' perspectives and the advantages and disadvantages of China's approach. The research question was the following: Is sacrificing privacy for technological benefits an acceptable approach? Prior research material on the subject is available, but the research question and recency of the study offer an important point of view to the subject as well as an optional viewpoint on the relationship between technology and privacy. Conducted as a systematic literature review, the study utilized 30 cross-evaluated English-language articles sourced from Google Scholar, Taylor & Francis, and Elsevier with terms like "Data privacy in China," "Social Credit System," and "Technology and privacy." Both international and Chinese studies were included. The research article found that because of China's group-based culture individual privacy has not been highly valued. However, its importance is growing especially because of technologies demanding sensitive information. China can collect large amounts of private information by analyzing big data, and sensitive private information is collected using technologies like facial recognition and GPS applications. The collected information is primarily used for the Social Credit System. While China's approach offers benefits such as enhanced security, its use of private information for minority discrimination and other issues raises serious concerns about the system's overall benefit to citizens.

Keywords: privacy, data privacy, collection of data, big data, machine learning, The Social Credit System

SISÄLLYS

TIIVISTELMÄ
ABSTRACT
KUVIOT JA TAULUKOT

1 JOHDANTO 5

2 YKSITYISYYS KÄSITTEENÄ 7
2.1 Yksityisyyden määritelmiä 7
2.2 Yksityisyys Kiinassa 10
2.3 Kiinan yksityisyys verkossa 12

3 TIETOJEN KERÄÄMINEN 15
3.1 Tiedon keräämisen teknologia 15
3.2 Yksityisen tiedon keräämisen käyttötarkoitus 17
3.3 Sosiaalinen luottoluokitusjärjestelmä 18
3.4 Kansalaisen näkökulma 21
3.5 Lähitulevaisuus 24

4 JOHTOPÄÄTÖKSET JA YHTEENVETO 26

LÄHTEET 29

1 JOHDANTO

Yksityisyyden määritelmä on kehittynyt paljon vuosien aikana ja se vaihtelee paljon eri kulttuurien, uskontojen, ja ihmisten välillä. Nykyään erityisesti yksityisyys verkossa on uhattuna nopeasti kehittyvän teknologian, kuten tekoälyn takia (Wisniewski & Page, 2022). Lisäksi ihmisten tarkkailu on muuttunut perusteellisesti määrätietoisesta tietyn informaation etsimisestä päämäärättömään massadatan keräämiseen kaikesta (Andrejevic & Gates, 2014). Tämä on aiheuttanut tarkkailun oletetun vaaran laskemisen yksilöiden mielessä, koska massadatan keräys on vaikeasti havaittavissa mutta Ahon ja Duffieldin (2020) mukaan se mahdollistaa käyttäytymisprofiilien luonnin ja jopa kansan massamanipuloinnin, mikä tekee siitä hyvin vaarallista. Tarkkailun huomaamattomuus ja sen suuri riski tekevät yksityisyyden turvasta hyvin ajankohtaisen ongelman.

Tilanne jakaa mielipiteitä ja reaktiot vaihtelevat suuresti valtioiden välillä. Esimerkiksi Euroopan Unionissa nojataan vahvasti demokraattisiin arvoihin ja yksilön oikeuksien suojeluun, joten yksityisyyttä vaarantavien teknologioiden käyttöä pyritään rajoittamaan. Kiinassa arvomaailma puolestaan on kommunitaristinen ja yhteisön etua arvostava ja yksityisyyttä vaarantavia teknologioita hyödynnetään esim. yleisen turvallisuuden edistämiseen.

Tutkielman tarkoitus on olla osa laajempaa keskustelua yksityisyydestä verkossa ja tiedonkeräämisestä. Nykyään on käytännössä mahdotonta suojautua kokonaan informaation keräämiseltä, joten vaihtoehtoiset lähestymistavat yksityisyyteen ovat tarpeellisia (Knijnenburg ym., 2022). Vaikka Kiinan lähestymistapa on monella tapaa länsimaisen arvomaailman vastainen, sitä tarkkailemalla voidaan lisätä vaihtoehtoja ja saada uusia näkökulmia vähenevän yksityisyyden ongelman ratkaisemiseksi.

Kiinan näkökulman lisäksi tutkielmassa on tärkeää perehtyä yleisesti yksityisyyden luonteeseen, jotta voidaan tutkia yksityistä informaatiota keräävien teknologioiden tuomia etuja ja haittoja. Kansalaisten tiivis valvonta massadatalla ja valvontakameroilla mahdollistaa hyvin turvallisen yhteiskunnan, koska rikollisia ja epäiltyjä rikollisia voidaan jäljittää miltei reaaliajassa (Leibold, 2019). Tässä tutkielmassa tutkitaan asiaa perehtymällä yksityisyyden eettisiin arvoihin ja yksilön oikeuteen luopua omasta informaatiostaan. Esimerkiksi Hallinanin

ym., (2012) mukaan yksilön on hankala ottaa vastuu omasta yksityisestä informaatiostaan, kun taas Farrall (2008) kommentoi, että päätösvalta yksilön yksityisyydestä tulisi olla täysin yksilöllä itsellään. Tämän takia tutkielmassa halutaan löytää kompromissi yksilön ja valtion vastuun väliltä yksityisen informaation suhteen.

Kiina käyttää kehittynyttä teknologiaa yhteiskunnan edun lisäksi myös omiin tarkoitusperiin, kuten poliittiseen sensuuriin ja sosiaaliseen manipulointiin (Hou & Fu, 2022). Ahon ja Duffieldin (2020) mukaan etenkin Kiinan pyrkimys olla kaikkinäkevä valtio sosiaalisen luottoluokitusjärjestelmän avulla huolestuttaa kansainvälistä yhteisöä. Sosiaalinen luottoluokitusjärjestelmä pyrkii taloudellisen, sosiaalisen, ja poliittisen informaation perusteella pisteyttämään jokaisen Kiinan toimijan ja pistemäärän perusteella jakamaan joko palkintoja tai rangaistuksia (Aho & Duffield, 2020). Tämä tutkielma pyrkii tutkimaan neutraalisti sosiaalisen luottoluokitusjärjestelmän sosiaalisia, teknologisia, ja yhteiskunnallisia etuja suhteessa yksilön yksityisyyteen.

Tutkielma on toteutettu kirjallisuuskatsauksena. Tutkielmassa käytettiin 30:tä englanninkielistä vertaisarvioitua tutkimusartikkelia joiden hakemiseen hyödynnettiin Google Scholar, Taylor & Francis, ja Elsevier– tietokantoja. Hakutermeinä käytettiin termejä kuten privacy, data privacy, social sredit system, GDPR, ja PIPL. Puolueettomuuden takaamiseksi tärkeää oli löytää sekä kansainvälisiä että kiinalaisia tutkimusartikkeleita. Lisäksi yksityisyyttä tutkittaessa oli mahdollista tutkia myös ikääntyneitä tutkimusartikkeleita, mutta teknologioita ja niiden käyttötarkoituksia tutkittaessa oli tärkeää etsiä mahdollisimman ajankohtaisia tutkimusartikkeleita.

Tutkielman toisessa luvussa perehdytään yksityisyyden määritelmiin, jotta eri kulttuurien näkemykset sen tärkeydestä ovat ymmärrettäviä. Lisäksi tutkitaan yksityisyyden luonteen monimutkaisuutta ja yksilön suhdetta yksityisyyteen. Etenkin keskitytään Kiinan näkemykseen yksityisyydestä ja yksityisyydestä verkossa ja sen vaikutuksesta yksityistä tietoa keräävien teknologioiden käyttöön. Kolmannessa luvussa tutkitaan, mitä teknologioita Kiina varsinaisesti hyödyntää tietojenkeräykseen ja kansalaisten tarkkailuun ja miten kerättyä tietoa hyödynnetään yleisesti sekä etenkin sosiaalisessa luottoluokitusjärjestelmässä. Lisäksi tarkastellaan Kiinan tiedonkeräämistä kansalaisen näkökulmasta ja tulosten perusteella pyritään ennakoimaan, kuinka tilanne tulee mahdollisesti etenemään lähitulevaisuudessa. Neljännessä luvussa tehdään yhteenveto ja pyritään vastaamaan tutkimuskysymykseen: onko yksityisyydestä luopuminen teknologian etujen saamiseksi hyväksyttävä lähestymistapa kansalaisen näkökulmasta.

2 YKSITYISYYS KÄSITTEENÄ

Yksityisyyden määritelmä on muuttunut ajan kanssa paljon, etenkin uusien teknologioiden tuodessa uusia haasteita. Lisäksi yksityisyys on subjektiivinen termi, joka usein määritellään eri tavalla riippuen yksilön uskonnosta, kulttuurista, sekä ihmisestä itsestään (Wang, 2011). Tässä luvussa perehdytään siis tarkemmin yksityisyyden eri määritelmiin ja miten yksityisyys nähdään Kiinassa. Lisäksi tarkastellaan Kiinan tietoturvaa ja yksityisyyttä verkossa.

2.1 Yksityisyyden määritelmiä

Ihmiset on perinteisesti nähty vain yhteiskunnan jäseninä ja yksityisyys sai ensimmäisen kunnollisen määritelmän vasta 1800-luvun lopussa (Lukacs, 2016). Tällöin määritelmä pohjautui yksinkertaisesti oikeuteen olla yksin (Nissim & Wood, 2018). Vasta 1950-luvulla alkoi yleistyä käsitys yksityisyydestä ihmisoikeutena (Lukacs, 2016). Monet filosofit, poliitikot, ja sosiaalitieteilijät ovat sen jälkeen yrittäneet parannella ja laajentaa yksityisyyden määritelmää.

Yksityisyyden rajat eivät olekaan objektiiviset vaan sen rajat vaihtelevat paljon riippuen mm. kulttuurista eikä sille ole yhtä universaalia määritelmää (Lyon, 2007; Wang, 2011; Lukacs, 2016; Liu, Huang, Yan, Wang & Zhang, 2022). Yksityisyyden eettisyys puolestaan perustuu yksilön ja yhteiskunnan prioriteetteihin, arvoihin, toiminnallisuuksiin ja käyttötarkoituksiin (Buck, Dinev & Anaraky, 2022). Wangin (2011) mukaan yksityisyyttä on verrattu myös vapauteen tai tasa-arvoon, sillä se on enemmänkin ideologinen arvo, kuin konkreettinen määritelmä. YK:n ihmisoikeuksien yleismaailmallinen julistus antaa yksityisyydelle kuitenkin ihmisoikeuden määritelmän, joten keskustelu yksityisyydestä keskittyy yleensä sen rajoihin ja tarpeellisuuteen (Wang, 2011).

Wangin (2011) mukaan yksityisyydestä käytetään monesti yksin jättämisen lisäksi kahta muuta määritelmää. Ensimmäisen määritelmän mukaan yksityisyys on henkilön oikeus päättää omasta elämästään ja toisen määritelmän mukaan

yksityisyys on kyky päättää itse, milloin, miten, ja kuinka paljon informaatiota kommunikoidaan muille (Wang, 2011). Nämä määritelmät ovat kuitenkin puutteellisia sillä ne ovat liian suppeita ja yrittävät eristää yksityisyyden omaksi erilliseksi käsitteeksi, vaikka se on sidoksissa muihin sosiaalisiin käsitteisiin kuten autonomiaan, luottamukseen, ja läheisyyteen (Wang, 2011; Wisniewski & Page, 2022).

Yksityisyyden määritelmä riippuu myös yksilön ympäristöstä, kulttuurista, uskonnosta, ja hänen persoonallisuudestansa (Wang, 2011; Lukacs, 2016; Wisniewski & Page, 2022). Tämän takia yksityisyyden määritteleminen ja tutkiminen on hyvin hankalaa, koska sitä ympäröivä konteksti muuttuu jatkuvasti ja näihin muutoksiin taas suhtaudutaan eri tavalla riippuen kulttuurista. Etenkin uudet teknologiat haastavat yksityisyyttä. Esimerkiksi kameroiden ja tietokoneiden yleistyminen mullisti käsityksen yksityisyydestä ja pakotti sen uudelleenmäärittelyn (Smith, 2004; Lucaks, 2016). Kameroiden yleistyminen oli esimerkiksi uhka kansalaisten julkisten paikkojen yksityisyydelle ja siitä on vieläkin erimielisyyksiä kontekstista riippuen (Smith, 2004; Proferes, 2022). Lisäksi ennen sosiaalista mediaa yksityisyys nähtiin yleisesti vain päätösvaltana siitä mitä informaatiota ei haluttu jakaa muille, mutta se on nykyään paljon monimutkaisempaa (Wisniewski & Page, 2022).

Toisaalta teknologia on mahdollistanut myös yksityisyyden suojelemisen esimerkiksi päästä päähän -salauksella ja HTTPS-protokollalla (Seamons, 2022). Yksityisyyden ja teknologian vaikutus toisiinsa on siis hyvin kriittinen. On myös selvää, että yksityisyyden määritelmä on vaihtunut vuosikymmenien sisällä paljon, koska uusi teknologia on mahdollistanut tehokkaamman tiedonkeräämisen.

Tämän perusteella voidaan kuitenkin päätellä, että vaihtoehtoiset lähestymistavat yksityisyyden suojaan eivät automaattisesti ole huonompia kuin toiset. Erilaiset näkemykset ovat historian, ympäristön, ja kulttuurin muovaamia suhtautumistapoja yksityisyyden suojaan.

Vastaavasti Buckin ym., (2022) ja Nissimin ja Woodin (2018) mukaan yksityisyydensuoja nähdään tilannekontekstin kautta johon sisältyy sosiaalinen alue, jossa tietoa jaetaan, kuinka tietoa jaetaan, tiedon jakoon kuuluvat aktorit, ja itse tiedon tyyppi. Normaali informaation vaihto voi rikkoa yksityisyyden suojaa jos mikään osa kontekstissa muuttuu (Buck ym., 2022). Yksityisyyteen sisältyy myös mm. ajatuksen vapaus, fyysisen tilan vapaus, hallinta henkilökohtaisista tiedoista, suoja tarkkailulta, ja maineen suojelu (Wang, 2011). Yksityisyydensuojan kontekstiriippuvaisuus ja yksityisyyden vaikeamäärittelevyys tekee siihen liittyvistä laeista vaikeita määritellä ja maiden välisistä eroista suuria.

Yksityisyyden määrittelemisen monimutkaisuus onkin herättänyt keskustelua sen tarpeellisuudesta. Suosituimman tulkinnan mukaan yksityisyys tarjoaa neljä toiminnallisuutta: henkilökohtaisen autonomian, tunnepohjaisen vapautuksen, reflektoinnin, ja suojellun ja rajoitetun kommunikoinnin (Westin, 1968). Monet muut sosiaalifilosofit tukevat tätä tulkintaa yksityisyyden tarpeesta lisäten, että yksityisyys mahdollistaa erilaisten sosiaalisten suhteiden ylläpidon (Wang, 2011).

Tämä viittaa siihen, että yksityisyyden merkitys mielenterveydelle ja normaaleille ihmissuhteille on suuri. On myös selvää, että vaikka yksityisyydelle on eri määritelmiä niistä löytyy paljon samoja piirteitä, kuten yksilön oikeus henkiseen ja fyysiseen rauhaan ja vapaus päättää itse oman informaation jakamisesta. Lisäksi koska YK määrittelee yksityisyyden ihmisoikeudeksi nämä huomiot viittaavat tiettyyn yksityisyyden perustasoon, joka tulisi turvata huolimatta kulttuurista tai kontekstista. YK:n määritelmä yksityisyydestä on kuitenkin hyvin avoin jättäen valtioille paljon varaa muokata sitä. Tämä monimutkaistaa kansainvälisen informaation kulkua ja lainsäädäntöä etenkin nykypäivänä, kun internet mahdollistaa massiivisten datamäärien liikkumisen maiden välillä hetkessä.

Toisaalta Wang (2011) toteaa, että moni valtio näkee yksityisyyden välttämättömänä ja tarkoin suojeltuna oikeutena demokratian mahdollistamiseksi. Hän lisää, että ilman yksityisyyttä poliittiset puolueet eivät voi luoda argumenttejaan tai näkemyksiään turvassa (Wang, 2011). Tämä viittaa siihen, että yksityisyys ei ole pelkästään yksilöä koskeva arvo vaan myös demokraattisen yhteiskunnan edellytys.

Lukacsin (2016) mukaan nykypäivän ongelmat yksityisyyden suhteen ei tule valvonnasta sillä ihmisiä on valvottu hyvin pitkään. Ongelmana on mittakaava, tiedon säilyvyys, sekä kerätyn tiedon poistamisen vaikeus (Lukacs, 2016). Yksityisyys ei ole pelkästään oman informaation salailua vaan myös yksinkertaisesti jostain pois jättäytymistä. Ihmisellä pitäisi nykyaikaisten yksityisyyden periaatteiden mukaan olla mahdollisuus hallita, mitkä tiedot hänestä ovat julkisia ja mitkä eivät mutta se ei ole varsinaisesti enää mahdollista (Knijnenburg ym., 2022).

Vähenevä yksityisyys on herättänyt paljon keskustelua sen luonteesta ja yksilön oikeuksista omaan yksityisyyteensä. Yksilöllä tulisi monen yksityisyysteorian mukaan olla mahdollisuus vaikuttaa omaan yksityisyyteensä, vaikka valtiot säätävät yksityisyydensuojalait. Yksilöt haluavat joko suojella omaa informaatiotaan tai luopua siitä ja tätä päätöstä tutkitaan oletettujen etujen suhteessa oletettuihin riskeihin (Liu, Yan & Hu, 2021). Jos yksilö olettaa, että yksityisyydestä voi luopua ilman suurta riskiä ja siitä on huomattavia etuja on todennäköistä, että yksilö suostuu luopumaan yksityisyydestään (Liu ym., 2021; Wisniewski & Page, 2022).

Yksityisyyden ongelmaan on ehdotettu vaihtoehtoisia ratkaisuja. Farrallin (2008) mukaan päätösvalta yksilön yksityisen informaation käsittelystä tulee olla yksilöllä, joten jopa lait, jotka rajoittaisivat informaatiosta luopumista olisivat yksityisyyttä rikkovia. Toisaalta taas Wisniewskin ja Pagen (2022) mukaan ihmiset todennäköisesti tekevät yksityistä informaatiota koskevat päätökset välittömän mielihyvän perusteella eikä pitkän aikavälin hyödyllä. Lisäksi vaikka ihmiset sanovat haluavansa täyden hallinnan informaatiostaan he eivät kuitenkaan käytä tätä hallintakykyä hyödyksi (Wisniewski & Page, 2022).

Buckin ym., (2022) mukaan ratkaisut, joissa otetaan huomioon yksilöiden erot tulee olemaan kriittisiä, jotta haavoittuvaisempia yksilöitä voidaan suojella. Näiden pohjalta järjestelmä, joka suojelee yksityisyyttä mutta antaa myös haluk-kaille yksilöille mahdollisuuden vaikuttaa siihen tiettyyn rajaan asti vaikuttaisi

olevan paras lähestymistapa. Mahdollinen ratkaisu olisi käyttäjän yksityisyysmalli (eng. User Privacy Model), joka käyttää älykkäitä oppimismalleja, analysoi käyttäjän toimintaa, ja mukautuu käyttäjän yksityisyydentarpeisiin siirtämättä vastuuta kokonaan käyttäjälle (Knijnenburg ym., 2022). Tällaista järjestelmää tukee myös Nissimin ja Woodin (2018) huomiot siitä, että yksityisyyden määritelmä laissa on aina liian kapea ja teoreettiset määritelmät aina liian epärealistisia, joten näiden yhdistelmästä pitää löytyä toimiva määritelmä, joka vaihtelee jatkuvasti. Tällainen järjestelmä suojelisi yksilöitä, joiden tietoisuus yksityisyyden suojasta ei ole korkealla, vähentäisi väärinymmärryksiä joita syntyy pitkistä tietoturvakäytännöistä ja antaisi mahdollisuuden halukkaille vaihtaa yksityistä informaatiotaan palveluihin. Toisaalta jatkuvasti vaihteleva tai epätarkka määritelmä tekee mahdollisesti tilaa väärinkäytölle.

Yksityisyyden vaikea määriteltävyys ja yksilön mahdollisuus vaikuttaa omaan yksityisyyteensä positiivisesti tai negatiivisesti ja jopa todennäköisyys käyttää sitä valuuttana etujen saamiseksi tekee siitä hyvin monimutkaisen käsitteen. Yksityisyyden tärkeys demokraattisessa yhteiskunnassa ja sosiaalisissa suhteissa on kuitenkin kiistämätön ja tutkimukset aiheeseen viittaavat perustasoon, joka on pakko turvata kaikille. Kuitenkin muut tutkimustulokset yksityisyyden luonteesta vaihtelevat paljon kenties viitaten siihen, että perustason jälkeen tarkempaa universaalia määritelmää yksityisyydelle on vaikeaa löytää.

2.2 Yksityisyys Kiinassa

Kiinassa on perinteisesti suhtauduttu yksityisyyteen hyvin eri tavalla kuin Euroopan Unionissa tai Yhdysvalloissa. Kun länsimaissa liberalismi ja individualismi nousivat yhä tärkeämmiksi arvoiksi, Kiinassa kollektivismi ja kommunitarismi nousivat yhteiskunnan johtaviksi arvoiksi (Liu & Zhao, 2021). Lisäksi Yao-Huai (2005) ja McDougall (2004) huomioivat, että yksityisyys nähtiin pitkään vain ryhmiä, kuten perheitä koskevana eikä niinkään yksilöä koskevana. Moni kiinalainen vieläkin yhdistää yksityisyyden kiinalaiseen sanaan ”Yinsi”, joka tarkoittaa hävettävää salaisuutta tai jotain mitä pitää piilotella (Yao-Huai, 2005). Tämä eroaa länsimaisesta näkemyksestä, jossa yksityisyys on nähty enemmän vain oikeutena jättäytyä pois jostain (Wisniewski & Page, 2022).

Kiinassa yksityisyys nähdään myös instrumentaalisena hyvänä eli arvona, joka johtaa johonkin hyvään kuten sosiaaliseen järjestykseen, kun taas länsimaissa se usein nähdään luontaisena hyvänä eli arvona, joka on sinällään tavoittelun arvoinen (Yao-Huai, 2005; Farrall, 2008). Nämä huomiot viittaavat hyvin perustavanlaatuiseen eroon siinä miten kiinalaiset suhtautuvat yksityisyyteen. Ne myös selittävät, miksi yhteiskunnan edut on Kiinassa laitettu yksilön etujen edelle (Yao-Huai, 2005).

Yao-Huain (2005) mukaan kuitenkin viime vuosikymmeninä etenkin globalisaation seurauksena yksilön yksityisyyden tärkeys on kasvanut ja individualismi on noussut. Hän lisää, että esimerkiksi ennen 1980-lukua vanhemmat

pystyivät avaamaan lastensa postin ja mennä heidän huoneisiinsa, mutta nykyään se ei ole automaattisesti hyväksyttyä (Yao-Huai, 2005).

Mielipiteet ja asenteet yksityisyyttä kohtaan vaihtelevat kuitenkin vielä suuresti. Vuonna 2003 tehdyssä tutkimuksessa noin puolet vastaajista oli sitä mieltä, että yksilön yksityisyyttä tulisi suojella ja kunnioittaa (Yao-Huai, 2005). Lisäksi Kostkan, Steinackerin ja Meckelin (2020) tekemän tutkimuksen mukaan eri ikäluokkien mielipiteet yksityisyydestä eivät vaihdelleet paljoa eivätkä pitäneet yksityisyyttä korkeassa arvossa.

Myös mm. Wangin (2011), Lukacsin (2016), ja Wisniewskin ja Pagen (2022) huomiot yksityisyyden monimuotoisuudesta tukevat kansan mielipiteiden kahtia jakautuneisuutta. Ei voi kuitenkaan vielä todeta, että Kiina olisi siirtymässä täysin individualistiseen kulttuuriin sillä Kiina on poliittisesti vahvasti kommunistinen, joten individualismin ei ole välttämättä mahdollista laajentua.

Kiinalaiset tutkijat ja filosofit ovat yksityisyyttä tarkkaillessaan päätyneet samankaltaisiin lopputuloksiin kuin länsimaalaiset tieteilijät. Eräät kiinalaiset filosofit ovat sanoneet yksityisyyden olevan ihmisen perustavanlaatuisin oikeus, koska ilman sitä ei voi olla sananvapautta ja ilman sananvapautta ei voi päättää henkilökohtaisista asioista (Yao-Huai, 2005). Eräät kiinalaiset professorit määrittelevät yksityisyyden näin: ihmisen henkilökohtainen informaatio, aktiviteetit, suhteet, ja muut asiat, jotka eivät liity Kiinan julkiseen etuun, ovat suojattu muulta maailmalta (Wang, 2011).

Ainoa suuri ero kiinalaisten professoreiden määritelmässä verrattuna länsimaalaisiin on maininta Kiinan julkisesta edusta. Tämä voi viitata mahdollisesti siihen, että myös korkeasti koulutetuilla henkilöillä näkyy ajattelutavassa kommunitarismi ja yhteiskuntakeskeisyys. Se voi siis mahdollisesti sallia hallituksen pääsyn hyvin arkaluontoiseen yksityiseen informaatioon, kunhan se on julkisen edun eteen hankittu.

Tästä hyvä esimerkki on hallituksen keräämät sijaintitiedot kansalaisista Covid-19-pandemian leviämisen rajoittamiseksi (Liu & Zhao, 2021). Tässä tapauksessa hallitus keräsi paljon arkaluontoista informaatiota yleisen turvallisuuden eteen ja siitä oli suora hyöty koko yhteiskunnalle.

Wangin (2011) mukaan länsimaalaiset tutkijat pitävät yksityisyyttä välttämättömänä edellytyksenä demokratialle ja vaikka Kiina on kommunistinen maa, sen perustuslaissa on luvattu demokraattiset vaalit. Hänen mukaansa yksityisyys kannustaa kansalaisia osallistumaan poliittisiin päätöksiin suojelemalla sananvapautta ja päätöksentekoa, joten olisi Kiinan lakien mukaista turvata kansalaisten yksityisyys (Wang, 2011).

Näiden huomioiden mukaan Kiinassa pitäisi ainakin teoriassa olla vastaava yksityisyyden taso kuin demokraattisissa maissa. Kiinan siviililaissa yksityisyys on määritelty henkilön yksityiseksi mielenrauhaksi, tilaksi, aktiviteeteiksi, ja informaatioksi, jota henkilö ei halua muille jakaa (Liu ym., 2021). Kiinan laissa yksityisyys on määritelty tarkasti eikä siitä näy yksilön yksityisyyden vähättely. On myös huomionarvoista, että määritelmä on hyvin samankaltainen kuin länsimaissa.

Kiinassa monet kokevat siis yksityisyyden nykypäivänä yhä tärkeämpänä, mutta kulttuurillisen historian sekä poliittisen ilmapiirin takia kommunitaristiset aatteet ovat vielä vahvoina. Kiinalaisten tutkijoiden määritelmät sekä laissa oleva määritelmä kuitenkin todistaa, että tietoisuus yksityisyydestä on kulttuurillisista ja historiallisista eroista huolimatta korkealla.

2.3 Kiinan yksityisyys verkossa

Yksityisyys verkossa on käsitteenä melko uusi sillä se nousi tärkeäksi vasta 1900-luvun loppupuolella tietokoneiden yleistyessä (Lucaks, 2016). Nykyään yksityinen informaatio nähdään valuuttana ja ihmiset laskettavina asioina, joita voidaan analysoida ja manipuloida (Pendergast, 2018). Informaatio valuuttana kytkee yksityisyyden taloudellisiin ja poliittisiin viitekehyksiin nostaen sen arvoa merkittävästi. Tämä entisestään korostaa Wangin (2011) ja Wisniewskin ja Pagen (2022) huomioita yksityisyydestä yhteiskunnallisena arvona eikä täysin yksilön arvona.

Ongelma on myös melko tuore, koska vasta sosiaalisen median myötä on normalisoitunut suuri informaation jako ja sen analysointi algoritmeilla on mahdollistunut (Aho & Duffiel, 2020). Ottaen huomioon yksityisyyden monimuotoisuus myös yksityisyys verkossa on hankalasti navigoitava aihe. Kuitenkin EU pyrkii tätä ilmiötä haastamaan ja Kiina hyödyntämään (Aho & Duffield, 2020). Monet tutkijat pitävätkin internetissä sijaitsevan informaation yksityisyyttä suurimpana yksityisyyden ongelmana (Wu, Lau, Atkin & Lin, 2011).

Ahon ja Duffieldin (2020) mukaan EU:n tietosuoja-asetus on rakennettu liberalistisen ja individualistisen arvomaailman pohjalta ja se pyrkii rajoittamaan erityisesti yritysten datan keräämistä. Tietosuoja-asetus pyrkii etenkin palauttamaan oikeuden tulla unohdetuksi, jonka häviäminen on ollut kasvava ongelma (Aho & Duffield, 2020). EU:n alueella kaikki yksityisen informaation käsittely on kielletty ilman yksilön lupaa ellei informaatiota käsitellä yleisen turvallisuuden ylläpitämiseksi (Buschel, Mehdi, Cammilleri, Marzouki & Elger, 2014). Diamantopouloun, Lambrinoudakisin, Kingin ja Gritzaliksin (2022) mukaan EU:n yleistä tietosuoja-asetusta pidetäänkin yksityisen datan suojelulaeista tehokkaimpana. He lisäävät, että EU:n tietosuoja-asetus määrittelee yksityisen datan suunnilleen samalla tavalla kuin Kiinan henkilökohtaisen informaation suojelulaki (eng. Personal Information Protection Law, PIPL) (Diamantopoulou ym., 2022). Kyseiseen lakiin viitataan tutkielmassa jatkossa kansainvälisesti tunnetulla lyhenteellä PIPL selvyyden vuoksi.

2000-luvun alussa lähes kaikki kiinalaiset internet sivustot keräsivät henkilökohtaista tietoa käyttäjiltään mutta vain noin 50 % kertoivat käyttäjille yksityisyyskäytänteistään (Kong, 2007). Vuonna 2021 Kiinassa julkaistu PIPL pyrkii kattavasti suojaamaan Kiinan kansalaisten datan ja antamaan heille lisää oikeuksia vaikuttaa heidän informaationsa käsittelyyn (Tan & Zhang, 2021). Laki määrittelee yksityisyyden verkossa yksilön oikeutena päättää, mikä henkilökohtainen informaatio on julkista eri toimijoille ja miten sitä voidaan käsitellä (Calzada, 2022; Liu ym., 2022). Henkilökohtainen informaatio puolestaan määritellään kaikeksi

informaatioksi, joka liittyy tunnistettuihin tai tunnistettavissa oleviin henkilöihin (Calzada, 2022). Laki antaa siis yksilölle paljon valtaa ja oikeuksia oman informaation hallintaan.

Calzadan (2022) mukaan PIPL myös määrittelee lukuisia sääntöjä ja velvollisuuksia tiedonkäsittelijöille ja asettaa yrityksille tietyt velvoitteet datansuojeluun. Esimerkiksi tiedonkäsittelijöiden täytyy suojata yksityinen informaatio turvallisiksi todetuilla käytänteillä ja palomuureilla. Lisäksi PIPL painottaa datan lokalisaatiota, kun yritykset käsittelevät suuria määriä dataa (Calzada, 2022). PIPL siis tarkentaa yleisiä yksityisen datan määritelmiä suojellaakseen sitä hyväksikäytöltä ja lisäksi tarkentaa fyysisiä ja teknologisia datankäsittelymalleja varmistaakseen datan turvallisuuden. Calzada (2022) huomaa, että PIPL pyrkii vahvasti rajoittamaan etenkin suuryritysten datankäsittelyä ja hallintaa. Kenties suurin PIPL:n tuoma vaatimus on, että suuria määriä kansalaisten dataa käsittelevien yritysten kuten Alibaban on annettava ulkopuolisen toimijan valvoa datankäsittelyprosessia. Lisäksi yritysten datankäsittelyä rajataan seuraavasti: asiakkaiden syrjiminen dataprofiloinnin perusteella on kielletty, käytettävällä datalla on oltava suora yhteys sen prosessointi tarkoitukseen, datan määrä on pidettävä minimissä, ja datan säilöntäaika on pidettävä minimissä (Calzada, 2022). Vaikuttaa siis siltä, että Kiina rajoittaa yritysten datankäsittelyä paljon vaikkakin osa rajauksista on laajoja ja tarkentamattomina ne voivat antaa yrityksille paljonkin tulkinnanvaraa. Kiina on kuitenkin jo poistanut sovelluksia sovelluskaupoista, koska ne eivät ole noudattaneet PIPL:n linjauksia (Huang ym., 2022).

Calzadan (2022) mukaan PIPL pyrkii myös suojelemaan arkaluontoista yksityistä informaatiota selventämällä, että se sisältää mm. kansalaisen uskonnon, taloudellisen tilanteen, terveydentilan, ja sijainnin. Hän lisää, että lain mukaan teknologiaa, joka kerää arkaluontoista informaatiota voidaan käyttää vain yleisen turvallisuuden ylläpitoon. Huomionarvoinen on EU:n tietosuoja-asetus, jonka mukaan arkaluontoista informaatiota on myös poliittinen mielipide ja etninen tausta (Calzada, 2022).

Näiden määritelmien pohjalta voidaan todeta, että PIPL vahvistaa kansalaisten datan yksityisyyttä ja sen turvallisuutta, mutta pääasiassa vain ulkopuolisilta tekijöiltä ja yrityksiltä. Laki jättää selvästi tilaa hallituksen omalle kansalaisten yksityisen tiedon keräämiselle ja käytölle. Kiina pyrkiikin siirtämään valvontainfrastruktuurin julkisen sektorin käyttöön ja rajoittamaan yritysten informaationkeräystä (Aho & Duffield, 2020). Esimerkiksi sosiaaliseen luottoluokitusjärjestelmään (eng. Social Credit System, SCS) Kiina hyödyntää kansalaisten poliittisia näkemyksiä. Lisäksi yleisen turvallisuuden ylläpito on laaja määritelmä, joka jättää paljon tulkinnanvaraan siitä, milloin hallituksen toimijat voivat hyödyntää kansalaisten arkaluontoista informaatiota.

Kuitenkin IoT ja tekoäly tuovat uusia haasteita yksityisyydensuojalle sillä ne kuuluvat monen eri toimijan vastuualueelle Kiinassa tehden niiden valvonnasta hankalampaa (Liu ym., 2022). Lisäksi haasteita tuo valtava datan määrä, jonka ominaisuudet ovat yksityisyyden kannalta hankalia. Informaatio ei saata yksittäisenä paljastaa henkilöllisyyttä, mutta myöhemmin uuteen informaatioon yhdistettynä se saattaa (Nissim & Wood, 2018). Julkisen sektorin

tiedonkerääminen mahdollistaa myös informaation yhdistämisen useasta lähteestä ja eri korrelaatioiden löytämisen.

3 TIETOJEN KERÄÄMINEN

Tässä luvussa tarkastellaan teknologiaa ja keinoja, joilla Kiina kerää informaatiota kansalaisistaan sekä kerätyn informaation käyttötarkoituksia. Erityisesti keskitytään Kiinan sosiaaliseen luottoluokitusjärjestelmään, sillä sen systemaattinen koko kansan pisteytysjärjestelmä on hyvin ainutlaatuinen hanke ja Kiinan tärkein 2000-luvun hanke (Aho & Duffield, 2020). Lisäksi tarkastellaan näiden vaikutusta Kiinan kansalaisiin ja tämän lähestymistavan mahdollisiin etuihin ja haittoihin.

3.1 Tiedon keräämisen teknologia

Nopeasti kehittyvän teknologian myötä tiedon keräämisen teknologia on täysin eri, kuin mitä se on ollut esimerkiksi kymmenen vuotta sitten ja tiedon keräykseltä on mahdotonta välttyä. Esimerkiksi nettisivuvierailut, älykellon käyttö, ulkona turvakameran ohi kävely, ja sairaalakäynnit kaikki kerää jonkinlaista dataa ja informaatiota, josta kaikki tallentuu pilveen (Aho & Duffield, 2020). Lisäksi älykotien lisääntymisen myötä kodin sisäiset asiat muuttuvat massadataksi, kun esimerkiksi älykaiuttimet kuljettavat dataa pilveen tekoälyn analysointiin (Liu ym., 2022). Massadatan mahdollistama tarkkailu onkin yksi suurimmista muutoksista yksityisyyden ja tarkkailun kannalta (Liang, Das, Kostyuk & Hussain, 2018). Perinteiset tarkkailumetodit keskittyivät tietyn asian tarkkailuun tai tietyn informaation keräykseen (Lyon, 2007). Kuitenkin Massadatalla voidaan kerätä kaikki tieto kaikesta koko ajan ilman selkeää päämäärää (Andrejevic & Gates, 2014).

Ahon ja Duffieldin (2020) mukaan massadataa keräämällä voidaan luoda kansalaisen käyttäytymisprofiili ja dataa analysoimalla voidaan ennustaa kuluttajakäyttäytymistä, johon voidaan sitten vaikuttaa. He arvioivat, että kuluttajakäyttäytymisen ennakointi voi johtaa kontrollointiin ja esimerkiksi poliittiseen manipulointiin. He lisäävät, että massadataa on voitu hyödyntää tiedonkeruussa

aiemminkin, mutta sen potentiaali on erityisesti kasvanut lähiaikoina koneoppimisen mahdollistaessa massiivisen määrän datan nopeaa analysointia, todennäköisyyksien laskentaa, ja korrelaatioiden löytämistä (Aho & Duffield, 2020).

Datan analysointi ja korrelaatioiden löytäminen koneoppimisella mahdollistaa johtopäätösten tekemisen ja yksilön käyttäytymisen ennakoimisen. Toisaalta samoin kuin kasvojentunnistusteknologian tämänkin teknologian voi nähdä joko hyvin tehokkaana keinona edistää palveluita ja turvallisuutta tai sitten hyvin vaarallisena teknologiana, jolla kansaa voidaan massamanipuloida (Liang ym., 2018). Ongelmallista on myös tämän valvonnan huomaamattomuus. Kansalaiset ovat tietoisia valvontakameroista, mutta massadatan kerääminen kaikilta elämän osa-alueilta ilman selkeää käyttötarkoitusta normalisoi hyvin huomaamattoman mutta suuren määrän informaation keräämistä (Ball & Wood, 2013).

Yksi tärkeä tapa, jolla Kiina kerää arkaluontoista yksityistä informaatiota on kasvojentunnistusteknologia (Facial Recognition Technology, FRT). Kasvojentunnistusteknologialla voidaan skannata ihmisen kasvot ja eritellä ne tietokantoihin käyttäen erilaisia tunnistusattribuutteja (Liu ym., 2021; Kostka ym., 2020). Liu ym., (2021) lisäävät, että skannauksen jälkeen teknologialla voidaan verrata skannattuja kasvoja muihin skannattuihin kasvoihin, valokuviin, ja videomateriaaliin. Kiina pyrkii hyödyntämään tätä teknologiaa todella suurella mittakaavalla luomalla n. 400 miljoonan kasvojentunnistusteknologialla varustetun kameran valvontakameraverkoston (Aho & Duffield, 2020).

Kasvojentunnistusteknologia on kuitenkin hyvin kiistanalainen. Sitä voidaan käyttää hyvin tehokkaana apuvälineenä turvallisuuden edistämisessä, mutta toisaalta sen käyttö tuo mukanaan eettisiä ongelmia, kuten mahdolliset virheelliset tunnistukset, syrjintä ihonvärin tai etnisen taustan perusteella, ja yksityisyyden rikkominen (Kostka ym., 2020). Vastaavasti Liu ym., (2021) ovat huolissaan tiedon määrästä, jota teknologia kerää. Henkilön kasvot skannaamalla voidaan saada selville hyvin arkaluontoista informaatiota, kuten ikä, sukupuoli, ja henkilöllisyys (Liu ym., 2021). Mielipiteiden jako näkyy myös valtioiden välillä. Kiinassa teknologiaa käytetään laajalti, mutta esimerkiksi Yhdysvaltojen osavaltio Kaliforniasta tuli ensimmäinen osavaltio, joka kielti kasvojentunnistusteknologian käytön viranomaistyössä vuonna 2019 (Kostka ym., 2020).

Kostkan ym., (2020) mukaan Kiinan mediassa on painotettu kasvojentunnistusteknologian potentiaalia tarkkailla korruptiota hallituksessa ja tämä puolestaan on lisännyt kansalaisten luottamusta tähän teknologiaan. Heidän tekemän kyselyn mukaan yli 50 % kansalaisista uskoo kasvojentunnistusteknologian lisäävän mukavuutta, n. 30 % uskoo sen rikkovan yksityisyyttä, ja vain 3 % uskoo sen mahdollisesti aiheuttavan syrjintää (Kostka ym., (2020). Kiinassa ei siis juurikaan koeta kasvojentunnistusteknologiaa uhkana vaan se nähdään mahdollisuutena lisätä turvallisuutta ja palveluita.

Kehittyneen teknologian lisäksi Kiinassa on jo pitkään ollut aluevalvontaprojekteja ihmisten päivittäisen elämän valvontaan (Liang ym., 2018; Leibold, 2019). Aluevalvontaprojekteissa viranomaiset valvovat alueita fyysisesti haastattelemalla asiakkaita ja pitämällä kirjaa heidän elämäntilanteistaan,

matkustamisesta, opinnoista, jne. Hän lisää, että Kiinan Xinjiangin alueella ihmiset on velvoitettu lataamaan älypuhelimiin tarkkailusovellukset, joiden tarkoitus on huomata ja ilmoittaa automaattisesti viranomaisille terrorismiin viittaavasta sisällöstä sekä laittomasta uskonnollisesta sisällöstä. Tämän lisäksi sovellus myös kerää SIM-kortti dataa, WIFI-dataa, ja sosiaalisiin medioihin liittyvää dataa (Leibold, 2019). Kiina siis lisää tarkkailua tarpeen vaatiessa alueilla jos siellä on mahdollisia turvallisuusriskejä. Kiina on ainakin Xinjiangin alueella linjannut muslimiuskon ja muut äidinkielet kuin mandariinikiinan hallituksen ajaman agendan vastaiseksi, jolloin se pystyy keräämään vähemmistöistä tietoa ja aktiivisesti asettamaan linjauksia niiden vähentämiseksi (Leibold, 2019).

Kiina käyttää siis tarkkailuun uusinta teknologiaa kasvojentunnistusteknologiasta tekoälyn analysoimaan massadataan. PIPL suojelee kansalaisten tiedonkeruuta jonkin verran, mutta eniten vain yritysten tiedon keruulta. Julkisen sektorin tiedonkeruuta ei rajoiteta paljoa ja etenkin yleisen turvallisuuden eteen Kiina pystyy keräämään suuren määrän yksityistä tietoa. Lisäksi uudet teknologiat pystyvät mahdollisesti kiertämään PIPL:n asettamat rajoitukset. Erityisesti koneoppimisen mahdollistama ennakointi ja korrelaatioiden löytäminen voi mahdollisesti paljastaa arkaluontoista informaatiota, joka on kuitenkin kerätty täysin PIPL:n sääntöjen mukaisesti.

3.2 Yksityisen tiedon keräämisen käyttötarkoitus

Kiina pyrkii keräämään massadataa yksilöistä ilman selkeää käyttökohdetta keräyshetkellä (Andrejevic & Gates, 2014). Tämä eroaa EU:n toimintamallista, jossa yksityistä informaatiota kerätään vain tiettyyn tarkoitukseen (Buschel ym., 2014). Massadataa käytetään Kiinassa esimerkiksi taloudellisten megatrendien tunnistamiseen ja ennakointiin, jota voidaan hyödyntää hallituksen linjauksissa (Calzada, 2022).

Tarkkailuteknologiaa käytetään Kiinassa paljon myös julkisten palveluiden ja turvallisuuden kehittämiseen. Liang ym., (2018) lisää, että massadataa analysoimalla tarkoituksena on myös ennakoida mahdollisia sosiaalisia ja poliittisia muuttujia ja riskejä. Heidän mukaansa analysoimalla suuria määriä toisiinsa liittymätöntä dataa voidaan löytää yllättäviä korrelaatioita ja tehdä johtopäätöksiä niiden pohjalta (Liang ym., 2018). Leiboldin (2019) mukaan massadataa keräämällä luodaan kansalaisprofiileja ja epäilyttävän toiminnan tai Kiinan hallitusta vastustavan toiminnan perusteella luodaan myös epäillyille rikollisille ja terroristeille profiileja. Kasvojentunnistusteknologiaa hyödyntämällä valvontakameroita voidaan käyttää epäiltyjen rikollisten ja terroristien aktiiviseen tarkkailuun (Leibold, 2019). On epäselvää, käytetäänkö teknologiaa enää näin, koska Leiboldin (2019) tutkimusartikkeli on julkaistu kaksi vuotta ennen PIPL:n käyttöönottoa. PIPL kieltää kasvojentunnistusteknologian käytön muuten, kuin yleisen turvallisuuden ylläpitoon. Epäiltyjen rikollisten arkaluontoisen informaation kerääminen tarkoittaisi mahdollisesti viattoman ihmisen yksityisyyden rikkomista,

mutta Kiina voi hyvinkin nähdä epäiltyjen rikollisten seurannan sisältyvän yleisen turvallisuuden ylläpitoon.

Näitä teknologioita hyödynnetään myös suoraan kansalaisten eduksi. Valvontakameroita käytetään ilmanpuhtauden mittaamiseen ja ruuhka-alueiden selvittämiseen (Calzada, 2022). Kasvojentunnistusteknologiaa hyödynnetään Kiinassa laajasti myös maksuvälineenä (Liu ym., 2021). Lisäksi Leiboldin (2019) mukaan Kiinassa on asennettu useita automaattisia elektronisia portteja mm. sairaaloiden, yliopistojen, ja huoltoasemien sisäänkäynneille. Nämä elektroniset portit tarkistavat mm. onko henkilö hallituksen mustalla listalla (Leibold, 2019). Tämä lisää kansalaisten turvallisuutta teoriassa paljon, koska sillä voidaan ehkäistä rikollisuutta ja häiriökäyttäytymistä. Esimerkiksi viranomaiset voivat massadataa analysoimalla tunnistaa mahdollisia rikollisia ja evätä heiltä pääsyn yliopiston kampukselle. Elektronisilla porteilla voidaan myös jäljittää mustalla listalla olevia henkilöitä ja seurata kansalaisten käyttäytymistä. On kuitenkin huomioitava, että mustalle listalle voi päätyä pelkästään uskonnollisista syistä tai jos yksilö esimerkiksi halventaa Kiinan hallitusta (Leibold, 2019). Tämä viittaisi siihen, että Kiina saattaa käyttää kasvojentunnistusteknologiaa kansalaisten systemaattiseen syrjintään.

Kiina käyttää paljon teknologiaa myös sensuuriin. Vuonna 2011 Kiinalla oli n. 30,000 sensoria internetissä sensuroimassa Kiinaa kritisoivaa sisältöä sosiaalisessa mediassa ja keskustelupalstoilla (Wu ym., 2011). Kansalaiset joutuvat siis sensuroimaan itseään kirjoitusvaiheessa rajoittaen sananvapautta. Kuitenkin suurin tarkoitus tiedonkeruulle on Kiinan sosiaalinen luottoluokitusjärjestelmä. Sosiaaliseen luottoluokitusjärjestelmään viitataan tutkielmassa jatkossa lyhenteellä SCS selvyyden vuoksi.

3.3 Sosiaalinen luottoluokitusjärjestelmä

Sosiaalinen luottoluokitusjärjestelmä on yksi Kiinan suurimmista teknologisista hankkeista. Sitä on kuvailtu digitaaliseksi Leninismiksi ja ihmiskunnan kunnianhimoisimmaksi hankkeeksi, joka pyrkii perustamaan kaikkinäkevän valtion (Aho & Duffield, 2020). Liangin ym., (2018) mukaan SCS pyrkii sosiaalisten, taloudellisten, ja poliittisten aktiviteettien ja datan perusteella pisteyttämään jokaisen Kiinan toimijan (henkilöt, yritykset, ja organisaatiot) luotettavuuden ja luottokelpoisuuden. Pisteiden perusteella toimijat saavat joko palkintoja tai rangaistuksia ja rajoituksia, joten vain toimijat jotka noudattavat Kiinan hallituksen linjauksia ja hyveellisiä normeja saavat hallituksen tukea ja pääsyn julkisiin palveluihin (Liang ym., 2018; Aho & Duffield, 2020). Houn ja Fun (2022) mukaan teot, jotka ovat Kiinan linjausten mukaisia ja täten hyveellisiä on mm. kommunistipuolueen kannatus ja roskien keräys. Rangaistavia tekoja on mm. Kiinan maineen vahingoittaminen tai julkisessa liikennevälineessä tupakointi. He kertovat kuitenkin, että suurimmaksi osaksi palkittavat ja rangaistavat teot keskittyvät taloudellisiin tekoihin, kuten ahkeraan työntekoon ja yksityisyrittäjyyteen (Hou & Fu, 2022).

Ahon ja Duffieldin (2020) mukaan yksilölle kohdistettuja palkintoja ovat mm. alennettu veroprosentti ja suurempi näkyvyys deittisovelluksissa. Rangaistuksia ovat mm. korkean koulutuksen evääminen, korkeampi verotus, julkinen nolaaminen, ja mustalle listalle laitto (Aho & Duffield, 2020). Etenkin rangaistuksien vakavuus huomioon ottaen vaikuttaa siltä, että SCS on hyvin tehokas keino kontrolloida kansalaisia Kiinan linjaamiin hyveellisiin tekoihin. Tämä voi olla tehokas keino motivoida kansalaisia objektiivisesti parempaan elämään ja hyveellisiin tekoihin. Toisaalta Hou ja Fu (2022) ovat huolissaan siitä, että nämä hyveelliset kannustimet ovat täysin linjassa Kiinan omien projektien kanssa. He lisäävät, että kun Kiina siirtyy muihin projekteihin, myös kannustimet todennäköisesti siirtyvät niiden mukana. Lisäksi SCS selkeästi rajoittaa sananvapautta rankaisemalla kommunistipuolueen vastaisista kommenteista, joka viittaa mahdollisiin ihmisoikeusrikkeisiin (Hou & Fu, 2022).

Liangin ym., (2018) mukaan SCS:n toiminnan voi jakaa eri vaiheisiin: Datankeräämisvaiheeseen, datankokoamisvaiheeseen, ja itse luottoluokitusjärjestelmään. Datankeräämisvaiheessa SCS:ään kerätään pääasiassa taloudellista dataa, sekä ei-taloudellista dataa kuten opintotiedot ja työhistoria.

Datankokoamisvaiheessa kaikki eri lähteistä kerätty data kootaan yhteen suureen datainfrastruktuuriin. Tässä infrastruktuurissa on puolestaan ainakin viisi eri alustaa: National Credit Information Sharing Platform (NCISP), Credit China, Credit Reference Center, National Enterprise Credit Information Publicity System (NECIPS), ja musta lista epärehellisistä toimijoista, joita täytyy rangaista tai joille täytyy asettaa rajoitteita. Toimijat, jotka eivät täytä vaatimuksia joutua tälle listalle, mutta ovat muuten epäilyttäviä joutuvat erityislistalle (Focus Group List). Jos erityislistalla oleva toimija mainitaan useasti eri datapaketeissa, NCISP siirtää toimijan massadatavaroituslistalle (Big Data Warning List) lisätutkimusta varten. Lopuksi Credit China päättää, kuuluuko toimija mustalle listalle (Liang ym., 2018).

Calzadan (2022) mukaan NCISP on Kiinan hallituksen data-alusta johon on kerätty tietoaineistoja koko Kiinasta. Hänen mukaansa NCISP:n datasta kaksi kolmasosaa keskittyy yrityksiin ja organisaatioihin ja noin viidesosa keskittyy kansalaisiin. Kolmasosa tästä datasta keskittyy epähyveelliseen käytökseen, kuten huonoihin tiliotteisiin ja rikosrekistereihin ja vain pieni osa palkintoaiheiseen tietoon, kuten taloudelliseen menestykseen (Calzada, 2022). Tämä viittaisi siihen suuntaan, että SCS keskittyy tärkeisiin taloudellisiin toimijoihin ja että motivointi tapahtuu enemmän epähyveellisten tekojen rangaistusten pohjalta, kuin hyveellisen palkittavan käytöksen pohjalta. Lisäksi tietoa kerätään laajasti NCISP:ään mm. informaatio- ja teollisuus virastoista, maatalousvirastosta, ja terveys ja perhesuunnittelu komissiosta (Calzada, 2022).

SCS:n merkitys poliittisen manipulaation välineenä herättää keskustelua. Houn ja Fun (2022) mukaan hallituksen maineen vahingoittaminen on rankaistava teko. Liang ym., (2018) lisäävät, että SCS:n avulla voidaan piilottaa poliittisia tavoitteita algoritmeihin ja linjauksiin tehden siitä hyvin hienovaraisen tavan vaikuttaa kansalaisiin. On huomionarvoista, että SCS:n luontiin sisältyi yli 50 hallituksen osaa ja virastoa, joista useimmat liittyvät taloudelliseen ja kaupalliseen

tietoon eikä poliittisen tai sosiaaliseen (Liang ym., 2018). Tämä viittaa siihen, että vaikka SCS kerää myös poliittista ja sosiaalista dataa, se keskittyy pääasiassa taloudelliseen informaatioon ja sen pisteytykseen.

SCS voi analysoida massadataa muuttuvista trendeistä ja muokata omia linjauksiaan ja palkintoja niin, että se tarpeen mukaan puskee kansalaisia säästämään rahaa, hakemaan lainoja tai matkustamaan. Ahon ja Duffieldin (2020) mukaan kansalaisia tarkkailemalla nähdään nopeasti millaisia tuloksia muutokset tekevät ja sen perusteella voidaan tehdä hienosäätöä. Esimerkkinä he antavat yrityksen työolosuhteiden tason mittaamisen keräämällä informaatiota siitä, kuinka paljon työntekijät käyvät työterveydenhuollossa. Jos työntekijät käyvät siellä keskimääräistä useammin ja ostavat paljon lääkkeitä, se voi viitata huonoihin työolosuhteisiin ja johtaa yrityksen luottoluokituksen alenemiseen ja rangaistukseen. SCS voi sitten seurata reaaliajassa tehoaako rangaistus (Aho & Duffield, 2020).

Liangin ym., (2018), sekä Ahon ja Duffieldin (2020) mukaan yksi kategoria, jonka mukaan SCS pisteyttää yrityksiä on vaikutus ympäristöön. Heidän mukaansa kategoriassa yritykset pisteytetään saastuttamisen vähentämisen, ekologisen suojelun, ja ympäristön hallinnan mukaan (Liang ym., 2018; Aho & Duffield, 2020). SCS:ää voidaan siis käyttää hyvin tehokkaasti koko maan tasolla tapahtuviin muutoksiin ja uusiin linjauksiin. Tällainen järjestelmä on mahdollista vain keräämällä massiiviset määrät dataa toimijoista.

Toisaalta järjestelmä voi väärinkäytettynä olla kansalaiselle vaarallinen, jopa ihmisoikeuksia rikkova hallituksen työkalu poliittiseen sensuuriin ja kansan manipulointiin. Kiina voi käyttää SCS:ää vähemmistöjen tehostettuun tarkkailuun ja niihin kohdistetuilla linjauksilla pyrkiä poistamaan ne. Lisäksi monet rangaistukset itsessään ovat hyvin ankaria. Esimerkiksi kaikkien mustalle listalle joutuneiden nimet, kasvot, ja rikkeet julkaistaan sosiaaliseen mediaan (Hou & Fu, 2022).

Liang ym., (2018) huomauttaa, että myös suuryrityksillä kuten Alibaballa on omat pisteytysjärjestelmänsä. Kiina kerää näiltä yrityksiltä dataa, mutta se myös luovuttaa sitä. Alibaba on kertonut, että sen pisteytysjärjestelmään käytettävästä informaatiosta vähemmän kuin 20 % tulee heiltä itseltään ja suurin osa tulee Kiinan tietokannoista. Tämä tarkoittaa suuryritysten ja hallituksen osittaista integraatiota yhdeksi suureksi tiedusteluinfrastruktuuriksi (Liang ym., 2018). Tämä viittaa siihen, että SCS hyödyntää hallituksen datatietokantojen lisäksi myös suuryritysten keräämää dataa ja antamalla dataa yrityksille Kiina myös kannustaa yrityksiä edistämään omia pisteytysjärjestelmiään. Julkisen ja yksityisen sektorin osittainen fuusio tarkoittaa myös yksilön yksityisyyden vähenemistä. Kansalaisen täytyy olettaa, että hallitus pystyy keräämään heidän informaatiotaan sosiaalisen mediasta, viestintäsovelluksista, ja älykaiuttimista. Lisäksi Houn ja Fun (2022) mukaan SCS kuuluu normaalin lainsäädännön ulkopuolelle, joten sen tietokantoja varten hallitus pystyy keräämään miltei mitä informaatiota se haluaa.

Aho ja Duffield (2020) kuitenkin huomauttavat, että konkreettisesti SCS voi kuitenkin olla liian massiivinen hanke toteutettavaksi kokonaisuudessaan. SCS

vaatii toimiakseen todella suuren määrän dataa eri lähteistä, joka voi Kiinan kokoisessa maassa olla vaikeaa kerätä byrokratian ja eri teknologian tasojen takia. Eri virastot ja yritykset saattavat tallentaa datapaketit eri tavoin etenkin eri alueilla ja teknologian taso varsinkin harvemmin asutuilla alueilla voi olla vähäistä mikä hankaloittaa datan siirtoa ja SCS:n infrastruktuuriin integrointia (Aho, & Duffield, 2020). Tämä jättäisi valtion tasolla mahdollisesti isojakin alueita, mitkä eivät kuulu SCS:n vaikutusalueeseen vakavasti vahingoittaen sen toimivuutta. Tällaisille alueille SCS:n mahdollistavan teknologian käyttöönotto tulisi myös vaatimaan suuren määrän resursseja. Lisäksi massadatan analysointi tapahtumien ennakointiin ja korrelaatioiden löytämiseen on vielä vain pienellä mittakaavalla tapahtuvaa (Liang ym., 2018).

Ahon ja Duffieldin (2020) mukaan Kiinan nouseva elintaso ja laskeva korruptio viittaa siihen, että ankara tarkkailu ja tiedonkeruu tuottaa tulosta verrattuna EU:n hidastuvaan kehitykseen, koska sen täytyy varjella demokraattisia yksilön etuja ja oikeuksia. Vertaus on ehkä hieman suppea otettavakseen täysin totuutena, mutta se viittaa silti selkeään taloudelliseen etuun, kun koko yhteiskunnan voi valjastaa hallituksen linjauksilla tiettyihin projekteihin ja aktiviteetteihin.

SCS siis pyrkii hyödyntämään uusinta teknologiaa ja keräämään kaiken mahdollisen datan Kiinan toimijoista. Tällä lähestymistavalla on selkeitä yhteiskunnallisia etuja kuten korotettu turvallisuus ja talouden kehitys, mutta lähestymistapa ei tuo suurta yksityisyyden turvaa. Sosiaalisen ja poliittisen ympäristön pisteytys, heikko lainsäädäntö, ja vähäinen yksilön yksityisyyden ja oikeuksien suojelu nostavat väärinkäytön suureksi riskiksi ja jopa todennäköiseksi. Se on kuitenkin hyvä esimerkki vaihtoehtoisesta lähestymistavasta teknologian ja yksityisyyden suhteeseen.

3.4 Kansalaisen näkökulma

Tutkimuskysymyksen kannalta oleellista on tietää, kuinka Kiinan lähestymistapa yksityisyyteen nähdään kansalaisten näkökulmasta. Mahdolliset hyödyt ja haitat, ja kuinka tehokas keino Kiinan lähestymistapa on kansalaisten mielestä ja heidän kannalta.

Kiina on perinteisesti ollut hyvin kommunitaristinen maa, jossa yksilön yksityisyyttä ei ole pidetty arvokkaana (Yao-Huai, 2005). Kiinassa on myös jo pitkään valvottu kansalaisten yksityiselämää, matkustamista, koulutusta, sekä kommunistipuolueen kannatusta (Aho & Duffield, 2020). Globalisaation myötä kiinalainen yhteiskunta on kuitenkin siirtynyt kohti individualismia ja yksilön tärkeyttä (Yao-Huai, 2005). Epäluottamus hallitukseen onkin noussut. Wangin ja Yun (2015) tekemän kyselyn perusteella yli kolmasosa (37.6 %) kiinalaisista ei luota hallitukseen. Erityisesti huolta aiheutti yksilöiden informaation kerääminen henkilökohtaisen vapauden ja sananvapauden rajoittamiseksi.

Useiden tutkimusten mukaan kuitenkin kiinalaiset luottavat hallitukseensa paljon. Liun ja Zhaon (2021) mukaan Covid-19 pandemian levitessä kiinalaiset suhtautuivat myönteisesti älypuhelimille ladattaviin arkaluontoista

informaatiota kuten sijaintitietoja kerääviin sovelluksiin, joilla saatiin tehokkaasti hidastettua ja rajoitettua pandemian leviämistä. He lisäävät, että Kiinassa yksityisestä informaatiosta luopuminen tai muu yhteisen hyvän eteen tehty teko nähdään monesti yksilön näkökulmasta sankarillisena uhrauksena (Liu & Zhao, 2021). Kiinalaiset myös sietävät vapauden rajoituksia vaihdossa sosiaaliseen ja taloudelliseen kasvuun (Wu ym., 2011). Lisäksi Ahon ja Duffieldin (2020) mukaan kansan kannatus SCS:ää kohtaan on pysynyt korkealla, koska se nähdään tapana saada turvallisempi ja totuudenmukaisempi yhteiskunta.

Kiinalaiset suhtautuvat yksityisyyteen myös teknologian kontekstissa myöntyen. Kostkan ym., (2020) mukaan yleisesti ottaen kiinalaiset keskittyvät selkeästi enemmän teknologian tuomiin etuihin ja palveluihin kuin sen mahdollisiin haittoihin. Tätä tukee myös heidän tekemä tutkimus, jonka mukaan 68 % kiinalaisista näkee kasvojentunnistusteknologiassa enemmän mahdollisuuksia kuin riskejä (Kostka ym., 2020). Lisäksi Liun ym., 2021 huomiot tukevat tätä lisäämällä, että kiinalaiset suhtautuvat keskimääräistä positiivisemmin uusien teknologioiden mahdollistamiin palveluihin, vaikka se tarkoittaisi vähenevää yksityisyyttä. Nämä huomiot viittaavat lisätyn avoimuuden alentavan informaation keräämisen riskejä ja lisäävän kansalaisten halukkuutta uusiin palveluihin ja teknologioihin.

Kulttuurillinen ympäristö Kiinassa siis pitkälti mahdollistaa hallituksen laajan tiedonkeräyksen ja sen takia kansalaiset ovat valmiita luopumaan informaatiostaan yhteisen edun eteen. Tämä viittaa siihen, että Kiinassa ainutlaatuinen kulttuuri voi mahdollistaa ympäristön jossa kansalaiset tietoisesti luopuvat omasta informaatiostaan yhteisen hyvän eteen ja näin saavutetaan turvallisempi ja tehokkaampi yhteiskunta. Havainto viittaa myös siihen, että vastaava järjestelmä voisi olla hankala implementoida demokraattisiin ja individualistisiin maihin. On kuitenkin huomioitava, että rangaistuksen pelko on saattanut vaikuttaa kiinalaisten vastauksiin kyselyissä.

Toisaalta Englannissa ihmiset ovat huolissaan yksityisen informaation käytöstä, mutta he kannattavat yksityisen tiedon käyttöä julkisen terveydenhuollon kehittämiseen (Buschel ym., 2014). Lisäksi Yhdysvalloissa 9/11 iskujen jälkeen enemmistö koki turvallisuuden yksityisyyttä tärkeämmäksi (Farrall, 2018). Myös EU:ssa ihmiset ovat valmiita luopumaan yksityisestä informaatiosta terrorismin vastaisen taistelun eteen (Papacostas, 2008). Tämä viittaa siihen, että myös individualistissa maissa ollaan valmiita tilanteen mukaan luopumaan tietystä määrästä yksityistä informaatiota yhteisen hyvän eteen. Tutkimusten tulokset myös osoittavat, että suurin osa kansalaisista näkee turvallisuuden yksityisyyttä tärkeämpänä.

Kuitenkin kansalaisten mielipiteet ovat kyseenalaisia (Farrall, 2018). Buckin ym., (2022) mukaan ihmiset luopuvat suurista informaatiomääristä, vaikka olisivat huolissaan yksityisyyden suojastaan ja tätä ilmiötä kutsutaan yksityisyysparadoksiksi. Heidän mukaansa mahdollinen selittäjä tälle ilmiölle on välittömän hyödyn tavoittelu. Lisäksi moni ihminen ajattelee, ettei heidän informaationsa ole hyödyksi kenellekään tai tilanteen vaatiessa valtio suojelee heidän

informaatiotansa (Buck ym., 2022). Myös kiinalaiset luottavat PIPL:n suojaavan heidän informaatiotaan (Liu ym., 2022).

Hallinanin, Friedewaldin ja McCarthyn (2012) mukaan yksilön on vaikeaa ottaa vastuu yksityisestä tiedostaan. Heidän mukaansa yksilöllä ei ole omat tiedot päällimmäisenä mielessä ja yksityisyyden suoja on ns. näkymätön kansalaiselle, joten se sivuutetaan herkästi. Lisäksi mahdollinen tiedoista luopuminen nähdään yksittäisinä tekoina eikä omien oikeuksien myyntinä. He lisäävät, että yksityisyys nähdään hyvin suppeasti ja usein suhteessa johonkin muuhun asiaan, kuten turvallisuuteen (Hallinan ym., 2012). Tätä tukee Soloven (2010) kommentti siitä, että yksityisyys nähdään yksilön oikeutena, jota tasapainotellaan yhteistä hyvää vastaan. Nämä huomiot taas viittaavat siihen, että yksityisyydessä on kyse ihmisoikeudesta, jota hallituksen ja organisaatioiden täytyy suojella, koska se on käsitteenä niin laaja ettei kansalaiset pysty sitä itse suojelemaan. Näiden huomioiden perusteella Kiinan mahdollinen sensuuri kansalaisten kommentteja tarkastellessa ei olisi relevanttia, koska kommentit itsessään ei olisi arvokkaita yksityisyyttä tarkastellessa. Toisaalta nämä huomiot myös viittaavat siihen, että Kiinan lähestymistapa on fundamentaalisesti väärä, koska vaikka Kiinan kulttuuri mahdollistaisikin tiedonkeräysyhteiskunnan se olisi silti yksilön yksityisyyden näkökulmasta väärin. On myös huomionarvoista, ettei Kiinan tiedusteluinfrastruktuurista ole hyötyä, jos kansalaiset saavat vaikuttaa informaation keräämiseen. Massadatan keräys ja sen hyödyntäminen massiivisiin linjauksiin perustuu suureen määrään dataa.

Kuitenkin jotkut Kiinan agendat ovat selkeästi haitallisia kansalaisille ja ne kyseenalaistavat koko järjestelmän hyödyn. Xinjiangin alueella sijaitseva Uighurien vähemmistön systemaattinen sorto on yksi Kiinan valvontainfrastruktuurin suurimpia varjopuolia (Leobold, 2019).

Kiinassa monet kaupungit on aloittaneet aluevalvontaprojekteja (eng. grid administrator project) ihmisten päivittäisen elämän valvontaan (Liang ym., 2018). Tämä tarkkailu sisältää valvontakamera materiaalin analysointia sekä kotivierailuja ja alueen asukkaiden elämäntilanteen kartoittamista (Leobold, 2019). Kansalaisen näkökulmasta kriittiseksi muodostuukin se, kuinka tätä tietoa käytetään.

Leoboldin (2019) mukaan huolta on aiheuttanut Xinjiangissa alueen vähemmistöjen ja etenkin Uyghurien autonomisen alueen tehostettu tarkkailu. Hänen mukaansa tätä tietoa ei myöskään käytetä pelkästään kannustamaan taloudelliseen edistykseen vaan myös muuhun hallituksen näkemään hyveellisyyteen, kuten äidinkieleen, tiettyyn uskontoon, ja kulttuuriin. Leobold lisää, että kansalaiset voivat joutua viranomaisten mustalle listalle, jos he tekevät laittomia uskonnollisia harjoitteita tai ilmaisevat tyytymättömyyttä yhteiskuntaan. Listalle joutuneet voidaan lähettää uudelleenkouluttautumiskeskuksiin, joissa ihmisistä pyritään mm. fyysisesti kiduttamalla muuttamaan hallituksen linjausten mukaisesti käyttäytyviä kansalaisia. Vähemmistöjen jäseniä on myös palkittu esimerkiksi mandariinikiinan puhumisesta ja kiinalaisten henkilöiden kanssa naimisiin menosta (Leobold, 2019). Leoboldin väitteet viittaavat siihen, että Kiinan keräämää suurta määrää yksityistä tietoa käytetään myös hyvin järjestelmälliseen uskonnolliseen ja kulttuurilliseen syrjintään ja vähemmistöjen poistamiseen. Tietyn

ryhmän laajempi tarkkailu ja sen rankaiseminen uskonnon tai äidinkielen takia rikkoo ihmisoikeuksia (UN, 2024).

Kiinan rakentama järjestelmä ei tarjoa kansalaisille paljoa vaihtoehtoja tilanteen muuttamiseen. Kansalaisten täytyy noudattaa Kiinan linjauksia ja hyveelliseksi toteamia elämäntapoja ja aktiviteetteja, joista osa edistää yhteiskunnan etua ja taloudellista etua, mutta osa keskittyy sosiaalisiin ja poliittisiin näkemyksiin ja uskomuksiin. Linjauksista poikkeavat kansalaiset voidaan jopa vangita (Leobold, 2019; Hou & Fu, 2022).

Yksityisyydestä luopuminen parannettujen palveluiden ja turvallisuuden saamiseksi voisi olla tehokas ratkaisu yhteiskunnan edistämiseksi, mutta informaation hyödyntäminen ihmisoikeuksien rikkomiseen tekee Kiinan järjestelmästä vaarallisen kansalaisille.

3.5 Lähitulevaisuus

Kiinan yksityisyyden kehityksen kannalta kriittiset muuttujat ovat vielä monilta osin kesken. PIPL julkaistiin vuonna 2021 ja SCS vuonna 2020, ja etenkin SCS:n implementointi on vielä kesken (Aho & Duffield, 2020). SCS on myös konkreettisesti hyvin vaikea toteuttaa, jonka takia sen koko maan mittainen täytäntöönpano voi olla hidasta tai jopa mahdotonta (Aho & Duffield, 2020). Esimerkiksi koneoppimisen mahdollistava massiivisella mittakaavalla tapahtuva datan analysointi ja sen perusteella tapahtuva ennakointi on toistaiseksi vain pienellä mittakaavalla tapahtuvaa (Liang ym., 2018).

Kiinalla on kuitenkin luottoluokitusjärjestelmien suhteen korkeat suunnitelmat. Liangin ym., (2018) mukaan Kiina on ehdottanut ”vyö ja tie hanketta” (eng. Belt and Road Initiative), jossa yhteensä 65 maata muodostaisi valtioiden välisen luottojärjestelmän kansainvälisen kaupankännin tehostamiseksi. Heidän mukaansa kiinalainen suuryritys Alibaba on kehottanut Kanadan pääministeriä hyväksymään kiinalaisten turistien viisumihakemukset käyttämällä Alibaban omaa luottojärjestelmää (Liang ym., 2018). Luottoluokitusjärjestelmistä voi siis tulla myös kansainvälisiä pisteytysjärjestelmiä joilla voidaan evätä kiinalaisten lähtö maasta tai seurata heidän vierailujaan muissa maissa.

Lisäksi aihetta ympäröivä kulttuurillinen, poliittinen, ja teknologinen ympäristö on isojen muutosten kynnyksellä, joten tilanne voi muuttua paljon. Yao-Huain (2005) mukaan Kiinan kulttuurillinen ympäristö on siirtymässä kohti individualismia ja demokraattisia aatteita, joten tulevaisuudessa kansalaiset saattavat osoittaa kovempaa vastustusta yksityisen informaation keräykseen. Hän myös arvioi, että eri näkökulmat yksityisyyden suhteen tulevat yleistymään ja täysin uusia filosofisia suhtautumisia syntyy (Yao-Huai, 2005). Tämä voisi myös viitata siihen, että tulevaisuudessa kaupankäynti yksityisellä informaatiolla yleistyy ja yksityisyydestä tulee entistä subjektiivisempi käsite.

Yao-Huai (2005) lisää, että tulevaisuudessa haasteet yksityisyyden suojaamiseksi kasvavat. Hän esittää esimerkin, että geenitutkimuksen yleistyessä se voi mahdollistaa geeniperimästä tehtävien johtopäätösten tekemisen mm. yksilön

älykkyydestä. Hänen mukaansa tämä voisi johtaa sosiaaliseen syrjintään geenien perusteella jolloin geeniyksityisyydestä syntyisi uusi määriteltävä yksityisyyden alue (Yao-Huai, 2005).

Myös teknologia kuten tekoäly on vasta potentiaalinsa alkupäässä ja sen mahdollistama tiedonkeruu on vielä pientä verrattuna siihen mitä se todennäköisesti tulee tulevaisuudessa olemaan (Jordan & Mitchell, 2015). Toisaalta riskit kasvavat paljon arkaluontoista informaatiota keräävää teknologiaa käyttäessä ja moni kansalainen ei ole halukas tällaista teknologiaa käyttämään (Liu ym., 2021). Tulevaisuudessa etenkin IoT:n kasvaessa saatetaan saavuttaa raja, jota kansalaiset eivät halua ylittää. Tutkielmassa on kuitenkin todettu, että valtaosa kansalaisista ei tee suuria toimia, vaikka heidän yksityisyytensä olisi uhattuna ja lisäksi Kiina saattaa rangaista linjausten vastaisia kansalaisia, joten mahdollinen vastarinta informaation keräämiseen ei todennäköisesti tule muuttamaan tilannetta.

Kiinassa yksityisyyden suhde teknologiaan kehittyy jatkuvasti. Monet tätä suhdetta koskevat elementit ovat muuttumassa, mutta toistaiseksi suuntaa on vielä vaikea ennakoida. Toisaalta käsitys yhteisestä edusta pysyy korkealla ja Kiinan hallituksen suunnitelmat SCS:n ja muiden luottoluokitusjärjestelmien kanssa viittaa siihen, että tiedon keräys tulee vain lisääntymään. Kiina myös panostaa hyvin paljon uusiin teknologioihin ja kansalaiset suhtautuvat niihin positiivisesti (Kostka ym., 2020). Todennäköisesti arkaluontoisen informaation kerääminen siis kasvaa ja uuden teknologian mahdollistama informaation käyttö kuten massadatan käyttö tarkkailuun ja tulevien trendien ennakointiin yleistyy.

4 JOHTOPÄÄTÖKSET JA YHTEENVETO

Nopeasti kehittyvä teknologia on yhä suurempi uhka yksityisyydelle ja tämän tutkielman tarkoituksena oli tutkia tätä Kiinan näkökulmasta. Lisäksi Kiinan lähestymistapaa tarkastelemalla haluttiin löytää vaihtoehtoisia ratkaisuja teknologian ja yksityisyyden suhteelle.

Tavoitteena oli selvittää, kuinka Kiinassa määritellään yksityisyys, jotta ymmärretään kansalaisten ja Kiinan hallituksen lähestymistapa teknologian käyttöön yksityisen tiedon keräämisessä. Lisäksi otettiin selvää, mitä teknologioita Kiina käyttää yksityisen tiedon keräämiseen ja mihin kerättyä tietoa käytetään. Tutkimuskysymyksenä pyrittiin selvittämään, onko yksityisyydestä luopuminen teknologian etujen saamiseksi hyväksyttävää kansalaisen näkökulmasta.

Tutkielma toteutettiin kirjallisuuskatsauksena, johon lähteet kerättiin pääasiassa Google Scholar, Taylor & Francis, ja Elsevier- tietokannoista. Aineistoina käytettiin sekä kansainvälisiä että kiinalaisia tutkimusartikkeleita, joiden kieli oli englanti.

Tutkielmassa tehtiin seuraavanlaisia havaintoja. Yksityisyys on yleisesti ottaen subjektiivinen käsite, jonka määritelmä riippuu paljon kulttuurista, uskonnosta, ja kontekstista (Wang, 2011). Kiinassa yksityisyys on perinteisesti nähty kollektiivisesta ja kommunitaristisesta näkökulmasta, jossa ryhmän etu on laitettu yksilön edelle (Liu & Zhao, 2021). Kuitenkin globalisaation myötä kiinalaisten arvomaailma on siirtynyt enemmän kohti länsimaalaisia arvoja ja yksityisyyden arvo on kasvanut (Yao-Huai, 2005).

Internetissä yksilön yksityisyyden taso on myös noussut Kiinassa huomattavasti lähivuosina. Vuonna 2021 julkaistu henkilökohtaisen informaation suojelulaki suojaa yksityisen informaation keräystä ja käsittelyä asettamalla pakotteita yrityksille (Calzada, 2022). Huomionarvoista on, ettei tämä laki rajoita Kiinan omaa informaation keräystä ja esimerkiksi sosiaalinen luottoluokitusjärjestelmä ei kuulu sen toimivaltaan (Hou & Fu, 2022).

Tutkielmassa havaittiin, että yksityistä informaatiota Kiina kerää pääasiassa massadatasta, jota analysoidaan koneoppimista hyödyntämällä (Aho & Duffield, 2020). Lisäksi arkaluontoista informaatiota kerätään pääasiassa

kasvojentunnistusteknologialla varustetuilla valvontakameroilla sekä älypuhelimiin asennettavilla jäljityssovelluksilla (Liu ym., 2021).

Kerättyä informaatiota Kiina käyttää julkisten palveluiden ja yleisen turvallisuuden kehittämiseen. Esimerkiksi massadataa analysoimalla Kiina pystyy ennakoimaan taloudellisia megatrendejä, seuraamaan yritysten ympäristön saastutusta tai jäljittämään epäiltyjä rikollisia (Liang ym., 2018).

Kuitenkin suurin osa kerätystä informaatiosta käytetään sosiaaliseen luottoluokitusjärjestelmään. Järjestelmä pyrkii taloudellisten, sosiaalisten, ja poliittisten aktiviteettien ja datan perusteella pisteyttämään jokaisen Kiinan toimijan (Liang ym., 2018). Pisteiden perusteella toimijat saavat joko palkintoja tai rangaistuksia. Palkinto voi olla esimerkiksi alennettu veroprosentti, kun taas rangaistuksia on esimerkiksi matkustusrajoitukset tai korkean koulutuksen evääminen (Hou & Fu, 2022). Kansalaisen näkökulmasta huolta aiheuttaa kuitenkin Kiinan linjaukset ja pisteidenjakojärjestelmä. Suurin osa linjauksista keskittyy talouteen, mutta osa liittyy politiikkaan ja sosiaalisiin aktiviteetteihin (Aho & Duffield, 2020). Leiboldin (2019) mukaan Kiinan linjaukset pyrkivät määrittelemään mm. kansalaisten äidinkielen, uskonnon ja mielipiteen hallituksesta. Etenkin Xinjiangin alueella tapahtuva vähemmistöjen syrjintä viittaa siihen, että Kiina pyrkii linjauksillaan poistamaan kokonaisia uskontoja ja etnisiä vähemmistöjä Kiinasta (Leibold, 2019). Lisäksi hallituksen kritisointi voi johtaa pisteiden laskuun tai jopa vankeustuomioon (Hou & Fu, 2022).

Tutkielmassa tehtiin ristiriitaisia havaintoja kansalaisten suhteesta yksityisyyteen. Kansalaiset näkevät yleisen turvallisuuden hyvin tärkeänä ja ovat valmiita luopumaan arkaluontoisesta yksityisestä informaatiosta sen ylläpitämiseksi (Aho & Duffield, 2020). Liu ym., (2021) lisää, että yksilö todennäköisesti luopuu yksityisyydestään, jos saa vaihdossa huomattavia etuja. Myös Farrallin (2008) mukaan päätösvalta yksityisyydestä on aina yksilöllä itsellään. Kuitenkin Hallinanin ym., (2012) mukaan yksilöillä ei ole riittävää tietämystä yksityisyydestä ja sen suojasta, eivätkä he siksi voi olla vastuussa oman informaation jakamisesta. Knijnenburg ym., (2022) esittää mahdolliseksi ratkaisuksi ongelmaan käyttäjän yksityisyysmallin, joka käyttää tekoälyä mukautuakseen yksilön yksityisyydentarpeisiin siirtämättä koko vastuuta yksilölle. Tällainen järjestelmä olisi mahdollinen kompromissi yksilön yksityisyyden hallintaan sillä siinä otetaan huomioon yksilön riittämätön tietämys yksityisyyden suojasta sekä yksilön oikeus vaikuttaa omaan yksityisyyteensä.

Tutkimustulokset viittaavat siihen, että Kiinassa yksilö pystyy itse päättämään yksityisen informaation luopumisesta, mutta vain jos yritykset keräävät sitä. Kiinan valtio pystyy keräämään käytännössä mitä informaatiota haluaa yleisen edun eteen. Tutkimus yksityisyyden luonteesta viittaa siihen, että yksilö luopuu yksityisestä informaatiosta vaihdossa välittömiin etuihin eikä yksilöllä ole riittävää tietämystä informaation luopumisen seurauksista. Tämän takia kansalaisen näkökulmasta sen ei pitäisi olla hyväksyttävää, mutta Kiinan kansalaisilla ei ole vaihtoehtoja.

Kiinan tapausta tutkiessa huomattiin, että pakollisella informaation keräyksellä on huomattavia teknologisia yhteiskunnallisia ja yksilöllisiä etuja. Lisäksi

kansalaiset suhtautuvat positiivisesti omasta informaatiosta luopumiseen. Kuitenkin osa Kiinan linjauksista rikkoo ihmisoikeuksia eivätkä ne ole kansalaisille eduksi, joten tätä lähestymistapaa ei voida nähdä hyväksyttävänä. Jos oletetaan, että yksilöllä olisi täysi tieto oman informaation käytöstä eikä sitä väärinkäytettäisi, niin silloin löytöjen mukaan olisi hyväksyttävää vaihtaa informaatiota teknologisiin etuihin.

Lisätutkimusta tulisi tehdä Kiinan päivittyneistä linjauksista ja etenkin vähemmistöjen sorrosta. Lisäksi tutkimusta tulisi tehdä sosiaalisen luottoluokitusjärjestelmän edistymisestä ja tehokkuudesta. Lisätutkimusta tehdessä tulisi varmistaa tiedon olevan faktuaalista ja kerätty ilman Kiinan hallituksen painostusta.

LÄHTEET

Aho, B & Duffield, R. (2020) Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China, Economy and Society, 49:2, 187-212. https://www.tandfonline.com/doi/full/10.1080/03085147.2019.1690275?casa_token=je8z2kUWUvYAAAAA%3A6Bus-iEQ2ajOZm8H1wHsfyKbCBZwGRvMdUes9-g6HI_woWMh9W45hxNMYBE--50Gq6NYeQdEXCqLbmA

Andrejevic, M., & Gates, K. (2014). Big Data Surveillance: Introduction. *Surveillance & Society*. s. 185-196

Ball, K. S., & Wood, D. M. (2013). Political Economies of Surveillance. *Surveillance & Society*. s. 1-3

Buschel, I., Mehdi, R., Cammilleri, A., Marzouki, Y., & Elger, B. (2014). Protecting Human Health and Security in Digital Europe: How to Deal With the "Privacy Paradox". *Springer.*

https://link.springer.com/article/10.1007/s11948-013-9511-y

Calzada I. (2022) Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). *MDPI*. https://doi.org/10.3390/smartcities5030057

Farrall, K. N. (2008). Global privacy in flux: Illuminating privacy across cultures in China and the US. *International Journal of Communication 2*.

Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. *Elsevier*.

Hou, R, & Fu, D. (2022) Sorting citizens: Governing via China's social credit system. *Wiley Online Library*.

Jordan, M & Mitchell, T. (2015). Machine learning: Trends, perspectives, and prospects. *Science*. https://www.science.org/doi/full/10.1126/science.aaa8415?casa_token=YuDwMyxSJ7cAAAAA%3AK7az2XbqLY5bWXTF8xJhFnpj8_J4FRu5Op0zleEWQo3sF0_MijtPQzKijavRmXGii2bvhpjQ_eRiLpU

Wisniewski, P, J., & Page, X. (2022). Privacy Theories and Frameworks. Teoksessa B. P. Knijnenburg, P. Wisniewski, N. Proferes, X. Page, H. R Lipford & J. Romano. (toim.), *Modern Socio-Technical Perspectives on Privacy* (s. 15-43). Springer.

Buck, C., Dinev, T., & Anaraky, R. G. (2022). Revisiting APCO. Teoksessa B. P. Knijnenburg, P. Wisniewski, N. Proferes, X. Page, H. R Lipford & J. Romano. (toim.), *Modern Socio-Technical Perspectives on Privacy* (s. 43-61). Springer.

Proferes, N. (2022). The Development of Privacy Norms. Teoksessa B. P. Knijnenburg, P. Wisniewski, N. Proferes, X. Page, H. R Lipford & J. Romano. (toim.), *Modern Socio-Technical Perspectives on Privacy* (s. 79-91). Springer.

Seamons, K. (2022). Privacy-Enhancing Technologies. Teoksessa B. P. Knijnenburg, P. Wisniewski, N. Proferes, X. Page, H. R Lipford & J. Romano. (toim.), *Modern Socio-Technical Perspectives on Privacy* (s. 149-171). Springer.

Knijnenburg, B. P., Anaraky, R. G., Wilkinson, D., Namara, M., He, Y., Cherry, D., & Ash, E. (2022). User-Tailored Privacy. Teoksessa B. P. Knijnenburg, P. Wisniewski, N. Proferes, X. Page, H. R Lipford & J. Romano. (toim.), *Modern Socio-Technical Perspectives on Privacy* (s. 367-395). Springer.

Diamantopoulou, V., Lambrinoudakis, C., King, J., & Gritzalis, S. (2022). EU GDPR: Toward a Regulatory Initiative for Deploying a Private Digital Era. Teoksessa B. P. Knijnenburg, P. Wisniewski, N. Proferes, X. Page, H. R Lipford & J. Romano. (toim.), *Modern Socio-Technical Perspectives on Privacy* (s. 427-449). Springer.

Kostka, G & Steinacker, L & Meckel, M. (2020). Between Privacy and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the UK and the US. *SSRN*. http://dx.doi.org/10.2139/ssrn.3518857

Kong, L (2007). Online Privacy in China: A Survey on Information Practices of Chinese Websites, *Chinese Journal of International Law*, s. 157–183, https://doi.org/10.1093/chinesejil/jml061

Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, *10*(4), s. 415-453.

https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.183?casa_token=RtYx3ZCX5Y8AAAAA:Pm1Jj0b_KzRgZA1-TlObJfwzidKGJ4NC-SKVs_4ESohQxWd8dVmKIiFMIc5QPBKg5JynL3WoAs32vjPVg

Liu, Y &Yan, W & Hu, B. (2021). Resistance to facial recognition payment in China: The influence of privacy-related factors. *Telecommunications Policy*.

(https://www.sciencedirect.com/science/article/pii/S0308596121000598)

Liu, J. & Zhao, H. (2021). Privacy lost: Appropriating surveillance technology in China's fight against COVID-19, *Business Horizons*, s. 743-756 (https://www.sciencedirect.com/science/article/pii/S0007681321001270)

Liu, Y., Huang, L., Yan, W., Wang, X., & Zhang, R. (2022). Privacy in AI and the IoT: The privacy concerns of smart speaker users and the Personal Information Protection Law in China. *Telecommunications Policy*.

Lukacs, A. (2016). *What is privacy? The history and definition of privacy*.

https://www.cag.edu.tr/uploads/site/lecturer-files/what-is-privacy-the-history-and-definition-of-privacy-ULpz.pdf

Lyon, D. (2007). Surveillance Studies: An Overview. *Oxford: Polity Press*.

McDougall, B. S. (2004). Privacy in modern China. *History Compass.*

Nissim, K., & Wood, A. (2018). Is privacy privacy? *The Royal Society*. http://doi.org/10.1098/rsta.2017.0358

Papacostas, A. (2008). *Flash Eurobarometer 225: Data Protection – General Public.*

Pendergast, T. (2018). The Next Cold War Is Here, and It's All About Data. *Wired*. https://www.wired.com/story/opinion-new-data-cold-war/. 17.6.2024.

Smith, R. E. (2004). Privacy and curiosity from plymouth rock to the internet. *Privacy Journal*.

Solove, D. J. (2010). Understanding Privacy. *Harvard University Press*.

Tan, Z., & Zhang, C. (2021). China's PIPL and DSL: Is China following the EU's approach to data protection? *Journal of Data Protection & Privacy*.

Wang, H. (2011). *Protecting privacy in China: A research on China's privacy standards and the possibility of establishing the right to privacy and the information privacy protection legislation in modern China.*

Wang, Z. & Yu, Q. (2015). Privacy trust crisis of personal data in China in the era of Big Data: The survey and countermeasures. *Computer Law & Security Review*, s. 782-792.

(https://www.sciencedirect.com/science/article/pii/S0267364915001296)

Westin, A. F. (1968). Privacy And Freedom. *Washington and Lee Review*.

Wu, Y. & Lau, T. & Atkin, D.J. & Lin, C.A. (2011). A comparative study of online privacy regulations in the U.S. and China, *Telecommunications Policy*, s. 603-616. (https://www.sciencedirect.com/science/article/pii/S0308596111001017)

Yao-Huai, L. (2005). Privacy and Data Privacy Issues in Contemporary China. *Ethics and Information Technology*. https://doi.org/10.1007/s10676-005-0456-y

https://www.un.org/en/about-us/universal-declaration-of-human-rights