RECOGNITION TECHNOLOGIES IN THE FINNISH POLICE AND BORDER GUARD

AN INTRODUCTORY MAPPING

SARA PYNTTÄRI WITH RUNE SAUGMANN AND SIRPA VIRTA

Sara Pynttäri with Rune Saugmann and Sirpa Virta

Recognition technologies in the Finnish police and Border Guard: An introductory mapping

ORCID iD

Rune Saugmann https://orcid.org/0000-0002-6936-8845

Tampere University 2023

Collection: Tampere University, Monographs and series

Cover image: Dutchy / iStock by Getty Images

ISBN: 978-952-03-3052-1 (pdf)

FOREWORD

This report is the first effort to map and understand how new AI-powered image recognition technologies have entered the authorities charged with keeping public order in Finland over the last decades. It maps the existing uptake of technology, sets out the main regulations and legislation guiding the use of recognition technologies, and gathers critical insights from activists and researchers following the implementation of new technologies by Finnish authorities.

This report is the result of two research projects anchored at Tampere University. The *Post-Visual Security* project, funded by the Academy of Finland, seeks to understand how digital images participate in security politics and security practices. It is investigating what digital images can do that analogue images could not do, and what digital images can do that other digital artefacts cannot do. The drive to understand computer vision technologies and how they are used in security management and politics runs through this project. The project *Understanding Nordic Digital Order (UNDO)* is a transnational project with partners in Denmark, Sweden, and Finland, funded by the KONE Foundation. It is concerned with digitalization of policing in the Nordics, activism, and surveillance oversight. UNDO seeks to bring digital policing, surveillance, and the concerns activists and researchers have about these issues out in the open, to facilitate that citizens can take active influence and oversee the development of technologies used to police society.

The research questions and priorities are set by the team, and the report written mainly by Sara Pynttäri from May to August 2023, during an internship with the *Post-Visual Security* project. Sara Pynttäri would like to extend her gratitude to Rune Saugmann and Sirpa Virta for offering guidance, feedback, and contacts during this project. A special thank you goes to all her interviewees, colleagues, and family members who helped in making this report happen and offered an overwhelming amount of support and encouragement as well.

EXECUTIVE SUMMARY

The research contained in this report shows that Finnish public order institutions use and want to expand the use of image recognition technologies, as well as wish to share data access with European counterparts – but are reluctant to give the public insight into questions surrounding these technologies. Information gathered from public sources tells that the Finnish police utilize face and license plate recognition mainly to investigate, solve and prevent crimes, while the Border Guard uses face recognition merely in automated passport checking, and license plate recognition in conducting border or regional surveillance, protecting security and property, or preventing and solving a crime. In addition, Finnish Customs has the right to use automated face recognition yet declines to disclose any details on the systems and practices related to this or any other recognition technologies currently in use.

This report relies solely on public information. In addition to news articles and public documents gathered from the internet and through information requests, the material of this report consists of discussions with security authorities, researchers, and activists in non-governmental organizations (NGOs). These discussions were had via email, phone, and both face-to-face and online interviews. The research was conducted between May and August 2023.

Finnish public order authorities seem to view these technologies as useful tools that can benefit the whole society, whereas activists and researchers interviewed for this report have raised critical questions on issues relating to privacy and data protection, misuse and malpractice, as well as insufficient impact assessment and imperfect education for authorities using recognition technologies. Currently, access to information seems arbitrary, with some authorities being more willing to share than others. For the public to be able to set political priorities regarding recognition, and independently assess risks and deficiencies in these technologies and systems, more information should be publicly available. If for some reason more oversight cannot be granted to citizens directly, we recommend the establishment of an independent oversight body (such as a committee or an ombudsman) that would monitor the use of recognition technologies in public order institutions.

TIIVISTELMÄ

Tässä raportissa esitelty tutkimus osoittaa, että Suomen turvallisuusauktoriteetit käyttävät tunnistusteknologioita ja toivovat saavansa laajemmat käyttövaltuudet sekä näihin teknologioihin että tietojen jakamiseen eurooppalaisten kollegoidensa kanssa – mutta ovat vastahakoisia vastaamaan julkisesti tunnistusteknologioihin liittyviin kysymyksiin. Tutkimuksessa selvisi, että poliisi käyttää kasvojen ja rekisterikilpien tunnistusta pääasiassa rikosten tutkimiseen, selvittämiseen ja ennaltaehkäisemiseen. Rajavartiolaitos puolestaan käyttää kasvojentunnistusta vain automaattisessa passintarkastuksessa ja rekisterikilpien tunnistusta rajojen tai alueiden valvonnassa, turvallisuuden ja omaisuuden suojelemisessa sekä rikosten selvittämisessä ja ennaltaehkäisemisessä. Oikeus automaattiseen kasvojentunnistukseen on myös Tullilla, joka valitettavasti kieltäytyi jakamasta mitään tietoja tähän tai muihinkaan käyttämiinsä tunnistusteknologioihin liittyen.

Tämä raportti pohjautuu ainoastaan julkisiin lähteisiin, kuten uutisiin sekä julkisiin dokumentteihin, joista osa on saatu tietopyynnöillä. Lisäksi tutkimuksessa haastateltiin turvallisuusviranomaisia, tutkijoita ja kansalaisjärjestöissä toimivia aktivisteja niin sähköpostitse, puhelimitse kuin kasvokkaisten ja videovälitteisten tapaamisten avulla. Tutkimus toteutettiin vuoden 2023 toukokuun ja elokuun välillä.

Turvallisuusviranomaisten näkemyksen mukaan tunnistusteknologiat edistävät koko yhteiskunnan turvallisuutta, kun taas tutkimuksessa haastatellut aktivistit ja tutkijat nostivat esiin kriittisiä kysymyksiä yksityisyyden- ja datansuojasta, mahdollisista väärinkäytöksistä sekä riittämättömästä vaikutustenarvioinnista ja puutteellisesta koulutuksesta teknologioita käyttäville viranomaisille. Jotta riskejä ja järjestelmien haavoittuvuuksia voitaisiin arvioida riippumattomasti, pitäisi julkista tietoa olla enemmän ja helpommin saatavilla. Tällä hetkellä vaikuttaa siltä, että mahdollisuus saada tietoja vaihtelee organisaation mukaan – salassapitosäännöt eivät siis ole samat kaikille. Mikäli tunnistusteknologioiden käyttöä turvallisuusauktoriteettien toiminnassa ei voida valvoa kansalaisten toimesta, tulisi sitä varten perustaa komitean tai asiamiehen kaltainen virallinen valvova elin.

Table of Contents

1. INTRODUCTION: RECOGNITION IN FINLAND

The objective of this report is to shed a light on the current use and purpose of recognition technologies in the Finnish police and Border Guard. There are, of course, other public order institutions using similar technologies as well but these two were selected as – in addition to Customs – they are the only ones that have the right to use automated face recognition in Finland. Originally, the report was supposed to cover Finnish Customs as well, but it was left out after the organization responded to an information request saying that all material and information related to recognition technologies in Customs was confidential – except for the Customs Personal Data Act. Therefore, it made more sense to focus on the organizations that could provide at least some information. The scope of this research was also limited to face, object, and license plate recognition technologies, with a special emphasis on face recognition (FR). It is necessary to point out that in addition to these, the category of *recognition technologies* includes, for instance, crowd flow and behavior analysis, anomaly detection, emotion recognition and biometric categorization systems. What is more, biometric recognition can be done with fingerprints, palm prints, iris scans, gait recognition, ear shape recognition, retina analysis, voice recognition, etc. The sheer quantity of different recognition technologies creates many potential research opportunities for researchers not only in the field of technology, but also in the field of social sciences.

The rapid development of artificial intelligence (AI), machine vision and recognition technologies generate significant possibilities and equally significant challenges for public order institutions. New technologies promise assistance and efficiency but also evoke security and privacy concerns. Since 9/11, *national security* and *counterterrorism* have been invoked in western countries to justify ever-extending surveillance, and the development and application of recognition technologies. Currently, debates around these issues run heatedly especially in the EU – not least because of the new Artificial Intelligence Act that is supposed to reach its final state by the end of 2023. Data protection and privacy activists are calling for a full-on ban on biometric recognition in public spaces whereas law enforcement authorities see it as a possibility to better prevent and solve serious crimes. In the US, the city of San Francisco banned the use of facial recognition software by the police and other agencies already in 2019.[1] Several other cities followed, and a similar ban was suggested in the European Union as well.

[1] The New York Times, 14.5.2019.

Recognition technologies can be easily associated with alarming examples of authoritarian regimes using them to surveil and oppress their citizens. In Finland, it seems unlikely that the situation would slip into such dystopia, but NGOs have raised questions on whether these technologies influence the freedom of assembly or freedom of speech, for instance. Authorities should be transparent with their practices and policies in a democratic society as democracy is largely built upon mutual trust.

2. RESEARCH QUESTIONS

With an introductory mapping of the current situation of recognition technologies in the Finnish police and Border Guard, this report contributes to the *Understanding Nordic Digital Order (UNDO)* –research project that critically investigates the role and transformation of the Nordic public in connection to digitalization of the police. In addition to an overview of the practices and systems of recognition technologies within the police and Border Guard, this report dives into related regulation both nationally and at EU level. EU regulation is especially important since it draws up the preconditions for national regulation in all Member States – and with the upcoming AI Act, national regulations might be influenced significantly in the next few years. Furthermore, this report introduces the critical debate of recognition technologies by presenting the views and concerns of data protection and privacy activists as well as researchers.

The research questions of this report are:

1. *How is face (and other) recognition technology currently utilized in the Finnish police and Border Guard?*
2. *How did we get there: when, why and by who was which recognition elements introduced?*
3. *What are the main objectives of using these technologies?*
4. *What are the possibilities and risks of these technologies?*
5. *How do authorities see these technologies as evolving in the near future? How do authorities assess how this affects police and other work, and are there plans to change (expand, re-direct, limit) the use of recognition technologies in the near future?*
6. *How do activists and researchers view these technologies?*

This report aims to be an informative overview of a highly topical and important theme that will – and already does – have crucial impacts on the security and privacy of ordinary citizens and society as a whole.

3. METHODOLOGY

This research was carried out between May and August of 2023. In addition to public documents gathered from the internet and through information requests, the material of this report consists of discussions with security authorities, researchers, and activists in non-governmental organizations (NGOs). These discussions were had via email, phone, and both face-to-face and online interviews. As the topic has attracted wide media interest in recent years, a great number of news articles were also of much help in the writing process.

Interviews were conducted mostly in June and July and there were in total six of them. In addition to the research questions listed in the previous chapter, several more specific questions were posed to the interviewees. Due to the research's limited schedule and long processing times for research permissions in several public order institutions, as well as the confidential and sensitive status of key documents and other material regarding the topic, the report relies solely on information that is available for the public either per se or by request.

4. EXISTING RESEARCH AND TERMINOLOGY

Research of the relationship between policing, control and technology has no clear tradition in any specific discipline. Surveillance studies, on the other hand, have a long tradition in criminology since the surveillance technology like CCTV started to control streets and houses, used by the police and private security companies in Britain and many other countries. From the beginning of 2000, in academic criminology conferences there has been a lot of research presented on policing and technology – mainly concentrated on the use (and misuse) of body-worn cameras and other equipment. Technology has not had a big role in the fields of policing research, though. In police science in Europe

and police education both nationally and internationally, the focus has been on how to use and get results in crime prevention and investigation. Especially in international police cooperation, international law enforcement organizations have used recognition technologies such as FR for tackling and preventing international organized crime. Despite all this, research on the relationship between policing, technology, strategy, and politics is lacking.[2] Furthermore, the amount of research on digital policing is scarce:

> Adoption of advanced digital technology is one of the most controversial and fundamental transformations in contemporary police practice. Despite its significance, empirical enquiry of these technologies, and the way they shape and are shaped by policing environments are rare.[3]

In the article *Policing regimes in transition in the Nordic countries: some critical notes from the Nordic reality*, technological development is not dealt with at all, but otherwise it offers a theoretical analysis of the political framework and the essence of the state (as contextual framework) that can be used also in analysis of policing and control.[4]

In International Relations (IR) and critical security studies research there is a limited but sustained engagement with digital and database-based technologies, policing and the distribution of (in)security, subjectivity, and agency. This has attended to issues like the production of digital bodies[5], predictive policing[6], computer vision[7], and algorithmic security governance[8]. In parallel to this report's efforts, Francesco Ragazzi and his team are working on a project called Security Vision[9] where they, inter alia, map the use of biometric and behavioral mass surveillance in EU Member States.

In order to understand the findings of this report, it is important to first clarify certain key terms and concepts:

---

[2] Virta, 2022.

[3] Marciniak 2021, 5.

[4] See Virta and Taponen, 2017.

[5] Bellanova and Fuster, 2013.

[6] Kaufmann, Egbert, and Leese, 2019.

[7] Saugmann, 2019.

[8] Bellanova, Irion, Lindskov Jacobsen, Ragazzi, Saugmann & Suchman, 2021.

[9] https://www.securityvision.io/

1:1	One-to-one facial comparison or identity verification. Can be either automatic or human based. Automatic 1:1 comparison is also referred to as biometric verification.
1:N	One-to-many database search, also referred to as one-to-many comparison or facial recognition or closed-set identification.
Algorithm	A series of step-by-step rules that is followed in order to solve a given problem or complete a task. In computer systems, algorithms are the instructions for what the system does computation-wise.
Artificial intelligence	A field of research studying the relationship between information systems and human intelligence – in particular, how to make computer systems mimic or conduct cognitive tasks traditionally taken to require human intelligence. Can also refer to specific systems or applications.
Biometric data	Concerns or represents the physical, physiological, or behavioral characteristics of a natural person, and such data can be used to detect, recognize, or identify natural persons, for example, or to assign them into categories which can be inferred from such data.
CCTV	Closed-Circuit TeleVision, also known as video surveillance.
Face/facial recognition (FR)	Machine vision technology allowing the automated searching of a facial image against a known collection (see 1:1 and 1:N for different types of FR).
Machine vision	Technology and methods to extract information from an image using training data, algorithms, and databases (a machine's ability to 'see').
Object recognition	Machine vision technology allowing the automated searching and identifying objects from a photo or a video (e.g., vehicles, people).
Real-time face recognition	Real-time search of faces caught by a camera against a database of persons of interest.

Sources for table: Sahlgren (2023, 13–15), TELEFI project (2021, 6–8).

As this topic is a highly complex one and involves interdisciplinary terms and concepts, it is necessary to note that this glossary and report as a whole take a social science approach to recognition

technologies. For instance, if face recognition was examined from an information technology perspective, the key word definitions would most likely be more technical.

5. THE CURRENT STATE OF RECOGNITION TECHNOLOGIES IN THE FINNISH POLICE AND BORDER GUARD

In Finland, both the police and the Border Guard belong to the Ministry of the Interior's area of responsibility. On the Ministry' website, the organizations are described as follows:

> The duty of the police is to secure the rule of law; maintain public order and security; prevent, detect and investigate crimes; and submit cases to prosecutors for the consideration of charges. The police are responsible for maintaining public order and security by patrolling, handling emergency duties, providing advice and guidance, and preventing unlawful activity. Ensuring traffic safety is an important part of this work.[10]
>
> The main duties of the Border Guard are:
>
> - surveillance of the country's land and maritime borders
> - conducting of border checks on persons at land border crossings, ports and airports
> - carrying out of rescue operations particularly at sea.
>
> The aim is to keep Finland's borders safe and secure. The Border Guard also performs police duties and is responsible for customs control at border crossing points not manned by customs officials. At sea the Border Guard cooperates with the Finnish Transport Infrastructure Agency, the Finnish Transport and Communications Agency, the Finnish Defence Forces and environmental authorities.[11]

In Finland, the use of recognition technologies is regulated by national and EU laws. The Finnish police utilize face, object, and license plate recognition for the purpose of solving and preventing crimes as well as to maintaining public order and security. The automated FR system KASTU has been in use since May 2020 and the license plate recognition system REVIKA since 2014. The Finnish Border Guard has been using automated FR at Schengen borders, airports, and harbors since 2005 as part of the automation of passport checking.[12] Finnish Customs got the rights to use automated FR as part of an

[10] Ministry of the Interior, 2023a.

[11] Ministry of the Interior, 2023b.

[12] HS, 7.7.2021.

update to the Personal Data Act in 2019.[13] In addition to these technologies, the police are also testing an object recognition system which can be used to recognize, for instance, specific objects in robbery situations.[14] Object recognition is not currently used although it is already legal. The Border Guard, too, uses real-time object recognition in border control to filter CCTV material and thus ease the work of control center operators: as most of the CCTV material is irrelevant for surveillance purposes (e.g., branches swaying in the wind, animals moving around), filtering out people and vehicles from the videos is practical and cost-efficient. According to the authorities, recognition technologies in general allow transferring workforce from the more manual tasks to core operations where humans can't be replaced with a machine.[15]

In this chapter face and license plate recognition as well as other image gathering technologies used by the police and the Border Guard are introduced with information based on public documents, news and interviews with authorities.

5.1. Recognition technologies in the Finnish police

Face recognition system KASTU

The Finnish police are not allowed to use real-time FR at all, and automated FR is only allowed when investigating suspected crimes that could lead to a prison sentence. The use of KASTU (acronym of *kasvojentunnistus*, engl. face recognition), – a one-to-many (1:N, *see glossary*) FR system that is intended to be utilized not only by the police but also by the Border Guard and Customs – is allowed if criminal investigation is ongoing and if the suspect's identity can't be uncovered otherwise (such as with a phone number or witness testimonies).[16] The system was implemented in May 2020 by the Criminal Intelligence Unit of the National Bureau of Investigation (NBI). Over 500 officers[17] have been

[13] Valtiovarainministeriö, 2019.

[14] Ojanen, Sahlgren, Vaiste, Björk, Mikkonen, Kimppa, Laitinen & Oljakka 2022, 30.

[15] Discussion with authority, 24.7.2023.

[16] Poliisihallitus 2020, 1–2.

[17] HS, 7.7.2021 *(There are probably more by now, but this is the most recent statistic that could be found from public sources.)*

trained to use the system, and the decision of the necessity to use KASTU is made by an individual officer in each individual situation.[18] In the National Police Board's (NPB) official KASTU guideline document, the system's working mechanism is explained as follows:

> The algorithm behind the KASTU system works best with faces looking straight at the camera, based on which the system searches for equivalences from a headshot server. As a result, the system presents up to 200 mathematically similar-looking persons for the authority conducting the face recognition. The results are only an approximation, and further elimination is done in order to limit the number of potential matches. Finally, the remaining images are compared to the source image and other possible images of the suspect, according to training. It is also possible that the person who is being searched for has never been registered in the background systems. Automated FR is always approximate, and one can't perform any actions that impact a person's fundamental rights solely based on the FR result. The identity received from the system must also be confirmed with other means available. The final decision of recognition is always made by a natural person, i.e., an authority, who also decides the subsequent actions. (Translation S.P.)

> KASTU-järjestelmän taustalla oleva algoritmi tunnistaa parhaiten kuvassa kameraa kohtisuoraan olevan henkilön kasvot, jonka perusteella järjestelmä hakee vastaavuuksia kasvokuvavertailupalvelimelta. Vastauksena järjestelmä tuo kasvojentunnistusta tekevälle virkamiehelle korkeintaan 200 lähintä matemaattisesti yhdennäköistä henkilöä. Vastaukset ovat suuntaa antavia ja niihin tehtävällä karsinnalla sopivien henkilöiden määrä rajataan pieneksi. Lopuksi jäljelle jääneitä kuvia verrataan lähdekuvaan ja mahdollisesti muihin epäillyistä oleviin kuviin koulutuksen mukaisesti. On myös mahdollista, että järjestelmästä haettavaa henkilöä ei ole koskaan edes rekisteröity käytettäviin taustajärjestelmiin. Automaattinen kasvonvertailu on aina suuntaa antavaa, eikä pelkästään sen tuloksen perusteella voida toteuttaa henkilön perusoikeuksiin vaikuttavia toimenpiteitä. Järjestelmästä saatu henkilöllisyys on pyrittävä varmistamaan myös muilla käytettävissä olevilla keinoilla. Lopullisen päätöksen henkilön tunnistamisesta tekee aina luonnollinen henkilö eli virkamies, joka päättää myös asiasta seuraavat jatkotoimenpiteet.[19]

After running the search, KASTU provides a photo-ID that can be used to find the suspect from the police's Vitja-RETU (acronym of *rekisteröidyn tuntomerkit*, engl. registered persons identifying features) register that has over 100 000 images of already convicted or suspected criminals.[20] The source image of the suspect is usually a screenshot from a CCTV of the crime scene. As facial features can change over time, the police aim to recognize persons based on immutable features such as ear shape. Searches are performed with side profile images as well, if possible.[21] While KASTU is a useful tool used for criminal investigation, a more thematic picture-to-picture recognition opinion for legal proceedings

[18] Discussion with NGO, 28.6.2023.

[19] Poliisihallitus 2020, 3.

[20] Ibid.; HS, 7.7.2021.

[21] Discussion with NGO, 28.6.2023.

must be asked from a forensic laboratory in the National Bureau of Investigation.[22] As such, KASTU doesn't change any preliminary investigation processes that already exist: it simply assists the identification of suspected criminals and other persons (such as partners in crime) involved in the case. For instance, a suspect can't be called for interrogation until their identity is confirmed by a natural person – identification with KASTU alone isn't enough.[23]

KASTU isn't allowed to be used in databases for passport and ID-card images. Manual searches, on the other hand, are allowed:

> Manual searches of passport and ID-card images can be conducted in cases where an individual is suspected of involvement in a criminal act that, on conviction, would carry a prison sentence. Access of this kind requires a certain amount of background information enabling a focused search leading to manual 1:1 comparison of images. There is no practical way to quickly search facial images through the whole passport and ID-card database as the system was not designed with that function in mind.[24]

According to the Coercion Act (*Pakkokeinolaki,* 806/2011) Article 9(3), the police are allowed to collect facial images of suspects and, based on pressing investigative reasons, of other parties relating to the crime. Since facial images are treated biometrically in KASTU, they belong to a group of special personal data that the police are allowed to use only when it is necessary in order to prevent or unveil a crime, or in relation to investigation and surveillance operations.[25] However, there is an exception to this rule: certain non-criminal databases can be used to identify victims in cases of large-scale incidents such as natural catastrophes.[26] According to the Police Personal Data Act (*Laki henkilötietojen käsittelystä poliisitoimessa*, 616/2019) Article 1(2), personal data must be treated in accordance with the demand to respect human- and fundamental rights, as well as with the principles of proportionality, purposefulness and least harm. Furthermore, according to the Data Protection Act for Criminal Matters (*Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä,* 1054/2018) Article 2(6), considering the purpose, only appropriate and necessary personal data can be treated, and all unnecessary data must be deleted without delay. Once the validity of images taken in

[22] Poliisihallitus 2020, 3.

[23] Discussion with NGO, 28.6.2023.

[24] TELEFI project 2021, 65.

[25] The Police Personal Data Act 616/2019 (*Laki henkilötietojen käsittelystä poliisitoimessa)* Article 2(15)); Poliisihallitus 2020, 1.

[26] TELEFI project 2021, 65.

relation to criminal database enrolment expires, they must be deleted. Personal identifying characteristics processed to establish identity, on the other hand, must be deleted no later than 10 years after the last entry concerning the suspected person, or no later than 10 years after the death of the data subject if the most serious punishment for the most severe offence recorded is a minimum imprisonment of one year.[27] The demands are slightly different with underage offenders: if the data subject was under 15 years old at the time of committing the offence, their personal identifying characteristics are erased no later than five years after the recording of the last entry concerning the person suspected of an offence, unless any of the entries concern an offence for which the only sanction is imprisonment.[28]

The use of KASTU is legally allowed in investigation and surveillance operations[29] as well as operations related to preventing or unveiling crimes[30]. Furthermore, the police have the right to use KASTU with the Aliens database where facial images collected from asylum seekers and aliens are entered.[31] Searches in this database are only allowed when it is necessary to prevent, unveil or solve the following crimes listed in the Penal Code (*Rikoslaki,* 39/1889):

- War-, treachery- and treason crimes, crimes against humanity and crimes against political rights (Articles 11–14)
- Riot and violent riot (Article 17(2–4)), state border offense (17(7)), territorial violation (17(7c)) and arrangement of gross illegal entry (17(8a))
- Aggravated destruction (Article 34(3)), aggravated endangerment of health (34(5)) and terrorism crimes (Article 34a)
- Regulation or aggravated regulation crimes (Article 46 (1–2)).[32]

Since the Aliens database can only be searched when these crimes are in question, KASTU is used extremely rarely for this purpose. Even with serious crimes such as murder or manslaughter, KASTU can't be used to search this database. Recognizing victims of, e.g., sex crimes or human trafficking is

[27] TELEFI project 2021, 66.

[28] Ibid.

[29] The Police Personal Data Act 616/2019, Article 2(5–6).

[30] The Police Personal Data Act 616/2019, Article 2(7–8)); Poliisihallitus 2020, 1–2.

[31] TELEFI project 2021, 26; persons are registered based on the Aliens law (*Ulkomaalaislaki* 301/2004, Article 7(131)).

[32] Poliisihallitus 2020, 2.

also not allowed. In addition to the police, the Aliens database can be accessed by the Border Guard, Customs, and the Finnish Immigration Service.[33]

As discussed later in this report, there are plenty of historical and international examples of face recognition technologies (FRT) being flawed or biased and thus causing significant harm to innocent people. Therefore, it is crucial to make sure that the systems are tested thoroughly before putting them to use. In Finland's case, the NBI conducted trials on KASTU's algorithm in 2017–2018. The finished system has also been tested in IT- and QA-environments as well as in a production environment.[34] According to these tests, the algorithm works reliably and doesn't include biases relating to, e.g., race. For several years already, the police have used this same algorithm to perform 1:1 verification in the process of granting license documents. Currently, the police are working on a new impact assessment where matters relating to KASTU will also be evaluated.[35] According to the police, so far experiences with the FR system have been largely positive and no major problems or malpractices have appeared.[36] Authorities seem to have a strong trust in the system and its unbiased nature – and even though KASTU hasn't caused any controversies or scandals as far as the public knows, evaluating its trustworthiness as a researcher is a challenge since most of the key documents and other important material are confidential and thus out of public's reach.

In addition to encompassing testing, user training is another essential matter in preventing unnecessary harm caused by FRT. The rights to use KASTU are distributed in a system called Portti, and the training can be completed independently as an online course.[37] The training takes approximately one workday and includes basic information about recognizing parts of faces and qualities that help to identify a person. A more in-depth-course takes three days and gives rights to use KASTU for searching the Aliens database.[38] The NPB is responsible for training police officers to use KASTU. In the Police University College's curriculum, there are no mentions about a course or other education modules for face

[33] Discussion with NGO, 28.6.2023.
[34] Discussion with NGO, 28.6.2023.
[35] Ibid.
[36] HS, 7.7.2021.
[37] Poliisihallitus 2020, 3.
[38] Discussion with NGO, 28.6.2023.

recognition technologies, which implies that they are not a part of the basic education for new police officers.[39] Furthermore, teaching of artificial intelligence in general is still in a rather rudimentary stage in the Police University College.[40]

A cautionary tale: the case of Clearview AI use by the Finnish police

In 2021, the National Bureau of Investigation infamously made itself known for using Clearview AI's FR software to recognize sexual abuse victims in the end of 2019 and start of 2020. Clearview AI is a FR software based on a database of more than 30 billion photos scraped from social media without consent. In 2020, the New York Times published an extensive article of the company and unveiled the software's working mechanism:

> The result: a system that uses what Mr. Ton-That [CEO of Clearview AI] described as a "state-of-the-art neural net" to convert all the photos into mathematical formulas, or vectors, based on facial geometry — like how far apart a person's eyes are. Clearview created a vast directory that clustered all the photos with similar vectors into "neighborhoods." When a user uploads a photo of a face into Clearview's system, it converts the face into a vector and then shows all the scraped photos stored in that vector's neighborhood — along with the links to the sites from which those photos came. (The New York Times, 18.1.2020.)

According to the company, more than 600 law enforcement agencies have used the FR software. In Finland, 120 searches were made by four NBI officers during a free demo period. Neither NBI's leadership nor the NPB were aware of this experiment – it came up over a year later when Buzzfeed News contacted the organization in March 2021. After that, the police reported the experiment and a possible data breach to the Data Protection Ombudsman who later gave a notice to NBI. What made the whole incident even more awkward was the fact that NBI first responded to Buzzfeed News that Clearview AI's software had not been used within the organization (only to find out that this was, in fact, a false statement), and also that NBI couldn't tell what happened to the photos after they were ran through the software. During the demo period only one hit was discovered, and it led to cooperation with social workers. Clearview AI is in no way connected to KASTU.

Sources: The New York Times (18.1.2020), Yle (28.9.2021) & Yle (23.4.2021).

[39] Poliisiammattikorkeakoulu, 2022.

[40] Discussion with NGO, 28.6.2023.

License plate recognition system REVIKA

Another widely used and popular recognition technology in the Finnish police is a license plate recognition system called REVIKA (acronym of *rekisterikilven lukulaite ja videokamerajärjestelmä,* engl. license plate registration and video camera system), developed by a Finnish company called Sunit Oy. It was first put to use by the Oulu police in 2014 and soon adapted into nationwide use. The system scans license plates and recognizes vehicles that are reported to have issues (e.g., uninspected or stolen vehicles, vehicles with unpaid taxes or vehicles known to be connected to criminals or wanted persons).[41] Official documents related to REVIKA are confidential information.[42] According to a magazine interview with Timo Vihervaara, a police officer responsible for the operative use of REVIKA, the software works in a fairly simple way:

> The software goes through recorded material one frame at a time and picks up license plates from the images in somewhat real-time. The license plates are compared to an updating database which includes inter alia, unpaid taxes registered by Trafi [Traficom is the Finnish traffic and communication agency], neglected scheduled vehicle inspections, and plenty of other information such as warrants. When the software discovers a match, an alarm shows up on the screen. After that, the patrol decides on subsequent actions. (Translation S.P.)

> Ohjelmisto kahlaa taltioitua materiaalia läpi ruutu kerrallaan ja poimii rekisterikilvet kuvista jokseenkin reaaliajassa. Niitä verrataan järjestelmän langattomasti päivittyvään tietokantaan, jossa on mukana muun muassa Trafin kirjaamat maksamattomat verot, hoitamatta olevat määräaikaiskatsastukset sekä liuta muita tietoja, kuten etsintäkuulutukset. Kun järjestelmä löytää listoiltaan vastaavuuden, antaa se hälytyksen näytölle. Sen jälkeen partio tekee suunnitelman jatkotoimista.[43]

The REVIKA user interface has different alarm sounds and colors for different offenses, which makes it easier for police officers to determine the urgency of the situation.[44] Vehicles without any issues are left unnoticed, giving the patrol more time to focus on actual offenses. Similarly as with KASTU, a match found by the software alone isn't enough: before any subsequent actions, the patrol does a real-time inquiry to make sure that the match is correct and that there is, in fact, a reason to stop the vehicle in question.[45] REVIKA keeps individual license plates' information and images saved for 24 hours, in which

[41] Yle, 8.6.2017.

[42] Discussion with authority, 9.6.2023.

[43] Moottori, 7.2.2016.

[44] Yle, 8.6.2017.

[45] Moottori, 7.2.2016.

time the police officers have to determine whether the records include some information that needs to be stored in the police's other information systems.[46] In addition to the Police Personal Data Act, the use of REVIKA is regulated with the Traffic Code (*Tieliikennelaki* 729/2018) Articles 7(181) and 7(182).

The current curriculum of the Police University College's undergraduate degree doesn't include any specific training on REVIKA – however, the device is introduced to new police officers as part of a course on police vehicles, and the system's data content is addressed during teaching about traffic and crime prevention. For students in further education, the system is taught during workplace training in police departments. Those who are responsible for this workplace training participate in a two-day seminar for REVIKA instructors – that way the topicality and uniformity of the training is ensured.[47]

Other image gathering technologies

The Finnish police use city cameras, body cameras and drones. City cameras are placed in multiple municipalities and cities to monitor city centers and other spaces where people tend to gather.[48] These cameras help the police to prevent and solve crimes and other disturbances both in real-time and afterwards. In Oulu, the police also have access to certain indoor cameras, for instance in schools – an arrangement that the Data Protection Ombudsman has deemed questionable.[49] However, FRT is utilized neither in indoor nor outdoor city cameras. In addition to these, the police have started to gather a map of private (e.g., citizen, store, mall, and company owned) surveillance cameras in Finland to make criminal investigation easier and more efficient with diverse video evidence.[50] So far approximately 5000 cameras have been registered in the map.[51]

Before the police decided to switch to a new "group video service system" (*ryhmävideopalvelujärjestelmä*) this year, they had been using body cameras for eight years. These

[46] Poliisihallitus 2021, 9.
[47] Ibid.
[48] Yle, 21.12.2022.
[49] Yle, 29.9.2019.
[50] Yle, 21.1.2020.
[51] HS, 28.5.2023.

were first tested for four years (during 2015–2019) in Helsinki police department and then adapted into nationwide use in 2021. The cameras needed to be turned on by officers themselves, who also looked through the recorded material afterwards to see if there was anything worth saving. All useless material was automatically deleted after 24 hours. Only a fraction of the recordings was eventually used as evidence.[52] At the end of 2022, the Finnish Parliament's Ombudsman came to a conclusion that the use of body cameras included many judicial issues, which in part led to the decision to replace them with other, less problematic system.[53] The new group video service system will be on trial run this year and potentially in full use next year already. According to the National Police Board, the system will transmit live video from vehicles, drones and officers' mobile devices to a server, making it easier to observe the police operation in question in real-time.[54] Furthermore, it would enable opening a video connection in case there are difficulties getting a connection with the field officers otherwise.[55] Video connection can be opened either by the police carrying the camera or by someone else, remotely from a computer. The recordings will be stored on the server for two weeks – after that, they are automatically deleted.[56]

Drones (i.e., Unmanned Aircraft Systems, UAS) are used for e.g., mass traffic and protest surveillance, filming accidents and crime scenes, and finding missing people.[57] They only utilize thermal cameras, not FRT. A majority of the Finnish police's drones are from a Chinese company DJI.[58] The first camera drone was purchased in 2015 and currently there are more than 600 trained pilots in the police force. Camera drones became more common in police operations because of the government's digitalization goals – with the intention to make the work more efficient:

> One of the important tasks of unmanned aviation is to enhance the view of the situation that the police have from the field to the command centre or, for example, to the control unit of the police. The benefits provided by drones are diverse. In addition to everyday police work, camera drones are also used for special operations, such as those of the national Rapid Response Unit Karhu. Aerial photography can be used, for example, to assist in safety inspections related to explosives.

[52] Yle, 21.1.2020.
[53] EOAK/2017/2021.
[54] Aamulehti, 5.5.2023.
[55] Discussion with authority, 9.6.2023.
[56] HS, 27.7.2023.
[57] Poliisi, 2023.
[58] Discussion with authority, 9.6.2023.

> Most recently, traffic control drones have been introduced. The police can also support other authorities with their drone operations.[59]

The training for drone use is provided by the Police University College.[60] In the undergraduate degree (AMK), students receive a concise introduction to drones as part of the teaching on surveillance and alarm operations. In graduate degree (YAMK), students orientate themselves more profoundly in using and leading the use of drones during an 8-hour training. In further education, there are three drone courses:

- Training for drone pilots (1,5 credits, 8 + 22 + 16 h)
- Training for drone instructors (1,5 credits, 8 + 36 h)
- Further training for drone instructors (3 days)

In addition to these, utilizing drones is touched upon in almost every further education course relating to operational field work.[61]

5.2. Recognition technologies in the Finnish Border Guard

Face and license plate recognition

Starting from 2005, the Finnish Border Guard has utilized automated FR in Helsinki-Vantaa airport to compare a passenger's face to the chip in their passport in order to identify them (1:1 verification, *see glossary*). According to the authorities, the adoption of this system was pushed by the rapid growth of air traffic volume and the consequent need to increase the number of border inspector personnel, as well as by requirements from EU legislation such as the Schengen Agreement. Although the verification process is automated, the ultimate decision is still made by a human in a control room: the FR system merely offers a suggestion of the similarity of a passenger's face and the image in their passport, based on which a human decides whether the passenger's identity can be verified.[62] In this process, only

[59] Poliisi, 2023.

[60] Poliisihallitus 2022b, 20.

[61] The Police University College's response to an information request, 5.7.2023.

[62] Discussion with authority, 24.7.2023.

technical data needed to monitor the system's technical quality is stored.[63] Currently, a 1:N identification (*see glossary*) is not used – although the Border Guard has the right to use KASTU in investigation operations[64] and in operations related to preventing or unveiling a crime[65]. The supplier of Helsinki-Vantaa's FR system and the algorithm that it runs on is Vision-Box S.A. – other technical details of the Border Guard's surveillance systems are confidential.[66] FR is not used in border surveillance yet other images and observations can be stored.[67] The Border Guard has taken part in multiple innovation and research projects relating to surveillance and recognition technologies, among them D4FLY[68], FOLDOUT[69] and ARESIBO[70] – to mention a few.

The Border Guard's RATAS (acronym of *rajatarkastusjärjestelmä,* engl. border control system) is an information system for border inspections. It's not based on biometric, automated or semiautomated decision-making but collects biometric data (such as facial images and fingerprints, *see chapter 6*) according to the EU's Entry-Exit System Act's (EU 2017/2226) requirements, and according to the restrictions of the Border Guard Personal Data Act (*Laki henkilötietojen käsittelystä Rajavartiolaitoksessa* 639/2019).[71] Personal data collected during a border inspection is stored in a register for the Border Guard's operations. This data, including biometrics such as facial image, can be processed to control and ensure the order and security of borders; to solve crimes and maintain the public order and security; to prevent and expose crimes; to handle informant data; to manage military law and to perform other Border Guard's legal tasks. Details on the processing of data can be found in the table below:

[63] The Border Guard's response to an information request, 20.6.2023.

[64] The Border Guard's personal data law 639/2019 (*Laki henkilötietojen käsittelystä Rajavartiolaitoksessa*), Article 2(8–9).

[65] Id., Article 2(10–11).

[66] The Border Guard's response to an information request, 20.6.2023.

[67] Discussion with authority, 24.7.2023.

[68] https://d4fly.eu/

[69] https://cordis.europa.eu/project/id/787021

[70] https://aresibo.eu/

[71] Discussion with authority, 24.7.2023; The Border Guard Personal Data Act 639/2019, Article 2.

Purpose of processing biometric data	Subjects of data processing	When will data be deleted?
Controlling and ensuring the order and security of borders	• Passengers crossing borders	After five years at the latest, starting from when the last entry is done. There are some exceptions with the deletion time ranging from six months to 25 years.
Solving crimes and maintaining the public order and security	• Suspects (both adult and under 15-year-olds) • Victims • Witnesses • Persons under preliminary investigation • Plaintiffs • Persons who have given additional information on the case	If the crime investigation is transferred to a prosecutor, related data will be deleted after 5–20 years (depending on the most serious punishment for the crime).
Preventing and exposing crimes	• Persons who can be legitimately suspected of committing or having committed a crime for which the most serious punishment is imprisonment • Persons related to the abovementioned person • Persons under the surveillance or other procedure of the Border Guard • If necessary: Other parties related to the crime (e.g., victims, witnesses, plaintiffs)	After 10 years at the latest, starting from when the last entry is done.
Handling informant data	• Informants	After 10 years at the latest, starting from when the last entry is done.
Managing military law	• Persons under preliminary investigation or force procedures • Informants, witnesses, plaintiffs	After 1–10 years, depending on the offense and consequent procedures in question.

Source for table: Rajavartiolaitos (2022). For a more comprehensive and detailed list of personal data processing, see: https://raja.fi/rajavartiotoiminnan-rekisteri (only in Finnish).

RATAS is currently being reformed as part of a threefold, comprehensive reform project RAVALU that lasts until the end of 2027. In the first two sections executed during 2020–2022, technical sensor and surveillance infrastructure was reformed. In the third section that started this year, an approximately 30 years old information system for the Border Guard's operations (*rajavartiotoiminnan tietojärjestelmä*, RVT), also including RATAS, will be renewed. As part of this RAVALU project's aim to modernize the whole enterprise resource planning system, object recognition analytics will be built straight into CCTVs – an objective that might be heavily influenced by the EU's Artificial Intelligence Act (*explained in detail in chapter 6*).[72]

The use of license plate recognition is allowed when conducting border or regional surveillance, protecting security and property, or preventing and solving a crime e.g., in closed headquarter areas. When license plate recognition is being used, a video record of the situation and the license plate's transcription is saved. The material can only be accessed by authorized persons with relevant justification, and the use of the material is monitored.[73] Terms for storing the surveillance material vary based on its purpose:

- If the surveillance is in relation to the security of property or space, the gathered material can be saved as long as necessary and justified,
- If the surveillance is in relation to border security, the gathered material will be deleted after six months at the latest,
- If the surveillance is based on the law for regional surveillance (and not connected to any preliminary investigation), the gathered material must be deleted after a year at the latest (starting from the moment it is no longer needed for the purpose it was collected for).[74]

A system similar to REVIKA has been tested and considered, yet it's not in wide operative use because of challenges in adapting it to the Border Guard's larger background systems, and lack of the organizations inner deliberation on matters of expenses and jurisdiction.[75] If deployed, this kind of

[72] Discussion with authority, 24.7.2023.

[73] The Border Guard's response to an information request, 20.6.2023.

[74] Ibid.

[75] Discussion with authority, 24.7.2023.

recognition system could be utilized to, for instance, perform first-hand identification of vehicles crossing a border, making it easier to target further actions where needed. Automatic license plate recognition technology would also make border inspections faster and easier by reducing the need for manual information searches. On the contrary, according to an interviewee, adding this kind of system to the Border Guard's patrol cars wouldn't make much sense as the organization mainly monitors limited border areas.[76]

Before the Covid pandemic and Russia's war in Ukraine, automated surveillance in border crossing stations between EU and Russia was considered. For obvious reasons, this is not currently topical as traffic on these borders has died down. Furthermore, Finland's weather conditions and half a year's darkness pose complicated requirements for the equipment for this kind of surveillance.[77]

There are no separate guidelines or documents for the use of recognition technologies in the Border Guard: national and EU laws are specific enough.[78] In addition to the Border Guard Personal Data Act, the use of these technologies is regulated by the Border Guard Act (*Rajavartiolaki* 578/2005), the Regional Surveillance Act (*Aluevalvontalaki* 755/2000) and the EES Regulation (EU 2017/2226)[79], which is presented more thoroughly in chapter 6. According to the Border Guard Act (578/2005) Article 2, all operations must be performed in accordance with the demand to respect human and fundamental rights, as well as with the principles of proportionality, purposefulness and least harm. Article 5 sets more specific limitations on recognition technologies and use of material collected with this surveillance method:[80]

- Article 5(31): The Border Guard has the right to use images collected via technical surveillance in border crossing stations to automatically identify persons who are wanted to be sued, detained, arrested, taken into detention, imprisoned, or otherwise monitored by authorities.

[76] Discussion with authority, 24.7.2023.

[77] Ibid.

[78] The Border Guard's response to an information request, 20.6.2023.

[79] Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011.

[80] The Border Guard Act 578/2005, Article 5.

- Article 5(36): Border guards have the right to get everyone's personal information in order to perform operations. If one declines to give this information, their identity can be figured out using identification marks.

The Regional Surveillance Act (755/2000) Article 6(30) states that border guards have the right to use technical surveillance and store video and audio material when performing regional surveillance or preventing and identifying suspects of territorial violations or illegal entry. In addition to these laws, the Border Guard has the right and sometimes responsibility to identify and compare the identity of persons based on fingerprints in EU's Visa Information System (VIS) and European Asylum Dactyloscopy Database (Eurodac).[81]

Furthermore, in the coming years the Border Guard's practices will be impacted by EU's Smart Border Package that consists of the Entry-Exit System (EES) and the European Travel Information and Authorization System (ETIAS). ETIAS will apply to visa-exempt third country nationals that will need to submit an online application before their trip to receive a travel authorization. The application information will be automatically processed against EU's and relevant Interpol's databases to determine whether there are grounds to refuse a travel authorization:[82]

> If there is a hit or an element requiring analysis, the application will be handled manually by the competent authorities. In this case, the ETIAS central unit will first check that the data recorded in the application file corresponds to the data triggering a hit. When it does or where doubts remain, the application will be processed manually by the ETIAS national unit of the responsible member state. The issuing or refusal of an application which has triggered a hit will take place no later than 96 hours after the application is submitted or, if additional information has been requested, 96 hours after this information has been received.[83]

However, the final decision on the right of entry or stay is still made by a border guard.

The Border Guard trains its own staff. Training includes the use of border surveillance and inspection tools as well as technical surveillance systems (such as drones) and related laws and restrictions to their

[81] The Border Guard's response to an information request, 20.6.2023.

[82] Council of the European Union, 2018.

[83] Ibid.

use (e.g., privacy issues), and it must be passed in order to use these systems.[84] The aspect of fundamental and human rights is also touched upon – yet not necessarily with the support of use case examples. However, according to the authorities, the deliberation of jurisdiction and protection of paramount rights is (or at least should be) done already when the systems are acquired.[85] Training for the use of border control automatons (used for automated identity verification in Helsinki-Vantaa airport) is given to border guards by the system supplier. While the field working border guards don't have to understand technical specifics of the system in question, they are required to have the basic knowledge to be able to identify any troubles in the verification process. The Border Guard's technical maintenance personnel, on the other hand, possess a more encompassing knowledge of the system to solve these troubles in cooperation with the system supplier.[86]

Other image gathering technologies

Serving the purpose of "flying binoculars"[87], the Border Guard uses drones in border surveillance, search, and rescue tasks as well as in other legal tasks when needed.[88] While the drones don't use FRT, they can include thermal cameras and automated object recognition technology to recognize humans, for instance. In some drones, different camera qualities are integrated in the device – others have the option to change cameras when needed. However, an interviewee argues that including recognition technology in drones doesn't automatically mean added value since it is also possible to fly closer to objects in order to recognize what they are.[89] An official document of the technical details of the Border Guard's drones is confidential on the grounds of cyber security reasons.[90] The Border Guard personnel's training in drone use includes legal matters, such as constitutional rights to privacy and domestic peace, data protection regulations as well as laws relating to crime prevention, preliminary investigation, and coercive means. As part of the training, it is emphasized that the preconditions to utilize drones vary

[84] The Border Guard's response to an information request, 20.6.2023.
[85] Discussion with authority, 24.7.2023.
[86] Ibid.
[87] Ibid.
[88] The Border Guard's response to an information request, 20.6.2023.
[89] Discussion with authority, 24.7.2023.
[90] Ibid.

based on the different operations: for instance, violating domestic peace is prohibited per se, yet it can be done in case sufficient preconditions are met and permission has been granted.[91]

6. REGULATIONS AND GOVERNANCE

As Finland is part of the European Union, the use of recognition technologies and related data sharing is regulated not only at a national level but also at EU level. The European Union has in recent years emphasized keeping its citizens' data safe and questioned the actions and policies of companies using this data, such as Facebook and Google. The intentions behind commercial use of personal data are, of course, different than utilizing data for preventing crimes and protecting citizens, but the means of doing this might be similar – as is in the case of FRT. A study commissioned by the European Parliament in 2021 suggested that real-time remote biometric identification should be allowed for law enforcement without limitations.[92] NGOs like Statewatch, on the other hand, have called for a full ban on real-time and post remote biometric identification in public spaces as well as strict restrictions and regulations on other AI systems so that fundamental human rights will be protected.[93]

6.1. Regulations within European Union

The Artificial Intelligence Act

EU's Artificial Intelligence Act (AI Act) is going to be one of the first major laws to regulate artificial intelligence and its applications such as FRT. The European Commission announced the Proposal for a Regulation on Artificial Intelligence in April 2021. In this Proposal, the four specific objectives were:

- ensuring that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values,
- ensuring legal certainty to facilitate investment and innovation in AI,

[91] Discussion with NGO, 28.6.2023.

[92] Policy Department for Citizens' Rights and Constitutional Affairs 2021, 61.

[93] Statewatch, 2023.

- enhancing governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems,
- facilitating the development of a single market for lawful, safe, and trustworthy AI applications and preventing market fragmentation.[94]

This first approach reminded the way other products, e.g., medicine, are regulated in the EU area. However, in the draft that was passed in June this year, the emphasis was more on protecting human rights and eliminating risks as well as establishing a technology-neutral, uniform definition for AI that could be applied to future AI systems.[95] Whether it is reasonable to try to come up with a specific definition has been debated by researchers and experts as the field of AI is so complex and ever-evolving that it complicates definitions.[96] Furthermore, tech industry actors have been concerned with the Act's possible innovation-inhibiting impact.[97] This fall, the European Commission, European Parliament and the Council of Europe will negotiate on the final terms for the Act and aim to reach a final agreement by the end of the year.

The AI Act takes a risk-based approach to regulating AI, meaning that it divides AI applications into four groups of risk – unacceptable, high, limited, and minimal:

Unacceptable risk	Unacceptable risk AI systems are systems considered a threat to people and will be banned. They include: • Cognitive behavioral manipulation of people or specific vulnerable groups: for example, voice-activated toys that encourage dangerous behavior in children • Social scoring: classifying people based on behavior, socio-economic status, or personal characteristics • **Real-time and remote biometric identification systems, such as facial recognition.**

[94] COM/2021/206.

[95] European Parliament, 2023.

[96] Yle, 13.6.2023.

[97] The New York Times, 14.6.2023.

	Some exceptions may be allowed: **For instance, "post" remote biometric identification systems where identification occurs after a significant delay will be allowed to prosecute serious crimes but only after court approval.**
High risk	AI systems that negatively affect safety or fundamental rights will be considered high risk and will be divided into two categories: 1. AI systems that are used in products falling under the EU's product safety legislation. This includes toys, aviation, cars, medical devices, and lifts. 2. AI systems falling into eight specific areas that will have to be registered in an EU database: • **Biometric identification and categorization of natural persons** • Management and operation of critical infrastructure • Education and vocational training • Employment, worker management and access to self-employment • Access to and enjoyment of essential private services and public services and benefits • **Law enforcement** • **Migration, asylum, and border control management** • **Assistance in legal interpretation and application of the law**. All high-risk AI systems will be assessed before being put on the market and also throughout their lifecycle.
Limited risk	Limited risk AI systems should comply with minimal transparency requirements that would allow users to make informed decisions. After interacting with the applications, the user can then decide whether they want to continue using it. Users should be made aware when they are interacting with AI. This includes AI systems that interact with humans (i.e., chatbots), emotion recognition systems, biometric categorization systems, and AI systems that generate or manipulate image, audio or video content (i.e., synthetic images and video such as deepfakes).

Minimal risk	All other AI systems presenting only low or minimal risk could be developed and used in the EU without conforming to any additional legal obligations. However, the proposed AI act envisages the creation of codes of conduct to encourage providers of non-high-risk AI systems to voluntarily apply the mandatory requirements for high-risk AI systems.

Sources for table: European Parliament (8.6.2023) & European Parliamentary Research Service (2023). Bolding added to demonstrate the parts that concern this report's organizations.

In addition, Member States would be required to establish a national supervisory authority responsible for supervising the application and implementation of the regulation, and EU would establish a European Artificial Intelligence Board composed of representatives from Member States and the Commission.[98]

Face recognition has been one important area of debate in the EU – mostly regarding the use of real-time FR and whether it should be banned altogether or not. In the 2021 Proposal, it was suggested that FR would be banned entirely in public spaces with the exception of finding missing children, dangerous criminals and terrorists.[99] In the current draft, FRTs belong in either "unacceptable" or "high risk" categories and are regulated based on their risk potential:

> The use of real-time facial recognition systems in publicly accessible spaces for the purpose of law enforcement would be prohibited, unless Member States choose to authorise them for important public security reasons, and the appropriate judicial or administrative authorisations are granted. A wide range of FRTs used for purposes other than law enforcement (e.g. border control, market places, public transport and even schools) could be permitted, subject to a conformity assessment and compliance with safety requirements before entering the EU market.[100]

It seems unlikely that there would be a full-on ban of FR in the final agreement, yet some amendments to allowed use situations might still occur. If included in the final version as suggested in the draft, and authorized by the Finnish government, Finnish public order institutions would get quite significantly

[98] European Parliamentary Research Service 2023, 6.

[99] Politico, 14.6.2023.

[100] European Parliamentary Research Service 2023, 5.

wider possibilities to use FR – even in real-time. This has been wished for by the security authorities and firmly opposed by human rights and privacy protection activists. However, since Finland usually complies with EU's regulations and might even go further with its national legislation, it seems somewhat unlikely that real-time FR in public spaces would be allowed. An interesting fact is, though, that the draft regulation does not apply to "AI systems developed or used exclusively for military purposes, to public authorities in a third country, nor to international organizations, or authorities using AI systems in the framework of international agreements for law enforcement and judicial cooperation".[101] It's hard to foresee exactly how this would impact Finnish authorities as the extent of the exceptions depends on the definition of, for example, international cooperation on judicial and law enforcement agreements.

According to the AI Act draft, scraping of biometric data from social media or CCTV footage to create facial recognition databases would also be prohibited,[102] making it difficult for companies such as Clearview AI to keep selling their services in Europe.

Other related EU regulation

A major EU law that impacts everything relating to personal (and biometric) data is, of course, the General Data Protection Regulation – more commonly called GDPR (EU 2016/679). According to GDPR, the processing of biometric data is only allowed in case one of the grounds of Article 6(1) is met:

> The processing is, inter alia, justified if the data subject has given consent, or if the processing is necessary for compliance with a legal obligation to the processing. As the processing of biometric data could create significant risks to the fundamental rights of data subjects, Article 9(1) GDPR generally prohibits the processing of biometric and other sensitive data for identification purposes. This general rule is subject to exceptions exhaustively listed in Article 9(2) GDPR.[103]

These exceptions include necessary processing for, e.g., the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, protecting the vital interests of the data subject or of another

[101] European Parliamentary Research Service 2023, 3.

[102] Id., 10.

[103] Policy Department for Citizens' Rights and Constitutional Affairs 2021, 26.

natural person where the data subject is physically or legally incapable of giving consent, and establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity – among many other purposes.[104] Considering law enforcement purposes, GDPR's Article 10 rules that:

> processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.[105]

The Law Enforcement Directive (LED) sets out general principles for the processing of personal data by law enforcement authorities. In addition to GDPR's Article 10 principles, LED rules that processing of biometric data is allowed only:

- where authorised by Union or Member State law,
- to protect the vital interests of the data subject or of another natural person or
- where such processing relates to data which are manifestly made public by the data subject.[106]

Furthermore, LED requires Member States to:

> implement appropriate security measures, including confidentiality and the current state of the art, especially concerning special categories of personal data like biometric data. These include measures like user control, storage control, access control and integrity and should take into account the risks that are presented by data processing, such as the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed, which may, in particular, lead to physical, material or non-material damage.[107]

Should the data be processed against the principles determined in LED's Article 4, 8 or 10, data subjects have the right to request the removal of their data.[108]

Several EU laws for border control and security issues impact the way biometric data is shared between Member States and with non-EU states. Here, the Entry-Exit System (EES), the Schengen Information System (SIS), the Visa Information System (VIS), the Prüm Convention and the European Asylum

[104] General Data Protection Regulation 2016/679, Article 9.

[105] Id., Article 10.

[106] Law Enforcement Directive 2016/680, Article 10.

[107] Policy Department for Citizens' Rights and Constitutional Affairs 2021, 27.

[108] Law Enforcement Directive 2016/680, Article 16(2).

Dactyloscopy Database (Eurodac) are examined more closely since they have an influence on Finnish authorities' work and possibilities to get access to and process biometric data.

One of the two parts of EU's Smart Borders Package, the **Entry-Exit System (EES)** will be a union-wide information system that aims to improve the management of external borders, prevent irregular immigration and facilitate the management of migration flows. The purpose of EES is to "register electronically the entry and exit data of third-country nationals who are authorized to stay in the territory of the Member States for a short period of time and to calculate the duration of their authorized stay".[109] The data in the system can be accessed by border, visa and immigration authorities as well as the police, the Border Guard, Customs and the Defense Forces (for the purpose of preventing, detecting and investigating terrorist offences and serious crimes).[110] EES collects and records:

- data listed in one's travel document (e.g., full name, date of birth, etc.)
- date and place of entry into and exit from a European country using the EES
- facial image and fingerprints
- refusal of entry, where relevant.[111]

The data will be stored for 3–5 years, depending on why it was recorded in the first place.[112] EES is not yet operational, and the schedule for its adoption is under evaluation – however, some have estimated that it might be up and running in 2025.[113] The national authority responsible for EES in Finland is the Border Guard.

The **Schengen Information System (SIS)** is an information exchange database where competent national authorities, such as the police and border guards, can enter and consult alerts on missing or wanted persons, illegal entrants in the Schengen area, stolen vehicles, and lost or stolen identity documents.[114] It was initially launched in 1995 and has been updated twice since: in 2013 (changing its

[109] Sisäministeriö, 2022a.
[110] Ibid.
[111] European Union, 2023.
[112] Ibid.
[113] Discussion with authority, 24.7.2023.
[114] European Commission, 2023a.

name to Second Generation Schengen Information System, or SIS II) and in 2023. SIS consists of a central system, national SIS systems in all countries using SIS, and a network between the systems.[115] Alerts are registered in SIS as follows:

1. A person or object is reported as missing, related to a crime, or of interest.
2. An official authority enters the personal information related to that person or object in SIS, and an alert is recorded.
3. All Member States have access to this information.
4. The person, object, or documents are located, and all those who have access to SIS can enter the information into the System.
5. Once an alert is complete (for example, a vehicle is located, a person is returned or found), the alert can be deleted.[116]

SIS is used at external borders and within the EU and Schengen area, making it possible to move freely and safely in the area without internal border checks. As of 2023, a variety of biometrics can be used to identify persons in SIS: photographs, palm and fingerprints, palm and fingermarks and DNA records (only in relation to missing persons). Finger and palmprints as well as finger and palm marks are used for biometric searches through the automated fingerprint identification system in SIS. Currently, photograph and face recognition technology are not used in the system, but studies have been made of the possibility to include this technology in SIS in the future.[117] The national authority responsible for SIS in Finland is the National Police Board.

In operation since 2011, **Visa Information System (VIS)** is a database that helps with the processing of short- and long-stay visas and exchanging visa data between Schengen states. Similarly to SIS, VIS consists of a central IT system and of a communication infrastructure that links the central system to national systems. It connects consulates in non-EU countries and all external border crossing points of Schengen states.[118] The database can be accessed by the following authorities:

[115] European Commission, 2023b.
[116] schengenvisainfo.com, 2023a.
[117] European Commission, 2023b.
[118] European Commission, 2023c.

- The authorities responsible for carrying out checks at external borders and within the national territories (for the purpose of verifying the identity of the person, the authenticity of the visa or whether the person meets the requirements for entering, staying in, or residing within the national territories)
- Asylum authorities (only for the purpose of determining the EU State responsible for the examination of an asylum application)
- In specific cases, national authorities and Europol (for the purposes of preventing, detecting and investigating terrorist and criminal offences).[119]

Data is stored for five years, starting from the expiry date of the issued visa, the date a negative decision is taken or the date a decision to modify an issued visa is taken.[120] The system uses Biometric Matching System (BMS) which is an Automated Fingerprint Identification System (AFIS) subsystem that allows border authorities to identify and verify third country nationals traveling to EU by linking biometric identifiers to individual persons. This is primarily done with fingerprints, but after a revision in 2021, live facial-image enrolment and matching has also been possible.[121] The national authority responsible for VIS in Finland is the Ministry for Foreign Affairs.

The **Prüm Convention** was adopted into EU legislation in 2008 and allows Member States to search other Member States' national databases on DNA, fingerprints and vehicle registration for law enforcement purposes, and in case of a hit, request the responsible state to send the needed data.[122] Currently, the European Parliament is negotiating on an update to this convention (called Prüm II), giving Member States access to other data categories, such as facial images, the police records of suspects and convicted criminals, and driving licenses. Furthermore, it would ”modernise the technical infrastructure supporting these exchanges by replacing the multitude of direct connections between national databases with a central router connecting them all” and integrate Europol into the system by ”allowing the agency to launch queries and to provide access to its databases containing non-EU

[119] European Commission, 2023c.
[120] Ibid.
[121] eu-LISA 2022, 4, 6–7.
[122] TELEFI project 2021, 8.

biometric data".[123] If adopted as proposed, the Prüm II would strengthen the cooperation between Member States' law enforcement authorities and Europol as well as make it easier and more efficient to solve and prevent cross-border crime. However, NGOs like Statewatch and European Digital Rights (EDRi) association have pointed out the threats and concerns relating to the proposed extension of Prüm, arguing that it "jeopardises rights to justice, fairness and data protection".[124] Activists are worried that extending authorities' access to sensitive data over borders would lead to authoritarian mass surveillance practices and put especially marginalized groups at great risk of unjustified policing. This might be a highly relevant argument since in EU Member States there are varying forms of democracy and understanding of human rights: for instance, the rights of sexual minorities are not protected throughout the whole Union.[125]

Launched in 2003, the **European Asylum Dactyloscopy Database (Eurodac)** is a database that helps EU Member States to better monitor the paths of asylum seekers and persons in an irregular situation. It contains the fingerprints of irregular migrants and asylum applicants who have been registered in EU Member States and associated countries. Currently, negotiations on adding new biometric data, such as facial images, to the database are ongoing.[126] Eurodac is used in 31 countries by national asylum authorities. Under strict conditions, Europol and law enforcement authorities can also get access to the database in order to prevent, detect and investigate terrorist and other serious criminal offences.[127] Fingerprints are saved in the database for 10 years, unless the data subject becomes a member state citizen (in which case, fingerprints are deleted before the 10-year period).[128] The national authority responsible for Eurodac in Finland is the Immigration Service.

Currently, eu-LISA (the European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice) is developing a shared Biometric Matching Service (sBMS) which will "manage biometric templates from the different systems, store them in a logically separate

[123] Council of the European Union, 2022a.
[124] European Digital Rights, 2022.
[125] BBC News, 8.7.2021.
[126] Council of the European Union, 2022b.
[127] eu-LISA, 2023.
[128] schengenvisainfo.com, 2023b.

form depending on their origin, and enable biometric data queries by the systems".[129] This is a part of a larger interoperability framework aiming at easing and improving information sharing between different EU information systems (such as VIS, SIS and Eurodac). The goal is to establish the following interoperability components:

- A **European search portal**, which would allow competent authorities to search multiple information systems simultaneously, using both biographical and biometric data.
- A **shared biometric matching service**, which would enable the searching and comparing of biometric data (fingerprints and facial images) from several systems.
- A **common identity repository**, which would contain biographical and biometric data of third-country nationals available in several EU information systems.
- A **multiple identity detector**, which checks whether the biographical identity data contained in the search exists in other systems covered, to enable the detection of multiple identities linked to the same set of biometric data.[130]

In addition to having access to some of the abovementioned databases, Europol has its own 1:N FR tool and database, both called FACE, which it implemented in 2017. The database is developed in-house and contains facial images of various groups such as suspects, victims, associates, contacts, and witnesses involved in a criminal procedure submitted by Europol Member States and Third Parties that have an operational agreement with Europol. It also includes facial images extracted from propaganda and other relevant materials stored in the Europol portal called Check-the-Web. Only accredited Europol officials have access to FACE, but Member States can request FR searches to be performed.[131]

6.2. National regulation

At a national level, the use of personal data is regulated with several Personal Data Acts that determine how, when, and how long personal data is allowed to be processed. In this report, Personal Data Acts of the police and the Border Guard have been examined, but there are similar laws for, e.g., Customs,

[129] eu-LISA 2022, 12.

[130] Council of the European Union, 2019.

[131] TELEFI project 2021, 149–150.

the Defense Forces, and the Immigration Service. Since in Finland only the police, the Border Guard and Customs have the right to use FR, this technology is not included in other organizations' laws. Finland also has the Data Protection Law (*Tietosuojalaki* 2018/1050) that determines general principles for the processing of personal data – upon which different organizations' specific Personal Data Acts are built.

According to a recently finished Virvotieto-project (*Viranomaisten välinen oma-aloitteinen tiedonvaihto*, engl. spontaneous interchange of information between authorities) carried out in cooperation with the Police University College, University of Eastern Finland, University of Uppsala and University of Vaasa, Finnish authorities would like to have the possibility to share data with each other more seamlessly. The project's interviewees pointed out that especially the establishment of GDPR has narrowed down the interpretation of law, making it difficult for authorities to cooperate with each other in terms of sharing data. For instance, a shared authority portal and a new data sharing law for authorities were suggested as solutions to these issues.[132] While data sharing between authorities seems to be a headache at a national level, EU is pushing for a smoother and faster exchange of data between security authorities in Member States. Recently, the Ministry of Interior announced a project aiming to prepare national legislation that the new EU data exchange directive requires.[133]

Furthermore, the possibility to utilize biometric data stored in passport and ID-card registers for crime prevention purposes has been examined a few times in Finland – without much success. In 2014, the investigation of utilizing passport register fingerprints for preventing serious crimes was thwarted by the opposing statements of the Constitutional Law Committee.[134] The matter was brought up and examined again in 2022 with the conclusion that it could be possible to use fingerprints in passport and ID-card registers to prevent serious crimes – but only under strict restrictions and after a thorough evaluation of possible human and fundamental rights issues as well as compatibility with EU regulation. The use of facial images was mentioned as well, yet not focused on precisely.[135] However, no changes to any related laws have been made yet.

[132] Laitinen & Kuukasjärvi 2023, 82–84, 90.
[133] Sisäministeriö, 2023.
[134] Sisäministeriö 2022b, 3.
[135] Id., 30–31.

7. RECOGNITION TECHNOLOGIES FROM THE VIEWPOINT OF ACTIVISTS AND RESEARCHERS

As mentioned earlier, many data protection and privacy activists see recognition technologies more as a threat than as a possibility. Especially ethical matters raise a lot of questions as these technologies are fairly new and thus there isn't an established understanding of what should or should not be accepted. With the approval of the AI Act's first draft and the publishing of ChatGPT, the debates about AI and related technologies have been active in the EU. In this chapter, the findings from discussions with researchers and activists are presented. The majority of their critique is directed towards biometric recognition technology and the attempts to adopt it into a wider surveillance use. In one interview, it was suggested that nowadays people are feeling too afraid considering the fact that we are living the most secure time in the history, and that security threats are imbalanced in the media: for instance, terrorism (which is often used as a reason to deploy more surveillance technology) is considered a major risk that everyone can agree on and that always makes the headlines, but climate change (which ultimately threatens the entire humankind) is seen as something that is not so urgent or not even a threat at all.[136] Nevertheless, all of the interviewees still saw potential with EU's new AI legislation and hoped for a positive turn in recognition technologies' future.

7.1. Risks and concerns of recognition technology

There are a few key risk areas that actors concerned about public order institutions using recognition technologies tend to point out: data safety and privacy matters, algorithmic biases and flaws, insufficient education to actors using these technologies, and the possibility of misuse and malpractice. These are especially concerning in the case of biometric recognition such as FR since biometric qualities are largely immutable. This is why many researchers and activists are calling for a complete ban on "unethical" recognition technologies (meaning, for instance, emotion recognition and FR in public spaces).[137]

[136] Discussion with activists, 25.7.2023.

[137] Ibid.; Sahlgren 2023, 53.

Data safety and privacy matters will grow to be – and already are – central to a stable and secure society. For instance, a poorly built object recognition camera in law enforcement's use could be a cybersecurity hazard if connected to larger background systems.[138] It is also worth questioning how the European Union plans to take care of data safety and privacy when building interoperable databases for shared use of all Member States. It's not insignificant where data is stored: it needs to be deliberated whether it's reliable to store data in servers in the US or China, for example.[139] Regardless of the server placement, the threat of biometric databases getting hacked remains. As biometric authentication is increasingly used to access mobile devices, bank accounts, emails and other sensitive personal information, a breach in data safety might cause tremendous harm for an individual.[140] This is also something that the EU should take into account: are all authorities in all Member States reliable enough to be granted access to information outside their national databases?[141]

Another point of criticism is that recognition technologies are by no means flawless and public order institutions don't necessarily have all the knowledge of possible **risks or biases** in the systems when putting them to use. There are countless historical and international examples of FRT failing to recognize women as well as Asian and Black people. Google's Photos app infamously used to label Black people as "gorillas" because the AI had been poorly trained to recognize people with darker skin.[142] In the United States, people have been mistakenly accused of crimes or even arrested as a result of errors in FRT used by law enforcement agencies.[143] It is a challenging controversy that in order to train FR algorithms to be more accurate and thus safer, the training data must consist of a vast number of facial images – yet this data must be acquired ethically and through legal ways. While Clearview AI's algorithms might be very accurate, they come with a price of breaking the law. And even gathering enough data might not erase the problems: after all, algorithms are developed by people with personal biases who might plant these biases into the systems – even unconsciously:

> Data always reflects existing power relations in a society. Algorithms trained on historical data can replicate and reinforce existing social inequalities, even if the data is representative and protected

[138] Discussion with authority, 24.7.2023.

[139] Discussion with researcher, 15.6.2023.

[140] Policy Department for Citizens' Rights and Constitutional Affairs, 2021.

[141] Discussion with activists, 25.7.2023.

[142] The New York Times, 22.5.2023.

[143] CBS News, 16.5.2021.

> attributes are excluded from it. This happens because AI systems learn to use 'proxy variables' — such as postcodes — to replicate historic biases.[144]

In mass surveillance, false positives can lead to more manual work, which in turn decreases the value of using recognition technology in the first place.[145] With risks relating to FRT, a special emphasis has been directed to non-citizens who are already in a vulnerable situation. For instance, in relation to the AI Act, Amnesty International has criticized the European Parliament for not taking into consideration the fact that remote biometric identification can't be used in a way that complies with the human rights of migrants, asylum seekers and refugees as these persons have a higher risk to become the targets of discriminatory profiling and risk assessment systems.[146] Hence, it's also legitimate to question why Finland's KASTU standards are different for citizens and non-citizens when it comes to the investigation of crimes.

Imperfect education and insufficient impact assessment were raised as major risk factors. While the police and the Border Guard do offer their personnel both technical and legal training in order to get access to face and license plate recognition technologies, activists and researchers argue that it is significant to include ethical aspects in the training as well.[147] To broaden one's perspective, training could include simulations of use-case examples where the participants would be divided into separate groups and treated unequally to demonstrate how it feels to be monitored and profiled. Education on algorithmic biases, on the other hand, could be offered as an online module and required to be renewed annually – much like information security training is executed in many organizations. Furthermore, in addition to studying technical risks, education should include analyzing one's own dangerousness: for instance, how one would react when blackmailed.[148] In regard to technical details, it should be ensured that each police and border guard using recognition technologies knows enough of the algorithms and systems' working mechanisms to truly understand how they work and why they might be problematic – including deficiencies in the systems (system suppliers can tweak the algorithms how they want and in that way influence the police's actions, for instance).[149]

[144] Ojanen, Björk & Mikkonen 2022, 2–3.
[145] Discussion with activists, 25.7.2023.
[146] Amnesty International, 2023b.
[147] Sahlgren 2023, 62.
[148] Discussion with activists, 25.7.2023.
[149] Ibid.

One way of preventing these troubles is to conduct encompassing impact and risk assessment. Since official documents of these are confidential information in many organizations (including the police and the Border Guard), it is difficult to analyze what they have covered. Researchers and activists call for humane aspects to be taken into consideration in impact assessments: for instance, it should be evaluated what kind of effect the increasing paranoia of being watched constantly can have on freedom of speech, freedom of assembly, societal participation etc.[150]

Misuse and malpractice may occur when data ends up in the wrong hands causing anything from small mischief to machine-led assaults.[151] It could hamper attempts to get a loan or a job, or even result in disturbing elections or igniting riots.[152] Furthermore, there's a slippery slope problem: once data is in a database, there is the temptation to use it for other purposes than it was collected for.[153] Moreover, recognition technologies make individual profiling way easier and faster – not only based on skin color or ethnicity, but also on gender, disabilities etc.[154] NGOs like Statewatch and Amnesty International have underlined that governments can also use recognition technologies deliberately to do harm. For example, in China, face and license plate recognition are being used to identify and arrest Uyghurs.[155] In Israel, face recognition is used by Israeli authorities in Occupied Palestinian Territories (OPT) to oppress and control Palestinians.[156] Amnesty Tech's Ban the Scan -campaign is trying to tackle this development and aims at banning harmful FRT in Israel, New York, and Hyderabad City. The organization considers FRT a threat to the freedom of peaceful assembly and to minority communities who might end up being the victims of discriminatory policing.[157]

In addition to the aforementioned, deploying recognition technologies in public order institutions might create inequality as not everyone wants and/or knows how to use them. It is also useful to deliberate

[150] Discussion with activists, 25.7.2023; Discussion with researcher, 22.6.2023.
[151] Discussion with activists, 25.7.2023.
[152] Discussion with researcher, 15.6.2023.
[153] Discussion with activists, 25.7.2023.
[154] Discussion with researcher, 22.6.2023.
[155] IPVM, 2022.
[156] Amnesty International, 2023a.
[157] Amnesty International, 2022.

the ethicalness of these technologies. On the other hand, the ethical issues will be there whether AI or recognition technologies are used or not – they are not the cause but a manifestation of these issues.[158]

7.2. Possibilities and benefits of recognition technology

Activists do also see the possibilities and benefits of recognition technologies in certain contexts – for example, in automated passport checking at airports or license plate recognition at parking garages. Overall, recognition technologies can be useful in cases where:

1. The person wants to be recognized,
2. The disadvantages of errors in the recognition technology are minor to the person in question (such as having to wait in a queue to do manual passport checking instead of using a machine),
3. The recognition situation is controlled (e.g., lighting is same for everyone).[159]

While recognition technologies carry the possibility of making life easier, faster, and more comfortable for an average person, the important question is whether enough societal discussion is had before implementing new technology, according to activists. Some argue that this criterion hasn't been fulfilled in Finland's case and that the operations of Finnish law enforcement have been too opaque.[160] Certainly, specific information from public order institutions can be quite difficult to get – as my experience with Customs shows. Activists also underline that in order to keep the trust in public order institutions high in Finland, it is crucial to be able to criticize them.[161]

Other benefits of law enforcement's use of recognition technologies include being able to better focus resources where needed the most, predicting harm more accurately and thus being able to prevent it, finding missing persons, supporting citizen's security, and advancing other positive goals.[162] In addition, these technologies offer cost-efficiency, better situational awareness and help to prepare for a wider use of AI in the future.[163] However, the list of positive standpoints is way shorter than the negative ones

[158] Discussion with researcher, 22.6.2023.
[159] Discussion with activists, 25.7.2023.
[160] Ibid.
[161] Ibid.
[162] Discussion with researcher, 22.6.2023.
[163] Discussion with researcher, 15.6.2023.

as activists and researchers tend to participate more on raising critical questions and scrutinizing dubious phenomena in society – a task that is of vitally important value in a democratic society.

8. CONCLUSION: CONFLICTING VIEWS AND CRITICAL QUESTIONS

This research shows that recognition technologies are a matter of conflicting views, challenging technology-related questions, and a workload for lawmakers both nationally and in the EU. Even though these technologies have been researched and developed for decades already, the public discussion of them has gathered momentum in the last 10 years or so with new legislations, the ability to utilize biometric data in everyday situations (such as opening one's smartphone or paying at a grocery store) and the introduction of new tools for security authorities' use. Currently, there are several databases and recognition technologies that are used in the everyday work of security authorities in Finland and in the EU.

Although the scope of this research is limited, it's enough to draw the conclusion that standpoints toward recognition technologies vary. On one hand, security authorities believe that these technologies would make their work easier and more efficient, which would ultimately benefit everyone in the Finnish society. On the other hand, these technologies carry risk potential and ethical issues that activists and researchers have emphasized. One of the most controversial implementations of recognition technologies is giving law enforcement a right to use real-time FR. The Finnish police have argued in favor of getting this right as it would help in searching for serious offense suspects from the CCTVs of harbors as well as monitoring unwanted comers. Furthermore, the police would like to be able to use photos and videos to recognize the victims of serious child sexual abuse from passport and ID-card registers as this would make it easier to identify and find both the victim and the offender.[164] As could be expected, security authorities see recognition technologies more as a useful and needed tool and not so much as a security hazard. However, there are differing opinions: some authorities are aware of risks and can provide multiple examples of how these are tackled in their organization, whereas

[164] HS, 7.7.2021.

others are – perhaps questionably – highly confident that the risks are either minimal or non-existent even though they have faced serious public criticism and concerns over their FR experimentation. It seems that the most confident authorities are also those most reluctant to share information, and some are not willing to give away any information whatsoever (meaning, in this case, Customs).

The sharing of personal data both between different national authorities and within EU Member States is another point of disagreement. Again, this is an issue where Finnish authorities are on the side of being able to share more data between different actors as the situation awareness is, according to them, currently quite shattered and some information is not received by any authority, which complicates the prevention and solving of crimes.[165] On the contrary, activists and researchers are worried that sensitive data will end up in the wrong hands – causing more security threats instead of removing them. However, among the EU Member States, there are largely positive views on the potential inclusion of facial images into Prüm data exchange, as TELEFI project's report presents.[166] Activists strongly disagree and argue that FR is more problematic than, for instance, fingerprint recognition as it can be done remotely without the subject knowing about it – meaning that there is also no ability to opt out or clarify, e.g., common mistakes.[167]

The technology itself should also be scrutinized and questioned. As mentioned in the previous chapter, it is important to understand the deficiencies in different systems. However, this is a rather difficult task for an independent critic to do if information about system suppliers is not shared with the public – as is the case with the police's KASTU system. What the police did disclose is that most of their drones are from a Chinese company called DJI. Now, not every Chinese company is necessarily suspicious per se, yet among western states there has been an increasing skepticism towards Chinese technology, starting with Huawei 5G and spreading to other areas. The Border Guard was also reluctant to share much about their system suppliers or systems' technical details, excluding the fact that the supplier of Helsinki-Vantaa's FR system and the algorithm that it runs on is a Portuguese company called Vision-Box S.A. This secrecy is justified in both organizations with the potential threat to cybersecurity. However, it is

[165] Discussion with researcher, 15.6.2023; see also Kautto, 2022.

[166] TELEFI project 2021, 33–34.

[167] Discussion with activists, 25.7.2023; European Digital Rights, 2020.

strange that not all information seems to be an equal cybersecurity threat: for instance, the police are quite open about information regarding their drones and REVIKA's system supplier, yet KASTU is a top-secret topic. Same with the Border Guard: disclosing information about Helsinki-Vantaa's FR system is apparently not as big of a threat as discussing other surveillance systems. And as mentioned in the opening words of this report, everything related to the use of image recognition in relation to Customs seems to be confidential. The varying degrees of access begs the question of what the grounds for non-disclosure and public insight are. It does not seem that applications closer to national security interests are those generating the highest levels of secrecy. Following a security-equals-secrecy logic, one would believe that of these three organizations, Customs wouldn't be the one that has the greatest need to hide its practices – thus it was surprising to get the opposite response. In the absence of regulations guaranteeing public oversight, more mundane or practical concerns may in practice also determine the level of access given to the public.

EU is facing a challenge with its attempt to regulate AI systems. The technology industry is worried that the upcoming AI Act will hinder innovation while academics are calling for clearer definitions and stricter allocation of responsibility.[168] Since the Act will impact not only Europe but also actors outside EU wanting to bring technology or services to EU Member States, it is crucial that the Act doesn't banish these actors altogether. However, some believe that the so-called Brussels Effect will work with the AI Act similarly as it did with GDPR a few years ago.[169]

9. DISCUSSION: LESS BLIND TRUST AND MORE PUBLIC OVERSIGHT

Finnish society has become more militarized and securitized as a result of, inter alia, Russia's war in Ukraine and the consequent decision for Finland to join NATO in 2022. The feeling of increasing threats leads to the discussions about *national security* getting more vocal which in turn can easily lead to more

[168] European Parliamentary Research Service 2023, 8.

[169] Discussion with researcher, 22.6.2023.

secrecy. However, national security and heightened threat perception puts extra stress on rights and limitations, as well as on the public's access to information that shouldn't be secret.

One questionable argument that was posed in the interviews was that rights are or can be built into the systems that security authorities use. This encourages a dangerous view or practice according to which just by having the right to use, and access to certain systems, it is ensured that these systems are safe and reliable. Furthermore, the authorities seem to be quite confident that having a natural person doing the final recognition decisions means that there are no issues in using recognition technology. This is a naive belief, as demonstrated in yet another false identification case in the US where a pregnant woman was falsely accused of carjacking:

> After her image was incorrectly matched to video footage of a woman at the gas station where the carjacking took place, her picture was shown to the victim in a photo lineup. According to the lawsuit, the victim allegedly chose Woodruff's picture as the woman who was associated with the perpetrator of the robbery. Nowhere in the investigator's report did it say the woman in the video footage was pregnant.[170]

Humans are not infallible and even if the machine isn't making the final decisions, it can create confirmation bias by offering options to an officer who places too much trust in the responses generated by the system, and thus may end up falsely identifying innocent people even in the face of obvious reasons for skepticism. Therefore, the officers working with technological systems must have enough insight to be able to question and critically reflect on the recommendations and suggestions offered up by recognition systems. Training should not merely aim at operating systems successfully but include familiarization with ideas like confirmation bias and error-rate fluctuations to ensure that citizens' right to equal and fair treatment is taken seriously.

As became clear during the research project, different authorities have different standards on the confidentiality of information. These standards may vary even within one organization: when trying to find interviewees, there was one instance where one authority was first willing to help with setting up interviews but later withdrew this consent – apparently after discussing the interview request with someone else in the organization. This goes to show that the authorities themselves are uncertain of their responsibilities and permissions to share information, which in turn makes them reluctant to share

[170] The Guardian, 15.8.2023.

anything.[171] It should be discussed whether individual authorities or even individual officers should be the ones to determine what is kept a secret and what can be disclosed publicly. Due to challenges in receiving all the information that was requested, many important questions remain unanswered:

- How are the systems' algorithms trained? What kind of image material is used to train them, and where does this material come from? Is there enough variation in the training images (e.g., different genders, different ethnicities) and does this match the differences in the Finnish population?
- What kind of impact or risk assessments have been done before deploying the systems?
- Which company supplies the FR system used by the Finnish police?
- On what grounds are images stored in different searchable databases, and for how long? If images of 'suspects' are stored, does it matter what the suspected crime is? Do storage times vary between e.g., convicted criminals and suspects?

Faced with what seems an arbitrary variation in public access to information about the use of image recognition in Finnish public order, it is legitimate to ask whether the public would be better served with a clearly defined right to certain classes of information. Without knowledge about how recognition is produced and managed it is hard for the public to make informed decisions about the use of recognition systems in policing. And in areas where there may be legitimate reasons to deny public access, access could be granted to an institution entrusted with oversight and accountability on behalf of the public.

Furthermore, questions that we, the citizens, need to ask ourselves is whether we want to have our personal information stored in multiple different databases that might in the future be processed by not only the national authorities but also the authorities in other EU Member States. In addition, we need to deliberate on how far we want these technologies to go: what kind of decisions will we let them make for us? How much privacy are we willing to give up for being able to run errands easier and faster?

With AI and recognition technologies, it's extremely hard to foretell what is to come in the future. Predictions vary from Orwell-like worst case scenarios to robust technology optimism. It might be safe

[171] Discussion with researcher, 15.6.2023.

to guess that the number of different applications will increase, and the technologies will become more advanced and complex – making sufficient education and system transparency even more essential. The performance of recognition depends both on the databases that are used for matching – including people who are in police archives – and the training data (unconnected databases) that was used to teach the recognition algorithms to do their work. Transparency with regards to these aspects of system development would strengthen democratic oversight, and being able to audit the training does not endanger law enforcement.

Interviewees were asked which changes/developments they would like to see in the future regarding recognition technologies. According to these answers, the future should include:

- Sufficient legislation that takes into consideration the privacy, security, and rights of people as well as climate impacts. Responsibilities in problem situations need to be figured out and clearly registered in law documents.
- Sufficient impact and risk assessment of different systems and practices before putting them to use. This includes deliberating where to buy the systems (the cheapest option is not necessarily the best one) and ensuring that there's a 'plan b' in case technology fails.
- Sufficient education for the actors using recognition technology.
- Transparency especially from the side of public order institutions. Excessive secrecy can also be a security threat as information accumulates only in the hands of few.
- Cooperation between public order institutions and civil society when developing systems. Most importantly, affected communities should be involved in the decision-making and development of these technologies.

This report builds on public information only. As some authorities are not very forthcoming even with information that cannot credibly be construed as operational secrets, any additional information is welcomed. Further information or insights regarding this report's topics can be sent to Academy Fellow and PI of the UNDO-project, Rune Saugmann (rune.saugmann.andersen@tuni.fi).

REFERENCES

Literature

Amnesty International (2023a). Israel and Occupied Palestinian Territories: Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT. Available <https://www.amnesty.org/en/documents/mde15/6701/2023/en/>, accessed 9.6.2023.

Bellanova, Rocco & González Fuster, Gloria (2013). Politics of Disappearance: Scanners and (Unobserved) Bodies as Mediators of Security Practices. *International Political Sociology* 7 (2): 188–209. https://doi.org/10.1111/ips.12017.

Bellanova, Rocco, Irion, Kristina, Lindskov Jacobsen, Katja, Ragazzi, Francesco, Saugmann, Rune & Suchman, Lucy (2021). Toward a Critique of Algorithmic Violence. *International Political Sociology* 15 (1): 121–50. https://doi.org/10.1093/ips/olab003.

Kaufmann, Mareile, Egbert, Simon & Leese, Matthias (2019). Predictive Policing and the Politics of Patterns. *The British Journal of Criminology* 59 (3): 674–92. https://doi.org/10.1093/bjc/azy060.

Laitinen, Kari & Kuukasjärvi, Kimmo (2023). Viranomaisten tietojenantaminen ja -vaihtaminen, tiedonkulku ja lainsäädäntö muuttuneessa turvallisuus- ja toimintaympäristössä. *Poliisiammattikorkeakoulun katsauksia* 34.

Marciniak, Daniel (2021). Data-driven policing: How digital technologies transform the practice and governance of policing. PhD thesis, University of Essex, UK.

Ojanen, Atte, Björk, Anna & Mikkonen, Johannes (2022). Promoting equality in the use of Artificial Intelligence – an assessment framework for non-discriminatory AI. Policy brief 2022: 25.

Ojanen, Atte, Sahlgren, Otto, Vaiste, Juho, Björk, Anna, Mikkonen, Johannes, Kimppa, Kai, Laitinen, Arto & Oljakka, Nea (2022). Algoritminen syrjintä ja yhdenvertaisuuden edistäminen: Arviointikehikko syrjimättömälle tekoälylle. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 2022: 54.

Sahlgren, Otto (2023). Ethics in the AI Lifecycle: Theoretical Perspectives, Practical Resources and Recommendations.

Saugmann, Rune (2019). Military Techno-Vision: Technologies between Visual Ambiguity and the Desire for Security Facts. *European Journal of International Security* 4 (3): 300–321. https://doi.org/10.1017/eis.2019.17.

Virta, Sirpa (2022). Digital Meets Political. Strategic preparedness of the police towards AI and disinformation. Keynote in CEPOL Research and science conference, Vilnius 8th June.

Virta, Sirpa & Taponen, Jari (2017). Policing regimes in transition in the Nordic countries: Some critical notes from the Nordic reality. In Devroe, Elke, Edwards, Adam & Ponsaers, Paul (eds) *Policing European Metropolises: The politics of security in city-regions.* Routledge. Abingdon.

News papers

Aamulehti

5.5.2023. Poliisi vaihtaa ongelmallisiksi havaitut haalarikamerat “ryhmävideopalvelujärjestelmään”. News article.

BBC News

8.7.2021. EU votes for action over Hungary’s anti-LGBT law. News article. Available <https://www.bbc.com/news/world-europe-57761216>, accessed 11.8.2023.

CBS News

16.5.2021. Police departments adopting facial recognition tech amid allegations of wrongful arrest. News article. Available <https://www.cbsnews.com/news/facial-recognition-60-minutes-2021-05-16/>, accessed 12.6.2023.

The Guardian

15.8.2023. TechScape: 'Are you kidding, carjacking?' – The problem with facial recognition in policing. News article. Available <https://www.theguardian.com/newsletters/2023/aug/15/techscape-facial-recognition-software-detroit-porcha-woodruff-black-people-ai>, accessed 21.8.2023.

Helsingin Sanomat

7.7.2021. Tekoälyyn perustuvasta kasvojentunnistuksesta tullut päivittäinen apuväline rikostutkinnassa – Poliisi haluaa laajemmat käyttövaltuudet. News article.

28.5.2023. Satatuhatta silmää. News article.

27.7.2023. Tällainen on nykyisten haalarikameroiden tilalle tuleva keksintö. News article.

Moottori

7.2.2016. Poliisin täsmäase liikenteessä – rekisterikilpien tunnistuslaite toimii kuin ajatus. News article. Available <https://moottori.fi/liikenne/jutut/poliisin-tasmaase-liikenteessa-rekisterikilpien-tunnistuslaite-toimii-kuin-ajatus/>, accessed 11.8.2023.

Politico

14.6.2023. Forget ChatGPT: Facial recognition emerges as AI rulebook's make or break issue. News article. Available <https://www.politico.eu/article/facial-recognition-artificial-intelligence-act-ai-issue-european-parliament/>, accessed 11.7.2023.

The New York Times

14.5.2019. San Francisco Bans Facial Recognition Technology. News article. Available <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>, accessed 19.7.2023.

18.1.2020. The Secretive Company That Might End Privacy as We Know It. News article. Available <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html?searchResultPosition=29>, accessed 22.8.2023.

22.5.2023. Google's Photo App Still Can't Find Gorillas. And Neither Can Apple's. News article. Available <https://www.nytimes.com/2023/05/22/technology/ai-photo-labels-google-apple.html?searchResultPosition=2>, accessed 12.6.2023.

14.6.2023. E.U. Takes Major Step Toward Regulating A.I. News article. Available <https://www.nytimes.com/2023/06/14/technology/europe-ai-regulation.html?searchResultPosition=2>, accessed 11.7.2023.

Yle

8.6.2017. Rekisterikilven lukulaitteesta tuli kolmessa vuodessa poliisin paras kaveri – "Kaikki kehuvat". News article.

29.9.2019. Oulun kaupungin ja poliisin kamerasopimus on tietosuojavaltuutetun mukaan ongelmallinen. News article.

21.1.2020. Yle selvitti: Poliisin kuvaamat haalarikameravideot päätyvät harvoin todisteeksi – tältä videomateriaali näyttää. News article.

23.4.2021. Amerikkalaismedia varoitti Suomen poliisia kiistanalaisen kasvojentunnistusohjelman käytöstä – KRP kompuroi vastauksessaan. News article.

28.9.2021. Poliisi tunnisti kasvoja ohjelmalla, jonka tietoturvariskejä ei selvitetty riittävän hyvin – KRP sai huomautuksen tietosuojavaltuutetulta. News article.

21.12.2022. Kaupunkikameran maksaa kunta, mutta kuvat katsoo vain poliisi – "Niistä pääsee näkemään vaikka että kuka löi ketä, jos on tappelunpoikanen ollut". News article.

13.6.2023. EU:n tekoälyasetus on paisunut tuotesääntelystä ihmisoikeuksien suojelijaksi – suurta huomiota saanut asetus etenee tällä viikolla. News article.

Laws and directives

Aluevalvontalaki 18.8.2000/755

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, OJ L 119, 89–131 (Law Enforcement Directive)

Laki henkilötietojen käsittelystä poliisitoimessa 10.5.2019/616

Laki henkilötietojen käsittelystä Rajavartiolaitoksessa 10.5.2019/639

Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä 5.12.2018/1054

Pakkokeinolaki 22.7.2011/806

Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206

Rajavartiolaki 15.7.2005/578

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions

for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (The EES Regulation)

Rikoslaki 19.12.1889/39

Tieliikennelaki 10.8.2018/729

Tietosuojalaki 5.12.2018/1050

Ulkomaalaislaki 3.4.2004/301

Other sources

Amnesty International (2022). Ban the Scan. Available <https://banthescan.amnesty.org/nyc/>, accessed 11.8.2023.

Amnesty International (2023b). EU: European Parliament adopts ban on facial recognition but leaves migrants, refugees and asylum seekers at risk. News article, 14.6.2023. Available <https://www.amnesty.org/en/latest/news/2023/06/eu-european-parliament-adopts-ban-on-facial-recognition-but-leaves-migrants-refugees-and-asylum-seekers-at-risk/>, accessed 11.7.2023.

Council of the European Union (2018). European travel information and authorisation system (ETIAS): Council adopts regulation. Press release, 5.9.2018. Available <https://www.consilium.europa.eu/en/press/press-releases/2018/09/05/european-travel-information-and-authorisation-system-etias-council-adopts-regulation/>, accessed 27.7.2023.

Council of the European Union (2019). Interoperability between EU information systems: Council adopts regulations. Press release, 14.5.2019. Available <https://www.consilium.europa.eu/en/press/press-releases/2019/05/14/interoperability-between-eu-information-systems-council-adopts-regulations/>, accessed 18.7.2023.

Council of the European Union (2022a). Council adopts two general approaches and a recommendation to improve operational police cooperation and information exchange. Press release, 10.6.2022.

Available <https://www.consilium.europa.eu/en/press/press-releases/2022/06/10/council-adopts-recommendation-two-negotiating-mandates-improve-operational-police-cooperation-information-exchange/>, accessed 17.7.2023.

Council of the European Union (2022b). Asylum and migration: the Council approves negotiating mandates on the Eurodac and screening regulations and 21 states adopt a declaration on solidarity. Press release, 22.6.2022. Available <https://www.consilium.europa.eu/en/press/press-releases/2022/06/22/migration-and-asylum-pact-council-adopts-negotiating-mandates-on-the-eurodac-and-screening-regulations/>, accessed 18.7.2023.

eu-LISA (2022). Report on the technical functioning of the Visa information System (VIS): August 2022. Available <https://www.eulisa.europa.eu/Publications/Reports/2021%20VIS%20Report.pdf>, accessed 18.7.2023.

eu-LISA (2023). Large-Scale IT Systems: Eurodac. Available <https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Eurodac>, accessed 18.7.2023.

European Commission (2023a). Schengen Information System. Available <https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system_en>, accessed 17.7.2023.

European Commission (2023b). What is SIS and how does it work? Available <https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-information-system/what-sis-and-how-does-it-work_en>, accessed 17.7.2023.

European Commission (2023c). Visa Information System (VIS). Available <https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/visa-information-system_en>, accessed 18.7.2023.

European Digital Rights (2020). Your face rings a bell: Three common uses of facial recognition. Blog post, 15.1.2020. Available <https://edri.org/our-work/your-face-rings-a-bell-three-common-uses-of-facial-recognition/>, accessed 18.8.2023.

European Digital Rights (2022). New EU law amplifies risks of state over-reach and mass surveillance. Briefing paper. Available <https://edri.org/our-work/new-eu-law-amplifies-risks-of-state-over-reach-and-mass-surveillance/>, accessed 17.7.2023.

European Parliament (2023). EU AI Act: first regulation on artificial intelligence. News article, 8.6.2023. Available <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>, accessed 11.8.2023.

European Parliamentary Research Service (2023). Briefing: Artificial intelligence act. Available <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf>, accessed 11.7.2023.

European Union (2023). Entry/Exit System: General information. Available <https://travel-europe.europa.eu/ees/general-information_en#what-data-will-the-ees-collect>, accessed 18.7.2023.

IPVM (2022). Hikvision Cameras Used to Catch Uyghurs Featured in Xinjiang Police Files. Available <https://ipvm.com/reports/xinjiang-police-files>, accessed 9.6.2023.

Kautto, Hannu (2022). Suomi jättää käyttämättä EU:n tarjoaman mahdollisuuden sisäisen turvallisuuden parantamiseen. Blog post, 6.10.2022. Available <https://poliisi.fi/blogi/-/blogs/suomi-jattaa-kayttamatta-eun-tarjoaman-mahdollisuuden-sisaisen-turvallisuuden-parantamiseen>, accessed 21.8.2023.

Ministry of the Interior (2023a). The police maintain public order and security. Available <https://intermin.fi/en/police/public-order-and-security>, accessed 27.7.2023.

Ministry of the Interior (2023b). The Finnish Border Guard is responsible for border management. Available <https://intermin.fi/en/border-management/border-surveillance>, accessed 27.7.2023.

Policy Department for Citizens' Rights and Constitutional Affairs (2021). Biometric Recognition and Behavioural Detection. PE 696.968.

Poliisi (2023). A police camera drone takes off every day and the operations are at the top in the world – drones save money and time, as well as lives. News article, 28.2.2023.

Poliisiammattikorkeakoulu (2022). Poliisi (AMK) -tutkinnon opetussuunnitelma (180 op) 2022–2024.

Poliisihallitus (2020). Kasvojentunnistukseen liittyvän KASTU-järjestelmän käyttö. POL-2020-12303.

Poliisihallitus (2021). Poliisin asiakirjajulkisuuskuvaus. POL-2021-75355.

Poliisihallitus (2022a). Poliisin liikennevalvonnan ja -turvallisuuden toiminta- ja kehittämissuunnitelma 2022–2030. Poliisihallituksen julkaisusarja 1/2022.

Poliisihallitus (2022b). Poliisin miehittämättömän ilmailun toimintakäsikirja.

Poliisin haalarikameratoiminnassa oikeudellisia ongelmia. EOAK/2017/2021.

Rajavartiolaitos (2022). Rajavartiotoiminnan rekisteri. Available <https://raja.fi/rajavartiotoiminnan-rekisteri>, accessed 28.7.2023.

schengenvisainfo.com (2023a). The Schengen Information System – SIS. Available <https://www.schengenvisainfo.com/security-system/sis/>, accessed 17.7.2023.

schengenvisainfo.com (2023b). EURODAC – The European Asylum Dactyloscopy Database. Available <https://www.schengenvisainfo.com/security-system/eurodac/>, accessed 18.7.2023.

Sisäministeriö (2022a). Älykkäät rajat –kokonaisuuteen liittyvät lait voimaan ensi vuonna. Press release, 20.12.2022. Available <https://intermin.fi/-/alykkaat-rajat-kokonaisuuteen-liittyvat-lait-voimaan-ensi-vuonna?languageId=fi_FI>, accessed 17.7.2023.

Sisäministeriö (2022b). Selvitys passirekisterin ja henkilökorttirekisterin biometristen tietojen käyttämisestä rikostorjunnassa. VN/5608/2022-SM-20.

Sisäministeriö (2023). Viranomaisten tietojenvaihtoa rikollisuuden torjunnassa tehostetaan EU-jäsenvaltioiden kesken. Press release, 13.6.2023. Available < https://intermin.fi/-/viranomaisten-tietojenvaihtoa-rikollisuuden-torjunnassa-tehostetaan-eu-jasenvaltioiden-kesken>, accessed 24.7.2023.

Statewatch (2023). EU: Civil society calls for rights to be prioritised in secret AI Act 'trilogue' negotiations. News article, 12.7.2023. Available <https://www.statewatch.org/news/2023/july/eu-civil-society-calls-for-rights-to-be-prioritised-in-secret-ai-act-trilogue-negotiations/>, accessed 13.7.2023.

TELEFI project (2021). Summary Report of the project "Towards the European Level Exchange of Facial Images". Available <https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf>, accessed 6.7.2023.

The Border Guard's response to an information request, 20.6.2023.

The Police University College's response to an information request, 5.7.2023

Valtiovarainministeriö (2019). Tullin henkilötietolaki uudistuu. Press release, 9.5.2019. Available <https://valtioneuvosto.fi/-//10623/tullin-henkilotietolaki-uudistuu>, accessed 22.6.2023.

APPENDIX: ACRONYMS

KASTU = *Kasvojentunnistus*, engl. face recognition. A FR tool used by the Finnish police.

NGO = Non-governmental organization

NPB = National Police Board of Finland

NBI = National Bureau of Investigation

RATAS = *Rajatarkastusjärjestelmä,* engl. border control system. The Finnish Border Guard's information system for border inspections.

REVIKA = *Rekisterikilven lukulaite ja videokamerajärjestelmä*, engl. license plate registration and video camera system. A license plate recognition system used by the Finnish police.

UAS = Unmanned Aircraft System, more commonly known as drone.

Vitja-RETU = *Rekisteröidyn tuntomerkit*, engl. registered persons identifying features. A database used by the Finnish police.